Communication of Information Privacy Practices in Consumer Information Systems

Dissertation for the acquisition of the academic degree
Doktor der Wirtschafts- und Sozialwissenschaften (Dr. rer. pol.)

at the Faculty of Economics and Management
of the University Kassel

by

Tobias Dehling

Kassel, December 19, 2017

Abstract

At the beginning of the 21th century, we live in a globally connected world with nearly ubiquitous information collection and ever-intensifying information privacy risks. This cumulative thesis substantiates approaches for information privacy risk reduction through organizational information privacy communication.

Organizational information privacy communication has been addressed by two dominant literature streams; one promotes overarching principles and guidelines too vague to improve information privacy communication to a degree much higher than punishing the worst offenders; the other provides too many technical solutions for too narrow problems. This thesis contributes to bridging the gap between the normative and empirical information privacy world by answering the research question: How could consumer information system components be designed to communicate organizational information privacy practices to consumers in a substantive way?

The employed research approach is mixed-methods and retroductive. It first clarifies the problem space by consolidating extant knowledge in research and practice, proceeds with development of a potential solution space in form of an information systems design theory, and concludes by substantiating the core underlying assumption of the proposed theory—the heterogeneity of consumers' information privacy information needs—with an online survey.

The contested and complex nature of information privacy makes it unlikely that organizations can satisfy consumers with a universal solution. This thesis addresses this problem by proposing a flexible, adaptive approach to organizational information privacy communication and by establishing a scientific foundation that supports entities striving to improve organizational information privacy communication to assess how to approach the challenge, to grasp the resource requirements, and to avoid sunk costs. Even if substantive organizational information privacy communication is never transformed from normative prescription into empirical reality, this work will serve as scientific foundation to investigate whether and why substantive organizational information privacy communication is not realized in practice and why it may not be socially desirable. Complementing extant normative guidance with a thorough understanding of consumers' information privacy information needs and an information systems design theory may just be the missing impulse for the emergence of truly useful and substantive organizational information privacy communication in consumer information systems.

German Abstract

Am Anfang des 21. Jahrhunderts leben wir in einer global vernetzten Welt. Die omnipräsente Datenerhebung bringt stetig anwachsende Risiken im Hinblick auf die Informationsprivatheit mit sich. Diese kumulative Dissertation beschäftigt sich mit der Gestaltung von Informationssystemkomponenten für substantielle Kommunikation von Datenverarbeitungspraktiken in verbraucherorientierenten Informationssystemen, im Hinblick auf die Informationsprivatheit (kurz: Informationsprivatheitskommunikation (IPK)).

In der bestehenden Literatur werden zwei dominante Ansätze für IPK verfolgt. In den Sozialwissenschaften werden hauptsächlich normative Richtlinien entworfen und im Feld getestet. In der Informatik werden vorwiegend technische Lösungen für spezifische, aber isolierte, Problemstellungen entworfen und getestet. Das Ziel der Dissertation ist es zur Verknüpfung der beiden Literaturströme beizutragen, indem die folgende Forschungsfrage beantwortet wird: Wie sollten Komponenten für Kommunikation zur Informationsprivatheit in verbraucherorientierten Informationssystemen gestaltet werden, um Datenverarbeitungspraktiken, auf eine substantielle Art und Weise, an Verbraucher zu kommunizieren? Im Rahmen der Dissertation werden einerseits bestehende normative Richtlinien in Form von Gestaltungswissen konkretisiert. Andererseits wird von konkreten Instantiierungen von IPK abstrahiert, um eine Übertragbarkeit der gewonnenen Erkenntnisse auf verschiedene Kontexte, in denen IPK relevant ist, zu ermöglichen.

Die Arbeiten im Rahmen der Dissertation gliedern sich in drei Schritte. Zuerst wird die Relevanz von IPK untersucht. Anschließend wird Gestaltungswissen für IPK entwickelt. Abschließend wird eine zentrale Annahme des entwickelten Gestaltungswissen – die Heterogenität der Nutzerbedürfnisse – empirisch untermauert. Methodisch werden vorwiegend qualitative Verfahren verwendet, die durch quantitative Verfahren ergänzt werden.

Aktuell werden normative Vorgaben am Markt für Verbraucher nicht zielführend umgesetzt und technische Lösungen scheitern am fehlenden Zugriff von Dritten auf die Datenverarbeitungspraktiken von verbraucherorientierten Informationssystemen. Die Dissertation zeigt den Gestaltungsraum zwischen den dominanten normativen und technischen Ansätzen auf und liefert erste Erkenntnisse, wie diese Vakanz, durch regulatorische, unternehmerische, verbrauchergetriebene oder kooperative Maßnahmen, gefüllt werden kann. Die Ergänzung von bestehenden normativen Richtlinien mit einem gründlichen Verständnis der Informationsbedürfnisse von Verbrauchern und einer Informationssystemgestaltungstheorie könnte den entscheidenden Impuls zur Verwirklichung von substantieller IPK in verbraucherorientierten Informationssystemen liefern.

Table of Contents

Index of Figures

Index of Tables

Index of Abbreviations

#	Number of something (eg, participants, apps, or articles)
AISeL	AIS (Association for Information Systems Research) Electronic Library
AM	Altmetric.com attention score
App	Application
AT	Archetype
Bash	Bourne-again shell
CCO	Consumer data collection
CIT	Google Scholar citation count
COPPA	Children’s Online Privacy Protection Act
FIPP	Fair information practice principles
GIPC	Global information privacy concern
GPS	Global Positioning System
h5	Google Scholar h5-index
HEW	US Federal Department of Health Education and Welfare
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
HTI	Health information technology infrastructure
HTML	Hypertext Markup Language
IBAN	International bank account number
ICO	Identifier collection
ID	Identifier
IF	Thomson Reuters 2016 journal citation reports impact factor
IHD	Information handling
IP	Internet Protocol
IS	Information system (PUB6: Information sensitivity)
ISCT	Integrative Social Contracts Theory
ISI	Information seeking intention
IT	Information technology
JQ3	VHB-JOURQUAL3 journal ranking
Lit	Literature
M	Mean
Mdn	Median
mHealth	Mobile health
n	Number of something (eg, participants, apps, or articles)
N	Number of something (eg, participants, apps, or articles)
N/A	Not available, not applicable
NFC	Near field communication
OECD	Organisation for Economic Cooperation and Development
P#	Proposition #
P3P	Platform for Privacy Preferences Project

PCT	Privacy controls
PHS	Patient-centered health information technology services
PP	Perceived privacy
PUB	Publication
RECIPE	Information relevant for communication of information privacy practices
RFID	Radio-frequency identification
RGL	Reading grade level
RQ	Research question
SD	Standard deviation
SEN	Information sensors
SQL	Structured Query Language
SRQ	Subordinate research question
TIPP	Transparency of information privacy practices
Typo	Typographical error; if you find one, you can keep it
WKWI	WKWI 2008 Ranking

Acknowledgements

I would like to thank Ali Sunyaev, who motivated me to do a PhD, supervised my PhD project, supported my work with his valuable insights, and encouraged me to pursue the research problems I found interesting and fascinating. I would also like to thank my family and friends who supported me along the way, especially, by shielding me from many duties daily life usually throws at you and who often spontaneously find some time whenever I am available. I would also like to thank my coauthors, coworkers, and the student assistants, who supported the work on the articles included in this thesis and without whom the articles would not have turned out as good as they are now. I would also like to thank those researchers, who already cited my work, which reaffirmed me that I was on the right track but also directed me towards interesting related work I might have missed otherwise. I would also like to thank all those reviewers, who took the time to criticize my manuscripts and supported me in polishing my manuscripts for publication. I would also like to thank those editors and track chairs who trusted me, even in the early stages of my academic life, to review manuscripts, which made me aware of interesting research streams and fostered my understanding of the research enterprise. I would also like to thank all those free and open source software developers, who already implemented many of the things I wanted my computers to do, provided me with the software and programming libraries I desired and required to complete my PhD project, and make using a computer actually fun. Finally, I would like to thank all those musicians whose music got me through the tedious parts of my PhD project and who often pointed me towards ideas for how to move on with my research when I hit obstacles in my steams of thought. I probably missed many people I should have mentioned here. If you feel forgotten, please feel assured that I appreciate your support.

1 Thesis Overview

1.1 Introduction

At the dawn of the information age, perception of the internet shifted from a network of distributed computers to a distributed space of information (Schatz and Hardin 1994). Since then, growth and evolution of the internet surged. A little over two decades later, the internet is accessible to a vast number of individuals across the globe and by diverse client devices, such as desktop computers, mobile devices, appliances, and autonomous machines. The internet is no longer only a useful tool for information retrieval; instead, it has evolved into an essential cornerstone for everyday activities, such as communication, shopping, work, health care, or political activities. With increasing dissemination and versatility of the internet, the number of means available for information collection and amount of collected information increased as well (Baraniuk 2011).

On the downside, the rapid growth of available information intensifies information security risks, such as unauthorized access and distortion of information or service disruptions of information systems (Fu and Blum 2013, Romanosky 2016, Whitman 2003), and risks of information privacy harms, such as misrepresentation of the self, chilling effects, or discrimination (Buitelaar 2017, Nissenbaum 2009, Stoycheff 2016). Individuals easily fall prey to these risks because of the complexity of the internet paired with low digital literacy in the population (Acquisti et al. 2015, Park 2013). In this thesis, I substantiate approaches for information security and information privacy risk reduction through communication of relevant organizational information security and information privacy practices. Communication of relevant organizational information security and information privacy practices makes it possible to ascertain whether the benefits of information system use outweigh the risks.

Due to the erratic relationship of information security and information privacy, which is reinforcing in some cases and debilitating in others[1], I focus on communication of organizational information privacy practices because information privacy harms are often a consequence of information security violations (Culnan and Williams 2009). Furthermore, I focus on communication of organizational information privacy practices in consumer information systems—that is, socio-technical systems open to consumers in which information technology is employed to process information—because such systems depend on voluntary use and organizations can use attention to information privacy as one potential lever to make their information systems more attractive to consumers than information systems of competitors.

[1] The following example illustrates the erratic relationship of information security and information privacy. On the one hand, security measures improving confidentiality reduce potential for information privacy harms such as embarrassment due to disclosure of sensitive information. On the other hand, security measures improving availability increase potential for information privacy harms due to increased risks for disclosure of sensitive information.

Communication of organizational information privacy practices has been approached by two dominant literature streams. On the one hand, organizational, legal, and public policy scholars focus predominantly on uniform, normative solutions to make information on organizational information privacy practices available to consumers in a consistent and controllable way—the communication generalization stream. Communication approaches proposed, investigated, and refined by the communication generalization stream are usually concerned with privacy notices or privacy seals (eg, Garrison et al. 2012, Milne and Culnan 2002, 2004, Miyazaki and Krishnamurthy 2002, Pollach 2006). On the other hand, computer science scholars focus predominantly on special-purpose tools that target specific information needs and may also work without organizational involvement—the communication specification stream. Communication approaches proposed, investigated, and refined by the communication specification stream focus on dedicated information needs, such as identifying select matches and mismatches between organizational information privacy practices and consumer preferences (eg, Bélanger et al. 2013, Tsai et al. 2011), revealing undisclosed information privacy practices (eg, Bal et al. 2015, Balebako et al. 2013), or facilitating information privacy management (eg, Abiteboul et al. 2015, Xu, Crossler, et al. 2012).

Both streams attest to the importance of organizational information privacy communication since they focus on making information on organizational information privacy practices available to consumers. Yet, neither generalized information privacy communications nor specific information privacy communications are suitable to satisfy consumers' information privacy information needs because they inadequately account for the contextual nature of information privacy (Miltgen and Peyrat-Guillard 2014, Nissenbaum 2009, Smith et al. 2011, Xu, Teo, et al. 2012). Generalized information privacy communications usually do not provide the information consumers are interested in (Earp et al. 2005). Even if generalized information privacy communications, such as privacy notices, offered all the information of interest to customers in all contexts, they would require too much effort for information retrieval to be of avail in real-world contexts and create practical value for consumers (McDonald and Cranor 2008). Specific information privacy communications, on the other hand, are too specialized to be of use in diverse contexts. Requiring consumers to keep track of and become accustomed with the wide range of special-purpose tools required to satisfy their information needs will, for most consumers, result in too high demands on digital and privacy literacy. In a nutshell, the communication generalization stream promotes overarching principles and guidelines that are too vague to improve communication of organizational information privacy practices to a degree much higher than identifying and punishing the worst offenders and the communication specification stream provides too many solutions for too narrow information privacy–related problems to be practically feasible and meaningfully integrated into an effective artifact for communication of organizational information privacy practices.

Information privacy–related organizational actions are obscured by enormous potential for hidden information and hidden action (Pavlou et al. 2007) so that organizations have strong incentives to respond to normative requirements through lip service or even stronger forms of resistance (Oliver 1991). Organizations that intend to act in a socially responsible way with respect to information privacy (Campbell 2007) are confronted with a vast array of opportunities for substantive action with unclear interdependencies, utility, and effects. To make substantive communication of organizational information privacy practices a reality, both literature streams must be bridged. On the one hand, normative principles must be refined to enable organizations, regulators, and consumers to differentiate between lip service and substantive communication of organizational information privacy practices and to identify deficiencies in organizational communications of information privacy practices. On the other hand, more general design knowledge is required to enable organizations that want to establish substantive communication of organizational information privacy practices to ascertain not only what can be done but to ascertain what should be done under what conditions.

The overarching goal of this cumulative thesis is to contribute to bridging this gap—that is, the gap between normative perspectives on and available technical solutions for communication of organizational information privacy practices—in a way that accounts for the diversity in consumer expectations for communication of organizational information privacy practices. The guiding research question (RQ) for the cumulative research agenda is:

> ***RQ****: How could consumer information system components be designed to communicate organizational information privacy practices to consumers in a substantive way?*

This work is prescient (Corley and Gioia 2011) since at the time of writing economic benefits of lip service and resistance in response to normative requirements appear to outweigh the resource commitments required for substantive communication of organizational information privacy practices by far (Greenaway et al. 2015). The merit of this thesis lies in the establishment of a scientific foundation that supports entities striving or required to improve communication of organizational information privacy practices to assess how to approach the challenge, to grasp the resource requirements, and to avoid sunk costs, for example, development of elaborate privacy notices, which are, albeit often advocated, not well suited for communication of organizational information privacy practices in consumer information systems (Jensen and Potts 2004, McDonald and Cranor 2008, Schwaig et al. 2005). Even if substantive communication of organizational information privacy practices is never transformed from normative prescription into empirical reality, this work will be useful because the findings serve as scientific foundation to investigate whether and why substantive communication of organizational information privacy practices is not realized in practice and why it is not socially desirable.

To answer the guiding research question (RQ), this research is divided into three subordinate research questions (SRQ). First, I establish the relevance of communication of organizational information privacy practices by identifying high-level information security and information privacy requirements, investigating potential harms of information security and information privacy violations, and assessing the utility of privacy notices, the dominant form of organizational information privacy communication. The first subordinate research question is:

> ***SRQ1****: Why is there a need to improve the design of information privacy communication in consumer information systems?*

After establishing the relevance of organizational information privacy communication and the need for improvement of the design of organizational information privacy communication, I develop design knowledge for substantive communication of organizational information privacy practices by investigating what information has to be communicated and proposing a design suitable to communicate the required information. The second subordinate research question is:

> ***SRQ2****: What are feasible designs of consumer information system components that facilitate communication of organizational information privacy practices?*

Finally, I substantiate the results of the investigation of SRQ2 by collecting evidence for the core underlying design rationale of the proposed solution—the heterogeneity of consumers' information privacy information needs. The third subordinate research question is:

> ***SRQ3****: What are the different types of consumers with respect to their information privacy information needs and how do they differ from each other?*

The cumulative findings of the investigation of SRQ1-3 allow to answer the main research question by establishing the relevance of organizational information privacy communication, by demonstrating the need for improvement of extant approaches to organizational information privacy communication, through the identification of core design characteristics of information systems components for organizational information privacy communication, and the investigation and characterization of consumers' information privacy information needs.

The remainder of the thesis is structured as follows. The following chapter clarifies the conceptual background of this thesis by briefly reviewing extant conceptualizations of information privacy, clarifying the view on information privacy employed within the scope of this thesis, and, for the sake of clarity, describing how the employed view on information privacy is related to information security. Afterwards I outline the overarching research approach and proceed by outlining the main findings of this work and presenting an overview of the publications included in this thesis. The thesis overview is concluded with a discussion of the limitations of this thesis, promising opportunities for future research, and of the main implications for research and practice. Afterwards, the publications included in the thesis are presented in chapters 2–7.

1.2 Information Privacy and Consumer Information Systems

1.2.1 Extant Conceptualizations of Information Privacy

The concept of privacy is constantly evolving with social change. While in ancient Greece revealing the naked body was perceived as a sign of being civilized, rising wealth and less dependence on servants increased demands for hiding one's private parts (Solove 2002). For information privacy a similar development, driven by technological change, is evident. In the late 19th century, increasing prevalence of newspapers led to a rights-based conceptualization of information privacy (Warren and Brandeis 1890). Computerization of governmental databases in the 1960s led to a conceptualization of information privacy as control over communication of information (Westin 1967). With the commercialization of information networks, market-based conceptualizations of information privacy that treat information as a commodity emerged (Laudon 1996).

At the beginning of the 21th century, we live in a globally connected world with nearly ubiquitous information collection. Hence, right-based conceptualizations of information privacy are hard to enforce on a global level and adapt too slowly to the rapid pace of technological innovation (Oetzel and Spiekermann 2014). Control-based conceptualizations of information privacy do not account for the sheer complexity of consumer information systems and the diversity and high number of consumer interactions with them (Landau 2015). Market-based approaches do not foster information privacy because they promote opportunistic behavior of information handlers, which can easily leverage the enormous potential for hidden information and hidden action (Clarke 1999, Pavlou et al. 2007). The diversity and incommensurability of information privacy conceptualizations (see Table 1 for a listing of select information privacy conceptualizations used in the literature) led Solove (2002) to propose that information privacy is best conceptualized as a set of related problems with no universal definition.

Table 1. Select, extant conceptualizations of information privacy used in the literature. The brief descriptions have been adapted to the context of consumer information systems. The listed references are illustrative and not necessarily the original source.

Conceptualization	Brief Description	References
Information Privacy as Boundary Management	Information privacy is the management of information in three distinct domains and the movement of information between domains. The domain of the consumer, the domain of the organization, and a joint domain. Involved parties have to ensure that information does not cross the domain boundaries in undesirable ways.	(Petronio 1991, Spiekermann and Cranor 2009)
Information Privacy as Commodity	Information privacy is a tradable good. Consumers give up some information privacy in exchange for benefits offered by organizations.	(Laudon 1996, Li et al. 2014)
Information Privacy as Confidentiality	Information privacy is the protection of confidentiality of information. Whenever consumers provide information, organizations must ensure that it is not revealed to third parties.	(Gürses 2014)
Information Privacy as Contextual Integrity	Information privacy is the treatment of information by organizations in a way that aligns with social norms and expectations that developed over time in society for different contexts (eg, consumers may expect that chat message are not treated differently than informal conversations in offline contexts).	(Nissenbaum 2004, 2009)
Information Privacy as Control	Information privacy is control of information flows. Organizations offer means for controlling information flows. Consumers control information flows so that their information privacy demands are met.	(Westin 1967)
Information Privacy as Relationship	Information privacy is concerned with a vertical relationship of information exchange between organizations and consumers or a horizontal relationship of information exchange between consumers.	(Krol and Preibusch 2015)
Information Privacy as Restricted Access and Limited Control	Information privacy is making sure that information can only be accessed by authorized parties and giving consumers a certain degree of control over uses of information.	(Tavani 2007)
Information Privacy as Right	Information privacy is a right that people have. Organizations have to ensure that they do not violate consumers' right to information privacy. Otherwise they can be sued by consumers, government agencies, or other involved parties.	(Warren and Brandeis 1890)
Information Privacy as Risk Calculus	Information privacy is a risk assessment to be conducted by consumers. Consumers weigh the perceived benefits of information exchanges against the perceived risks.	(Dinev and Hart 2006a, Li 2012)
Information Privacy as Social Good	Information privacy is a social good that must be protected to maintain a free and democratic society, foster autonomy and free thought, and avoid risks like informational discrimination.	(DeCew 2004, Nissenbaum 2004)
Information Privacy as State	Information privacy is a continuum of states of information ranging from private information to public information.	(Laufer and Wolfe 1977)
Information Privacy as Statistical Disclosure Control	Information privacy is assuring that the absence or presence of a consumer in a data set cannot be inferred during data analyses. Organizations implement technical measures to ensure that the assurance is upheld.	(Soria-Comas et al. 2017)

1.2.2 Information Privacy Communication

From an information systems perspective, the lack of a common conceptualization of information privacy is problematic because it prohibits to ascertain how to reflect information privacy in information system design. To remedy this, a conceptualization of information privacy is required that accounts for the global nature of consumer information systems, their complexity, and the conflicting objectives of consumers and organizations. Since such conceptualization of information privacy is not available in research or practice, I developed an own view on information privacy over the course of this thesis, which has been inspired by the ideas of information privacy as a relationship (Krol and Preibusch 2015) and as contextual integrity (Nissenbaum 2004, 2009). I view information privacy as a vertical communication relationship between organizations and consumers—in other words, information privacy communication (Figure 1).[2]

Beyond the alignment with the research objective, the salient advantage of this view on information privacy is that it employs a role-based perspective. To adapt information privacy communication to other contexts than consumer information systems, the entity organization could be exchanged with any other entity with information privacy practices (eg, consumer, government, employee, or a generic information handler) and the entity consumer could be exchanged with any other entity with information privacy perceptions (eg, organization, government, employee, or a generic information subject). From a role-based perspective, I argue that the relationship between an organization and a consumer is the lowest common denominator for any information privacy problem. This relationship is shaped by the information privacy practices employed by the organization and the perception of them by the consumer. Accordingly, information privacy practices are practices employed by organizations in their information systems to address the information privacy challenges perceived as relevant by the organization. How the information privacy practices are perceived by consumers depends on consumers' mental model of information privacy (eg, rights-based, control-based, commodity-based, or some self-contrived conceptualization). Hence, the proposed view on information privacy allows to abstract from the incommensurability of extant information privacy conceptualizations and allows to focus on the phenomenon of interest in this thesis—communication of organizational information privacy practices.

1.2.3 The Relationship of Information Security and Information Privacy

An in-depth discussion of the relationship between information security and information privacy and potential reinforcing and debilitating impacts of information security practices on information privacy is beyond the scope this thesis. The purpose of this subchapter is to foster understanding of the complexity inherent to the relationship between information security and information privacy and to give the reader a broad idea

[2] This view on information privacy was shaped and refined over the course of this dissertation. Accordingly, it is only to a lesser extent reflected in the early publications included in this thesis.

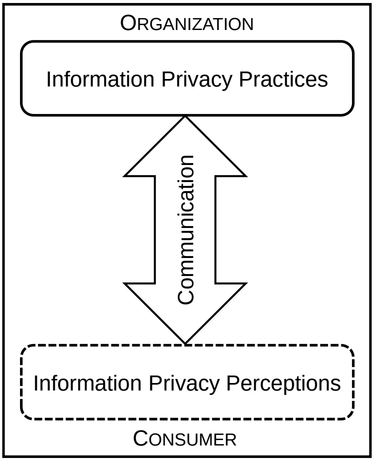

ORGANIZATION
Information Privacy Practices
Communication
Information Privacy Perceptions
CONSUMER

Figure 1.The view on information privacy adopted in this thesis. Information privacy is a vertical communication relationship between organizations and consumers.

of potential interactions between information security and information privacy. In everyday discourse, individuals sometimes treat the relationship as intuitive or assume that information security is a subset of information privacy (eg, claims that careful attention to information security will also result in information privacy) or the other way around (eg, conceptualization of information privacy as confidentiality). Information security and information privacy are distinct concepts that have a relationship and should be treated as such.[3] I propose to view information security as the driving force of the relationship between information security and information privacy. Up to a certain degree, implementation of information security practices reinforces information privacy by either making organizational information privacy practices more desirable to consumers or by enabling consumers to protect themselves from undesirable organizational information privacy practices. However, there will always be a turning point where implementation of additional information security practices will debilitate information privacy.

Information security is generally defined as the maintenance of confidentiality, integrity, and availability of information (ISO 2016). A more tangible metaphor for the characterization of the relationship between information security and information privacy is to envision information security as an order machine (see Figure 2). An information security order machine is composed of an information territory and a safe zone (Vuorinen and Tetri 2012). The machine maintains confidentiality, integrity, and availability of information in an information territory—"a material medium comprising information that always possesses a particular order" (Vuorinen and Tetri 2012, p. 703). The information

[3] The presented conceptualization of the relationship between information security and information privacy emerged during the preparation of this thesis. Accordingly, the early publications do not differentiate that expressively between information security and information privacy.

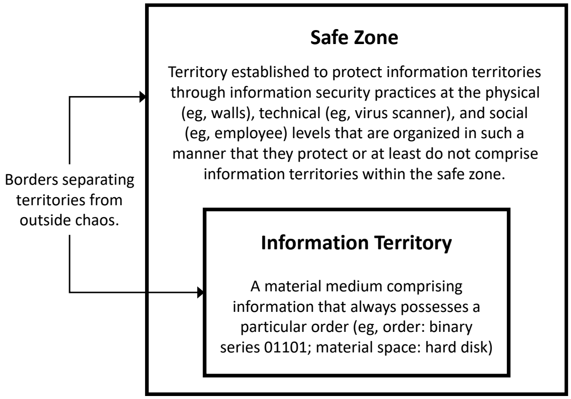
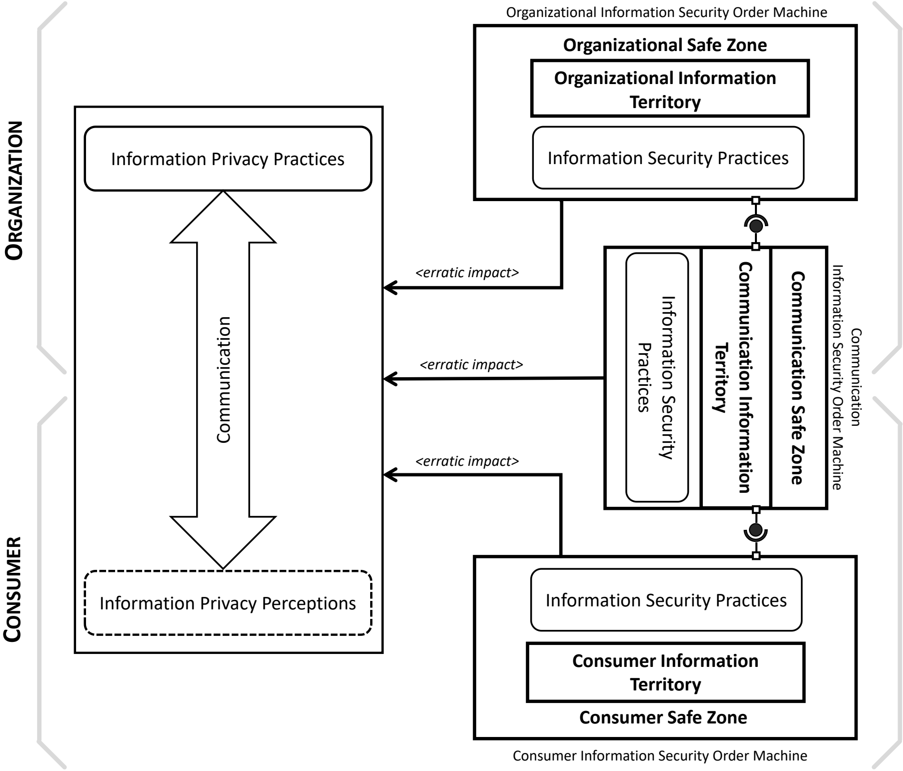

Safe Zone
Territory established to protect information territories through information security practices at the physical (eg, walls), technical (eg, virus scanner), and social (eg, employee) levels that are organized in such a manner that they protect or at least do not comprise information territories within the safe zone.
Borders separating territories from outside chaos.
Information Territory
A material medium comprising information that always possesses a particular order (eg, order: binary series 01101; material space: hard disk)

Figure 2. Schematic representation of information security as an order machine. Information to be protected is kept in order in the information territory, which is encapsulated in a safe zone employing information security practices to shield the information territory from external chaos. Adapted from Vuorinen & Tetri (2012, p. 703).

territory is encapsulated by a safe zone where information security practices protecting the information territory from outside chaos are in place (Vuorinen and Tetri 2012). Information security practices are practices employed to maintain information security.

To characterize the relationship between information security and information privacy, three distinct information security order machines are relevant (see Figure 3). One information security order machine in the domain of the organization, one in the domain of the consumer, and one connecting both domains to facilitate communication and information exchange. All these information security order machines can exhibit reinforcing and debilitating impacts on information privacy depending on implemented information security practices. Reinforcing impacts are, for example, caused through encryption, which prevents undesirable information access by third parties, through access control, which ensures that information can only be accessed by authorized parties, or through information disturbance and pseudonymization techniques, which ensure that information cannot be easily linked back to individuals. However, the same information security practices can exhibit debilitating effects on information privacy depending on situational circumstances. Encryption and access control can, for example, prevent or create unnecessarily high burdens for sharing information in cases where consumers want to share their information. Information disturbance and pseudonymization techniques may lead to undesirable misrepresentations of the self or promote false inferences from consumer information. Accordingly, I propose that the relationship between information security and information privacy needs to be viewed as erratic. The relationship between information security and information privacy depends, not only, on consumer perceptions of organizational information privacy practices and impacts of information security practices implemented at the provider side, but also, on the impacts



Organization
Consumer
Organizational Information Security Order Machine
Organizational Safe Zone
Organizational Information Territory
Information Security Practices
Information Privacy Practices
Communication
Information Privacy Perceptions
<erratic impact>
<erratic impact>
<erratic impact>
Information Security Practices
Communication Information Territory
Communication Safe Zone
Communication Information Security Order Machine
Information Security Practices
Consumer Information Territory
Consumer Safe Zone
Consumer Information Security Order Machine

Figure 3. Erratic relationship between information security and information privacy. Three distinct information security order machines (organization, consumer, communication channel) can have reinforcing and debilitating impacts on information privacy.

of information security practices implemented by the consumer and at the communication channel.

To sum up, information security and information privacy are both valuable and desirable characteristics of consumer information systems. Yet, it is impossible to have both at the same time. Information systems design in research and in practice has to focus on achieving either one or the other or has to account for the inevitable tradeoffs between information security and information privacy. Within the scope of this thesis, I focus on information privacy and consider information security only as far as necessary for this research on substantive communication of organizational information privacy practices.

1.3 Research Approach

The overarching research approach could be broadly characterized as a retroductive, mixed-methods approach for creation of nomothetic design knowledge (Baskerville et al. 2015, Sæther 1998, Venkatesh et al. 2016). Since I aim to bridge normative perspectives on and empirical reality of organizational information privacy communication, neither a purely deductive nor a purely inductive form of reasoning is suitable to create design knowledge for communication of organizational information privacy communication. Hence, I employ a retroductive form or reasoning, which shifts between a predominant focus on investigation of empirical reality and a predominant focus on derivation of novel insights from extant knowledge encapsulated in theory (Mueller and Urbach 2017, Sæther 1998). Figure 4 organizes the six publications included in this thesis by the predominant form or reasoning used (see chapter 1.5 for an overview of the six publications).

The overarching goal of this cumulative thesis is the creation of nomothetic design knowledge; that is, “design knowledge applicable to an identifiable section of a given population” (Baskerville et al. 2015, p. 549). First, I clarify the problem space (Venable 2006) for communication of organizational information privacy practices and establish its relevance in the work on SRQ1. Second, I outline a potential solution space (Venable 2006) in the work on SRQ2—that is, nomothetic design knowledge for the class of artifacts suitable for substantive communication of organizational information privacy practices in consumer information systems. With the work on SRQ3, the proposed information systems design theory is substantiated by demonstrating that consumers’ information privacy information needs are in fact heterogeneous—the main assumption underlying the proposed design for substantive communications of organizational information privacy practices.

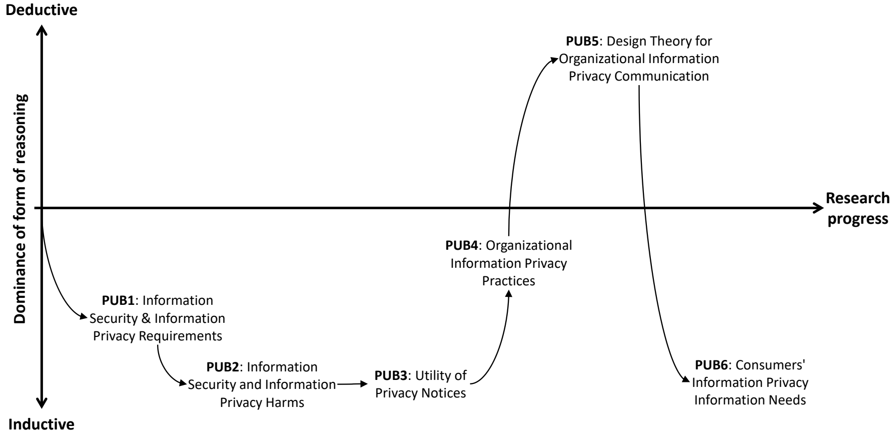

Deductive
Dominance of form of reasoning
Inductive
Research progress
PUB5: Design Theory for Organizational Information Privacy Communication
PUB4: Organizational Information Privacy Practices
PUB1: Information Security & Information Privacy Requirements
PUB2: Information Security and Information Privacy Harms
PUB3: Utility of Privacy Notices
PUB6: Consumers' Information Privacy Information Needs

Figure 4. Overview of form of reasoning used in the six publications (PUB) included in this cumulative thesis.

To benefit from the breadth of quantitative methods and from the depth of qualitative methods, I employ a mixed-methods research design (Venkatesh et al. 2013, 2016). As the research questions, RQ and SRQ1-3, are intentionally broad to cover the research conducted in all six publications included in this thesis, the research questions are neither explicitly quantitative nor explicitly qualitative. I addressed SRQ1 with a predominantly qualitative (PUB1) and two predominantly quantitative publications (PUB2-3), SRQ2 with two predominantly qualitative publications (PUB4-5), and SRQ3 with a predominantly quantitative publication (PUB6). Figure 5 presents an overview of the dominance of the methodological approaches used. Finally, the findings of the work on SRQ1-3 are consolidated to answer RQ. Since this research is cumulative in nature, the research questions are dependent on each other. Furthermore, they are of an emergent nature because identification of the relevant research questions was dependent on the clarity of the problem space, which was constantly improved with increasing research progress.

The primary purpose of employing a mixed-methods design was expansion—mixed-methods research was used "to explain or expand on the understanding obtained in a previous strand of a study" (Venkatesh et al. 2016, p. 478). A secondary purpose was development—use of "the findings from one method to help inform another method" (Venkatesh et al. 2016, p. 478). For instance, the survey instruments in PUB6 were developed based on the ontology developed in PUB4. Another secondary purpose was complementarity—use of "mixed-methods research to seek elaboration, enhancement, illustration, and clarification of the results from one method with results from the other method" (Venkatesh et al. 2016, p. 478). For instance, the survey in PUB6 was conducted to illustrate the assertions made during the theory building in PUB5.

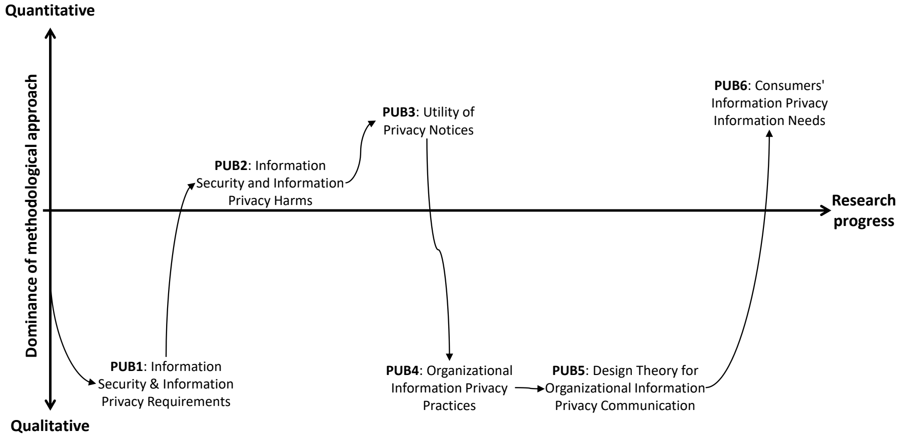

Quantitative
Dominance of methodological approach
Qualitative
Research progress
PUB1: Information Security & Information Privacy Requirements
PUB2: Information Security and Information Privacy Harms
PUB3: Utility of Privacy Notices
PUB4: Organizational Information Privacy Practices
PUB5: Design Theory for Organizational Information Privacy Communication
PUB6: Consumers' Information Privacy Information Needs

Figure 5. Overview of dominance of methodological approaches used in the seven publications (PUB) included in this cumulative thesis.

Although some positivistic traits are apparent in the publications included in this thesis (eg, PUB3, PUB4, or PUB6), the dominant paradigmatic stance is interpretivism; that is, I focus on “the understanding of human and social interaction by which the subjective meaning of the reality is constructed” (Chen and Hirschheim 2004, p. 201). In particular, I focus on potential for improvement of communication between organizations and consumers with respect to information privacy.

In line with the cumulative nature of this thesis, I employed a mixed-methods multistrand design (Venkatesh et al. 2016). The employed mixing strategy can be characterized as partially mixed methods. Methods were predominantly mixed in the data collection and analysis phases across the sequential research strands. Since substantive organizational information privacy communications do not exist at the time of writing, this research is predominantly exploratory; that is, I focus on theory development and not on theory testing (Venkatesh et al. 2016). Since qualitative research methods were more suitable for the research questions addressed in this thesis, the mixed-methods research design is qualitative dominant. Three publications (PUB1, PUB4, PUB5) are purely qualitative. The other three publications mix quantitative and qualitative research methods to different degrees (see Figure 5).

Before focusing on substantive communication of organizational information privacy practices in consumer information systems in general, I initially focused on consumer information systems in health care because information privacy is of particular relevance in health care information systems. Health care information systems face various risks, such as intentional and unintentional disclosure or manipulation of information (Landry et al. 2011, Shahri and Ismail 2012). While health care information systems are diverse in terms of offered functionality, implementation, and targeted consumers, a common and constant trait is the handling of personal, sensitive medical information that needs to be protected (Rindfleisch 1997). Even if health care information systems do not explicitly access personal, medical information of consumers, sole observation of consumer behavior can lead to information privacy violations (Slamanig and Stingl 2008). Mobile client devices, such as smartphones, introduce further challenges. On the large app markets of Apple (itunes.apple.com) and Google (play.google.com) everyone can deploy and distribute mobile health (mHealth) applications (apps). In addition, many apps are financed through advertisements (Zhang et al. 2012), which requires access to consumer information to tailor advertisements, thereby, introducing new privacy challenges.

1.4 Outline of Main Results

The main result of this thesis is the conceptualization of a design space for substantive organizational information privacy communications in form of an information systems design theory for transparency of organizational information privacy practices (TIPP theory). In essence, the TIPP theory prescribes that substantive organizational information privacy communications must balance offering access to a comprehensive selection of information and avoiding cognitive overload by focusing on topical relevance and interactivity.

Development of the TIPP theory was motivated by an analysis of the privacy notices of the 300 most-frequently rated mHealth apps in the iOS and the Android app store, which revealed the inadequacy of the most prevalent form of organizational information privacy communication—that is, privacy notices. The analysis reveals that, even in the information privacy–sensitive domain of mHealth, privacy notices are often not available, do not impact app ratings, offer only scarce information on the actual mHealth apps to which they pertain, and require high reading grade levels to be understood.

As an expository instantiation of the TIPP theory and to clarify what constitutes a comprehensive selection of information on organizational information privacy practices, I developed an ontology of the information relevant for communication of organizational information privacy practices (RECIPE ontology). The RECIPE ontology consolidates extant knowledge in research and practice into a hierarchical model of common organizational information practices. The hierarchical model organizes 132 different categories of information relevant for communication of organizational information privacy practices across five hierarchy levels by consumers' main information privacy concerns—information collection, rationale for collection, handling of information, and offered information privacy controls (Ackerman et al. 1999, Antón et al. 2010, Earp et al. 2005). Relations across hierarchy levels between information categories represent 'is_a' relations (Smith 2004). The RECIPE ontology serves organizations as a starting point to understand what information should be made available in organizational information privacy communication.

To ensure topical relevance of communicated information and interactivity, the TIPP theory prescribes that consumer information systems suitable for substantive communication of organizational information privacy practices should comprise at least two components. First, a component for management of information on organizational information privacy practices. This component could be implemented with a central repository for organizational information privacy practices to ensure swift and consistent retrieval of required information, an update functionality to account for changes in organizational practices, and a machine-interpretable version of the RECIPE ontology to remove irrelevant information. Second, a component for interactive communication of organizational information privacy practices to consumers. This component could be implemented by offering tailoring capabilities to ensure adaptation to consumer preferences and needs (Germonprez et al. 2007), by arranging ready-made interface configurations for different tasks relevant for communication of organizational information privacy practices, and by allowing consumers to select different presentations modes (eg, text, tables, lists, charts, graphs, animations) to support intuitive communication.

The design knowledge captured in the TIPP theory and the design rationale for TIPP instantiations is made explicit in form of testable propositions based on the model of

TIPP Instantiation Design Quality (see Figure 6), which captures the underlying concepts of transparency of organizational information privacy practices and their laws of interaction (Dubin 1978). Fulfillment of TIPP metarequirements (ie, comprehensiveness, topical relevance, and interactivity) is represented as a relational concept determined by perceived need for the metarequirement in relationship with the implementation extent of the metarequirement.

TIPP instantiations can be in four states. First, design of TIPP instantiations is optimal if all perceived needs for metarequirements equal the respective implementation extent. Second, TIPP instantiations will be unsuitable for substantive communication of organizational information privacy practices if at least one perceived need for a metarequirement is greater than the respective implementation extent. Third, if at least one perceived need for a metarequirement is less than the respective implementation extent, TIPP instantiations are better than they must be. Fourth, TIPP instantiations are unsuitable for substantive communication of organizational information privacy practices if at least one perceived need for a metarequirement is greater than the respective implementation extent and at least one other perceived need for a metarequirement is less than the respective implementation extent.

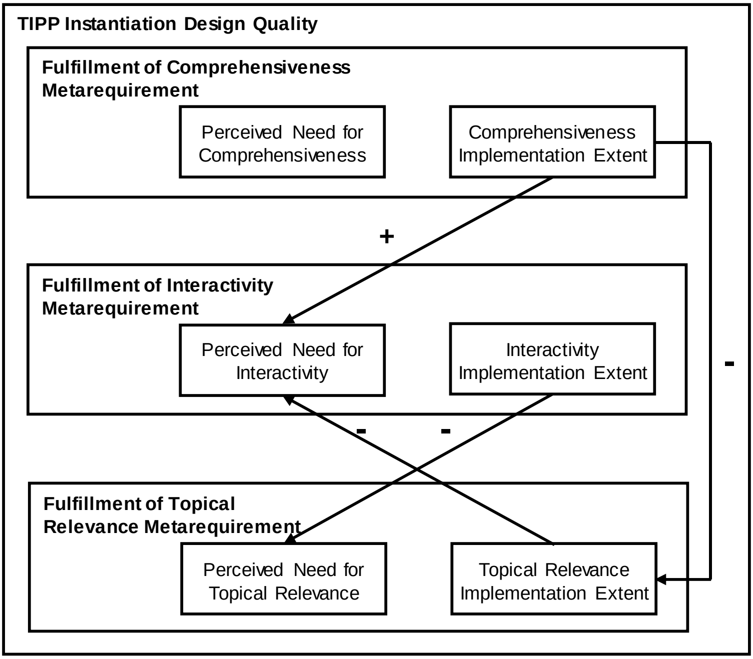

TIPP Instantiation Design Quality
Fulfillment of Comprehensiveness Metarequirement
Perceived Need for Comprehensiveness
Comprehensiveness Implementation Extent
+
Fulfillment of Interactivity Metarequirement
Perceived Need for Interactivity
Interactivity Implementation Extent
-
-
-
Fulfillment of Topical Relevance Metarequirement
Perceived Need for Topical Relevance
Topical Relevance Implementation Extent

Figure 6. Model of TIPP Instantiation Design Quality with the underlying concepts of transparency of organizational information privacy practices and their laws of interaction.

The TIPP theory reveals four salient laws of interaction between perceived needs for metarequirements and implementation extents of metarequirements. First, increases in comprehensiveness implementation extent reduce topical relevance implementation extent because provision of more information makes it more likely that irrelevant information is provided. Second, increases in comprehensiveness implementation extent increase perceived need for interactivity because the more information is provided the more tasks are supported, accordingly, more interactive features are required to adapt communicated information to current tasks of consumers. Third, increases in interactivity implementation extent decrease perceived need for topical relevance because interactivity simplifies retrieval of relevant information. Fourth, increases in topical relevance implementation extent decrease perceived need for interactivity because there is reduced need for filtering irrelevant information or identifying relevant information. The underlying concepts of transparency of organizational information privacy practices, their laws of interaction, and the possible states of TIPP instantiations give rise to six prominent testable propositions (P#):

> ***P1:*** *Organizational information privacy communications that do not fulfill the topical relevance metarequirement will be perceived as transparent if they fulfill the comprehensiveness metarequirement and remedy the lack of topical relevance through overfulfillment of the interactivity metarequirement.*
>
> ***P2:*** *Organizational information privacy communications that fulfill all TIPP metarequirements (comprehensiveness, topical relevance, and interactivity) will be better designed than organizational information privacy communications that fulfill the comprehensiveness metarequirement and overfulfill the interactivity metarequirement.*
>
> ***P3:*** *Design quality of organizational information privacy communications decreases over time because of changes of perceived needs for metarequirements resulting in overfulfillment or nonfulfillment of metarequirements.*
>
> ***P4:*** *Decreasing time where organizational information privacy communications are not in an optimal state requires constant elicitation and assessment of perceived needs for metarequirements and consequent adaption of implementation extents.*
>
> ***P5:*** *When perceived need for a metarequirement is greater than the respective implementation extent, the implementation extent should be increased to obtain meaningful organizational information privacy communications.*
>
> ***P6:*** *When perceived need for a metarequirement is less than the respective implementation extent, it is only beneficial to decrease the implementation extent in such situations where associated costs for instantiation operation outweigh additional implementation efforts.*

A central assumption of the TIPP theory—the assumption that consumers' information privacy information needs are diverse—was supported in a concluding investigation of consumers' information privacy information needs. The online survey study revealed nine distinct consumer archetypes with diverse information privacy information needs that organizational information privacy communication must cater to. Some consumer archetypes exhibit low, moderate, or high information privacy information needs across all organizational information privacy practices included in the survey. Other consumers have more refined information privacy information needs. Some consumer archetypes exhibit higher information needs for organizational information privacy practices related to identifier collection, information handling, offered information privacy controls, or combinations thereof. Some archetypes exhibit lesser interests for organizational information privacy practices related to information sensors and consumer data collection. Within the scope of the TIPP theory, the diversity of consumers' information privacy information needs was grounded in extant research on human information seeking and processing (eg, Rouse and Rouse 1984, Sweller 1988). The online survey demonstrates that human information needs are also diverse in the domain of information privacy.

The main results of this thesis can be summarized as the creation of knowledge on how organizations can account for information privacy in consumer information systems, through substantive communication of organizational information privacy practices, in a more versatile manner than extant approaches offering only narrow support for satisfying consumers' information privacy information needs by offering either too general or too specialized information. The TIPP theory constitutes a metaspecification of the interface communication information practices conducted in organizations' inner environment to external environments (Simon 1996) and offers guidance how organizations can account for differences in information privacy information needs during electronic interactions with consumers. The contested and complex nature of information privacy (Mulligan et al. 2016, Solove 2002) makes it unlikely that organizations can satisfy consumers' information privacy needs with a universally applicable solution. The TIPP theory addresses this problem by proposing a flexible, adaptive approach to organizational information privacy communication.

1.5 Overview of Publications Included in this Thesis

Table 2. Overview of publications included in this thesis with publication statistics (CIT=Google Scholar citation count, AM=Altmetric.com attention score, h5=Google Scholar h5-index, IF=Thomson Reuters 2016 Impact Factor, JQ3=VHB-JOURQUAL3, WKWI=WKWI 2008 Ranking)

ID	Publication	Statistics	Dominant form of reasoning	Dominant methodological approach	Research context	SRQ
1	Dehling T, Sunyaev A (2014) Secure Provision of Patient-Centered Health Information Technology Services in Public Networks—Leveraging Security and Privacy Features Provided by the German Nationwide Health Information Technology Infrastructure. Electronic Markets (EM) 24(2):89–99.	*Publication:* CIT: 14 AM: 2 *Outlet:* h5: 21 IF: 1.864 JQ3: B WKWI: A	Inductive	Qualitative	Patient-centered health information technology services	1
2	Dehling T, Gao F, Schneider S, Sunyaev A (2015) Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Applications on iOS and Android. JMIR mHealth uHealth (JMU) 3(1):e8.	*Publication:* CIT: 70 AM: 13 *Outlet:* h5: N/A IF: 4.636 JQ3: N/A WKWI: N/A	Inductive	Quantitative	Mobile health applications	1
3	Sunyaev A, Dehling T, Taylor PL, Mandl KD (2015) Availability and Quality of Mobile Health App Privacy Policies. Journal of the American Medical Informatics Association (JAMIA) 22(e1):e28–e33.	*Publication:* CIT: 95 AM: 280 *Outlet:* h5: 61 IF: 3.698 JQ3: N/A WKWI: N/A	Inductive	Quantitative	Mobile health applications	1
4	Dehling T (2017) RECIPE: An Ontology of the Information Relevant for Organizational Information Privacy Communication. Working Paper Series. (Kassel, Germany).	*Publication:* CIT: 0 AM: N/A *Outlet:* h5: N/A IF: N/A JQ3: N/A WKWI: N/A	Inductive	Qualitative	Consumer information systems	2
5	Dehling T, Sunyaev A (2017) Meaningful Organizational Information Privacy Communication in Consumer Information Systems. European Journal of Information Systems (EJIS), under review (first round).	*Publication:* CIT: 0 AM: N/A *Outlet:* h5: 40 IF: 2.356 JQ3: A WKWI: A	Deductive	Qualitative	Consumer information systems	2
6	Dehling T, Schmidt-Kraepelin M, Sunyaev A (2017) Consumer Archetypes for Organizational Information Privacy Communication. Information Systems Research (ISR), under review (first round).	*Publication:* CIT: 0 AM: N/A *Outlet:* h5: 54 IF: 2.763 JQ3: A+ WKWI: A	Inductive	Quantitative	Consumer information systems	3

1.5.1 PUB1: Dehling T, Sunyaev A (2014) Secure Provision of Patient-Centered Health Information Technology Services in Public Networks—Leveraging Security and Privacy Features Provided by the German Nationwide Health Information Technology Infrastructure

PUB1 investigates general information security and information privacy requirements for consumer information systems. The research context for PUB1 are patient-centered health information technology services (PHS), which provide personalized electronic health services to patients. PUB1 is a qualitative inductive study. In a first step, information security and information privacy requirements for PHS are consolidated from extant literature. Afterwards, it is investigated how features of the German health information technology infrastructure (HTI) can be leveraged for improving information security and information privacy of PHS. In a third step, additional information security measures to fulfill the requirements that are not covered by features of the German HTI are proposed based on extant literature. Finally, a five-step guideline for ensuring information security in PHS is proposed to consolidate the findings of the study. Key findings of the study are that information security features of health information technology networks can be used to create a solid foundation for protecting information security and information privacy in PHS offered in public networks like the internet.

PUB1 contributes to SRQ1 by establishing a high-level overview of information security and information privacy requirements for consumer information systems and by revealing insights into measures available for accounting for information security in consumer information systems and into the challenges that organizations face in meeting information security and information privacy requirements.

I contributed to PUB1 by developing the research problem and approach, by performing the literature review, the analysis of the documentation of the German HTI, and all ensuing data analyses, and by writing the initial draft of the manuscript and all revisions.

1.5.2 PUB2: Dehling T, Gao F, Schneider S, Sunyaev A (2015) Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Applications on iOS and Android

PUB2 investigates potential for harm through information security and information privacy violations in consumer information systems. The research context for PUB2 are mHealth apps for the mobile operating systems iOS and Android. PUB2 is an inductive study that is predominantly quantitative. First, we identified mHealth apps by crawling the app categories Medical and Health & Fitness in the iOS and Android app stores. Second, we manually coded the descriptions of 200 mHealth apps with a focus on health-related app characteristics. Third, we leveraged the resulting coding scheme to automatically tag the descriptions of the remaining 37,064 apps and excluded all apps that were not health-related or not available in English from further assessment. Fourth, we constructed a graph, where nodes represent apps and edges represent codes that apps have in common, based on the 24,405 remaining apps and applied a modularity-based, hierarchical, agglomerative clustering algorithm to identify similar apps (Louvain method; Blondel et al. 2008). Fifth, we coded information security and information privacy implications of the 245 resulting clusters based on the health specificity of information available to apps, potential damage through information leaks, potential damage through information manipulation, potential damage through information loss, and potential value of app-accessible information to third parties. Sixth, we grouped app clusters into twelve archetypes with similar information security and information privacy implications. Key findings of the study are that less than a quarter of mHealth apps are in more or less widespread use, that the majority of apps (96.63%) have at least some potential for harm, and that 11.67% of apps scored the highest possible assessments for potential for harm through information security and information privacy violations.

PUB2 complements the insights from PUB1 and contributes to SRQ1 by demonstrating that various kinds of consumer information systems (mHealth apps) collect and offer critical, sensitive, private medical information calling for a special focus on information security and information privacy to protect consumers from potential harm.

I contributed to this publication by developing the research problem and approach, by implementing the Android app store crawler in Java, by setting up and administering the infrastructure for all data management in MySQL, by overseeing development of the app description coding scheme and the app description coding process, by developing the algorithm for automated coding of app descriptions in Java, by developing the algorithm for graph construction based on the coding results in Java, by implementing the clustering algorithm in Java, by coding the information security and information privacy implications of the identified clusters, by developing scripts for data analysis in Bash, R, and SQL, by performing all required statistical analyses, by grouping the clusters into archetypes and naming them, and by writing the initial draft of the manuscript and all revisions.

1.5.3 PUB3: Sunyaev A, Dehling T, Taylor PL, Mandl KD (2015) Availability and Quality of Mobile Health App Privacy Policies

PUB3 investigates the utility of privacy notices[4] for communication of organizational information privacy practices in consumer information systems. The research context for PUB3 are privacy notices of mHealth apps for the mobile operating systems iOS and Android. PUB3 is an inductive study that is predominantly quantitative. First, we identified the 300 most frequently rated English language mHealth apps in the iOS app store and in the Android app store based on the data set of PUB2. Second, we retrieved privacy notices for the 600 apps from the app store, from the developer homepage, or with Google Search. Third, we assessed length, reading grade level, scope, and content

[4] Within the scope of this thesis, I use the term privacy notice to refer to organizations' natural language descriptions of the information privacy practices of their consumer information systems because the term is less ambiguous than the term privacy policy, which also refers to organizational directives and guidelines with respect to information privacy. However, in cases where the publications included in this thesis use the term privacy policy, the original wording is retained.

of retrieved privacy notices. Key findings of the study are that only 183 (30.5%) of the apps in the sample have privacy notices, that the average length of privacy notices is 1755 (SD=1301) words with a reading grade level of 16 (SD=2.9), and that two thirds (66.1%) of the privacy notices do not specifically address the app itself.

PUB3 complements the insights from PUB1 and PUB2 and contributes to SRQ1 by showing that organizations often fail to provide privacy notices for mHealth apps and that the privacy notices that are available do not make information privacy practices transparent to consumers, require college-level literacy, and are often not focused on the app itself.

I contributed to PUB3 by developing initial ideas for the research problem and approach, by setting up and administering the infrastructure for all data management in MySQL, by overseeing the retrieval of privacy notices, by implementing custom software for assessment of privacy notice length and reading grade level in Java, by coding the privacy notices with respect to scope and content, by developing the privacy notice coding scheme, by developing scripts for data analysis in Bash, R, and SQL, by performing all required statistical analyses, and by writing the initial draft of the manuscript and performing all revisions. In addition, I contributed to the creation of the mHealth app data set, which was reused from PUB2 for identification of the most frequently rated mHealth apps, as described in section 1.5.2.

1.5.4 PUB4: Dehling T (2017) RECIPE: An Ontology of the Information Relevant for Organizational Information Privacy Communication

PUB4 investigates the information relevant for information privacy communication in consumer information systems. The research context is information privacy communication in consumer information systems in general, but the mHealth app privacy notices retrieved in PUB3 are used as one of the data sources. PUB4 is a qualitative study that is predominantly inductive. In PUB4, the RECIPE ontology, which captures the information relevant for communication of information privacy practices, is developed in three iterations. First, an initial version of the RECIPE ontology was developed based on the specification of the Platform for Privacy Preferences Project (P3P; Cranor et al. 2006). Second, the RECIPE ontology was complemented through expert review and employed for a more detailed assessment of the content of the privacy notices retrieved in PUB3. Third, the RECIPE ontology was refined based on a review of extant literature on privacy notices. Finally, the ontology was evaluated through a comparison to the content of the Wikipedia privacy notice. The key result of PUB4 is the developed RECIPE ontology.

After establishing the need for improvements of the design of information privacy communication in consumer information systems in PUB1–3, PUB4 contributes to SRQ2 and establishes the foundation for improving the design of organizational information privacy communications by consolidating the information relevant for organizational information privacy communication from extant knowledge in research and practice in form of an ontology. Knowledge of the information relevant for communication of information privacy practices is a prerequisite for development of relevant and purposeful artifacts intended to communicate information privacy practices.

I contributed to this publication by developing the research problem and approach, by setting up and administering the infrastructure for all data management in MySQL, by performing the P3P review, by coding the mHealth app privacy notices, by performing the literature review, by developing all iterations of the RECIPE ontology, by developing scripts for data analysis in Bash and SQL, and by writing the manuscript and all revisions.

1.5.5 PUB5: Dehling T, Sunyaev A (2017) Meaningful Organizational Information Privacy Communication in Consumer Information Systems

PUB5 explores how to make organizational information privacy communication in consumer information systems meaningful. The research context is information privacy communication in consumer information systems in general. PUB5 is a qualitative deductive study. PUB5 draws from the empirical insights gained throughout PUB1–4. However, it is a publication that focuses solely on theory development and grounding of the developed theory in two kernel theories from the domains of interpersonal communication and educational psychology—Uncertainty Reduction Theory (Berger and Calabrese 1975) and Cognitive Load Theory (Kalyuga 2011, Sweller 1988). PUB5 advances extant research on organizational information privacy communication by conceptualizing a design space for organizational information privacy communication that bridges the communication generalization and the communication specification stream in form of an information systems design theory (Gregor and Jones 2007) for transparency of information privacy practices—the TIPP theory. First, metarequirements for organizational information privacy communications are derived from Uncertainty Reduction Theory and Cognitive Load Theory. Second, an abstract architecture for TIPP instantiations is proposed as principles of form and function. Third, the RECIPE ontology from PUB4 is presented as expository instantiation of the TIPP theory. Fourth, the design knowledge captured in the TIPP theory and the design rational for TIPP instantiations is made more explicit in form of testable propositions, which are based on a theoretical model of TIPP instantiation design quality, to demonstrate the utility of the TIPP theory. Fifth, an illustrative example, which ranks potential, abstract TIPP instantiations by suitability for establishing transparency of organizational information privacy practices based on simplified, illustrative measurements for the fulfillment of TIPP metarequirements, is presented to demonstrate that operationalization of the TIPP theory is theoretically feasible and, consequently, that the TIPP theory is falsifiable. The key result of PUB5 is the developed TIPP theory.

PUB5 contributes to SRQ2 by conceptualizing design of substantive organizational information privacy communications in form of an information systems design theory for transparent communication of information privacy practices, which accounts for the deficiencies of extant approaches revealed in PUB3 and the diversity of relevant information identified in PUB4. In essence, organizations aiming to establish transparency of organizational information privacy practices must balance comprehensiveness of communicated information and avoidance of cognitive overload. The TIPP theory is a metaspecification of what to build to communicate information about organizational information privacy practices to consumers in a substantive way and offers insights that question common organizational practices, such as posting privacy notices or privacy seals.

I contributed to this publication by developing the research problem, by conceiving, developing, and articulating the TIPP theory through literature study, discussions with fellow researchers, and contemplation, and by writing the manuscript and all revisions.

1.5.6 PUB6: Dehling T, Schmidt-Kraepelin M, Sunyaev A (2017) Consumer Archetypes for Organizational Information Privacy Communication

PUB6 explores consumer preferences for organizational information privacy communication. The research context is information privacy communication in consumer information systems in general. However, different types of mobile apps are used as exemplary scenarios in the survey. PUB6 is an inductive study that is predominantly quantitative. First, we developed eighteen generic descriptions for common types of apps available in the iOS and Android app stores and elicited consumer perceptions of information sensitivity and perceived privacy (Dinev et al. 2013) for the different types of apps with an online survey with 145 valid responses. Each participant was presented with four randomly selected types of apps. Second, we conducted an additional online survey to elicit consumers general information privacy information needs. To control for situational impacts, survey participants were presented with one randomly selected app description and instructed to imagine using such an app when answering the questions regarding their information privacy information needs. The presented app description was randomly selected out of four app descriptions (one with high, two with medium, and one with low information sensitivity) that were chosen based on the results of the first survey. The questions eliciting participants' information privacy information needs were developed based on the RECIPE ontology (PUB4). We elicited 909 valid responses for the online survey. Third, we employed an agglomerative hierarchical community detection algorithm (Ward's method; Ward 1963) to identify consumer archetypes with similar information privacy information needs. Fourth, we named and characterized the identified archetypes and examined their differences in information privacy information needs based on five latent variables identified through exploratory factor analysis. The key result of PUB6 is the identification of nine consumer archetypes with diverse information privacy information needs. Thus, PUB6 complements extant research on consumers' information privacy preferences by demonstrating that not only information privacy perceptions, behaviors, and concerns (Acquisti et al. 2015, Nissenbaum 2009) but also information privacy information needs are diverse.

PUB6 answers SRQ3 and provides the final missing link to answer RQ. PUB5 already delineates a design space for consumer information system components that communicate organizational information privacy practices to consumers in a substantive war. PUB6 substantiates the knowledge captured in the TIPP theory by providing evidence for a central assumption of the TIPP theory—the assumption that consumers' information privacy information needs are diverse. Within the scope of PUB5, the diversity of consumers' information privacy information needs was grounded in extant research on human information seeking and processing (eg, Rouse and Rouse 1984, Sweller 1988). PUB6 demonstrates that human information needs are also diverse in the domain of information privacy.

I contributed to PUB6 by developing initial ideas for the research problem and approach, by shaping the final research problem and approach, by contributing to the survey design and execution, by implementing custom software for the community detection analysis in Python, by performing the exploratory factor analysis in SPSS, by naming the consumer archetypes, by developing scripts for data analysis in Bash and Python, by performing all statistical analyses except for the statistical analyses reported for the first survey, and by writing the manuscript and all revisions.

1.6 Discussion of Main Findings and Implications

The main objective of this cumulative thesis is to bridge the gap between normative perspectives on and available technical solutions for communication of organizational information privacy practices. To address the objective, I first refined the research problem and established its relevance by consolidating information security and information privacy requirements for consumer information systems and common measures to address them from extant literature (PUB1), by demonstrating that consumer information systems have the potential to harm consumers through information security and information privacy violations (PUB2), and by establishing the inadequacy of privacy notices for organizational information privacy communication (PUB3). Subsequently, I consolidated the information relevant for communication of organizational information privacy practices from extant knowledge in research and practices in form of an ontology (PUB4) and developed an information systems design theory for the class of information systems that are capable to communicate organizational information privacy practices in a substantive way (PUB5). Finally, I substantiated the TIPP theory through an examination of the information privacy information needs of consumers and the identification of nine distinct consumer archetypes with diverse information privacy information needs (PUB6), which constitutes further evidence that organizational information privacy communication must be not only comprehensive and topically relevant but also interactive to adapt to the diverse information privacy information needs of consumers.

1.6.1 Limitations

This thesis is not without limitations. First, the investigation of SRQ1 is focused on consumer information systems in the domain of health care. The findings may thus not be transferable to consumer information systems in other domains (eg, games, e-commerce, or search engines). However, information privacy is a concept of general interest in the information systems domain (Bélanger and Crossler 2011). In addition, consumer information systems in the health care domain have access to sensitive consumer information which makes information privacy particularly relevant (Rindfleisch 1997). Thus, health care constitutes an appropriate research context for information privacy in consumer information systems. Besides the focus on health care, the investigation of SRQ1 is also focused on privacy notices. This was motivated by the dominance of privacy notices for communication of organizational information privacy practices in practice and the extensive body of extant research on privacy notices (Bélanger and Crossler 2011). Furthermore, over the course of this thesis, I did not come across any extant approach to communication of organizational information privacy practices in consumer information systems that seemed more suitable than privacy notices, which themselves are, however, unsuited for communication of organizational information privacy practices in consumer information systems (Earp et al. 2005, McDonald and Cranor 2008, Sunyaev et al. 2015).

Second, the findings of the work on SRQ3 cannot be directly translated to consumers' information privacy information needs with respect to situated consumer information systems. For specific, situated consumer information systems, the size of some consumer archetypes may be negligible. For example, consumer information systems running on air-gapped systems are likely to be predominantly confronted with Laid-Back Information Seekers. Consumer information systems that are only occasionally used will likely not be confronted with many Committed Information Seekers. The goal of this thesis is the investigation of organizational information privacy communication in consumer information systems in general. Hence, an overview of the diversity and range of consumer archetypes that organizations providing consumer information systems may be confronted with was established. What consumer archetypes situated consumer information systems are confronted with needs to be determined based on the characteristics and use cases of the respective consumer information system.

Third, at the time of writing, the phenomenon studied in this thesis—substantive organizational information privacy communication—is virtually non-existent in the consumer information systems landscape. Hence, this thesis is focused on the deficits of extant approaches to organizational information privacy communication, is grounded in extant theory, and draws from consumer expectations for organizational information privacy communication. However, it was not possible to draw insights from extant information privacy communications that actually communicate organizational information privacy communications in a substantive way. In addition, it was not possible to test the developed information systems design theory within the scope of this thesis. As illustrated by the debate about the information privacy paradox (eg, Hallam and Zanella 2017, Hoffmann et al. 2016, Pentina et al. 2016), experimental findings in the information privacy domain are usually not confirmed in real-world settings. Reliable tests of the TIPP theory would thus require studies of real organizations with real consumer information systems and real consumers with real tasks and real problems (Sun and Kantor 2006). Although not impossible in general, such test of the TIPP theory was unrealistic within the scope of this thesis for several reasons. First, a consumer information system with information privacy practices of some complexity would be required because most consumers would not be interested in communication of organizational information privacy practices in case of trivial organizational information privacy practices. Second, communication of organizational information privacy practices is not cheap. Extensive resources would be required—for example, to pay the individuals required to elicit the necessary information on organizational information privacy practices, to keep track of organizational information privacy practices over the course of the study, to ensure that intended information privacy practices correspond with actual information privacy practices so that study participants are not deceived, and to develop user interfaces for the communication channels desired by consumers. Third, a longitudinal study would be required to track how changes of organizational information privacy practices and of organizational information communication impact consumer information privacy perceptions and to capture consumers with diverse tasks and problems that evoke information privacy information needs. This thesis is focused on developing the fundamental knowledge required for testing the TIPP theory and establishes prescient, nomothetic design knowledge on communication of organizational information privacy practices in consumer information systems. The theoretical assertions made are substantiated through grounding in extant knowledge in research and practice.

1.6.2 Potential for Future Research

Promising avenues for future research include the extension of the RECIPE ontology with domain specific ontologies, for example, with extant ontologies in the health care domain (Blobel 2011). Gold standards could be developed for what information must be communicated by what types of consumer information systems in which domains to ease instantiation of organizational information privacy communications. Furthermore, the TIPP theory could be tested and extended in different contexts. Research cooperation with organizations already attempting to communicate organizational information privacy practices in a substantive way seems promising. The TIPP theory represents a general conceptualization of a design space for substantive communication of organizational information privacy practices. Future research could explore different approaches for implementing TIPP instantiations, for example, leveraging ontology visualization methods (Katifori et al. 2007) or natural language interfaces (Kaufmann and Bernstein 2007). It would also be interesting to investigate how consumer archetypes with respect to information privacy are formed and whether consumers exhibit traits of different consumer archetypes in different contexts. Distributions of consumers across consumer archetypes could, for example, be linked to characteristics of organizations operating consumer information systems, tasks performed with consumer information systems, information collected by consumer information systems, handling of information collected by consumer information systems, situations in which consumer information systems are used, or traits of consumers (eg, personality traits, technology literacy, or cultural traits). An in-depth understanding of when and why consumers switch between consumer archetypes would go a long way in crafting organizational information privacy practices that align with consumer preferences and in designing situated artifacts for communication of organizational information privacy practices that provide consumers with the information they desire in an intuitive way.

1.6.3 Theoretical Implications

This thesis contributes to the scientific knowledge base in multiple ways. First, I propose a view on information privacy (chapter 1.2.2) that is tailored to the context of organizational information privacy communication, accounts for the global nature of consumer information systems, their complexity, and the conflicting objectives of consumers and organizations. Extant research has developed diverse conceptualizations of information privacy and there is neither a working approach to consolidate extant conceptualizations nor consensus how to conceptualize information privacy in consumer information systems (Mulligan et al. 2016, Solove 2002). Information privacy as a vertical communication relationship between organizations and consumers is a parsimonious view on information privacy that boils the complexity inherent to information privacy down to the essentials for organizational information privacy communication: an entity with information privacy practices, an entity with information privacy perceptions, and their communication relationship.

Second, I propose to view information security as the driving force of the relationship between information security and information privacy (chapter 1.2.3). In research and practice, the relationship between information security and information privacy is often treated as intuitive and not carefully delineated. Acknowledgement that the relationship is impacted by information security measures in the domain of the organization, in the domain of the consumer, and at the communication channel allows to pay more mindful attention to interdependencies of information security and information privacy. Up to a certain degree, implementation of information security practices reinforces information privacy by either making organizational information privacy practices more desirable to consumers or by enabling consumers to protect themselves from undesirable organizational information privacy practices. However, there will always be a turning point where implementation of additional information security practices will debilitate information privacy. Information systems design in research and practice has to focus on achieving either one or the other or has to account for the inevitable tradeoffs between information security and information privacy.

Third, I developed the Simplified Model of Organizational Information Privacy Communication (PUB4) as an abstract view on organizational information privacy communication in consumer information systems. The Simplified Model of Organizational Information Privacy Communication illustrates the central challenges inherent to communication of organizational information privacy practices. Consumers' information privacy information needs are diverse (PUB6) and would best be satisfied with individualized responses. Yet, it is practically unfeasible for organizations to satisfy each information request individually due to the number of consumers served by consumer information systems so that organizations have to fall back to predefined responses to future information requests. In other words, due to the absence of feasible alternatives, organizational information privacy communication poses the predicament of having to provide upfront answers to unknown and diverse questions.

Fourth, the TIPP theory (PUB5) introduces a conceptualization of transparency of organizational information privacy practices. Prior literature has developed unspecific instruments to assess transparency (eg, Oulasvirta et al. 2014) and its importance (eg, Awad and Krishnan 2006, Dinev et al. 2013) in quantitative studies or has relied on the intuitiveness of the concept (eg, Fischer-Hübner et al. 2014, Horvitz and Mulligan 2015). Transparency of organizational information privacy practices is not concerned with arbitrary information practices or normative claims regarding fair information practices. Instead, substantive communication of organizational information privacy practices must provide consumers with the information they desire in an intuitive way.

Fifth, I introduce the information privacy communication continuum (PUB5) as a new lens for information privacy research. The information privacy communication continuum illustrates a range of opportunities for organizational information privacy communication that lies between general approaches considered in public policy and legal discourse and technical solutions from the computer science domain. Although the endpoints are well studied, the intermediate area of this range remains largely unexplored. Instead of a focus on approaches that regulators and the market have introduced thus far or that rely predominantly on technical solutions, the information privacy communication continuum motivates investigation of new approaches.

Sixth, I propose the Information Privacy Communication Circle (PUB6) as a more effective system for development of organizational information privacy communications than extant approaches predominantly driven by privacy legislation. The Information Privacy Communication Circle is not intended to replace traditional, privacy legislation–driven approaches for development of organizational information privacy communication. It rather constitutes a refined lens on organizational information privacy communication that also accounts for the diversity of consumers' information privacy information needs. From this perspective, organizational information privacy communication is conceptualized as a circle rearranging itself on a spectrum between vicious and virtuous (Masuch 1985). The circle represents consumer information systems with three components relevant within the context of organizational information privacy communication—organizations, their information privacy communications, and consumer archetypes with diverse information privacy information needs. All components reciprocally interact with each other. Organizational information privacy communication will be least effective if the information privacy information needs of only one consumer archetype are satisfied. Introduction of additional information privacy communications will satisfy the information privacy information needs of more consumer archetypes and increase the effectiveness of organizational information privacy communication until the information privacy information needs of all relevant consumer archetypes are satisfied. Conversely, changes in organizational information privacy practices may render current organizational information privacy communications inadequate for some consumer archetypes and organizational information privacy communication will become less effective.

Finally, the TIPP theory (PUB5) conceptualizes a design space for substantive organizational information privacy communication in form of an information systems design theory for transparency of organizational information privacy practices. Substantive organizational information privacy communication must balance offering access to a comprehensive selection of information and avoiding cognitive overload by focusing on topical relevance and interactivity. Related research concerned with organizational information privacy communication is mostly focused on building and evaluating individual tools that address specific threats, for example, blocking tools or opt-out tools or on testing and critiquing extant tools, for example, the effectiveness of privacy notices or seals (Cranor 2012). The TIPP theory takes a step back and contributes to the scientific knowledge base by first establishing more general design knowledge on what to build for substantive communication of organizational information privacy practices. The contested and complex nature of information privacy (Mulligan et al. 2016, Solove 2002) makes it unlikely that organizations can satisfy consumers’ information privacy needs with a universally applicable solution. The TIPP theory addresses this problem by proposing a flexible, adaptive approach to organizational information privacy communication.

1.6.4 Implications for Practice

With respect to public policy and practical audiences this thesis reveals multiple insights. First, the investigation of information security and information privacy requirements for PHS and of the German HTI (PUB1), illustrates that maintenance of information security and information privacy is a continuous process that needs to be reiterated in case of events such as changes to consumer information systems, identification of new vulnerabilities, or identification of malicious activity. In addition, there are no gold standards for maintaining information security and information privacy, which was also substantiated in the investigation of potential for harm through information security and information privacy violations in mHealth apps (PUB2). What measures need to be implemented depends on the characteristics of the respective consumer information system and its environment, which may already offer suitable protection measures that can be reused to leverage synergies and benefit from existing expertise.

Second, the twelve mHealth app archetypes identified in the investigation of potential for harm in mHealth apps (PUB2), elucidate information security and information privacy challenges. The archetypes are useful to guide public policy aiming to prioritize information security and information privacy requirements for distinct types of consumer information systems and to develop collections of information security and information privacy measures suitable to establish base line levels of protection. For developers, the archetypes are useful to understand information security and information privacy implications of consumer information systems and to guide application designs that are feasible to maintain information security and information privacy. Finally, the archetypes can be employed by consumers to assess and understand information security and information privacy implications of consumer information systems or can be integrated into artifacts aiming to make consumers more knowledgeable about information security and information privacy (eg, Brüggemann et al. 2016).

Third, the mHealth app analysis revealed that only a quarter of the large number of mHealth apps are in more or less widespread use (PUB2). In such convoluted and competitive markets, substantive communication of organizational information privacy practices may be an especially promising lever to increase visibility and attractiveness of consumer information systems. The assertion that there is a market potential for substantive organizational information privacy communications is supported by the investigation of mHealth app privacy notices (PUB3), which revealed that even organizations offering popular mHealth apps do not communicate organizational information privacy practices in a useful way. In addition, the survey of consumers' information privacy information needs (PUB6) revealed that consumers do want to be informed about organizational information privacy practices. Accordingly, there is demand for substantive organizational information privacy communication but no supply.

Fourth, I developed the RECIPE ontology (PUB4) as a metaspecification of a comprehensive selection of organizational information privacy practices that are topically relevant for organizational information privacy communication. The RECIPE ontology can serve organizations and public debate as a starting point to understand what information must be contained in organizational information privacy communication and how to satisfy corresponding information requests issued by consumers with predefined responses. The RECIPE ontology constitutes a metaspecification for the content of predefined organizational responses to information requests issued by consumers without imposing restrictions on aspects like message formatting, message redundancy, means for communication available, the number of messages required to convey the response, or actual manifestations of organizational information privacy practices.

Fifth, the analysis of consumers' information privacy information needs (PUB6) revealed nine distinct consumer archetypes with diverse information privacy information needs that organizational information privacy communication must cater to. The identified consumer archetypes can be employed by organizations and public policy makers to better understand the information privacy information needs of the consumers they are serving. The identified archetypes could also be used to develop an evaluation framework for the suitability and effectiveness of information system components designed to support substantive communication of organizational information privacy practices.

Finally, the TIPP theory (PUB5) offers insights that bring common organizational practices, such as posting privacy notices and privacy seals, into question. Neither privacy notices nor privacy seals seem suitable for substantive communication of organizational information privacy practices. Indeed, privacy seals (eg, TRUSTe; Benassi 1999) convey only limited information and are static. In empirical reality, privacy notices are often not comprehensive, are bloated with irrelevant legal boilerplate (Milne and Culnan 2004), and remain static text documents that cannot adapt to consumers' information privacy information needs. New approaches must be developed for making substantive communication of organizational information privacy practices a reality. The TIPP theory can be used to clearly communicate organizational information practices. This would allow organizations to differentiate themselves from competitors by implementing more consumer-friendly information privacy practices. Today, organizational information privacy practices remain largely opaque to consumers. This thesis presents nomothetic design knowledge to change this situation and to transform information privacy practices into a tangible quality attribute of organizations by fostering holistic attention to information privacy practices, stimulating internalization of information privacy, and allowing for enough flexibility to account for contextual influences (Wijen 2014).

1.6.5 Conclusion

The evolution of normative information privacy standards over the past decades fell short in promoting organizational information privacy communication capable to satisfy consumers' information privacy information needs. As a result, organizations and consumers are prohibited from leveraging the full potential of consumer information systems due to impediments in recognizing the right consumer information systems for tasks they want to perform, occurrence of defensive consumer practices, and consumer or regulator backlash once undesirable organizational information privacy practices come to light (Choi et al. 2016). The research conducted in this cumulative thesis contributes to closing the gap between the normative and the empirical information privacy world by substantiating the utility of organizational information privacy communication, demonstrating the inadequacy of extant approaches to organizational information privacy communication, revealing the diversity of consumers' information privacy information needs, and proposing a design space for substantive communication of organizational information privacy practices in consumer information systems. Complementing normative guidance for organizational information privacy communication with a thorough understanding of consumers' information privacy information needs and an information systems design theory for substantive communication of organizational information privacy practices may just be the missing impulse for the emergence of truly useful and substantive communication of organizational information privacy practices.

1.7 References

Abiteboul S, André B, Kaplan D (2015) Managing Your Digital Life. Communications of the ACM 58(5):32–35.

Ackerman MS, Cranor LF, Reagle J (1999) Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. 1st ACM Conference on Electronic Commerce. (ACM, Denver, CO, USA), 1–8.

Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and Human Behavior in the Age of Information. Science 347(6221):509–514.

Antón AI, Earp JB, Young JD (2010) How Internet Users' Privacy Concerns Have Evolved Since 2002. IEEE Security & Privacy 8(1):21–27.

Awad NF, Krishnan M (2006) The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. MIS Quarterly 30(1):13–28.

Bal G, Rannenberg K, Hong JI (2015) Styx: Privacy Risk Communication for the Android Smartphone Platform Based on Apps' Data-Access Behavior Patterns. Computers & Security 53(1):187–202.

Balebako R, Jung J, Lu W, Cranor LF, Nguyen C (2013) "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. Proceedings of the Ninth Symposium on Usable Privacy and Security. SOUPS '13. (ACM, New York, NY, USA), 12:1–12:11.

Baraniuk RG (2011) More Is Less: Signal Processing and the Data Deluge. Science 331(6018):717–719.

Baskerville RL, Kaul M, Storey VC (2015) Genres of Inquiry in Design-Science Research: Justification and Evaluation of Knowledge Production. MIS Quarterly 39(3):541–564.

Bélanger F, Crossler RE (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly 35(4):1017–1041.

Bélanger F, Crossler RE, Hiller JS, Park JM, Hsiao MS (2013) POCKET: A Tool for Protecting Children's Privacy Online. Decision Support Systems 54(2):1161–1173.

Benassi P (1999) TRUSTe: An Online Privacy Seal Program. Communications of the ACM 42(2):56–59.

Berger CR, Calabrese RJ (1975) Some Explorations in Initial Interaction and Beyond: Toward a Developmental Theory of Interpersonal Communication. Human Communication Research 1(2):99–112.

Blobel B (2011) Ontology Driven Health Information Systems Architectures Enable pHealth for Empowered Patients. International Journal of Medical Informatics 80(2):e17–e25.

Blondel VD, Guillaume JL, Lambiotte R, Lefebvre E (2008) Fast Unfolding of Communities in Large Networks. Journal of Statistical Mechanics: Theory and Experiment 2008(10):P10008.

Brüggemann T, Hansen J, Dehling T, Sunyaev A (2016) An Information Privacy Risk Index for mHealth Apps. Schiffner S, Serna J, Ikonomou D, Rannenberg K, eds. Proceedings of the 4th Annual Privacy Forum. (Springer International Publishing, Frankfurt (Main), Germany), 190–201.

Buitelaar JC (2017) Post-Mortem Privacy and Informational Self-Determination. Ethics and Information Technology 19(2):129–142.

Campbell JL (2007) Why Would Corporations Behave in Socially Responsible Ways? An Institutional Theory of Corporate Social Responsibility. Academy of Management Review 32(3):946–967.

Chen W, Hirschheim R (2004) A Paradigmatic and Methodological Examination of Information Systems Research from 1991 to 2001. Information Systems Journal 14(3):197–235.

Choi BCF, Kim SS, Jiang ZJ (2016) Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior. Journal of Management Information Systems 33(3):904–933.

Clarke R (1999) Internet Privacy Concerns Confirm the Case for Intervention. Communications of the ACM 42(2):60–67.

Corley KG, Gioia DA (2011) Building Theory about Theory Building: What Constitutes a Theoretical Contribution? Academy of Management Review 36(1):12–32.

Cranor L, Dobbs B, Egelman S, Hogben G, Humphrey J, Langheinrich M, Marchiori M, et al. (2006) The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. Retrieved (March 3, 2017), http://www.w3.org/TR/2006/NOTE-P3P11-20061113.

Cranor LF (2012) Necessary but not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. Journal on Telecommunications and High Technology Law 10:273–307.

Culnan MJ, Williams CC (2009) How Ethics can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches. MIS Quarterly 33(4):673–687.

DeCew JW (2004) Privacy and Policy for Genetic Research. Ethics and Information Technology 6(1):5–14.

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

Dinev T, Xu H, Smith JH, Hart P (2013) Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts. European Journal of Information Systems 22(3):295–316.

Dubin R (1978) Theory Building (Collier Macmillan Publishers, London, UK).

Earp JB, Antón AI, Aiman-Smith L, Stufflebeam WH (2005) Examining Internet Privacy Policies Within the Context of User Privacy Values. IEEE Transactions on Engineering Management 52(2):227–237.

Fischer-Hübner S, Angulo J, Pulls T (2014) How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used? Hansen M, Hoepman JH, Leenes R, Whitehouse D, eds. Privacy and Identity Management for Emerging Services and Technologies. (Springer Berlin Heidelberg), 77–92.

Fu K, Blum J (2013) Controlling for Cybersecurity Risks of Medical Device Software. Communications of the ACM 56(10):35–37.

Garrison L, Hastak M, Hogarth JM, Kleimann S, Levy AS (2012) Designing Evidence-Based Disclosures: A Case Study of Financial Privacy Notices. Journal of Consumer Affairs 46(2):204–234.

Germonprez M, Hovorka D, Collopy F (2007) A Theory of Tailorable Technology Design. Journal of the Association for Information Systems 8(6):351–367.

Greenaway KE, Chan YE, Crossler RE (2015) Company Information Privacy Orientation: A Conceptual Framework. Information Systems Journal 25(6):579–606.

Gregor S, Jones D (2007) The Anatomy of a Design Theory. Journal of the Association for Information Systems 8(5):312–335.

Gürses S (2014) Can You Engineer Privacy? Communications of the ACM 57(8):20–23.

Hallam C, Zanella G (2017) Online Self-Disclosure: The Privacy Paradox Explained as a Temporally Discounted Balance Between Concerns and Rewards. Computers in Human Behavior 68:217–227.

Hoffmann CP, Lutz C, Ranzini G (2016) Privacy Cynicism: A New Approach to the Privacy Paradox. Cyberpsychology: Journal of Psychosocial Research on Cyberspace 10(4).

Horvitz E, Mulligan D (2015) Data, Privacy, and the Greater Good. Science 349(6245):253–255.

ISO (2016) ISO/IEC 27000:2016: Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

Jensen C, Potts C (2004) Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. (ACM, New York, NY, USA), 471–478.

Kalyuga S (2011) Cognitive Load Theory: How Many Types of Load Does It Really Need? Educational Psychology Review 23(1):1–19.

Katifori A, Halatsis C, Lepouras G, Vassilakis C, Giannopoulou E (2007) Ontology Visualization Methods—A Survey. ACM Computing Surveys 39(4):10:1-10:43.

Kaufmann E, Bernstein A (2007) How Useful Are Natural Language Interfaces to the Semantic Web for Casual End-Users? Aberer K, Choi KS, Noy N, Allemang D, Lee KI, Nixon L, Golbeck J, et al., eds. The Semantic Web. Lecture Notes in Computer Science. (Springer Berlin Heidelberg), 281–294.

Krol K, Preibusch S (2015) Effortless Privacy Negotiations. IEEE Security & Privacy 13(3):88–91.

Landau S (2015) Control Use of Data to Protect Privacy. Science 347(6221):504–506.

Landry JP, Pardue JH, Johnsten T, Campbell M, Patidar P (2011) A Threat Tree for Health Information Security and Privacy. Sambamurthy V, Tanniru M, eds. Proceedings of the 17th Americas Conference on Information Systems. (AIS, Detroit, MI, USA).

Laudon KC (1996) Markets and Privacy. Communications of the ACM 39(9):92–104.

Laufer RS, Wolfe M (1977) Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues 33(3):22–42.

Li C, Li DY, Miklau G, Suciu D (2014) A Theory of Pricing Private Data. ACM Transactions on Database Systems 39(4):34:1-34:28.

Li Y (2012) Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework. Decision Support Systems 54(1):471–481.

Masuch M (1985) Vicious Circles in Organizations. Administrative Science Quarterly 30(1):14–33.

McDonald AM, Cranor LF (2008) The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 4(3):540–565.

Milne GR, Culnan MJ (2002) Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys. Information Society 18(5):345–359.

Milne GR, Culnan MJ (2004) Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don’t Read) Online Privacy Notices. Journal of Interactive Marketing 18(3):15–29.

Miltgen CL, Peyrat-Guillard D (2014) Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries. European Journal of Information Systems 23(2):103–125.

Miyazaki AD, Krishnamurthy S (2002) Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. Journal of Consumer Affairs 36(1):28–49.

Mueller B, Urbach N (2017) Understanding the Why, What, and How of Theories in IS Research. Communications of AIS forthcoming.

Mulligan DK, Koopman C, Doty N (2016) Privacy is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy. Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 374(2083):1–17.

Nissenbaum H (2004) Privacy as Contextual Integrity. Washington Law Review 79:119–157.

Nissenbaum H (2009) Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press, Stanford, CA, USA).

Oetzel MC, Spiekermann S (2014) A Systematic Methodology for Privacy Impact Assessments: A Design Science Approach. European Journal of Information Systems 23(2):126–150.

Oliver C (1991) Strategic Responses to Institutional Processes. Academy of Management Review 16(1):145–179.

Oulasvirta A, Suomalainen T, Hamari J, Lampinen A, Karvonen K (2014) Transparency of Intentions Decreases Privacy Concerns in Ubiquitous Surveillance. Cyberpsychology, Behavior, and Social Networking 17(10):633–638.

Park YJ (2013) Digital Literacy and Privacy Behavior Online. Communication Research 40(2):215–236.

Pavlou PA, Liang H, Xue Y (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. MIS Quarterly 31(1):105–136.

Pentina I, Zhang L, Bata H, Chen Y (2016) Exploring Privacy Paradox in Information-Sensitive Mobile App Adoption: A Cross-Cultural Comparison. Computers in Human Behavior 65:409–419.

Petronio S (1991) Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples. Communication Theory 1(4):311–335.

Pollach I (2006) Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions. Journal of Organizational and End User Computing 18(1):23–49.

Rindfleisch TC (1997) Privacy, Information Technology, and Health Care. Communications of the ACM 40(8):92–100.

Romanosky S (2016) Examining the Costs and Causes of Cyber Incidents. Journal of Cybersecurity 2(1):121–135.

Rouse WB, Rouse SH (1984) Human Information Seeking and Design of Information Systems. Information Processing & Management 20(1):129–138.

Sæther B (1998) Retroduction: An Alternative Research Strategy? Business Strategy and the Environment 7(4):245–249.

Schatz BR, Hardin JB (1994) NCSA Mosaic and the World Wide Web: Global Hypermedia Protocols for the Internet. Science 265(5174):895–901.

Schwaig KS, Kane GC, Storey VC (2005) Privacy, Fair Information Practices and the Fortune 500: The Virtual Reality of Compliance. SIGMIS Database 36(1):49–63.

Shahri AB, Ismail Z (2012) A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS. Journal of Information Security 3(2):169–176.

Simon HA (1996) The Sciences of the Artificial 3rd ed. (MIT Press, Cambridge, MA, USA).

Slamanig D, Stingl C (2008) Privacy Aspects of eHealth. 3rd International Conference on Availability, Reliability and Security. ARES'08. (IEEE, Washington, DC, USA), 1226–1233.

Smith B (2004) Beyond Concepts: Ontology as Reality Representation. Proceedings of the International Conference on Formal Ontology and Information Systems. (IOS Press, Turin, Italy), 73–84.

Smith HJ, Dinev T, Xu H (2011) Information Privacy Research: An Interdisciplinary Review. MIS Quarterly 35(4):989–1015.

Solove DJ (2002) Conceptualizing Privacy. California Law Review 90(4):1087–1155.

Soria-Comas J, Domingo-Ferrer J, Sánchez D, Megías D (2017) Individual Differential Privacy: A Utility-Preserving Formulation of Differential Privacy Guarantees. IEEE Transactions on Information Forensics and Security 12(6):1418–1429.

Spiekermann S, Cranor LF (2009) Engineering Privacy. IEEE Transactions on Software Engineering 35(1):67–82.

Stoycheff E (2016) Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. Journalism & Mass Communication Quarterly 93(2):296–311.

Sun Y, Kantor PB (2006) Cross-Evaluation: A New Model for Information System Evaluation. Journal of the American Society for Information Science and Technology 57(5):614–628.

Sunyaev A, Dehling T, Taylor PL, Mandl KD (2015) Availability and Quality of Mobile Health App Privacy Policies. Journal of the American Medical Informatics Association 22(e1):e28–e33.

Sweller J (1988) Cognitive Load During Problem Solving: Effects on Learning. Cognitive Science 12(2):257–285.

Tavani HT (2007) Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy. Metaphilosophy 38(1):1–22.

Tsai JY, Egelman S, Cranor L, Acquisti A (2011) The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Information Systems Research 22(2):254–268.

Venable J (2006) A Framework for Design Science Research Activities. Khosrow-Pour M, ed. Proceedings of the Information Resources Management Association International Conference. (Idea Group Publishing, Washington, DC, USA), 184–187.

Venkatesh V, Brown SA, Bala H (2013) Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. MIS Quarterly 37(1):21–54.

Venkatesh V, Brown SA, Sullivan YW (2016) Guidelines for Conducting Mixed-Methods Research: An Extension and Illustration. Journal of the Association for Information Systems 17(7):2.

Vuorinen J, Tetri P (2012) The Order Machine-The Ontology of Information Security. Journal of the Association for Information Systems 13(9):695–713.

Ward JH (1963) Hierarchical Grouping to Optimize an Objective Function. Journal of the American Statistical Association 58(301):236–244.

Warren SD, Brandeis LD (1890) The Right to Privacy. Harvard Law Review 4(5):193–220.

Westin A (1967) Privacy and Freedom (Ig Publishing, New York, NY, USA).

Whitman ME (2003) Enemy at the Gate: Threats to Information Security. Communications of the ACM 46(8):91–95.

Wijen F (2014) Means versus Ends in Opaque Institutional Fields: Trading off Compliance and Achievement in Sustainability Standard Adoption. Academy of Management Review 39(3):302–323.

Xu H, Crossler RE, Bélanger F (2012) A Value Sensitive Design Investigation of Privacy Enhancing Tools in Web Browsers. Decision Support Systems 54(1):424–433.

Xu H, Teo HH, Tan BCY, Agarwal R (2012) Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. Information Systems Research 23(4):1342–1363.

Zhang L, Gupta D, Mohapatra P (2012) How Expensive are Free Smartphone Apps? SIGMOBILE Mobile Computing and Communications Review 16(3):21–32.

2 Secure Provision of Patient-Centered Health Information Technology Services in Public Networks—Leveraging Security and Privacy Features Provided by the German Nationwide Health Information Technology Infrastructure

Authors: Tobias Dehling, Ali Sunyaev

Abstract: Patient-centered health information technology services (PHS) provide personalized electronic health services to patients. Since provision of PHS entails handling sensitive medical information, a special focus on information security and privacy aspects is required. We present information security and privacy requirements for PHS and examine how security features of large-scale, inter-organizational health information technology networks, like the German health information technology infrastructure (HTI), can be used for ensuring information security and privacy of PHS. Moreover, we illustrate additional security measures that complement the HTI security measures and introduce a guideline for provision of PHS while ensuring information security and privacy. Our elaborations lead to the conclusion that security features of health information technology networks can be used to create a solid foundation for protecting information security and privacy in patient-centered health information technology services offered in public networks like the internet.

Keywords: Health information technology, Security, Privacy, Patient-centered, eHealth, Infrastructure

2.1 Introduction to PHS and Health IT Networks

The introduction of a nationwide health information technology infrastructure (HTI) in Germany is one of the largest eHealth/health information technology (IT) projects in the world. Similar to other international initiatives like HIPAA/HITECH in the US (Delgado 2011) or the Japanese Community Medicine Recovery Plan (Abraham et al. 2011), the project tries to leverage benefits of large-scale health IT networks to improve quality and save cost in healthcare. Nationwide access via public networks to patient identifiers and security services offered by the HTI can create a solid foundation for the provision of patient-centered health IT services (PHS), which can be defined as follows: PHS are scalable information systems that leverage information technology to support patients in managing and becoming knowledgeable on their own health; PHS are designed to fulfill patients' needs, do not have to incorporate requirements of care providers, and can be provided by anyone who can finance the required resources.

The concept of PHS is similar to patient-facing health IT services (Ahern et al. 2011), which also include clinical and inpatient health IT services incorporating requirements of medical professionals or institutions. In contrast to patient-facing health IT services, PHS solely target needs/requirements of patients. Thus, patients always have data sovereignty and further parties like care providers or researchers are only involved if desired by patients. Basically, PHS can provide any functionality patients find useful, like management of health-related information in a personal health record (Blechman et al. 2012), support for self-management of chronic diseases (Sunyaev and Chornyi 2012), or provision of information on pharmaceuticals a patient is taking (Dehling and Sunyaev 2012b, 2013). Cloud computing presents itself as promising deployment type for PHS (Fan et al. 2011, Zhang and Liu 2010). Characteristics of cloud computing like broad network access, on-demand resource access, and rapid elasticity (Mell and Grance 2011) facilitate the provision of PHS, which need to be easily accessible and available whenever necessary. Besides the standardized access over TCP/IP, further standardized internet technologies allow for interoperability so that synergies of complementary services can be leveraged (Ekonomou et al. 2011, Sunyaev and Chornyi 2012). Moreover, cloud computing suits PHS even literally since the term 'patient-centered health IT services' unites the patient-focus of patient-centered eHealth (Wilson 2009) with the cloud computing paradigm of offering "ubiquitous, convenient, on-demand network access to a shared pool of configurable resources" (Mell and Grance 2011, p. 2) as a service. Obtaining, substituting, and combining services in the style of mobile phone platforms (Mandl et al. 2012) or the Unix tools philosophy (Raymond 2003) lets users choose preferred services, reduces development effort, and the increased focus of individual services eases handling and control of information security and privacy aspects.

Pagliari (2007) pointed out the increasing breadth and complexity of health IT. Stakeholders alone expanded from technical experts and managers to an assemblage containing health system managers, IT experts, healthcare organizations, medical researchers, health professionals, support staff, policy makers, system vendors, patients, the general public, and mass media (Pagliari 2007). With the increasing availability of PHS in form of mHealth and mHealth applications (apps) (d'Heureuse et al. 2012, Istepanian et al. 2004) further stakeholders like amateur developers or advertisement networks become involved. On the large app markets of Apple (itunes.apple.com) and Google (play.google.com) everyone can deploy and distribute mHealth apps. Many amateur developers develop and publish their own apps to, for instance, address a problem they encountered, alleviate management of their disease, kill some time, or just to make a quick buck. Therefore, at least some developers might only marginally consider information security and privacy aspects since they lack the required resources and focus more on functional aspects. In addition, many apps are financed through advertisements (Zhang et al. 2012) which introduces new privacy challenges for shared information. Focusing on PHS reduces the number of stakeholders to the patient (the user), the service provider, and third parties that might have access to shared patient information. Patients can use any PHS as long as they deem it beneficial and believe that the service provider offers sufficient protection for shared information. Sharing of patient information with third parties might be in the interest of patients (eg, integration with other PHS, access for treating medical professionals) but might also be undesired by patients (eg, sharing with advertisement networks or insurance companies).

While PHS are diverse in terms of offered functionality, implementation, and targeted users, a common and constant trait is the handling of private, sensitive medical information that needs to be protected (Rindfleisch 1997). PHS that control aspects of patients' health, like personal health records, obviously store and create sensitive information. However, even if PHS do not explicitly access personal, medical information of users, sole observation of users' behavior can lead to privacy infractions (Slamanig and Stingl 2008). Characteristics of cloud computing like multitenancy (ie, deployment of service instances of different organizations on the same physical host) introduce new information security and privacy challenges that need to be addressed (Garber 2012, Song et al. 2012, Subashini and Kavitha 2011, Yau and An 2011). Patients deem access to health information and related services beneficial, but they are concerned with information security and privacy issues and want to control access to their information (Pyper et al. 2004, Simon et al. 2009). Overcoming the information security and privacy challenges, which impede patients' willingness to share personal health information (Bélanger and Crossler 2011), could serve as enabler for new services and business models that improve the quality of healthcare with round-the-clock access to personalized health IT offerings.

In this paper, we aim to illustrate the potential of leveraging security features of preexisting health information technology networks, like the German HTI, with innovative services to cater the rising demands of patients who want to access health information and services as conveniently as they are used to when doing their banking or vacation planning (Forkner-Dunn 2003). A wide-spread, established, and solid foundation of security measures for the provision of PHS would be advantageous since, for example, PHS providers would not have to implement all required measures on their own and do not have to develop and manage the required expertise. For patients, use of a common foundation is also more trustworthy and tangible in contrast to an individual solution of every service provider. Furthermore, a common foundation leads to synergies: All clients could, for instance, benefit from tests and improvements of the centralized components and functionality offered by the centralized components can be implemented and maintained by specialized experts. Furthermore, research and insights from various fields are consolidated and orchestrated for the provision of PHS via public networks while ensuring information security and privacy. Therefore, we want to answer the following research question: "How can large-scale health information technology networks like the German HTI be used to enforce information security and privacy of PHS?"

We address the research question by answering the following ancillary research questions:

RQ1*: What are information security and privacy requirements of PHS?*

RQ2*: Which information security and privacy requirements of PHS can be fulfilled with security measures provided by the German HTI?*

RQ3*: Can the requirements not fulfilled by security measures of the German HTI be fulfilled with additional measures ensuring information security and privacy?*

2.2 Related Work

Research on information security and privacy in the domain of health IT can be categorized in four primary areas: healthcare providers, inter-organizational, public policy, and healthcare consumers (Appari and Johnson 2010). The domain names alone insinuate that health IT research focuses to a large degree on needs of medical professionals, administrations, and healthcare organizations. Patient-centered eHealth that focuses on the needs of patients, facilitates patient participation, and contributes to patient empowerment (Wilson 2009) receives less attention. Although design science research in information privacy yields research and practical implications, this research area was only sparsely focused in the past (Bélanger and Crossler 2011). Patient-centered eHealth as a dedicated research focus is motivated by the increasing diversification of health IT and the rising demand of patients for tailored, easy-to-use healthcare web applications (Ahern et al. 2011, Forkner-Dunn 2003, Wilson 2009). Personal health records (PHR), which enable patients to store medical information while maintaining data sovereignty, represent a type of PHS that received exceptionally much attention and has been investigated from various perspectives (eg, Blechman et al. 2012, Kaletsch and Sunyaev 2011, Ozdemir et al. 2011, Sunyaev, Chornyi, et al. 2010).

Extant research on information security and privacy of PHS concentrates mostly on individual technologies and security aspects (eg, Chan et al. 2001) or introduces specialized architectures and applications (eg, Calvillo et al. 2013). Broader applicable research is scarce in the literature, especially such that builds on security features of existing networks. Yet, such research is useful to enhance the understanding of PHS and can facilitate the fulfillment of the rising demand for PHS (Forkner-Dunn 2003, Wilson 2009) while maintaining information security and privacy.

2.3 Methods

To derive information security and privacy requirements of PHS, we look at extant research focusing on security requirements of cloud or health IT services published in journals and conferences focusing on information systems, computer science, or medical informatics, which are likely to yield results and insights germane to the development and design of PHS (in the following, we refer to ‘information security and privacy requirements’ with the shorter term ‘security requirements’). Subsequently, three researchers independently read identified articles that examine security requirements of cloud or health IT services, record and categorize therein proposed security requirements, and assess these for relevancy. Afterwards, the independent results are consolidated in a group discussion.

Thereafter, according to HTI specifications and further information provided by the gematik – the association responsible for the HTI (see www.gematik.de for more information), we study the establishment process and architecture design of the HTI. This enables us to identify security requirements that can (at least partially) be fulfilled with security services and measures provided by the HTI. In order to address the security requirements not covered by the HTI, we illustrate potential security measures that complement the security services and measures offered by the HTI. Finally, we consolidate our answers to RQ 1-3 in a guideline for the provision of PHS in public networks while ensuring information security and privacy. Besides summarizing our results, the guideline can serve as foundation for future work and as introduction to the secure provision of PHS in public networks.

2.4 Security Requirements of PHS

PHS face threats ranging from intentional/unintentional disclosure or manipulation of information through insiders or outsiders over user errors, maintenance errors, software failures, or hardware failures to environmental threats (Landry et al. 2011, Shahri and Ismail 2012). The following examples illustrate potential damage of PHS use: PHS can have access to information with low sensitivity like users' height, weight, or common past illnesses and treatments like a cough or broken bones (Rindfleisch 1997, Rohm and Milne 2004). On the other hand, PHS can have access to information with high sensitivity like abortions, mental illness, sexually transmitted diseases, HIV status, substance abuse, or genetic predispositions to disease (Johnson 2009, Rindfleisch 1997, Rohm and Milne 2004). Leaks of such information can cause potential damage to users through socio-economic repercussions (Appari and Johnson 2010), embarrassment or damage of reputation (Appelbaum 2002, Gritzalis 1998, Johnson 2009, Kotz 2011, Rindfleisch 1997, Rohm and Milne 2004), social stigma (Appelbaum 2002), loss of affection or respect of family members (Shea 1994), monetary repercussions through fraud or medical identity theft (Appari and Johnson 2010, Johnson 2009, Kotz 2011), more expensive insurance coverage or problems to obtain insurance coverage (Appelbaum 2002, Barrows and Clayton 1996, Rindfleisch 1997, Rohm and Milne 2004, Shea 1994), or lessened employment possibilities (Appelbaum 2002, Kotz 2011, Rindfleisch 1997, Rohm and Milne 2004, Shea 1994). Furthermore, information manipulation can cause harm to users because erroneous information might be added to their information due to medical fraud, medical identity theft or other threats (Johnson 2009, Kotz 2011); consequentially, treatment might be based on erroneous information, which could impact patients' quality of care, cause harm to health or death, or might impede later efforts to obtain medical, life, or disability insurance (Appari and Johnson 2010, Gritzalis 1998, Johnson 2009, Kotz 2011). Similarly, loss of information can lead to situations where important information required for patients' care is no longer available (Appelbaum 2002, Gritzalis 1998, Rindfleisch 1997). Information accessible by health IT can also be of value to third parties, which makes infringements of information security or privacy more likely because infringements are more rewarding to third parties. Information like insurance policy information, government identity numbers, date of birth, or social security numbers is for instance valuable to third parties if it can be used for medical identity theft (obtainment of medical services with a faked medical identity) or medical fraud (billing for treatments never rendered) (Johnson 2009, Kotz 2011, Rindfleisch 1997). Further abuses of other's personal medical information to satisfy greed include the selling of health information of celebrities (Rindfleisch 1997), better fitting of insurance policies to insurees' risks and selection of insurees (Barrows and Clayton 1996, Rindfleisch 1997, Rothstein and Talbott 2007), selection of healthy employees (Barrows and Clayton 1996, Kotz 2011, Rindfleisch 1997, Rothstein and Talbott 2007), or targeted marketing (Barrows and Clayton 1996, Rindfleisch 1997, Rohm and Milne 2004).

The six main security requirements and associated sub-requirements determined in our literature analysis (Dehling and Sunyaev 2014a) support developers and providers in dealing with PHS-specific threats: the CIA triad (*confidentiality*, *integrity*, and *availability*), *accountability*/*non-repudiation*, *perimeter definition*, and *usability*. ***Confidentiality*** entails that only authorized users can access information. This requires *transmission and storage security*, that is, protection of information during transmission and in storage, and proper *authorization* so that users can only access information they need to access (Barrows and Clayton 1996, van der Linden et al. 2009, Rindfleisch 1997, Slamanig and Stingl 2008, Subashini and Kavitha 2011, Zhang and Liu 2010). By implementing a *limited access right duration*, it must be ensured that unnecessary access rights are revoked (Wainer et al. 2008). It should not be possible to link users to their real identity (*anonymity*) and *unlinkability* demands that records cannot be linked through observation (Slamanig and Stingl 2008). *Non-disclosure* implies that users cannot be forced to reveal information they want to keep secret (Slamanig and Stingl 2008, Zhang and Liu 2010). ***Integrity*** requires that information is protected against unauthorized modification or deletion as well as irrevocable, accidental, and undesired changes by authorized users (Barrows and Clayton 1996, van der Linden et al. 2009, Rindfleisch 1997, Subashini and Kavitha 2011, Wainer et al. 2008, Zhang and Liu 2010). To ensure ***availability***, the system needs to be accessible and fully operational whenever a user requires access to the system so that stored information and services can be retrieved and used when needed. Accordingly, PHS need to be adaptable to changing performance needs (*scalability*) and have to offer *resilience* to software and hardware failures of individual components, which should not severely impact the performance of the whole PHS (Subashini and Kavitha 2011). Availability entails *up-to-datedness* so that updates are almost instantaneously disseminated to all affected users (van der Linden et al. 2009, Wainer et al. 2008). Furthermore, appropriate *backup* mechanisms are required so that information can be restored from redundant storage (Barrows and Clayton 1996, van der Linden et al. 2009, Subashini and Kavitha 2011, Wainer et al. 2008, Zhang and Liu 2010). To correct errors and inconsistencies that are detected after some time, *recoverability* is required so that it is possible to restore information to a previous state at any point in time (van der Linden et al. 2009, Rindfleisch 1997, Wainer et al. 2008). Furthermore, it must be possible to preserve information for *long storage times* because some health information may be relevant across a whole lifetime or even longer (van der Linden et al. 2009, Wainer et al. 2008).

The CIA triad is a generally accepted foundation for information security. For PHS, additional main security requirements need to be addressed. ***Accountability/non-repudiation*** ensures that users cannot deny actions and accesses of information. *Authentication* measures need to be implemented so that it can be verified that users are who they claim to be and communications remain between the intended senders and recipients (Barrows and Clayton 1996, van der Linden et al. 2009, Rindfleisch 1997, Slamanig and Stingl 2008, Subashini and Kavitha 2011, Zhang and Liu 2010). Moreover, *audit trails* must be used to monitor PHS activity, sound alarms if undesired activity is detected, and retrace user activity if necessary (Barrows and Clayton 1996, van der Linden et al. 2009, Rindfleisch 1997, Zhang and Liu 2010). Establishment of a ***perimeter definition*** demands that the physical and logical boundaries of the information system are known and controlled. Unauthorized access needs to be prevented and network access rights need to be managed (*network security*) and *physical hardware security* needs to be ensured so that theft and tampering with the hardware is prevented and effects of natural disasters are lessened (Barrows and Clayton 1996, Rindfleisch 1997, Subashini and Kavitha 2011). *System vulnerability analyses* should be conducted so that unknown vulnerabilities can be detected and fixed, and the PHS is protected from malware like viruses or trojans (Rindfleisch 1997, Subashini and Kavitha 2011). This should be complemented by *intrusion detection* so that information security or privacy compromises are detected and can be countered (Barrows and Clayton 1996, Subashini and Kavitha 2011). Last but not least ***usability*** is important for information security and privacy because important information needs to be easily accessible and security measures should not severely impede PHS use. *Emergency access* requires that vital information is accessible without patient consultation in case of an emergency (Wainer et al. 2008). If credentials are lost, compromised, or need to be replaced for another reason, *credential substitutability* warrants that credentials (eg, smart cards, keys, or passwords) can be replaced (Wainer et al. 2008, Zhang and Liu 2010). *Education, alerts, and reminders* are important to reinforce user ethics and proficiency (Barrows and Clayton 1996, Rindfleisch 1997). *Patient access* requires that users are able to access their information and information on them (van der Linden et al. 2009). For use of patients' information, *informed consent* needs to be given by patients (Barrows and Clayton 1996, van der Linden et al. 2009, Zhang and Liu 2010). Moreover, it is important that patients are provided with *access control* so that patients are able to easily and granularly configure who can access their information (Barrows and Clayton 1996, van der Linden et al. 2009, Rindfleisch 1997, Subashini and Kavitha 2011, Wainer et al. 2008, Zhang and Liu 2010).

This compilation of information security and privacy requirements answers **RQ1**: What are information security and privacy requirements of PHS? However, since PHS can provide any functionality as long as users find it helpful, the individual explicit security requirements and priorities of PHS are manifested in various ways: For instance, in contrast to a PHS that provides decision support functionality and requires access to unencrypted sensitive medical information, a secure processing environment is of lesser importance in a PHS that only stores encrypted information. Therefore, while the elicited requirements should be applicable to a broad range of PHS, their importance depends on the respective PHS and some requirements might even not be necessary in certain PHS.

2.5 PHS Security Requirements Covered by the German HTI

The HTI introduction is an ambitious, expensive, and protracted project (Tuffs 2010). In 2013, seven years after the initially targeted date for HTI introduction, the project is still ongoing; however, many hurdles have been taken and first changes of the project are rolled out to the general population (Dehling and Sunyaev 2012a, Sunyaev, Leimeister, et al. 2010). By the end of 2012, 70% of German insurees had to be issued a smart card (called electronic health card (eHC)) that replaces the previous insurance card and enables patients to access HTI functionality. Similarly, medical professionals are equipped with health professional cards (HPC) and medical institutions with secure module cards (SMC). At first, a basic, preliminary infrastructure implementing functionality required for online verification of insuree information will be established. Subsequently, the preliminary infrastructure will be adjusted and extended to host the functionality envisioned for the target infrastructure. The HTI represents an inter-organizational network that connects all stakeholders, including 2,200 hospitals, 123,000 general practitioners, 21,000 pharmacies, and 80,000,000 patients (Tuffs 2010), in the healthcare system over the internet. Accordingly, the HTI employs security measures and services to protect offered functionality and communication (Dehling and Sunyaev 2012a).

As illustrated in Figure 7, the HTI uses a tiered architecture and features centralized and decentralized components. Centralized components, the backbone and the central systems, manage for instance the access to available services, verify corresponding access rights, compile logs for auditing, and ensure that the identity of patients is not known to the professional services. Professional services provide functionality like verification of insurance information or manage medical information. Virtual private networks (VPN) are used to secure communication. Additionally, security gateways block not whitelisted traffic and link trusted networks. Decentralized components enable clients to connect to centralized parts of the HTI. Necessary functionality to use centralized parts of the HTI is provided by a device called connector. Connector functionality entails net-

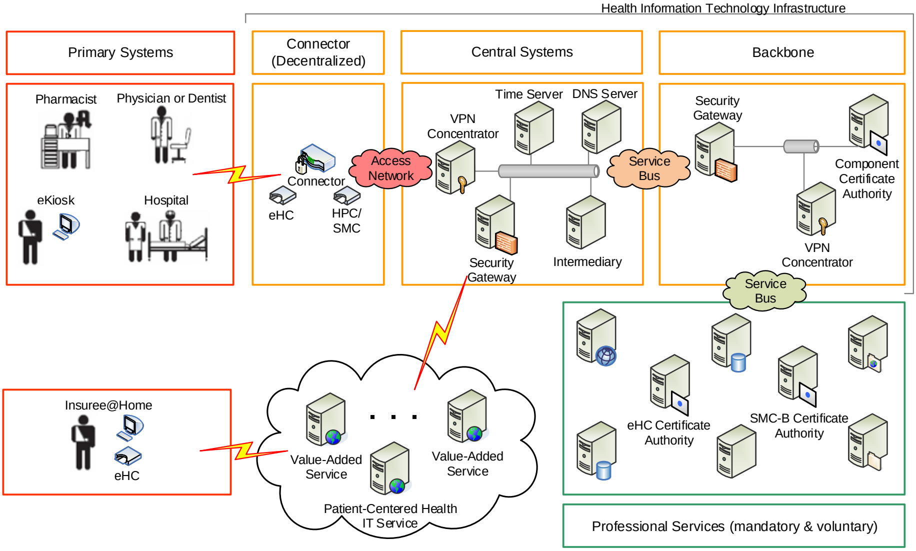


Figure 7: High-level architecture of German Health Information Technology Infrastructure. Adapted from www.gematik.de.

work connectivity, security functionality (eg, encryption and signatures), and authentication of clients. To facilitate authentication, card readers for the smart cards are hooked up to the connector. Intermediaries handle communication between connectors and professional services. By concentrating many point-to-point connections in service buses, intermediaries relieve other central components and professional services from traffic. Clients can access HTI services from their primary systems (eg, hospital IS, pharmacy IS, practice IS). Furthermore, clients can access further services provided by networks beyond the protected perimeter of the HTI, like a PHS located somewhere in the internet. Corresponding traffic is routed through central security gateways that are extended with further capabilities like virus or malware detection.

In contrast to professional services, PHS are not inspected by the gematik. However, to gain access to HTI services and be approved by the gematik, providers need to verifiably demonstrate that PHS functionality corresponds to specification, that the PHS employs sufficient measures to ensure information security and privacy, and does not endanger other HTI services. HTI components are designed in such a way that information and configurations of newly approved PHS can be loaded upon approval (eg, keys of the PHS can be registered with the Component Certificate Authority, the PHS can be authorized in the security gateways, the PHS can be accessed via intermediaries). Approved PHS can access some functionality provided by the HTI: creation of secure communication channels with HTI components, authentication of signatures, signing, and encryption. Furthermore, functionality required by all offered services like creation and display of access logs for patients' information will be centrally provided by the HTI. With an eHC-compatible card reader featuring a keypad, patients are able to access PHS at home via the internet while using eHC security functionality. A keypad is necessary to verify ownership of an eHC by entering a personal identification number (PIN).

The listing in Table 3 answers **RQ2**: Which information security and privacy requirements of PHS can be fulfilled with security measures provided by the German HTI? Table 3 lists the derived security requirements of PHS and indicates, according to the HTI description provided above, whether these can be fulfilled by HTI security measures. HTI security measures do not completely relieve PHS providers from implementing security measures. Yet, HTI security measures provide a foundation and fulfill, at least partly, a sizeable amount of security requirements. Contributions of HTI security measures are mainly based on user authentication through smart cards, encryption and signature functionality, as well as the general hardware and administration infrastructure. Hence, the HTI security measures deal with requirements important for most PHS and are thus broadly applicable. Encryption of information and authentication of users and/or services is for instance required whenever sensitive information is involved. Moreover, establishment of a nation-wide public key infrastructure (PKI) or dissemination of smart cards among all German inhabitants would be unfeasible tasks for individual PHS providers due to the magnitude and complexity of these tasks, but are well suited for an association like the gematik.

Table 3: PHS information security and privacy requirements covered by HTI security measures. The 'HTI' column indicates whether a requirement can be fulfilled by HTI security measures. Partly means that a requirement cannot be completely fulfilled by HTI requirements. The requirement categories are not disjunct. Categories are provided for the sake of clarity. Integrity has for instance no sub-requirements because these (backup, transmission/storage security, audit trails, …) are already listed in other categories.

Security/Privacy Requirement	HTI	Security/Privacy Requirement	HTI
Confidentiality	Partly	**Usability**	Partly
Anonymity	No	Access control	Partly
Authorization	Partly	Credential substitutability	Yes
Limited access right duration	No	Education, alerts, and reminders	No
Non-Disclosure	No	Emergency access	No
Transmission and storage security	Yes	Informed consent	Partly
Unlinkability	No	Patient access	Partly
Integrity	Partly	**Accountability/Non-Repudiation**	Yes
Availability	No	Audit trails	Yes
Backup	No	Authentication	Yes
Long storage times	No	**Perimeter Definition**	Partly
Recoverability	No	Intrusion detection	Partly
Resilience to failures	No	Network security	Partly
Scalability	No	Physical hardware security	No
Up-to-Datedness	No	System vulnerability analysis	No

2.6 Security Measures for PHS Security Requirements Not Covered by the HTI

To cover all elicited security requirements, the security measures offered by the HTI need to be complemented with additional security measures. In this section, we focus on PHS-specific additional security measures; see Table 4 and Table 5 for a full listing. To hide compromising information from prying eyes (*non-disclosure*), users should have multiple profiles or identities (Slamanig and Stingl 2008). This way, when forced to disclose information, users could use uncompromising profiles and there would be no simple way of telling whether users disclosed real or fake profiles. To address cloud computing characteristics like virtualization/multitenancy, PHS should run in community clouds for healthcare so that all involved service providers have similar security requirements, but, in contrast to private clouds, smaller providers can also leverage synergies (Zhang and Liu 2010).

In the HTI, a patient can authorize others, who identify themselves with a smartcard, to access her information by presenting her eHC and approving access requests by entering a PIN. While this is appropriate in a treatment scenario where medical professional and patient are in the same location, it is a cumbersome approach for *authorization* in PHS where access rights to multiple resources need to be managed in an easy, user-friendly way (*access control*). A more fitting approach, where access rights are managed by a person-oriented virtual organization (POVO), was proposed by Calvillo

Table 4: Mapping of confidentiality, integrity, and availability requirements to non-exhaustive sets of fitting measures for ensuring information security and privacy of PHS.

Security/Privacy Requirement	Measures
Confidentiality	Minimization principle; data segregation; secure processing environment
Anonymity	Pseudonyms, protection of metadata; certification
Authorization	Person-oriented virtual organization; semantic technologies
Limited access right duration	Revoke at specific event; expire/renew after timespan
Non-Disclosure	Multiple profiles/identities
Transmission and storage security	HTI PKI for encryption/signatures
Unlinkability	Pseudonyms, obfuscation, protection of metadata
Integrity	Signatures; backup; authorization; secure processing environment
Availability	Network security; physical hardware security
Backup	Database replication; offsite storage
Long storage times	Digital preservation techniques
Recoverability	Versioning; no deletion of data
Resilience to failures	Deployment in community cloud; redundancy; load balancing
Scalability	Deployment in community cloud; database replication; load balancing
Up-to-Datedness	Database replication

Table 5. Mapping of usability, accountability/non-repudiation, and perimeter-definition requirements to non-exhaustive sets of fitting measures for ensuring security and privacy of PHS.

Security/Privacy Requirement	Measures
Usability	Focus on users' needs and proficiency
Access control	Graphical access policy editor
Credential substitutability	HTI card management
Education, alerts, and reminders	Tutorial, manual, in-application help and notifications, support team, …
Emergency access	Define emergency access policies
Informed consent	Encryption, access policies
Patient access	Let users see and modify all information stored on them
Accountability/Non-Repudiation	Signatures; versioning
Audit trails	Central HTI audit service
Authentication	HTI smart cards; PINs
Perimeter Definition	Control of all physical, logical and technological borders
Intrusion detection	Package filtering; intrusion detection systems
Network security	Firewalls; package filtering
Physical hardware security	Guard and secure hardware; cooling systems, fire suppression, …
System vulnerability analysis	Analyses by specialists; offering finders' fees

et al. (2013). In their approach, a POVO is created for each individual patient, patients can control access policies for all their resources, and the POVO is maintained across patients' lifetime. For interoperability, semantic technologies, which enrich information with machine- and human-interpretable context, are employed so that the authorization functionality can be used in various services. Easy *access control* is provided by an access policy editor that offers a graphical user interface, requires no special computer proficiency, allows for policies with different granularity, and makes technical details transparent to the user. Additionally, the approach allows for policies that facilitate access to required information in emergencies (*emergency access*). Their approach also implements the requirement of *informed consent*: Due to encryption, other users cannot access patients' information unless according access policies are specified. Yet, some PHS might require access to patients' information in order to provide personalized services. Such PHS, which could principally misuse patients' information, need to follow the minimization principle (ie, request only information necessary for the service and delete information as soon as possible. POVOs could be operated by a third party (eg, an organization approved by the gematik) and then used by a variety of services that store information or require access to information.

Slamanig and Stingl (2008) present an approach to realize *anonymity* and *unlinkability* through the reduction of unprotected metadata by employing pseudonyms and obfuscating relationships between users and their information. However, a PHS might require access to very specific information, like genetic information, so that even anonymized information can be reidentified (Lunshof et al. 2008). In such a case, pseudonymization and obfuscation would only cause performance overhead and users need to trust in the confidential handling of their information. This trust-relationship could be improved by inspection or monitoring of PHS and PHS providers through independent third parties (Lansing et al. 2013, Sunyaev and Schneider 2013).

The presented compilation of potential additional security measures that realize requirements not fulfilled by HTI security measures answers **RQ3**: Can the requirements not fulfilled by security measures of the German HTI be fulfilled with additional measures ensuring information security and privacy? In Table 4 and Table 5 these security measures are mapped to the corresponding security requirements. While the proposed security measures present viable realizations, it has to be kept in mind that, depending on the respective PHS, alternative measures might provide better results or are already in place and would thus be more cost-efficient.

2.7 Discussion

Our answers to RQ 1-3 can be consolidated in a guideline for provision of PHS in public networks while ensuring information security and privacy, which is depicted in Figure 8. The guideline consists of two blocks. The first block ‘Preparation and Justification’ (step 1-3), needs to be addressed before PHS deployment and ensures that appropriate security measures are implemented. The second block ‘Handling of Runtime Events’ (steps 4-5), handles events that happen while the PHS is deployed and that might necessitate justifications or adaptions of security requirements considered relevant and security measures implemented.

At first (step 1), it is necessary to establish a complete, in-depth understanding of the functionality provided by the PHS because otherwise it would not be possible to reliably assess what PHS aspects require protection and how the PHS can be protected. In step 2, security requirements of the PHS are assessed and adapted. Some requirements might not be relevant for the specific PHS or need adaption and additional requirements pertinent to the specific PHS may have to be added. In the following step 3, security measures need to be selected and implemented according to security requirements determined relevant in step 2.

During runtime, some events might require the reassessment of security requirements and measures. If the PHS functionality is changed, a jump back to step 1 is required because a change in functionality may also change PHS security aspects. If malicious activity is detected, immediate actions are required (step 4): For instance, it might be possible to prevent the attacker from accessing the service or some parts/the whole PHS needs to be temporarily taken offline. Subsequently, step 5 needs to be performed so that the security vulnerability used for the attack can be determined; this will also be necessary if a security vulnerability is detected without an attack (eg, through a system vulnerability analysis). Afterwards, it is necessary to go to step 2 to weed out identified security vulnerabilities. This guideline can be useful because of its simplicity and flexibility. The guideline consists of five steps that cover the protection of information security

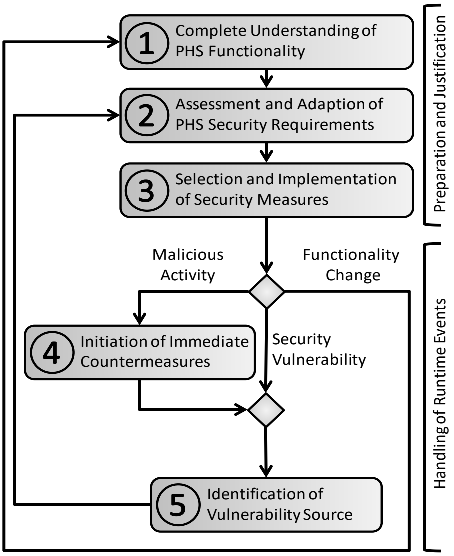

1
Complete Understanding of PHS Functionality
2
Assessment and Adaption of PHS Security Requirements
3
Selection and Implementation of Security Measures
Preparation and Justification
Malicious Activity
Functionality Change
4
Initiation of Immediate Countermeasures
Security Vulnerability
5
Identification of Vulnerability Source
Handling of Runtime Events

Figure 8: Illustration of guideline for provision of PHS offered in public networks while ensuring security and privacy.

and privacy of PHS offered in public networks from initial preparations over runtime events to the handling of runtime events. Security requirements and corresponding measures can however be adapted according to the individual PHS and its environment so that the guideline is applicable to a broad or even exhaustive range of PHS and can serve as a valuable guide for ensuring information security and privacy.

It is worth to notice that individual information security and privacy requirements were mentioned with varying frequency. Requirements like authorization, backup, authentication, or access control were mentioned in far more articles than anonymity, unlinkability, resilience to failure, or emergency access. This should however not be taken as indication for varying importance. It is rather an indication for the interdisciplinary influences on PHS and the lack of more general research. More specialized research focuses only on the information security and privacy requirements pertinent to the respective research focus so that some requirements, otherwise important, are not mentioned. Emergency access is, for instance, highly unlikely to be seen as information security and privacy requirement without an influence like the medical context of PHS. Similarly, long storage times are often not that important, but when managing personal health information (eg, in a personal health record) it needs to be ensured that information remains accessible and modifiable across a lifetime or even longer (eg, to represent family history).

Another important aspect is that fulfilling information security and privacy requirements comes at some cost. Implemented measures might increase the effort required for operating or maintaining the system and they obviously require some monetary efforts for their implementation and operation. If a PHS is, for example, only used in a specific facility (eg, a hospital) some appropriate measures may already be in place (patient identification, measures for perimeter definition). Thus, it is worth to looks at the system environment.

Contributions of HTI security measures are mainly based on user authentication through smart cards, encryption and signature functionality, as well as the general hardware and administration infrastructure. Especially, use of effective but complex and costly security measures can be realized with HTI functionality and services. HTI security measures deal with requirements important for most PHS and are thus broadly applicable. While it is not likely that something like the HTI will be available on a global scale in the near future, it is definitely worth to consider other initiatives in the application environment for PHS development or provision in order to benefit from standardized, centralized components and leverage associated synergies. In the coming years, personal health records (Carrión Señor, Aleman, et al. 2012) may rise to a central hub for global safekeeping and access to personal health information, but the HTI goes even further, at least on a national level.

A limitation of our article is that the HTI is not yet established so that we could not incorporate real-world experiences with the HTI. However, to ensure that health IT networks like the German HTI are used to their full potential in a timely fashion, it is important that important aspects like information security and privacy that, if not treated properly, could impede patients' intention to use PHS (Bélanger and Crossler 2011) are studied early on. Another aspect for future research, which is in line with the rising globalization, is ensuring information security and privacy in PHS on a trans- or even international level. Due to different and potentially conflicting technological, regulatory, and cultural environments, maintaining information security and privacy in transnational PHS poses a challenging task. Other opportunities for further research include the assessment of security measures with respect to selected requirements. This is especially interesting for requirements where usability is affected and measures are not readily available in the application environment or the scientific knowledge base; for instance, different approaches for facilitation of emergency access (Dünnebeil et al. 2011).

Our research contributes to overcoming the information security and privacy challenges of PHS by establishing a foundation for secure and privacy-preserving provision of PHS. We contribute to the scientific knowledge base by illustrating information security and privacy aspects of the provision of PHS and examining the utility of the HTI for provision of PHS. For praxis-oriented audiences, this research can serve as introduction to PHS, illustrates HTI aspects directly benefitting patients, and offers a foundation and guide for the secure provision of PHS via public networks. Improved information security and privacy of PHS is also advantageous for patients: Patients may be more willing to share personal, medical information so that PHS can be better tailored to their needs and individual situation, which allows patients to reap more benefits from PHS use.

2.8 Conclusion

Development of health IT applications is challenging (Pagliari 2007): Many stakeholders have to be considered. Old-fashioned established processes need to be reengineered or incorporated into new systems. Complex medical relationships might need to be modeled. Errors should not happen since lives are at stake and the access to security-sensitive health information creates high demand for information security and privacy protection. As a contribution to mastering the information security and privacy challenges, we present a list of information security and privacy requirements for PHS and related health IT services. Requirements engineering represents an early, important step in the software engineering process (Nuseibeh and Easterbrook 2000). We focused on compiling a list of information security and privacy requirements that are applicable to a broad range of PHS to account for the diversity of PHS. PHS can provide any functionality patients find useful and can be developed for a range of technology like conventional workstations, client server architectures, cloud computing, or mobile end user devices. Besides illustrating PHS aspects that need to be considered when providing PHS while maintaining information security and privacy, the collection of information security and privacy requirements can also be used to assess the quality of information security and privacy practices of an individual PHS. An HTI can serve as central hub for PHS. Hence, PHS providers and developers do not have to implement all required functionality on their own; instead, they can leverage HTI functionality to ensure information security and privacy. Yet, HTI security measures do not completely relieve PHS providers from implementing security measures, but provide a foundation and fulfill, at least partly, a sizeable amount of security requirements. As long as information security and privacy aspects are handled properly, health IT networks can serve as enabler for innovative services that cater the rising demand of patients who want to access health information and services as conveniently as patients are used to when doing their banking or vacation planning (Forkner-Dunn 2003).

2.9 References

Abraham C, Nishihara E, Akiyama M (2011) Transforming Healthcare with Information Technology in Japan: A Review of Policy, People, and Progress. International Journal of Medical Informatics 80(3):157–170.

Ahern DK, Woods SS, Lightowler MC, Finley SW, Houston TK (2011) Promise of and Potential for Patient-Facing Technologies to Enable Meaningful Use. American Journal of Preventive Medicine 40(5 Suppl 2):162–172.

Appari A, Johnson ME (2010) Information Security and Privacy in Healthcare: Current State of Research. International Journal of Internet and Enterprise Management 6(4):279–314.

Appelbaum PS (2002) Privacy in Psychiatric Treatment: Threats and Responses. The American Journal of Psychiatry 159(11):1809–1818.

Barrows RC, Clayton PD (1996) Privacy, Confidentiality, and Electronic Medical Records. Journal of the American Medical Informatics Associations 3(2):139–148.

Bélanger F, Crossler RE (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly 35(4):1017–1041.

Blechman EA, Raich P, Raghupathi W, Blass S (2012) Strategic Value of an Unbound, Interoperable PHR Platform for Rights-Managed Care Coordination. Communications of the Association for Information Systems 30(1):Article 6.

Calvillo J, Román I, Roa LM (2013) Empowering Citizens with Access Control Mechanisms to their Personal Health Resources. International Journal of Medical Informatics 82(1):58–72.

Carrión Señor I, Aleman JLF, Toval A (2012) Personal Health Records: New Means to Safely Handle Health Data? IEEE Computer 45(11):27–33.

Chan ATS, Cao J, Chan H, Young G (2001) A Web-Enabled Framework for Smart Card Applications in Health Services. Communications of the ACM 44(9):76–82.

Dehling T, Sunyaev A (2012a) Information Security of Patient-Centred Services Utilising the German Nationwide Health Information Technology Infrastructure. 3rd USENIX Workshop on Health Security and Privacy. (USENIX, Bellevue, WA, USA).

Dehling T, Sunyaev A (2012b) Architecture and Design of a Patient-Friendly eHealth Web Application: Patient Information Leaflets and Supplementary Services. 18th Americas Conference on Information Systems. (AIS, Seattle, WA, USA).

Dehling T, Sunyaev A (2013) Improved Medication Compliance through Health IT: Design and Mixed Methods Evaluation of the ePill Application. 34th International Conference on Information Systems. (AIS, Milano, Italy).

Dehling T, Sunyaev A (2014) Information Security and Privacy of Patient-Centered Health IT Services: What needs to be done? 47th Hawaii International Conference on System Sciences. (IEEE, Big Island, HI, USA), 2984–2993.

Delgado M (2011) The Evolution of Health Care IT: Are Current U.S. Privacy Policies Ready for the Clouds? 2011 IEEE World Congress on Services. (Washington, DC USA), 371–378.

Dünnebeil S, Köbler F, Koene P, Leimeister JM, Krcmar H (2011) Encrypted NFC Emergency Tags Based on the German Telematics Infrastructure. Proceedings of the 2011 Third International Workshop on Near Field Communication. (IEEE, Hagenberg, Austria), 50–55.

Ekonomou E, Fan L, Buchanan W, Thüemmler C (2011) An Integrated Cloud-Based Healthcare Infrastructure. Proceedings of the 3rd IEEE International Conference on Cloud Computing Technology and Science (IEEE CloudCom 2011). (IEEE, Athens, Greece), 532–536.

Fan L, Buchanan W, Thümmler C, Lo O, Khedim A, Uthmani O, Lawson A, Bell D (2011) DACAR Platform for eHealth Services Cloud. Proceedings of the 2011 IEEE 4th International Conference on Cloud Computing. (IEEE, Washington, DC, USA), 219–226.

Forkner-Dunn J (2003) Internet-Based Patient Self-Care: The Next Generation of Health Care Delivery. Journal of Medical Internet Research 5(2):e8.

Garber L (2012) The Challenges of Securing the Virtualized Environment. IEEE Computer 45(1):17–20.

Gritzalis DA (1998) Enhancing Security and Improving Interoperability in Healthcare Information Systems. Medical Informatics 23(4):309–323.

d'Heureuse N, Huici F, Arumaithurai M, Ahmed M, Papagiannaki K, Niccolini S (2012) What's App?: A Wide-Scale Measurement Study of Smart Phone Markets. ACM SIGMOBILE. Mobile Computing and Communications Review 16(2):16–27.

Istepanian RSH, Jovanov E, Zhang YT (2004) Guest Editorial Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-Care Connectivity. IEEE Transactions on Information Technology in Biomedicine 8(4):405–414.

Johnson ME (2009) Data Hemorrhages in the Health-Care Sector. Dingledine R, Golle P, eds. Financial Cryptography and Data Security. Lecture Notes in Computer Science. (Springer-Verlag, Berlin, Heidelberg), 71–89.

Kaletsch A, Sunyaev A (2011) Privacy Engineering: Personal Health Records in Cloud Computing Environments. 32th International Conference on Information Systems. (AIS, Shanghai, China).

Kotz D (2011) A Threat Taxonomy for mHealth Privacy. 3rd International Conference on Communication Systems and Networks. (IEEE, Bangalore, India).

Landry JP, Pardue JH, Johnsten T, Campbell M, Patidar P (2011) A Threat Tree for Health Information Security and Privacy. Sambamurthy V, Tanniru M, eds. Proceedings of the 17th Americas Conference on Information Systems. (AIS, Detroit, MI, USA).

Lansing J, Schneider S, Sunyaev A (2013) Cloud Service Certifications: Measuring Consumers' Preferences for Assurances. Proceedings of the 27st European Conference on Information Systems (ECIS 2013). (Utrecht, Netherlands), paper 181.

van der Linden H, Kalra D, Hasman A, Talmon J (2009) Inter-Organizational Future Proof EHR Systems: A Review of the Security and Privacy Related Issues. International Journal of Medical Informatics 78(3):141–160.

Lunshof JE, Chadwick R, Vorhaus DB, Church GM (2008) From Genetic Privacy to Open Consent. Nature Reviews Genetics 9(5):406–411.

Mandl KD, Mandel JC, Murphy SN, Bernstam EV, Ramoni RL, Kreda DA, McCoy JM, Adida B, Kohane IS (2012) The SMART Platform: Early Experience Enabling Substitutable Applications for Electronic Health Records. Journal of the American Medical Informatics Association 19(4):597–603.

Mell P, Grance T (2011) The NIST Definition of Cloud Computing. Retrieved (August 22, 2012), csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Nuseibeh B, Easterbrook S (2000) Requirements Engineering: A Roadmap. Proceedings of the Conference on The Future of Software Engineering. ICSE '00. (ACM, New York, NY, USA), 35–46.

Ozdemir Z, Barron J, Bandyopadhyay S (2011) An Analysis of the Adoption of Digital Health Records Under Switching Costs. Information Systems Research 22(3):491–503.

Pagliari C (2007) Design and Evaluation in eHealth: Challenges and Implications for an Interdisciplinary Field. Journal of Medical Internet Research 9(2):e15.

Pyper C, Amery J, Watson M, Crook C (2004) Access to Electronic Health Records in Primary Care - A Survey of Patients' Views. Medical Science Monitor 10(11):SR17-22.

Raymond ES (2003) The Art of UNIX Programming 1st ed. (Addison-Wesley, Boston, MA, USA).

Rindfleisch TC (1997) Privacy, Information Technology, and Health Care. Communications of the ACM 40(8):92–100.

Rohm AJ, Milne GR (2004) Just What the Doctor Ordered: The Role of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern. Journal of Business Research 57(9):1000–1011.

Rothstein MA, Talbott MK (2007) Compelled Authorizations for Disclosure of Health Records: Magnitude and Implications. The American Journal of Bioethics 7(3):38–45.

Shahri AB, Ismail Z (2012) A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS. Journal of Information Security 3(2):169–176.

Shea S (1994) Security Versus Access: Trade-Offs are only Part of the Story. Journal of the American Medical Informatics Association 1(4):314–315.

Simon SR, Evans JS, Benjamin A, Delano D, Bates DW (2009) Patients' Attitudes Toward Electronic Health Information Exchange: Qualitative Study. Journal of Medical Internet Research 11(3):e30.

Slamanig D, Stingl C (2008) Privacy Aspects of eHealth. 3rd International Conference on Availability, Reliability and Security. ARES'08. (IEEE, Washington, DC, USA), 1226–1233.

Song D, Shi E, Fischer I (2012) Cloud Data Protection for the Masses. IEEE Computer 45(1):39–45.

Subashini S, Kavitha V (2011) A Survey on Security Issues in Service Delivery Models of Cloud Computing. Journal of Network and Computer Applications 34(1):1–11.

Sunyaev A, Chornyi D (2012) Supporting Chronic Disease Care Quality: Design and Implementation of a Health Service and its Integration with Electronic Health Records. ACM Journal of Data and Information Quality 3(2):3:1-3:21.

Sunyaev A, Chornyi D, Mauro C, Krcmar H (2010) Evaluation Framework for Personal Health Records: Microsoft Health Vault vs. Google Health. Proceedings of the Hawaii International Conference on System Sciences (HICSS 34). (IEEE, Kauai, HI, USA).

Sunyaev A, Leimeister JM, Krcmar H (2010) Open Security Issues in German Healthcare Telematics. Proceedings of the 3rd International Conference on Health Informatics. (INSTICC, Valencia, Spain), 187–194.

Sunyaev A, Schneider S (2013) Cloud Services Certification. Communications of the ACM 56(2):33–36.

Tuffs A (2010) Germany Puts Universal Health e-Card on Hold. BMJ 340(1):c171.

Wainer J, Campos CJR, Salinas MDU, Sigulem D (2008) Security Requirements for a Lifelong Electronic Health Record System: An Opinion. Open Medical Informatics Journal 2:160–165.

Wilson EV (2009) Patient-Centered E-Health Wilson EV, ed. (IGI Publications, Hershey, PA, USA).

Yau SS, An HG (2011) Software Engineering Meets Services and Cloud Computing. IEEE Computer 44(10):47–53.

Zhang L, Gupta D, Mohapatra P (2012) How Expensive are Free Smartphone Apps? SIGMOBILE Mobile Computing and Communications Review 16(3):21–32.

Zhang R, Liu L (2010) Security Models and Requirements for Healthcare Application Clouds. Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing. (IEEE, Miami, FL, USA), 268–275.

2.10 Appendix

Table 6: Security and privacy requirements of patient-centered services and mapping to corresponding literature. '1' indicates that the article proposed the requirement. A missing '1' does, however, not indicate that the article rejects the requirement.

	Rindfleisch	Wainer et al.	Slamanig and Stingl	Barrows and Clayton	Zhang and Liu	Linden et al.	Subashini and Kavitha	
Confidentiality	1	1	1	1	1	1	1	No unauthorized person may inspect the contents of a patient's records
+ Anonymity			1					Real identity of users should not be revealed
+ Authorization	1		1	1	1	1	1	Only access to necessary information; data segregation (ensure that users cannot access other users' data)
+ Limited access right duration		1						Revoke unnecessary access rights
+ Non-Disclosure			1		1			Users cannot be forced to reveal information they do not want to reveal
+ Storage and transmission security	1		1	1	1			Prevent eavesdropping (transmission and storage)
+ Unlinkability			1					Relationships between items cannot be determined through observation
Integrity	1	1		1	1	1	1	Ensure information content is as intended and not unintentionally changed
Usability	1	1		1	1	1	1	Important information needs to be easy accessible; security measures should not impede system operation; ensure that users know why and how they can contribute to information security
+ Access control	1	1		1	1	1	1	Patients need to be able to control who can access what information
+ Credential substitutability		1			1			Authorization details need to be substitutable (loss, technological obsolescence)
+ Education, alerts, and reminders	1			1				Reinforce user ethics and proficiency; provide relevant instructions; make users aware of necessary actions
+ Emergency access		1						In an emergency medical professionals must be able to access vital information
+ Informed consent				1	1	1		Users need to agree to uses of their information; patients' consents need to be managed
+ Patient access						1		Patients need to be able to retrieve information stored on them

	Rindfleisch	Wainer et al.	Slamanig and Stingl	Barrows and Clayton	Zhang and Liu	Linden et al.	Subashini and Kavitha	
Availability	1	1		1	1	1	1	Ensure that up-to-date information is available when needed
+ Backup		1		1	1	1	1	Employ redundancy to ensure that data can be restored
+ Long storage times		1				1		Certain information needs to be preserved a lifetime
+ Recoverability	1	1				1		Restore the information to a specific point in time; information can only be added; versioning for modifications/corrections
+ Resilience to failures							1	Failure of single nodes should not impede the performance of the whole service
+ Scalability							1	Application needs to be adaptable to performance needs
+ Up-to-Datedness		1				1		There should be no significant delay between when data entry into the record and its availability to different users
Accountability/ Non-Repudiation	1	1	1	1	1	1	1	Ensure that users are responsible for their access to and use of information; ensure that users cannot deny actions
+ Audit trails	1			1	1	1		Log relevant activity (eg, document accesses); give alerts
+ Authentication	1		1	1	1	1	1	Determine who is connecting and verify that they are who they claim to be
Perimeter Definition	1			1			1	Know and control the boundaries of trusted access to the information system
+ Intrusion detection				1			1	Detect unintended actions/service activity
+ Network security	1			1			1	Avoid unauthorized access and manage network access rights
+ Physical hardware security	1			1			1	Prevent impairment of hardware (theft; natural disasters, …)
+ System vulnerability analysis	1						1	Detect unintended system vulnerabilities; guard against viruses, trojans, …

3 Exploring the Far Side of Mobile Health—Information Security and Privacy of Mobile Health Applications on iOS and Android

Authors: Tobias Dehling, Fangjian Gao, Stephan Schneider, Ali Sunyaev

Background: Mobile health (mHealth) applications (apps) aim at providing seamless access to tailored health information technology and have the potential to alleviate global health burdens. Yet, they bear risks to information security and privacy because users need to reveal private, sensitive medical information to redeem certain benefits. Due to the plethora and diversity of available mHealth apps, implications for information security and privacy are unclear and complex.

Objective: The objective of this research is to establish an overview of mHealth apps offered on iOS and Android with a special focus on potential damage to users through information security and privacy infringements.

Methods: We assessed apps available in English and offered in the categories ‘Medical’ and ‘Health & Fitness’ in the iOS and Android app stores. Based on the information retrievable from the app stores, we established an overview of available mHealth apps, tagged apps to make offered information machine-readable, and clustered the discovered apps to identify and group similar apps. Subsequently, information security and privacy implications were assessed based on health specificity of information available to apps, potential damage through information leaks, potential damage through information manipulation, potential damage through information loss, and potential value of information to third parties.

Results: We discovered 24,405 health-related apps (iOS: 21,953; Android: 2,452). Absence or scarceness of ratings for 81.36% of iOS and 76.14% of Android apps indicates that less than a quarter of mHealth apps are in more or less widespread use. Clustering resulted in 245 distinct clusters, which were consolidated into 12 app archetypes grouping clusters with similar assessments of potential damage through information security and privacy infringements. The majority of apps (95.63% of apps) pose at least some potential damage through information security and privacy infringements. 11.67% of apps scored the highest assessments of potential damages.

Conclusions: Various kinds of mHealth apps collect and offer critical, sensitive, private medical information calling for a special focus on information security and privacy of mHealth apps. In order to foster user acceptance and trust, appropriate security measures and processes need to be devised and employed so that users can benefit from seamlessly accessible, tailored mHealth apps without exposing themselves to the serious repercussions of information security and privacy infringements.

Keywords: Mobile Health, Mobile Apps, Data Security, Software and Application Security, Patient Privacy, Health Information Technology

3.1 Introduction

Mobile health (mHealth) leverages various wireless technologies to provide health-related information and services on diverse mobile devices and is a promising subset of health information technology (IT) (Collins 2012, Istepanian et al. 2004, Kumar et al. 2013, Mechael 2009, Steinhubl et al. 2013, Sunyaev 2014). mHealth has the potential to alleviate global health burdens due to rising dissemination of mobile devices, standardized and easy access to cloud or internet services, and the possibility of affordable global deployment (Anthes 2012, d'Heureuse et al. 2012, Mechael 2009, Muñoz 2010). mHealth applications (apps) target for instance prevalent global diseases (Chomutare et al. 2011, Martínez-Pérez, de la Torre-Díez and López-Coronado 2013) and offer vital health information at an individual as well as population level (Chen et al. 2012). On the other hand, users, albeit deeming access to health information and related services beneficial, are concerned with information security and privacy issues and want to control access to their information (Dhopeshwarkar et al. 2012, Khalid et al. 2015, Simon et al. 2009).

Information security and privacy issues impede users' willingness to share information (Anderson and Agarwal 2011, Bélanger and Crossler 2011) and render thus the promising benefits to be reaped from mHealth apps moot: In order to tailor offered information and services to users' needs, mHealth apps require access to relevant personal health information. Thus, mHealth apps will only offer more general services or cannot be used at all if users are not willing to share their health information. Moreover, infringements of information security and privacy lead not only to leakage or manipulation of private, sensitive information, but make also serious consequences like worsened morbidity or death more likely (Avancha et al. 2012).

Typical mobile devices for mHealth are smartphones and tablets (Martínez-Pérez, de la Torre-Díez and López-Coronado 2013), which are characterized by a rapidly rising market penetration and access to a wide range of embedded technology like sensors for audio, video, location, orientation, and acceleration (d'Heureuse et al. 2012, Lane et al. 2010, Martínez-Pérez, de la Torre-Díez and López-Coronado 2013, Weiss and Lockhart 2012). The main platforms for mobile devices are Google's Android and Apple's iOS (d'Heureuse et al. 2012). The associated app stores (Apple iTunes (Apple 2014a), Google Play (Google 2014a)) offer a vast amount of mHealth apps. These mHealth apps provide a variety of functionality requiring access to different kinds of information and supporting users in different ways: For example, support for weight management, tracking of workouts or medication regimens, facilitation of physician patient communication, management of chronic diseases, or implementation of web-based interventions (Barak et al. 2009).

Mobile devices and apps have been addressed from various perspectives: For instance, security aspects (Chin et al. 2011, Enck et al. 2011, Gregory Goth 2012), privacy (Avancha et al. 2012, Egele et al. 2011, Liccardi et al. 2013, Wicker 2012), software engineering (Estrin and Sim 2010, Heitkötter et al. 2013, Mojica et al. 2014), medical implications (Freifeld et al. 2010, Ozdalga et al. 2012), hardware (Lane et al. 2010, Pathak et al. 2012), or user implications (Weiss and Lockhart 2012, Q. Xu et al. 2011, Xu, Gupta, et al. 2012). In contrast, pertinent governmental regulation (eg, European Commision 2012, Food and Drug Administration 2013) and extant reviews of mHealth apps (eg, Abroms et al. 2011, Bender et al. 2013, Bierbrier et al. 2014, Breton et al. 2011, Chomutare et al. 2011, Donker et al. 2013, Huckvale et al. 2012, Lewis and Wyatt 2014, Liu et al. 2011, Martínez-Pérez, de la Torre-Díez and López-Coronado 2013, Martínez-Pérez, de la Torre-Díez, López-Coronado, et al. 2013, Martínez-Pérez et al. 2014, Mosa et al. 2012, Muessig et al. 2013, Plaza et al. 2013, Rosser and Eccleston 2011, West et al. 2012, Wolf et al. 2013) focus mostly on functional aspects and utility of apps for specific diseases or health conditions. Information security and privacy of mHealth apps is only scarcely addressed by extant research. With respect to information security and privacy, extant research offers, to the best of our knowledge, neither clear analyses of the peculiarities that distinguish mHealth apps from ‘common apps’ (eg, weather apps or games) nor of the differences distinguishing apps available from each other. In short, understanding of information security and privacy implications of mHealth apps is lacking and hard to grasp due to diversity and range of mHealth apps available. In order to address this gap, the objective of our research is to establish an overview of mHealth apps offered on iOS and Android with a special focus on potential damage to users through information security and privacy infringements.

Our research contributes to practice and the knowledge base by shedding light on information security and privacy of mHealth apps. Aside from providing an overview of available mHealth apps, we contribute to the scientific knowledge base by deepening the understanding of information security and privacy of mHealth apps. Instead of treating mHealth apps as a monolithic technology, we focus on the multi-facetted nature of mHealth apps and identify different mHealth app archetypes with respect to information security and privacy. For practical audiences, our work fosters awareness of information security and privacy implications of mHealth apps. Besides substantiating the need for attention to information security and privacy of mHealth apps, our work demonstrates that mHealth apps are of a diverse nature and require tailored attention to information security and privacy. For developers and end users of mHealth apps, the identification of mHealth app archetypes is especially useful to recognize where and understand when attention to information security and privacy is of particular importance. Deepening the understanding of information security and privacy of mHealth apps is an important step towards realization of the promising potential of mHealth apps to transform and improve the health care environment (Steinhubl et al. 2013).

3.2 Methods

3.2.1 App Discovery

We surveyed English language mHealth apps in the official iOS and Android app stores. App stores organize their offerings in categories (eg, Books, Games, and News).

We selected apps from the Medical and Health & Fitness categories, offered in both stores in May 2013. The iOS app store lists all apps by category and offers the desired information in plain hypertext markup language (HTML), enabling us to automatically parse app information to extract data. The Android app store employs dynamically generated HTML pages so that the HTML texts displayed in the browser do not convey useful information, which is dynamically loaded from an underlying database. Hence, we used a third party open-source interface for retrieving app information (android-market-api 2014). However, Google imposes various constraints on app store access (d'Heureuse et al. 2012, Viennot et al. 2014); for instance, only a maximum of 500 apps is returned per search request, even if more apps match the query. Our approach for Android app discovery builds search queries based on words from a publicly-available English word list (SIL International Linguistics Department 2014) appended once with the string ' medical' and once with the string ' health'. Supplemented with missing health-related words and phrases identified during app tagging (see section App selection), the word list consists of 111,632 distinct words and phrases.

Apps that were not available in English, did not have an English description, or were not health-related, despite being offered in the categories Medical or Health & Fitness (eg, apps offering wallpapers), were excluded from further assessment. We employed tagging, that is, assignment of arbitrary terms describing an object to that object, to filter the initially discovered apps (iOS: 32,614; Android: 4,632). Instead of assigning tags directly to an app, we assigned tags to corresponding strings in app descriptions. Only tags referring to health-related information collected by apps, health-related app purposes, handling of information, or other health-related app characteristics were used. For example, apps that provide medication-related functionality should be tagged with the tag 'Medication'. Yet, app descriptions use different wording (eg, medication, pharmaceutical, or drug). Assigning tags to all encountered strings referring to medication reduces the number of redundant tags and establishes a corpus of string tag relationships that facilitates automated tagging of apps. Since extant research offered no clear guidance to determine cut-off points for manual tagging or the number of required tag matches, cut-off points were determined according to the available data in group discussions of the authors. We manually tagged 200 frequently-rated apps (100 Health & Fitness, 100 Medical). Based on this initial tag corpus, we employed string matching (Faro and Lecroq 2012) to automatically tag the remaining apps. With this approach, apps that do not offer English descriptions or health-related functionality are not assigned any or assigned only a small number of tags because tags are assigned based on English, health-related words. Apps not matched by at least four distinct tags were excluded from further assessment.

3.2.2 App Clustering

Clustering Approach. App tagging created a machine-readable description of app functionality. Since all apps were tagged based on the same tag corpus, apps with similar characteristics are assigned similar tags. We clustered (Jain 2010) apps based on their tags to aggregate the data and identify the various kinds of apps in our sample. We used a graph—a set of vertices which are connected by a set of edges (Newman 2003)—to represent the apps and their tag relationships. Vertices represent apps and edges represent tags both vertices have in common.

For identification of clusters, we used a heuristic by Blondel et al. (2008), called Louvain Method, which is based on modularity optimization. Modularity is a measure for cluster quality introduced by Newman and Girvan (2004). Basically, modularity measures the fraction of edges in the graph that connect vertices within the same cluster minus the expected value of connections within a cluster if edges were inserted at random. Hence, a higher modularity value indicates that detected clusters are less random. The Louvain Method performed well in comparative analyses of clustering algorithms (Lancichinetti and Fortunato 2009, Tibély et al. 2011), has low runtime so that it breaks our dense app tag graph down into clusters within a feasible amount of time, and does not require a-priori determination of the number of clusters to be discovered, which is unfeasible due to the large numbers of apps, tags, and possible combinations. The Louvain Method is an agglomerative clustering algorithm (Jain 2010) that runs in multiple iterations until a maximum of modularity is reached (Blondel et al. 2008). Required algorithms were implemented in PHP and Java. JGraphT (Naveh 2003) was used to represent graphs. MySQL was used for data management.

Cluster Assessment. Health IT faces various threats, for instance, intentional and unintentional disclosure or manipulation of information through insiders or outsiders, user errors, maintenance errors, software failures, or hardware failures as well as environmental threats (Dehling and Sunyaev 2014b, Greg Goth 2012, Kotz 2011, Shahri and Ismail 2012). If such threats materialize, users will be in harms' way. Based on extant research on information security and privacy in health care (Appari and Johnson 2010, Appelbaum 2002, Barrows and Clayton 1996, Gritzalis 1998, Johnson 2009, Kotz 2011, Rindfleisch 1997, Rohm and Milne 2004, Rothstein and Talbott 2007, Shea 1994), we assess information security and privacy implications according to five characteristics: (1) health specificity of information available to apps, (2) potential damage through information leaks, (3) potential damage through information manipulation (change), (4) potential damage through information loss, and (5) potential value of information to third parties (Table 7). Cluster assessment is focused on risks specific to mHealth apps. Hence, risks associated with information ordinarily available to apps (Egele et al. 2011, Enck et al. 2011), like location information or device identifier, do not contribute to a more grave assessment.

Characteristic-1, health specificity of information available to apps, assesses whether the app has access to medical user information, access to other non-standard information, or only access to standard information ordinarily available to apps like location information or device identifiers (Egele et al. 2011, Enck et al. 2011). Characteristic-2 assesses the potential damage through information leaks, which can be classified as

Table 7. Cluster assessment characteristics.

#	Name	Definition	Possible values
1	Specificity	Health specificity of information available to apps (eg, phone identifiers, eating habits, disease history)	standard, non-standard, medical
2	Leaks	Potential damage through leaks of information (eg, embarrassment, lessened employment prospects)	none, low, high
3	Change	Potential damage through manipulation (change) of information. (eg, treatment errors)	none, low, high
4	Loss	Potential damage through loss of information (eg, loss of information important for treatment)	none, low, high
5	Value	Value of information to third parties (eg, medical identity theft, selection of employees)	none, low, high

none, low, or high. Depending on offered functionality, health IT has access to information with low sensitivity like users' height, weight, or common past illnesses and treatments like a cough or broken bones (Rindfleisch 1997, Rohm and Milne 2004). Other health IT offerings have however access to information with high sensitivity like abortions, mental illness, sexually transmitted diseases, HIV status, substance abuse, or genetic predispositions to disease (Johnson 2009, Milne et al. 2004, Rindfleisch 1997). Leaks of such information increase the likelihood of potential damage to users through socio-economic repercussions (Appari and Johnson 2010), embarrassment or damage of reputation (Appelbaum 2002, Gritzalis 1998, Johnson 2009, Kotz 2011, Rindfleisch 1997, Rohm and Milne 2004), social stigma (Appelbaum 2002), loss of affection or respect of family members (Shea 1994), monetary repercussions through medical fraud (billing for treatments never rendered) or medical identity theft (obtainment of medical services with a fake medical identity) (Appari and Johnson 2010, Johnson 2009, Kotz 2011), more expensive insurance coverage or problems to obtain insurance coverage (Appelbaum 2002, Barrows and Clayton 1996, Rindfleisch 1997, Rohm and Milne 2004, Shea 1994), or lessened employment possibilities (Appelbaum 2002, Kotz 2011, Rindfleisch 1997, Rohm and Milne 2004, Shea 1994). Characteristic-3 assesses potential damage through information manipulation (change), possible values are none, low, or high. Potential damage through information manipulation was, for instance, assessed as low for information on eating patterns or past workouts. Manipulation of such information is inconvenient and undesirable but poses only low potential damage. Potential damage through information manipulation was assessed as high for apps where information manipulation causes greater harm to users. If, for example, erroneous information is added to users' information due to medical fraud, medical identity theft, negligence, malicious intent, or other threats, treatment can be based on erroneous information (Johnson 2009, Kotz 2011). In addition, users' quality of care is affected, potential for harm to health or death is increased, and later efforts to obtain medical, life, or disability insurance are impeded (Appari and Johnson 2010, Gritzalis 1998, Johnson 2009, Kotz 2011). Potential damage through loss of information is assessed with characteristic-4, possible values are none, low, or high. Loss of uncritical information or information that can be restored was assessed as low. Loss of information was assessed as high in cases where, for instance, important information required for users' care is no longer available (Appelbaum 2002, Gritzalis 1998, Rindfleisch 1997). Finally, the potential value of information for third parties is assessed by characteristic-5, possible values are none, low, or high. If apps have access to information valuable to third parties, infringements of information security and privacy are more likely because they are more rewarding for third parties. For mHealth apps that have only access to information commonly available to mobile apps value was assessed as none. Value was assessed as low for collected information that is not directly useful to third parties, like unspecific information or information not attributable to users. On the other hand, information like insurance policy information, government identity numbers, date of birth, or social security numbers is highly valuable to third parties; for instance, to commit medical identity theft or medical fraud (Johnson 2009, Kotz 2011, Rindfleisch 1997). Further uses of others' private medical information that are not in the best interest of the data subject include the selling of medical information of celebrities (Rindfleisch 1997), better fitting of insurance policies to insurees' risks and selection of insurees (Barrows and Clayton 1996, Rindfleisch 1997, Rothstein and Talbott 2007), selection of healthy employees (Barrows and Clayton 1996, Kotz 2011, Rindfleisch 1997, Rothstein and Talbott 2007), or targeted marketing (Barrows and Clayton 1996, Rindfleisch 1997, Rohm and Milne 2004).

Two researchers assessed all discovered clusters. To maintain a consistent interpretation of clusters during assessment, each rater annotated each cluster with a short description based on connotation and prevalence of tags assigned to the cluster. These descriptions were verified through comparison to apps contained in the respective cluster. Subsequently, clusters were assessed according to the five characteristics addressing information security and privacy implications. Reliability assessment with Janson's and Olsson's ı, an multivariate extension of Cohen's κ for multiple judges on the same scale (Janson and Olsson 2001), led to a 'substantial' (Landis and Koch 1977) agreement score of ı=0.71. All remaining differences were resolved by discussion; if necessary, a third researcher was consulted for dispute resolution.

In a final aggregation step, mHealth app archetypes (AT) with respect to information security and privacy are identified by grouping clusters with identical assessments. An archetype is "the original pattern or model of which all things of the same type are representations or copies" (Merriam-Webster 2014). Hence, archetypes constitute underlying or core conceptions of objects observed in the real world. Real-world representations of archetypes may however materialize in different forms. For example, from an information security and privacy perspective, a medication reminder as well as a patient interaction app are real-world representations of the same archetype: They both have access to sensitive medical information that should not be leaked to third parties, must remain accurate, and is of value to third parties; yet, there is only a low demand for data preservation: Medication reminders only need to store information until they reminded the user to take her medication and patient interaction apps only need to store the data until the interaction happened. Identification of mHealth app archetypes with respect to information security and privacy establishes thus a graspable overview of the thousands of mHealth apps offered in the app stores. To foster interpretability of app archetypes, identified app archetypes are numbered and additionally characterized by a natural language descriptor. The medication reminder and patient interaction app from the previous example are for instance both representations of the archetype AT-11 (Treatment Reminders). Due to the large diversity of possible real-world representations of mHealth app archetypes, it is unfeasible to identify meaningful descriptors capturing all facets of functionality offered by real-world archetype representations. The final descriptors were determined in group discussions of the authors. Hence, the archetype descriptors characterize exemplary functionality of real-world representations to foster archetype interpretability.

3.3 Results

3.3.1 Discovered Apps

We discovered a total of 37,246 apps (iOS: 32,614; Android: 4,632) in the categories Medical and Health & Fitness (Figure 9). After automatic tagging 34.48% of apps (12,841; iOS: 32.69% (10,661); Android: 47.06 % (2,180)) were excluded from further assessment. The ratio of iOS mHealth apps to Android mHealth apps is 8.95 (21,953 to 2,452).

In both stores users rate apps on 5-star integer rating scales, ranging from 1 to 5 stars. Mean rating scores of rated iOS and Android mHealth apps are 3.1 (MEDIAN=3, SD=1.01) and 3.7 (MEDIAN=3.92, SD=1.08), respectively. Figure 10 and Figure 11 illustrate app ratings and rating counts in more detail. 81.36% (17,860) of iOS and 76.14% (1,867) of Android apps have been rated less than 10 times. 75.76% (16,631) of iOS and 42.37% (1,039) of Android apps have not been rated. 1.38% (302) of iOS and 1.55% (38) of Android apps have been rated more than 1,000 times. 39.36% (2,095) of rated iOS apps are rated four stars or more and 27.85% (1,482) of rated iOS apps are rated two stars or less. On Android, 64.83% (916) of rated apps are rated four stars or more and 14.23% (201) of rated apps are rated two stars or less. As illustrated in Figure 10, Android mHealth apps are rated higher than iOS mHealth apps (Mann Whitney U(6,733)=2,592,190; P<.001; r=0.31;CI(95%)=[0.99997,0.99998]). App category has no significant influence on app rating (iOS: Mann Whitney U(5,320)=3,516,696; P=.92; r=0.002; Android: Mann Whitney U(1411)=203,559.5; P=.13; r=0.05).

For Android apps, rating count and download count are strongly positively correlated (Spearman ρ=0.89, n=2,452, P<.001) indicating that rating count is a good proxy for download count (Figure 12).

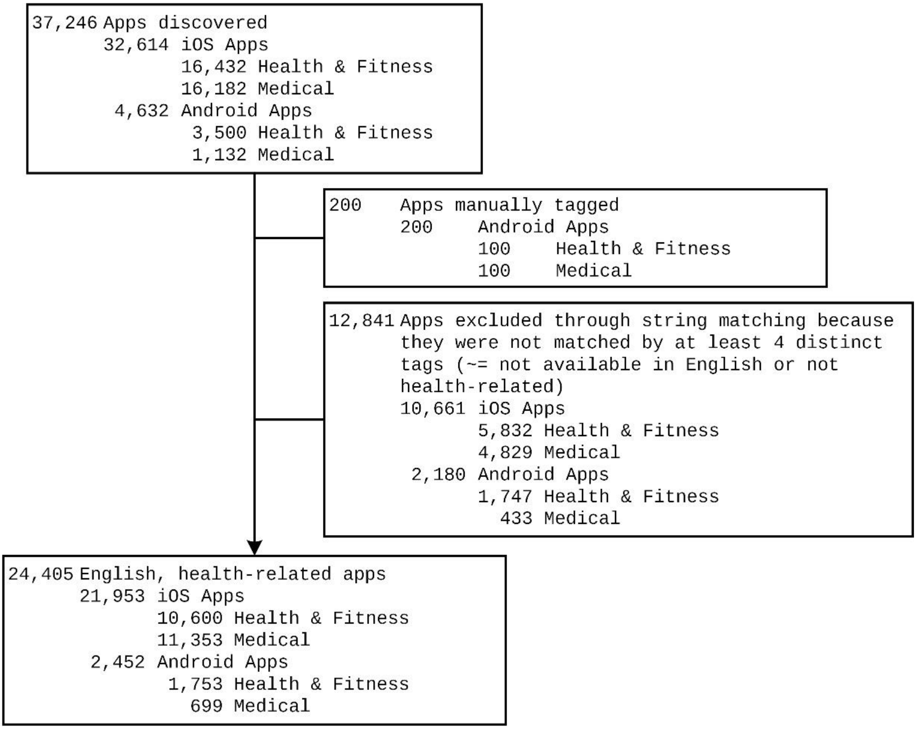


Figure 9. Flow chart of app selection.

3.3.2 App Clustering

Application of the Louvain Method (Blondel et al. 2008) grouped the 24,405 apps applicable for clustering into 245 distinct clusters with a modularity score of 0.47, which indicates a good division of the graph (Newman 2004, Newman and Girvan 2004). Discovered clusters have a mean size of 99.6 apps (MIN=2; MAX=910; MEDIAN=90; SD=113.6). 28.6% (70) of clusters containing 26.33% (6,426) of apps conveyed no information relevant to our research scope and were excluded from further assessment. Some clusters are for instance too ambiguous because contained apps match mainly a single tag (eg, ‘pain’ or ‘care giver’) that is uninformative on its own with respect to our research scope. Cluster assessment according to the five characteristics led to further consolidation of the 175 informative clusters into 12 app archetypes grouping clusters with identical characteristic assessments. The 12 app archetypes have a mean size of 14.6 clusters (MIN=3; MAX=58; MEDIAN=8; SD=4.6) and 1,498.25 apps (MIN=60; MAX=5,603; MEDIAN=615; SD=506.18). Figure 13 outlines the clustering process.

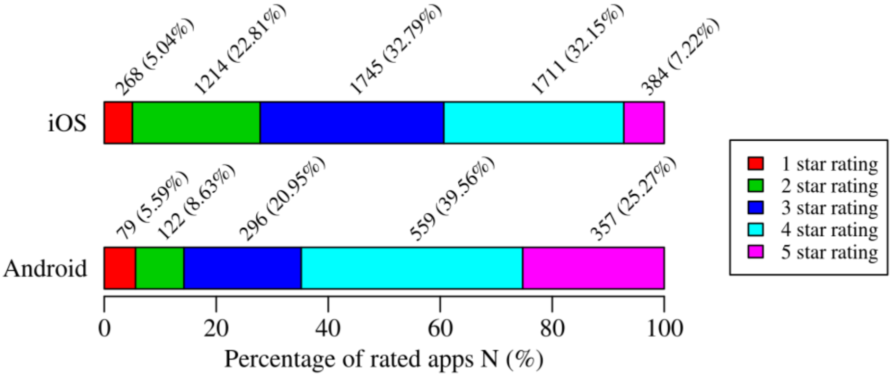


Figure 10. Rating of rated mHealth apps by store.

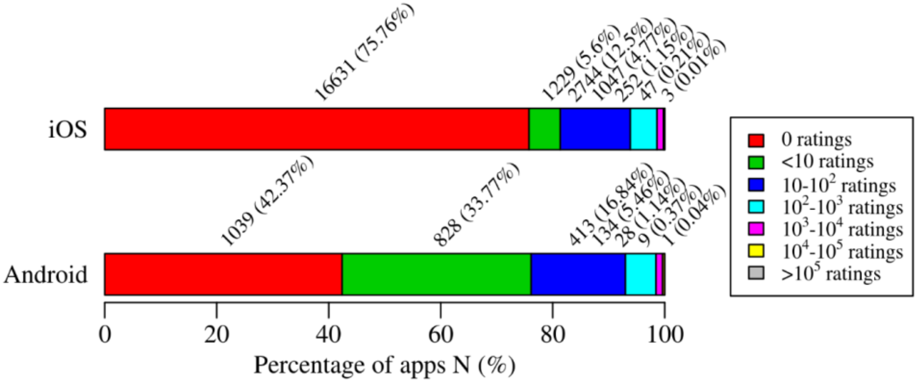


Figure 11. Rating count of mHealth apps by store. Number of ratings increases from left to right.

Table 8 provides an overview of the cluster assessments with respect to health specificity of information, potential damage through leaks, manipulation, or loss of information, and value of collected information to third parties. Medical information is available to apps in 33.1% (58) of clusters. 16.6% (29) of clusters have access to information not available to ordinary apps (Egele et al. 2011, Enck et al. 2011) and apps in 50.3% (88) of clusters do not have access to more information than ordinary apps. Apps in 76.6% (134) of clusters have no or low potential damage through leaks of information. 39.4% (69) of clusters are comprised of apps with high potential damage through manipulation of information. There is no potential damage through loss of information in 67.4% (118) of clusters. 77.7% (136) of clusters consist of apps that have only access to information with no or low value for third parties.

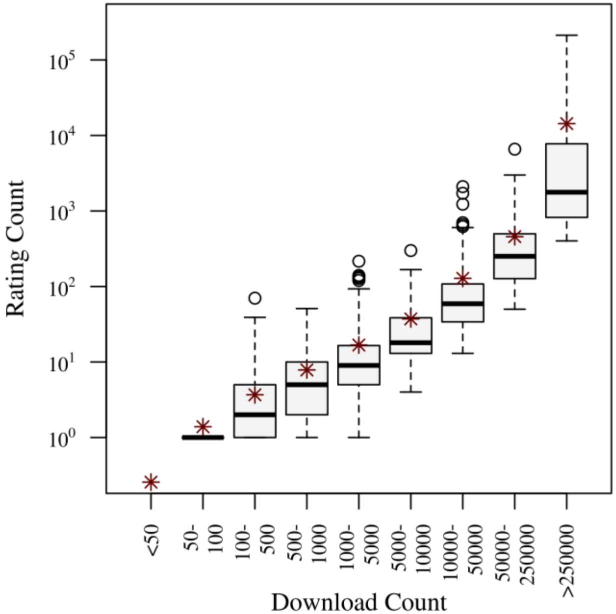


Figure 12. Boxplot of Android app rating count (log-scaled) and download count. Mean values are indicated with asterisks.

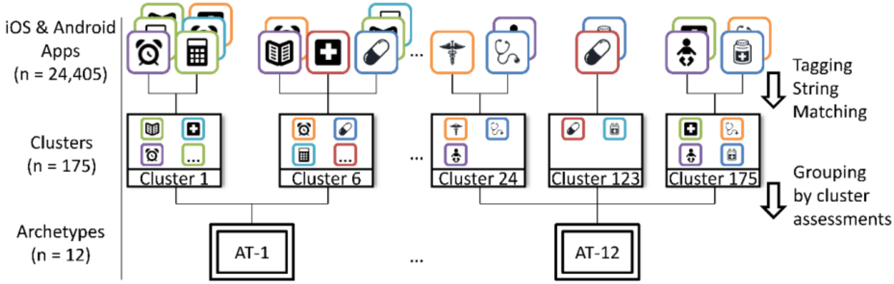


Figure 13. Outline of clustering process.

Archetype descriptors and examples for functionality offered by apps of the different app archetypes are listed in Table 9. Table 10 illustrates the twelve discovered app archetypes with distinct value combinations according to the five characteristics. AT-1 (Casual Tools) represents 5.1% (9) of clusters and 4.37% (786) of apps. Apps of AT-1 only have access to information also available to ordinary apps and provide no critical

Table 8. Cluster assessments with respect to the five information security and privacy characteristics.

		Clusters %[a] (n)	**Apps %[a] (n)**
1 – Specificity[b]	standard[c]	50.3% (88)	47.07% (8463)
	non-standard[d]	16.6% (29)	27.47% (4939)
	medical[e]	33.1% (58)	25.46% (4577)
2 – Leaks[f]	none	50.3% (88)	47.07% (8463)
	low	26.3% (46)	33.36% (5998)
	high	23.4% (41)	19.57% (3518)
3 – Change[g]	none	5.1% (9)	4.37% (786)
	low	55.4% (97)	64.75% (11641)
	high	39.4% (69)	30.88% (5552)
4 – Loss[h]	none	67.4% (118)	55.89% (10049)
	low	18.3% (32)	32.44% (5832)
	high	14.3% (25)	11.67% (2098)
5 – Value[i]	none	50.3% (88)	47.07% (8463)
	low	27.4% (48)	33.97% (6108)
	high	22.3% (39)	18.96% (3408)

[a] *Uninformative clusters are not included in percentages.*
[b] *Health specificity of information available to apps*
[c] *Apps only have access to information ordinarily available to apps (eg, phone identifiers or location information)*
[d] *Apps have access to information not ordinarily available to apps but no access to medical information (eg, workout history or eating habits)*
[e] *Apps have access to medical information (eg, disease history or insurance information)*
[f] *Potential damage through leaks of information (eg, embarrassment, lessened employment possibilities)*
[g] *Potential damage through manipulation (change) of information (eg, treatment based on erroneous information)*
[h] *Potential damage through loss of information (eg, loss of information important for treatment)*
[i] *Value of information to third parties (eg, medical identity theft, selection of employees)*

functionality so that their use cannot cause more damage than the use of any other app. Apps of AT-1 offer mostly generic information and are only marginally health-related. AT-2 (Common Knowledge Providers) is the archetype with the most representations in our sample (33.1% (58) of clusters, 31.16% (5,603) of apps). Apps of AT-2 also have no access to other information than ordinary apps so that there is no damage through leaks or loss of information. Apps of AT-2 have low potential damage through manipulation of information. More critical information is provided by apps of AT-3 (Treatment Guides), which provide information directly relevant for (self-)treatment or intended to guide users in emergency situations. Information provided by apps of AT-3 needs to be correct to serve as reliable foundation for (self-)treatment decisions; accidental or malicious provision of erroneous information promotes wrong or counterproductive treatment decisions. AT-3 represents 12% (21) of clusters and 11.54% (2,074) of apps. AT-4 and AT-5 (Fitness Ad-Hoc Tools and Fitness Trackers; 16% (28) of clusters, 26.8% (4,818) of apps) have access to more information than ordinary apps. Yet, they do not collect medical information so that there is at most low potential damage because collected information

Table 9. Exemplary functionality of apps represented by the app archetypes (AT).

Archetype	Descriptor	Exemplary kinds of contained apps
AT-1	Casual Tools	life improvement guides; mosquito repellents; brain fitness trainer
AT-2	Common Knowledge Providers	information provision for education; alarm clocks; fitness guides
AT-3	Treatment Guides	first aid guides; home remedy guides; medication guides
AT-4	Fitness Ad-Hoc Tools	diet calculators; weight control calculators; fitness calculators
AT-5	Fitness Trackers	workout tracker; smoking cessation tools; diet tracker
AT-6	Treatment Support Tools	diabetes calculators; dosage calculators; diagnosis support tools
AT-7	Intimate Ad-Hoc Tools	fertility calculators; pregnancy calculators; physician finder
AT-8	State of Health Tests	acuity tests; color vision tests; blood alcohol calculators
AT-9	Intimate Trackers	menstruation, intercourse, fertility, and pregnancy tracker
AT-10	Health Monitors	heart rate monitors; disease counseling; tools for blood test analysis
AT-11	Treatment Reminders	medication reminder; patient interaction and communities
AT-12	Health Records	health/emergency records; disease management; medication tracker

is not sensitive, not crucial for provision of medical services, not important for future endeavors, and not valuable to third parties. The remaining seven app archetypes collect medical information (33.1% (59) of clusters, 26.13% (4,698) of apps). AT-6 (Treatment Support Tools) is the only app archetype that collects medical information and has low potential damage through leaks of information. AT-6 represents calculators and tools for medical professionals or tools offering very specific functionality so that collected information is either not attributable to patients or not informative. Hence, there is only low potential damage through leaks of information and low value of information to third parties. AT-3 (Treatment Guides), AT-6 (Treatment Support Tools), AT-10 (Health Monitors), AT-11 (Treatment Reminders), and AT-12 (Health Records) offer functionality directly relevant for treatment or decision making so that there is high potential damage through information manipulation. Four app archetypes (AT-8 (State of Health Tests), AT-10 (Health Monitors), AT-11 (Treatment Reminders), and AT-12 (Health Records)) collect medical information detailed enough to be of high value to third parties (eg, blood test results, medication histories, or health records). While the other app archetypes do not require long storage times of collected information, AT-12 (Health Records) collects medical information relevant for future decision making (eg, disease management records, medication history, or health records) so that potential damage through loss of information is high. Since apps of AT-12 also tend to collect very detailed, personal information, potential damage through leaks or manipulation and value of information to third parties is high as well.

Table 10. App archetypes (AT) with respective assessments of the five information security and privacy characteristics and contained clusters and apps.

AT	Specificity[a]	Leaks[e]	Change[f]	Loss[g]	Value[h]	Clusters % (n)	Apps % (n)
1	standard[b]	none	none	none	none	5.1% (9)	4.37%(786)
2	standard	none	low	none	none	33.1% (58)	31.16% (5603)
3	standard	none	high	none	none	12.0% (21)	11.54% (2074)
4	non-standard[c]	low	low	none	low	4.0% (7)	1.20% (216)
5	non-standard	low	low	low	low	12.0% (21)	25.60% (4602)
6	medical[d]	low	high	none	low	7.4% (13)	3.17% (570)
7	medical	high	low	none	low	1.7% (3)	0.33% (60)
8	medical	high	low	none	high	2.3% (4)	2.78% (500)
9	medical	high	low	low	low	2.3% (4)	3.67% (660)
10	medical	high	high	none	high	1.7% (3)	1.33% (240)
11	medical	high	high	low	high	4.0% (7)	3.17% (570)
12	medical	high	high	high	high	14.3% (25)	11.67% (2098)

[a] Health specificity of information available to apps
[b] Apps only have access to information ordinarily available to apps (eg, phone identifiers or location information)
[c] Apps have access to information not ordinarily available to apps but no access to medical information (eg, workout history or eating habits)
[d] Apps have access to medical information (eg, disease history or insurance information)
[e] Potential damage through leaks of information (eg, embarrassment, lessened employment possibilities)
[f] Potential damage through manipulation (change) of information (eg, treatment based on erroneous information)
[g] Potential damage through loss of information (eg, loss of information important for treatment)
[h] Value of information to third parties (eg, medical identity theft, selection of employees)

3.4 Discussion

3.4.1 Principal Results

Discovered Apps. Since their inception in 2008, the iOS and Android app stores underwent a rapid development. After a few years, the app portfolios of both stores encompass hundreds of thousands of apps (d'Heureuse et al. 2012, Liccardi et al. 2013, Viennot et al. 2014) which include thousands of mHealth apps. However, absence or scarceness of ratings for 81.36% of iOS and 76.14% of Android apps indicates that over three quarters of mHealth apps are not in widespread use. A fraction of users who download apps provide ratings (Girardello and Michahelles 2010, Khalid et al. 2015). Hence, apps less often rated are likely to be less often used than more often rated apps. An explanation for this is the increased visibility of better-rated apps (Pagano and Maalej 2013): Apps with higher and more ratings are more prominently displayed in app stores and thus more likely to be discovered by potential users. More ratings make the resulting app assessment also more reliable, which attracts more users. Furthermore, many apps offer similar or competing functionality (eg, calculation of the body mass index, tracking of workouts, or prediction of date of birth) so that only a few first-movers, heavily promoted apps, or high quality apps will gain a large user base. App ratings indicate that most users are not dissatisfied with rated apps: 72.16% of iOS and 85.78% of Android apps are rated average or above. Another impediment for more widespread use of mHealth apps might be users' concerns about information security and privacy implications (Khalid et al. 2015). Our cluster analysis of mHealth apps sheds some light on the potential damage through information security and privacy infringements.

App Clustering. Since mHealth apps usually offer functionality related to users' health, it is not a surprising finding that information security and privacy infringements cause potential damage for the majority of apps (94.9% of clusters, 95.63% of apps). mHealth apps offer however diverse functionality so that potential for damage through information security and privacy infringements differs. Manipulation of information is a threat common to most mHealth apps (94.9% of clusters; 95.63% of apps). Even apps that do not collect any medical information, like AT-2 (Common Knowledge Providers) or AT-3 (Treatment Guides), must ensure that information they provide is correct and stays correct because, at least, some users will act on offered information and base (self-)treatment decisions on provided information. Apps offering information or functionality directly relevant for treatment or care must especially ensure that offered information is not accidentally or maliciously manipulated. mHealth apps that only provide information have however no information security and privacy implications through leaks or loss of collected information since no information is collected. About one half of the apps in our sample (50.2% of clusters; 47.07% of apps) only provide information. Such apps are probably the most 'pleasant' apps when it comes to protecting information security and privacy since no user-collected information must be protected. Thus, providers can focus on protection of integrity of information in rest and during transport as well as offering accurate information from the onset. Still, extant research shows that information provided by some apps does not concur with current evidence and recommendations or is even contradicting (Breton et al. 2011, Huckvale et al. 2012).

33.7% of clusters and 26.12% of apps have access to medical user information. All of these apps have high potential damage through information security and privacy infringements in at least one characteristic. Some apps (eg, AT-6 (Treatment Support Tools)) do not collect detailed information or information attributable to users and do not retain entered information so that there is no potential damage through loss of information, low potential damage through leaks of information, and low value of information for third parties; yet, they serve as foundation for treatment decisions (eg, appropriate medication dosage) so that there is high potential damage through manipulation of information. Other apps collect information users want to keep private (eg, AT-9 (Intimate Trackers)) so that there is high potential damage through leaks of information, but collected information is not directly relevant for treatment or state of health so that the other characteristics pose only low potential damage. Potential damage of other apps (AT-12 (Health Records)) was rated with the most critical assessment in all five characteristics since contained information is sensitive and must be kept private, has to be accurate and accessible to inform treatment decisions, and allows for misuse motivated by financial gain. Consequentially, there is no one-size-fits-all approach for ensuring information security and privacy of mHealth apps. mHealth apps offer different functionality so that they are also subject to different threats. Accordingly, measures for protection of information security and privacy must be tailored to the app to be protected (Dehling and Sunyaev 2014b).

Our identification of the twelve mHealth app archetypes elucidates information security and privacy of mHealth apps: Instead of a hazy collection comprised of the thousands of mHealth apps available in the app stores, the archetypes constitute a lucid, descriptive collection of twelve mHealth app archetypes with different information security and privacy characteristics. Future research can build on the archetypes, for instance, to prioritize information security and privacy requirements with respect to app type, devise collections of security measures ensuring sound protection of information security and privacy, analyze user perceptions of information security and privacy with respect to different kinds of apps, or to further theory and methodology for app development that takes information security and privacy implications into account. For example, potential damage through information security and privacy infringements would obviously be reduced, if apps that mainly provide information did not store any user information and focused rather on secure interoperability with specialized storage apps. An overview of app archetypes with respect to information security is also helpful for practical audiences. Associating an mHealth app of interest with the respective archetype improves for instance the understanding of perks and perils associated with app use. The overview of the archetypes alone is useful to foster user comprehension and awareness of information security and privacy implications of mHealth app use. In order to continuously benefit from mHealth apps, users must be able to make informed decisions about mHealth app adoption and use.

The apps with the most serious assessment of potential damage through information security and privacy infractions (AT-12 (Health Records); 14.3% of clusters; 11.67% of apps) may also offer the most benefits to users (Steinhubl et al. 2013). AT-12 (Health Records) represents all the different facets of health records and disease management tools (Caligtan and Dykes 2011, Dorr et al. 2007, Sunyaev 2013, Sunyaev and Chornyi 2012), which collect detailed health information allowing them to offer functionality tailored to users' needs and individual peculiarities or to provide other apps with the information required for tailoring offered functionality. Apps of AT-12 could rise to central hubs in the emerging mHealth environment if interoperability issues are solved (Chen et al. 2012, Hufnagel 2009) and information security and privacy is sufficiently addressed so that users can safely trust apps of AT-12 to protect their information (Dhopeshwarkar et al. 2012, Klasnja et al. 2009, Spiekermann 2012).

It is noteworthy that some threats are common to all kinds of mHealth apps, even those without any data collection. Users' behavior or the sole fact that a guide for stress relief or fighting depression, a support tool for hypertension, or an app providing information on cancer, chronic diseases, infertility, or incontinence is installed on a device reveals sensitive, private, or embarrassing information (Seneviratne et al. 2014). In the end, it is up to users which apps they use and what information they intend to share. To support users in this decision, it is important that they are sensitized to the risks associated with sharing private, sensitive, medical information (Bélanger and Crossler 2011, Wilson and Valacich 2012) and offered means to gauge, configure, and control information security and privacy practices of mHealth apps (Sunyaev et al. 2015, Sunyaev and Schneider 2013). Moreover, app stores need to establish processes that ensure protection of information security and privacy prior to making apps publicly accessible, at least, for apps with high potential damage and value to third parties. App developers and providers need to implement appropriate security measures to protect information security and privacy. While ease of app development, free access to helpful apps, and fast dissemination of innovations is desirable, it is imperative that these do not come at the price of lacking information security and privacy. Last but not least, experienced users, researchers, and further independent entities need to contribute as well by identifying malicious and harmful apps, publishing their findings, and eliminating sources of harm and malice.

Table 11. Overview of core findings and directions for future research.

#	Core findings
1	Less than a quarter of apps are in more or less widespread use
2	Information security and privacy infringements cause potential damage for the majority of apps
3	Information manipulation is a threat common to most mHealth apps
4	There is no one-size-fits-all approach for ensuring information security and privacy of mHealth apps
5	With respect to information security and privacy, diversity of mHealth apps can be captured with twelve archetypes

Table 12. Overview of future research directions.

#	Future research directions
1	Deepening the understanding of app design and adoption to focus development and research efforts on apps that will actually be used
2	Detailed analysis of information security and privacy for individual archetypes and their representations
3	Foster awareness for information security and privacy of mHealth apps
4	Secure interoperability of mHealth apps
5	Develop and establish means and processes for identification and retraction of mHealth apps with insufficient level of protection before they are publicly accessible

3.4.2 Limitations

Since we established a broad overview of available mHealth apps and assessed all discovered apps fitting our selection criteria, it was unfeasible to install and test all apps so that we focused on the information provided in app stores. This is however a common approach (eg, Breton et al. 2011, d'Heureuse et al. 2012, Rosser and Eccleston 2011, West et al. 2012), which allowed us to analyze a large sample of over 30,000 apps. Moreover, we cannot ascertain how many of the English apps available on the Android app store we discovered because the app store offers no complete listing of available apps and search results are limited to 500 apps. Extant reviews of apps in all categories offered in the Android app store report around 20,000 apps offered in the categories Medial and Health & Fitness. However, these reviews collected apps independent of language and did not assess whether the apps actually offer functionality fitting the categories Medical or Health & Fitness. Our diverse wordlist, comprised of 111,632 distinct words and phrases, introduced diversity to search queries and led to the discovery of a wide array of apps while avoiding bias towards specific types of apps. Creation of search strings based on English words favored discovery of apps offered in English. While this may have reduced the number of discovered Android apps, it suits our research approach and objectives because apps not-available in English were excluded from further assessment. Nevertheless, the reported difference in number of apps available on iOS and Android should be treated with care. For now the iOS and Android app stores offer far more apps than any other app store (d'Heureuse et al. 2012). The dominant position of iOS and Android supports our focus on the iOS and Android app store.

3.4.3 Conclusions

The iOS and Android app stores offer a wide selection of mHealth apps. Analysis of rating counts indicates however that less than a quarter of available apps are in more or less widespread use. One of the issues impeding app dissemination might be users' information security and privacy concerns (Khalid et al. 2015). Our cluster analysis shows that most mHealth apps require access to sensitive personal information or offer other services potentially impacting users' treatment or state of health, which increases the potential damage through information security and privacy infringements. The diversity of mHealth apps prevents however a one-size-fits-all approach to ensuring information security and privacy of mHealth apps. To address arising challenges, app providers, developers, stores as well as users must be sensitized to potential threats and further research and development efforts are required to facilitate protection from information security and privacy infringements. It would be undesirable to diminish or undermine the promising potential of mHealth apps to transform and improve the health care environment (Steinhubl et al. 2013) through lacking attention to information security and privacy.

3.5 Acknowledgements

Required computing resources were provided by the Regional Computing Center of the University of Cologne.

3.6 Author Contributions

AS, SS, and TD conceived of the project. AS, FG, and TD wrote the manuscript. Data acquisition and analysis were conducted by FG, SS, and TD. TD performed the statistical analyses. SS and TD implemented required custom software. All authors were responsible for research concept and design, critical revision of the manuscript, and approved the final version.

3.7 Abbreviations

app: application
AT: app archetype
HTML: Hyper Text Markup Language
IT: information technology
mHealth: mobile health

3.8 References

Abroms LC, Padmanabhan N, Thaweethai L, Phillips T (2011) iPhone Apps for Smoking Cessation: A Content Analysis. American Journal of Preventive Medicine 40(3):279–285.

Anderson CL, Agarwal R (2011) The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. Information Systems Research 22(3):469–490.

android-market-api (2014) android-market-api. Retrieved (February 2, 2014), http://code.google.com/p/android-market-api . Archived at: http://www.webcitation.org/6NNh225JS.

Anthes G (2012) HTML5 Leads a Web Revolution. Communications of the ACM 55(7):16–17.

Appari A, Johnson ME (2010) Information Security and Privacy in Healthcare: Current State of Research. International Journal of Internet and Enterprise Management 6(4):279–314.

Appelbaum PS (2002) Privacy in Psychiatric Treatment: Threats and Responses. The American Journal of Psychiatry 159(11):1809–1818.

Apple (2014) Apple iTunes App Store. Retrieved (February 14, 2014), https://itunes.apple.com/us/genre/ios/id36?mt=8.

Avancha S, Baxi A, Kotz D (2012) Privacy in Mobile Technology for Personal Healthcare. ACM Computing Surveys 45(1):3:1–3:54.

Barak A, Klein B, Proudfoot JG (2009) Defining Internet-Supported Therapeutic Interventions. Annals of Behavioral Medicine 38(1):4–17.

Barrows RC, Clayton PD (1996) Privacy, Confidentiality, and Electronic Medical Records. Journal of the American Medical Informatics Associations 3(2):139–148.

Bélanger F, Crossler RE (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly 35(4):1017–1041.

Bender LJ, Yue KRY, To JM, Deacken L, Jadad RA (2013) A Lot of Action, But Not in the Right Direction: Systematic Review and Content Analysis of Smartphone Applications for the Prevention, Detection, and Management of Cancer. Journal of Medical Internet Research 15(12):e287.

Bierbrier R, Lo V, Wu CR (2014) Evaluation of the Accuracy of Smartphone Medical Calculation Apps. Journal of Medical Internet Research 16(2):e32.

Blondel VD, Guillaume JL, Lambiotte R, Lefebvre E (2008) Fast Unfolding of Communities in Large Networks. Journal of Statistical Mechanics: Theory and Experiment 2008(10):P10008.

Breton ER, Fuemmeler BF, Abroms LC (2011) Weight Loss-There is an App for That! But does it Adhere to Evidence-Informed Practices? Translational Behavioral Medicine 1(4):523–529.

Caligtan CA, Dykes PC (2011) Electronic Health Records and Personal Health Records. Seminars in Oncology Nursing 27(3):218–228.

Chen C, Haddad D, Selsky J, Hoffman JE, Kravitz RL, Estrin DE, Sim I (2012) Making Sense of Mobile Health Data: An Open Architecture to Improve Individual- and Population-Level Health. Journal of Medical Internet Research 14(4):e112.

Chin E, Felt AP, Greenwood K, Wagner D (2011) Analyzing Inter-Application Communication in Android. Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services. MobiSys '11. (ACM, Washington, DC, USA), 239–252.

Chomutare T, Fernandez-Luque L, Arsand E, Hartvigsen G (2011) Features of Mobile Diabetes Applications: Review of the Literature and Analysis of Current Applications Compared Against Evidence-Based Guidelines. Journal of Medical Internet Research 13(3):e65.

Collins F (2012) The Real Promise of Mobile Health Apps. Scientific American 307(1).

Dehling T, Sunyaev A (2014) Secure Provision of Patient-Centered Health Information Technology Services in Public Networks—Leveraging Security and Privacy Features Provided by the German Nationwide Health Information Technology Infrastructure. Electronic Markets 24(2):89–99.

Dhopeshwarkar RV, Kern LM, O'Donnell HC, Edwards AM, Kaushal R (2012) Health Care Consumers' Preferences Around Health Information Exchange. The Annals of Family Medicine 10(5):428–434.

Donker T, Petrie K, Proudfoot J, Clarke J, Birch MR, Christensen H (2013) Smartphones for Smarter Delivery of Mental Health Programs: A Systematic Review. Journal of Medical Internet Research 15(11):e247.

Dorr D, Bonner LM, Cohen AN, Shoai RS, Perrin R, Chaney E, Young AS (2007) Informatics Systems to Promote Improved Care for Chronic Illness: A Literature Review. Journal of the American Medical Informatics Association 14(2):156–163.

Egele M, Kruegel C, Kirda E, Vigna G (2011) PiOS: Detecting Privacy Leaks in iOS Applications. Proceedings of the Network and Distributed System Security Symposium (NDSS 2011). (The Internet Society, San Diego, CA, USA).

Enck W, Octeau D, McDaniel P, Chaudhuri S (2011) A Study of Android Application Security. Proceedings of the 20th USENIX Conference on Security. SEC'11. (USENIX Association, Berkeley, CA, USA), 21–21.

Estrin D, Sim I (2010) Open mHealth Architecture: An Engine for Health Care Innovation. Science 330(6005):759–760.

European Commision (2012) Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation) (Brussels, Belgium).

Faro S, Lecroq T (2012) Twenty Years of Bit-Parallelism in String Matching. Holub J, Watson BW, Žďárek J, eds. Festschrift for Bořivoj Melichar. (Prague Stringology Club, Prague, Czech Republic), 72–101.

Food and Drug Administration (2013) Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff (Food and Drug Administration).

Freifeld CC, Chunara R, Mekaru SR, Chan EH, Kass-Hout T, Ayala Iacucci A, Brownstein JS (2010) Participatory Epidemiology: Use of Mobile Phones for Community-Based Health Reporting. PLOS Medicine 7(12):e1000376.

Girardello A, Michahelles F (2010) Explicit and Implicit Ratings for Mobile Applications. Fähnrich KP, Franczyk B, eds. Informatik 2010. LNI. (GI, Leipzig, Germany), 606–612.

Google (2014) Google Play App Store. Retrieved (February 14, 2014), https://play.google.com/store/apps.

Goth Gregory (2012) Analyzing Medical Data. Communications of the ACM 55(6):13–15.

Goth Greg (2012) Mobile Security Issues Come to the Forefront. IEEE Internet Computing 16(3):7–9.

Gritzalis DA (1998) Enhancing Security and Improving Interoperability in Healthcare Information Systems. Medical Informatics 23(4):309–323.

Heitkötter H, Majchrzak TA, Kuchen H (2013) Cross-Platform Model-Driven Development of Mobile Applications with md2. Proceedings of the 28th Annual ACM Symposium on Applied Computing. SAC '13. (ACM, Coimbra, Portugal), 526–533.

d'Heureuse N, Huici F, Arumaithurai M, Ahmed M, Papagiannaki K, Niccolini S (2012) What's App?: A Wide-Scale Measurement Study of Smart Phone Markets. ACM SIGMOBILE. Mobile Computing and Communications Review 16(2):16–27.

Huckvale K, Car M, Morrison C, Car J (2012) Apps for Asthma Self-Management: A Systematic Assessment of Content and Tools. BMC Medicine 10(1):144.

Hufnagel SP (2009) Interoperability. Military Medicine 174(5):43–50.

Istepanian RSH, Jovanov E, Zhang YT (2004) Guest Editorial Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-Care Connectivity. IEEE Transactions on Information Technology in Biomedicine 8(4):405–414.

Jain AK (2010) Data Clustering: 50 Years Beyond K-Means. Pattern Recognition Letters 31(8):651–666.

Janson H, Olsson U (2001) A Measure of Agreement for Interval or Nominal Multivariate Observations. Educational and Psychological Measurement 61(2):277–289.

Johnson ME (2009) Data Hemorrhages in the Health-Care Sector. Dingledine R, Golle P, eds. Financial Cryptography and Data Security. Lecture Notes in Computer Science. (Springer-Verlag, Berlin, Heidelberg), 71–89.

Khalid H, Shihab E, Nagappan M, Hassan A (2015) What Do Mobile App Users Complain About? A Study on Free iOS Apps. IEEE Software 32(3):70–77.

Klasnja P, Consolvo S, Choudhury T, Beckwith R, Hightower J (2009) Exploring Privacy Concerns about Personal Sensing. Pervasive '09. (Springer, Nara, Japan), 176–183.

Kotz D (2011) A Threat Taxonomy for mHealth Privacy. 3rd International Conference on Communication Systems and Networks. (IEEE, Bangalore, India).

Kumar S, Nilsen W, Pavel M, Srivastava M (2013) Mobile Health: Revolutionizing Healthcare Through Transdisciplinary Research. IEEE Computer 46(1):28–35.

Lancichinetti A, Fortunato S (2009) Community Detection Algorithms: A Comparative Analysis. Physical Review E 80(5):056117.

Landis JR, Koch GG (1977) The Measurement of Observer Agreement for Categorical Data. Biometrics 33(1):159–174.

Lane ND, Miluzzo E, Lu H, Peebles D, Choudhury T, Campbell AT (2010) A Survey of Mobile Phone Sensing. IEEE Communications Magazine 48(9):140–150.

Lewis TL, Wyatt JC (2014) mHealth and Mobile Medical Apps: A Framework to Assess Risk and Promote Safer Use. Journal of Medical Internet Research 16(9):e210.

Liccardi I, Pato J, Weitzner DJ (2013) Improving Mobile App Selection through Transparency and Better Permission Analysis. Journal of Privacy and Confidentiality 5(2):1–55.

Liu C, Zhu Q, Holroyd KA, Seng EK (2011) Status and Trends of Mobile-Health Applications for iOS Devices: A Developer's Perspective. The Journal of Systems and Software 84(11):2022–2033.

Martínez-Pérez B, de la Torre-Díez I, López-Coronado M (2013) Mobile Health Applications for the Most Prevalent Conditions by the World Health Organization: Review and Analysis. Journal of Medical Internet Research 15(6):e120.

Martínez-Pérez B, de la Torre-Díez I, López-Coronado M, Herreros-González J (2013) Mobile Apps in Cardiology: Review. JMIR mHealth uHealth 1(2):e15.

Martínez-Pérez B, de la Torre-Díez I, López-Coronado M, Sainz-De-Abajo B (2014) Comparison of Mobile Apps for the Leading Causes of Death Among Different Income Zones: A Review of the Literature and App Stores. JMIR mHealth uHealth 2(1):e1.

Mechael PN (2009) The Case for mHealth in Developing Countries. Innovations: Technology, Governance, Globalization 4(1):103–118.

Merriam-Webster (2014) Archetype - Definition. Retrieved (July 27, 2014), http://www.merriam-webster.com/dictionary/archetype . Archived at: http://www.webcitation.org/6QdwYwRgI.

Milne GR, Rohm AJ, Bahl S (2004) Consumers' Protection of Online Privacy and Identity. Journal of Consumer Affairs 38(2):217–232.

Mojica IJ, Adams B, Nagappan M, Dienst S, Berger T, Hassan AE (2014) A Large-Scale Empirical Study on Software Reuse in Mobile Apps. IEEE Software 31(2):78–86.

Mosa AS, Yoo I, Sheets L (2012) A Systematic Review of Healthcare Applications for Smartphones. BMC Medical Informatics and Decision Making 12(1):67.

Muessig KE, Pike EC, Legrand S, Hightow-Weidman LB (2013) Mobile Phone Applications for the Care and Prevention of HIV and other Sexually Transmitted Diseases: A Review. Journal of Medical Internet Research 15(1):e1.

Muñoz RF (2010) Using Evidence-Based Internet Interventions to Reduce Health Disparities Worldwide. Journal of Medical Internet Research 12(5):e60.

Naveh B (2003) JGraphT. Retrieved (February 22, 2013), http://jgrapht.org . Archived at: http://www.webcitation.org/6NYMn4Z4V.

Newman MEJ (2003) The Structure and Function of Complex Networks. SIAM Review 45:167–256.

Newman MEJ (2004) Analysis of Weighted Networks. Physical Review E 70(5):056131.

Newman MEJ, Girvan M (2004) Finding and Evaluating Community Structure in Networks. Physical Review E 69(2):026113.

Ozdalga E, Ozdalga A, Ahuja N (2012) The Smartphone in Medicine: A Review of Current and Potential Use among Physicians and Students. Journal of Medical Internet Research 14(5):e128.

Pagano D, Maalej W (2013) User Feedback in the AppStore: An Empirical Study. Proceedings of the 21st IEEE International Conference on Requirements Engineering. (IEEE, Rio De Janeiro, Brasil), 125–134.

Pathak A, Hu YC, Zhang M (2012) Where is the Energy Spent Inside my App?: Fine Grained Energy Accounting on Smartphones with Eprof. Proceedings of the 7th ACM European Conference on Computer Systems. EuroSys '12. (ACM, Bern, Switzerland), 29–42.

Plaza I, Demarzo PMM, Herrera-Mercadal P, García-Campayo J (2013) Mindfulness-Based Mobile Applications: Literature Review and Analysis of Current Features. JMIR mHealth uHealth 1(2):e24.

Rindfleisch TC (1997) Privacy, Information Technology, and Health Care. Communications of the ACM 40(8):92–100.

Rohm AJ, Milne GR (2004) Just What the Doctor Ordered: The Role of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern. Journal of Business Research 57(9):1000–1011.

Rosser BA, Eccleston C (2011) Smartphone Applications for Pain Management. Journal of Telemedicine and Telecare 17(6):308–312.

Rothstein MA, Talbott MK (2007) Compelled Authorizations for Disclosure of Health Records: Magnitude and Implications. The American Journal of Bioethics 7(3):38–45.

Seneviratne S, Seneviratne A, Mohapatra P, Mahanti A (2014) Predicting User Traits from a Snapshot of Apps Installed on a Smartphone. SIGMOBILE Mobile Computing and Communications Review 18(2):1–8.

Shahri AB, Ismail Z (2012) A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS. Journal of Information Security 3(2):169–176.

Shea S (1994) Security Versus Access: Trade-Offs are only Part of the Story. Journal of the American Medical Informatics Association 1(4):314–315.

SIL International Linguistics Department (2014) English Wordlists. Retrieved (February 14, 2014), http://www-01.sil.org/linguistics/wordlists/english . Archived at: http://www.webcitation.org/6NS0EItXU.

Simon SR, Evans JS, Benjamin A, Delano D, Bates DW (2009) Patients' Attitudes Toward Electronic Health Information Exchange: Qualitative Study. Journal of Medical Internet Research 11(3):e30.

Spiekermann S (2012) The Challenges of Privacy by Design. Communications of the ACM 55(7):38–40.

Steinhubl SR, Muse ED, Topol EJ (2013) Can Mobile Health Technologies Transform Health Care? JAMA 310(22):2395–2396.

Sunyaev A (2013) Evaluation of Microsoft HealthVault and Google Health Personal Health Records. Health and Technology 3(1):3–10.

Sunyaev A (2014) Consumer Facing Health Care Systems. e-Service Journal 9(2):1–23.

Sunyaev A, Chornyi D (2012) Supporting Chronic Disease Care Quality: Design and Implementation of a Health Service and its Integration with Electronic Health Records. ACM Journal of Data and Information Quality 3(2):3:1-3:21.

Sunyaev A, Dehling T, Taylor PL, Mandl KD (2015) Availability and Quality of Mobile Health App Privacy Policies. Journal of the American Medical Informatics Association 22(e1):e28–e33.

Sunyaev A, Schneider S (2013) Cloud Services Certification. Communications of the ACM 56(2):33–36.

Tibély G, Kovanen L, Karsai M, Kaski K, Kertész J, Saramäki J (2011) Communities and Beyond: Mesoscopic Analysis of a Large Social Network with Complementary Methods. Physical Review E 83(5):056125.

Viennot N, Garcia E, Nieh J (2014) A Measurement Study of Google Play. Proceedings of the 2014 ACM International Conference on Measurement and Modeling of Computer Systems. SIGMETRICS '14. (ACM, Austin, TX, USA), 221–233.

Weiss GM, Lockhart JW (2012) The Impact of Personalization on Smartphone-Based Activity Recognition. Proceedings of the Activity Context Representation Workshop. (Association for the Advancement of Artificial Intelligence, Toronto, Canada), 98–104.

West JH, Hall PC, Hanson CL, Barnes MD, Giraud-Carrier C, Barrett J (2012) There's an App for That: Content Analysis of Paid Health and Fitness Apps. Journal of Medical Internet Research 14(3):e72.

Wicker SB (2012) The Loss of Location Privacy in the Cellular Age. Communications of the ACM 55(8):60–68.

Wilson DW, Valacich JS (2012) Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. Proceedings of the Thirty Third International Conference on Information Systems (ICIS 2012). (Orlando, FL, USA), paper 101.

Wolf JA, Moreau JF, Akilov O, Patton T, English JC, Ho J, Ferris LK (2013) Diagnostic Inaccuracy of Smartphone Applications for Melanoma Detection. JAMA Dermatology 149(4):422–426.

Xu H, Gupta S, Rosson MB, Carroll JM (2012) Measuring Mobile Users' Concerns for Information Privacy. Proceedings of the Thirty Third International Conference on Information Systems (ICIS 2012). (Orlando, FL, USA).

Xu Q, Erman J, Gerber A, Mao ZM, Pang J, Venkataraman S (2011) Identifying Diverse Usage Behaviors of Smartphone Apps. Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference. IMC '11. (ACM, Berlin, Germany), 329–344.

4 Availability and Quality of Mobile Health App Privacy Policies

Authors: Ali Sunyaev, Tobias Dehling, Patrick L. Taylor, Kenneth D. Mandl

Abstract: Mobile health (mHealth) customers shopping for applications (apps) should be aware of app privacy practices to make informed decisions about purchase and use. We sought to assess availability, scope, and transparency of mHealth app privacy policies on iOS and Android. Over 35,000 mHealth apps are available for iOS and Android. Of the 600 most commonly used apps, only 183 (30.5%) had privacy policies. Average length was 1755 (SD=1301) words with reading grade level of 16 (SD=2.9). Two thirds (66.1%) of privacy policies did not specifically address the app itself. Our findings show that currently mHealth developers often fail to provide app privacy policies. The privacy policies that are available do not make information privacy practices transparent to users, require college-level literacy, and are often not focused on the app itself. Further research is warranted to address why privacy policies are often absent, opaque, or irrelevant, and to find a remedy.

Keywords: mobile health, patient data privacy, privacy policy, privacy practices, mHealth

4.1 Introduction

Apple's iOS and Google's Android operating systems and associated application (app) stores, itunes.apple.com and play.google.com, are becoming the de facto global platforms for mobile Health (mHealth) (d'Heureuse et al. 2012, Istepanian et al. 2004). In summer 2014, both platforms additionally announced to roll out their own apps fostering app interoperability and offering central storage for all mHealth apps and sensors of users' devices (Apple 2014b, Google 2014b). mHealth apps leverage a wide range of embedded technology in iOS and Android devices for collecting and storing personal data, including contacts and calendars, patient-reported data, as well as information collected with cameras and sensors, including location, acceleration, audio, or orientation (Lane et al. 2010, Steinhubl et al. 2013, Weiss and Lockhart 2012). Though patients value control of their personally identifiable data (Pyper et al. 2004, Simon et al. 2009) and the Federal Trade Commission (Federal Trade Commission 2013) recommends provision of privacy policies for mobile apps, little attention has been paid to the information security and privacy policies and practices of mHealth app vendors. Though both app stores retain the right to remove apps for infringements of privacy, neither has explicit policies addressing the information security and privacy of medical information. Users choose amongst an ecosystem of substitutable mHealth apps (Mandl and Kohane 2009) and should have transparency as to which apps have privacy practices best aligned with their individual preferences. We sought to assess mHealth apps for the presence and scope of privacy policies, and what information they offer.

4.2 Methods

We surveyed (Figure 14) the most-frequently rated and thus popular English language mHealth apps in the Apple iTunes Store and the Google Play Store. App stores organize their offerings in categories (eg, Books, Games, and News). We selected apps from the Medical and Health & Fitness categories, offered in both stores in May 2013. The iOS app store lists all apps by category and offers the desired information in plain hypertext markup language (HTML), enabling us to automatically parse app information to extract data. On the other hand, the Android app store uses dynamically generated HTML pages so that the HTML texts displayed in the browser contain not much useful information, which is dynamically loaded from an underlying database. Hence, we used a third-party open-source interface, the android-market-api (http://code.google.com/p/android-market-api), for retrieving app information.

Upon initial review, many apps were not available in English, did not have an English description, or were not health-related, despite being offered in the categories Medical or Health & Fitness (eg, apps offering wallpapers). In order to exclude such apps from further assessment, we tagged all app descriptions with descriptive terms. The tags characterize health-related app functionality, access to information, and handling of information. We manually tagged 200 apps (100 Health & Fitness, 100 Medical) establishing an initial tag corpus and employed string matching (Faro and Lecroq 2012) to automatically tag the remaining apps. Apps not matched by at least four distinct tags were excluded from further assessment.

4.2.1 Discovery and Evaluation of Privacy Policies

We used a three step manual procedure for privacy policy discovery looking for typical locations of privacy policies. Privacy policies were abstracted from March 2013 to June 2013. First, we checked for a privacy policy on the app store web site for the particular app. Then, we checked the web page maintained by the developer to advertise and introduce the company and products. Finally, we reviewed the first 30 results of a Google search for the query ‘$APPNAME “privacy” “policy”’. Once a privacy policy was discovered, we omitted the remaining steps.

We surveyed the 300 most-frequently rated apps in our sample for privacy policies on the iOS as well as the Android app store. We were interested in the most commonly used apps, a property best reflected by download count. However, since only Android (and not iOS) reports download count, we instead selected apps for privacy policy assessment based on their rating count. For Android apps, rating count and download count are strongly positively correlated (Spearman ρ=0.89, $p<0.001$) indicating that rating count is a good proxy for download count.

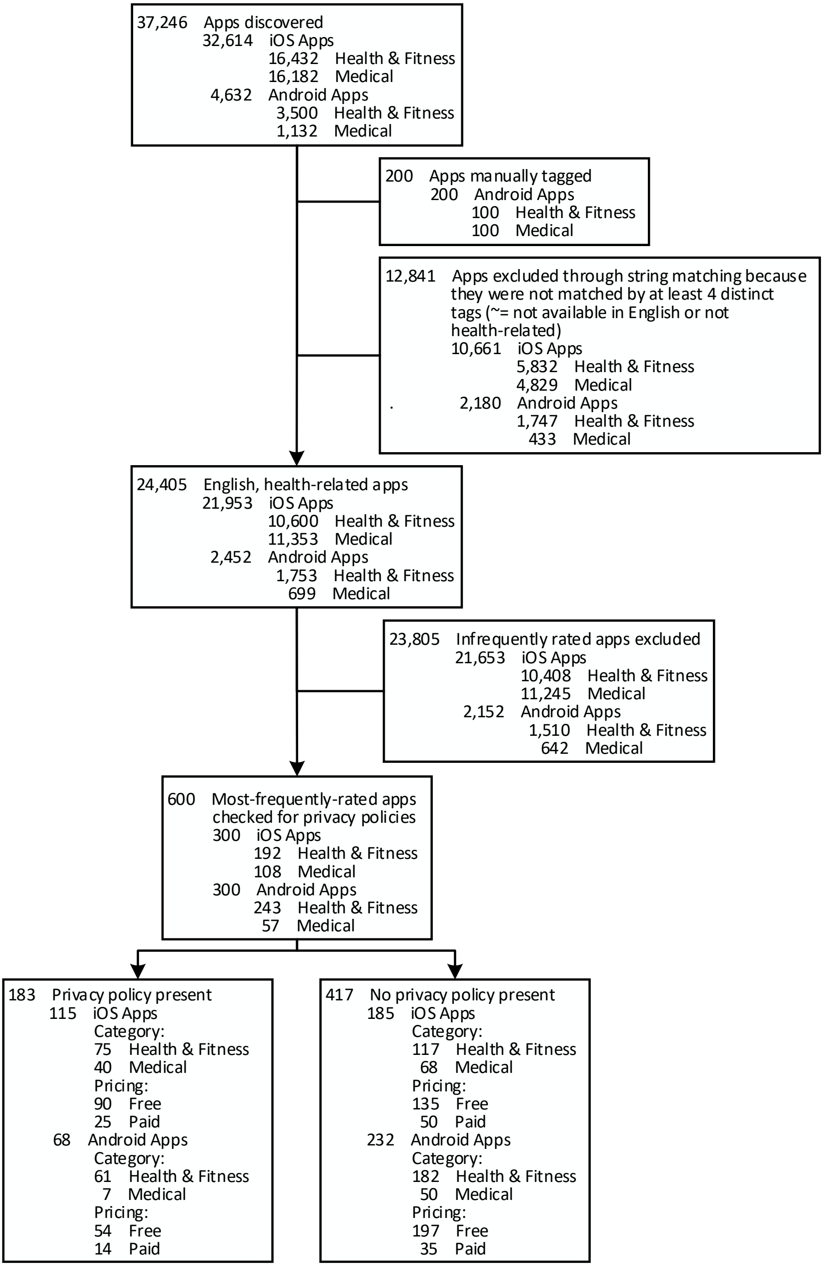


Figure 14. Flow diagram for app discovery and processing.

To identify differences in availability of privacy policies, we used independence of proportions with the Pearson chi-square. Grade-level readability was calculated as the average of the Flesh Kincaid, Gunning Fog, and SMOG formulas (Ley and Florio 1996, Walsh and Volsko 2008). Length was assessed as the number of words in the privacy policy. Two-sample Student's t-tests were used to compare privacy policy lengths. Privacy policy scope could be limited to the single app in question, apply to multiple apps, or pertain to a backend application supporting the app(s), other products and services offered by a developer, or seemingly unrelated topics. To assess transparency of privacy policies focusing on apps or backend applications, we determined whether the privacy policies address: type of information collected (operational, behavioral, sensitive), rationale for collection (app operation, personalization, secondary use), sharing of information (service provision, social interaction, third party), and user controls (supervision, notification, correction) (Ackerman et al. 1999, Antón et al. 2010, Earp et al. 2005). Privacy policies rationalizing collection of personal information on the basis of 'personalization' indicated tailoring of app functionality based on collected user information. Similarly, privacy policies were categorized as addressing collection of 'sensitive' information if they referenced street address, finances, ideological orientation, location, government identifiers, or state of health. Privacy policies enabling users to supervise information-privacy-related aspects were assessed as addressing user controls regarding 'supervision'; this includes, informing users about the limits of the privacy policy, about which app modules collect what information, or whether users are provided with access audits for shared information. Two researchers evaluated privacy policies along two axes—privacy policy scope and offered content. Reliability assessment with Janson's and Olsson's ı, an multivariate extension of Cohen's κ for multiple judges on the same scale (Janson and Olsson 2001), led to an 'almost perfect' (Landis and Koch 1977, p. 8) agreement score of ı=0.94. In the end, all differences were resolved through group discussion.

4.3 Results

Initial search identified 32614 mHealth apps in the iOS and 4632 mHealth apps in the Android app store. Tagging reduced the number of discovered apps to 21953 iOS apps and 2452 Android apps that are available in English and offer some health-related functionality (Figure 14).

4.3.1 Availability of Privacy Policies

Only 30.5% of apps had privacy policies. iOS apps were more likely to have privacy policies (38.3% vs. 22.7%, Chi Sq p<0.001, see Figure 14). Chi-square revealed no influence of app category or app pricing on the availability of privacy policies. Correlation of privacy policy availability and app rating count is weak (iOS: Spearman ρ=0.22, p<0.001; Android: Spearman ρ=0.31, p<0.001).

4.3.2 Privacy Policy Characteristics

Privacy policies have an average length of 1755 (SD=1301) words and range from 65-6424 and 17-5333 on iOS and Android, respectively. Android privacy policies are shorter (Student's t, p<0.001) with an average length of 1353 (SD=1018) words in contrast to 1991 (SD=1393) words. Privacy policies have an average reading grade level (RGL) of 16 (SD=2.9) and two discovered privacy policies have a RGL below the recommended eighth grade level (Ley and Florio 1996, Walsh and Volsko 2008). Privacy policy length and RGL have a weak positive correlation (Spearman ρ=0.31, p<0.001). Table 13 shows the scope of the privacy policies. The six different scope categories are mutually exclusive and were determined according to the scope of obtained privacy policies. Aside from initial differences in naming, privacy policy scope assessments were unanimous. 66.1% of discovered privacy policies do not focus the app, but a developer homepage, all services offered by a developer, or topics unrelated to the app.

We assessed transparency of privacy policies that focus on a backend application, multiple apps, or a single app (Table 14). Some aspects of each privacy policy content category most important to users (Ackerman et al. 1999, Antón et al. 2010, Earp et al. 2005) are addressed in over 85% of assessed privacy policies. All assessed privacy policies indicate whether information is shared with third parties. Whether sensitive information is collected is addressed in 74.2% of assessed privacy policies. Secondary use of information is addressed in 77.4% of assessed privacy policies. Information regarding supervision of information access and use is offered in 79% of assessed privacy policies. Means for notifying users about changes to privacy policies or privacy practices are mentioned in 59.7% of assessed privacy policies.

4.4 Discussion

Information privacy (Smith et al. 2011) is a highly charged concept, very subject to personal intuitions, and its right protection in the context of a purchase-sale bargain, a trade-off between sought-for personal benefits and real as well as hypothetical costs, is an open question heightened by great legal and cultural uncertainty, and lack of an organized industry policy. Privacy policies are often present as detached, legalistic documents that seem to be potentially fungible or borrowable from someone else because they are mostly incomprehensible, out-of-scope, and lacking transparency. There are

Table 13: Privacy policy scope for iOS and Android apps.

	Store	iOS N (%)	Android N (%)
Privacy Policy Scope	Single app, N (%)	4 (3.5)	10 (14.7)
	Multiple apps, N (%)	6 (5.2)	9 (13.2)
	Backend application, N (%)	21 (18.3)	12 (17.6)
	Developer homepage, N (%)	15 (13.0)	5 (7.4)
	All developer services, N (%)	55 (47.8)	27 (39.7)
	No app-related scope, N (%)	14 (12.2)	5 (7.4)

Table 14: Single, multiple, and backend application privacy policies addressing content categories important to users.

Privacy Policy Content Categories	Privacy Policies, N (%)	Privacy Policy Content Subcategories	Privacy Policies, N (%)
Type of information collected	56 (90.3)	Operational	54 (87.1)
		Behavioral	56 (90.3)
		Sensitive	46 (74.2)
Rationale for collection	59 (95.2)	App operation	41 (66.1)
		Personalization	58 (93.5)
		Secondary use	48 (77.4)
Sharing of information	62 (100.0)	Service provision	57 (91.9)
		Social interaction	34 (54.8)
		Third party	62 (100.0)
User controls	54 (87.1)	Supervision	49 (79.0)
		Notification	37 (59.7)
		Correction	32 (51.6)

neither general international standards for information a privacy policy should offer, for uses and disclosures it should permit, whether with consent or without it, nor for the rights consent can waive. Public policies that do govern private information include the California Online Privacy Protection Act of 2003 (California Business and Professions Code 2004) which requires provision of privacy policies for all online services accessible by Californian residents, and the Federal Trade Commission encourages app developers to provide privacy policies as well as just-in-time disclosures requesting consent for information collection (Federal Trade Commission 2013). Extant guidance and regulation regarding privacy policies are however abstract and limited in scope while corresponding IT offerings provide diverse functionality and are globally available.

In the domain of health information where many consumers are concerned about what happens to their private, sensitive data, our key finding is startling: Apps are being highly rated and successfully sold although privacy policies are either absent, opaque, or irrelevant. There are several possible explanations, ranging from consumers' confidence in the general legal climate to protect them even absent or despite app privacy policies, over consumers falling for the privacy paradox (Smith et al. 2011) and choosing short term benefits despite potential exposure to harm in the long term, complete misunderstanding of the extent to which such apps may compromise personal privacy, to an absence of real choice, which would be assisted by clear 'gold standards' against which consumers could compare app policies.

We assessed privacy policies of the 300 most-frequently rated apps. Still, our results show that privacy policies have poor availability rates, correlation of app ratings and privacy policy availability is weak, privacy policy scope is lacking, high reading grade levels are required to understand privacy policies, and that privacy practices are not made transparent in a comprehensive fashion. Although depending on our association of ratings with number of downloads, these results indicate that app developers seem to be competing without benefitting from protection against clear harm of failing to address information privacy or from availability and quality of privacy policies, which one might expect to be reflected in customer choice.

Many privacy policies did not focus on the app at all, and therefore were not informative for end users. On the one hand, consumers may be blissfully ignorant and more likely to use apps with unclear or difficult to find privacy policies. On the other hand, concerns about information privacy may inhibit physicians' (Dünnebeil et al. 2012) and patients' (Agaku et al. 2014) information sharing, even for patients who are willing to share for altruistic purposes (Weitzman et al. 2010).

An agreed upon community standard of not collecting personal data which is not necessary for the app's central function would go a long way toward eliminating issues. And the privacy policies should reflect use of best technical practices for designing privacy protection into mobile applications. Preventing undesirable breaches of privacy will be much more cost-efficient than remedying unwanted disclosures of private health information.

For information that does need to be collected and stored for future reference by the app, complete transparency about subsequent disclosures or sales in a standardized format, at the sixth grade reading level should be expected. Because an overwhelming amount of text is unlikely to be read by users (McDonald and Cranor 2008), a bulleted, graphical, or tabular executive summary should be provided.

Assuming that privacy policies do fill an important niche in legal protection and consumer confidence, their relative absence points to an imperfection in the market, and deserves further research on the substantive ways the market fails and on whether failure is self-correcting or would benefit from a step that places collaboration above competition, such as creation of quality standards, self-regulation, or government regulation.

4.5 Acknowledgements

Computing resources were provided by the Regional Computing Center of the University of Cologne.

4.6 Contributors

KM and AS conceived of the project. Data acquisition and analysis were conducted by TD and AS. TD and AS performed the statistical analyses and implemented required custom software. All authors wrote the manuscript, were responsible for research concept and design as well as critical revision of the manuscript, and approved the final version.

4.7 Funding

This project was supported by Strategic Health IT Advanced Research Projects Award 90TR000101 from the Office of the National Coordinator of Health Information Technology.

4.8 References

Ackerman MS, Cranor LF, Reagle J (1999) Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. 1st ACM Conference on Electronic Commerce. (ACM, Denver, CO, USA), 1–8.

Agaku IT, Adisa AO, Ayo-Yusuf OA, Connolly GN (2014) Concern About Security and Privacy, and Perceived Control over Collection and Use of Health Information are Related to Withholding of Health Information from Healthcare Providers. Journal of the American Medical Informatics Association 21(2):374–378.

Antón AI, Earp JB, Young JD (2010) How Internet Users' Privacy Concerns Have Evolved Since 2002. IEEE Security & Privacy 8(1):21–27.

Apple (2014) Health. Retrieved (July 7, 2014), http://www.apple.com/ios/ios8/health . Archived at: http://www.webcitation.org/6QtK0lqTv.

California Business and Professions Code (2004) California Online Privacy Protection Act of 2003. Business and Professions Code Sections 22575-22579. Retrieved (May 14, 2014), http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579. Archived at: http://www.webcitation.org/6Rv9DRvtC.

Dünnebeil S, Sunyaev A, Blohm I, Leimeister JM, Krcmar H (2012) Determinants of Physicians' Technology Acceptance for e-Health in Ambulatory Care. International Journal of Medical Informatics 81(11):746–760.

Earp JB, Antón AI, Aiman-Smith L, Stufflebeam WH (2005) Examining Internet Privacy Policies Within the Context of User Privacy Values. IEEE Transactions on Engineering Management 52(2):227–237.

Faro S, Lecroq T (2012) Twenty Years of Bit-Parallelism in String Matching. Holub J, Watson BW, Žďárek J, eds. Festschrift for Bořivoj Melichar. (Prague Stringology Club, Prague, Czech Republic), 72–101.

Federal Trade Commission (2013) Mobile Privacy Disclosures Building Trust Through Transparency (Federal Trade Commission).

Google (2014) The Google Fit SDK. Retrieved (July 7, 2014), https://developers.google.com/fit . Archived at: http://www.webcitation.org/6QtJkTpQE.

d'Heureuse N, Huici F, Arumaithurai M, Ahmed M, Papagiannaki K, Niccolini S (2012) What's App?: A Wide-Scale Measurement Study of Smart Phone Markets. ACM SIGMOBILE. Mobile Computing and Communications Review 16(2):16–27.

Istepanian RSH, Jovanov E, Zhang YT (2004) Guest Editorial Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-Care Connectivity. IEEE Transactions on Information Technology in Biomedicine 8(4):405–414.

Janson H, Olsson U (2001) A Measure of Agreement for Interval or Nominal Multivariate Observations. Educational and Psychological Measurement 61(2):277–289.

Landis JR, Koch GG (1977) The Measurement of Observer Agreement for Categorical Data. Biometrics 33(1):159–174.

Lane ND, Miluzzo E, Lu H, Peebles D, Choudhury T, Campbell AT (2010) A Survey of Mobile Phone Sensing. IEEE Communications Magazine 48(9):140–150.

Ley P, Florio T (1996) The Use of Readability Formulas in Health Care. Psychology, Health & Medicine 1(1):7–28.

Mandl KD, Kohane IS (2009) No Small Change for the Health Information Economy. New England Journal of Medicine 360(13):1278–1281.

McDonald AM, Cranor LF (2008) The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 4(3):540–565.

Pyper C, Amery J, Watson M, Crook C (2004) Access to Electronic Health Records in Primary Care - A Survey of Patients' Views. Medical Science Monitor 10(11):SR17-22.

Simon SR, Evans JS, Benjamin A, Delano D, Bates DW (2009) Patients' Attitudes Toward Electronic Health Information Exchange: Qualitative Study. Journal of Medical Internet Research 11(3):e30.

Smith HJ, Dinev T, Xu H (2011) Information Privacy Research: An Interdisciplinary Review. MIS Quarterly 35(4):989–1015.

Steinhubl SR, Muse ED, Topol EJ (2013) Can Mobile Health Technologies Transform Health Care? JAMA 310(22):2395–2396.

Walsh TM, Volsko TA (2008) Readability Assessment of Internet-Based Consumer Health Information. Respiratory Care 53(10):1310–1315.

Weiss GM, Lockhart JW (2012) The Impact of Personalization on Smartphone-Based Activity Recognition. Proceedings of the Activity Context Representation Workshop. (Association for the Advancement of Artificial Intelligence, Toronto, Canada), 98–104.

Weitzman ER, Kaci L, Mandl KD (2010) Sharing Medical Data for Health Research: The Early Personal Health Record Experience. Journal of Medical Internet Research 12(2):e14.

5 RECIPE: An Ontology of the Information Relevant for Organizational Information Privacy Communication

Author: Tobias Dehling

Abstract: Once information privacy invasions are perceived by the public, they have severely detrimental effects on organizational value due to losses in reputation and monetary repercussions. If consumers knew organizational information privacy practices, consumers would be enabled to select online offerings treating their information in ways that align with their preferences and needs. In this study, I aim to make communication of information privacy practices more tangible with a focus on organizational actions and services related to information privacy—that is, organizational information privacy practices. We develop an ontology of the information relevant for communication of organizational information privacy practices (RECIPE ontology). The RECIPE ontology constitutes a metaspecification of a comprehensive selection of topically relevant organizational information privacy practices and is derived from extant knowledge in research and practice. Knowledge of the information relevant for communication of organizational information privacy practices is a prerequisite for development of relevant and purposeful artifacts intended to communicate organizational information privacy practices to consumers. The RECIPE ontology supports organizations in communicating their information privacy practices to consumers and, thereby, in differentiating themselves from their competitors in a web of exchangeable consumer information systems. Hence, providers can build on the RECIPE ontology to increase their attractiveness to consumers by reducing uncertainty and increasing perceived behavioral control. Features offered by many online consumer information systems are often easily copied; substantive organizational information privacy communication is not.

Keywords: information privacy practices, ontology, organizational privacy communication, design science research

5.1 Introduction

In online environments, information privacy is a puzzling problem: Establishment, maintenance, and growth of a consumer base is a key success factor for organizations operating in online environments (Hanseth and Lyytinen 2010). In combination with surveys showing that consumers are concerned with information privacy (eg, Roeber et al. 2015, Wisniewski et al. 2016), it seems intuitive to expect that organizations' attention to information privacy is an important driver for sustainable business models in online environments. Yet, in reality, organizations are successful with superficial attention to information privacy since consumers' information privacy concerns are often outweighed by other factors like the sheer complexity of online environments, situational influences, or organizations' expertise in trimming consumers' information privacy preferences (Acquisti et al. 2015). With rising pervasiveness of internet use, organizations are gathering ever-increasing knowledge on consumers, while consumers have to rely on trust signals and past experience to find organizations likely to supply consumer information systems[5] fitting their preferences and needs, especially, with respect to the handling of their personal information (Clarke 1994, Sunyaev and Schneider 2013). The power scales are obviously tipped in favor of organizations. However, once information privacy invasions are perceived by the public they have a severely detrimental effect on organizational value, for instance, due to losses in reputation and monetary repercussions (Culnan and Williams 2009, Martin et al. 2017). From a long term perspective, it is thus in the interest of organizations to even the playing field by communicating their organizational information privacy practices to consumers (Bansal et al. 2015, Pavlou 2002). If consumers knew organizational information privacy practices, consumers would be enabled to select consumer information systems treating consumer information in a way that aligns with consumer preferences and needs and it would be possible for consumers and organizations to engage in mutually beneficial relationships (Berger and Calabrese 1975, Oulasvirta et al. 2014).

In this study, I aim to make communication of information privacy practices more tangible by focusing on organizational actions and services related to information privacy—that is, organizational information privacy practices. While organizational information privacy practices are a tangible reflection of organizational attention to information privacy, they are not tangible for consumers who cannot observe internal organizational business processes. To overcome this issue and communicate their attention to information privacy, organizations often post privacy notices—natural language descriptions of an organization's information privacy practices. A severe impediment for effective privacy notices is the absence of a clear conceptualization of the information to be provided. The only common denominator for content of privacy notices is that fair information practice principles should be addressed (Ciocchetti 2007). Fair information practice principles remain however far too abstract so that they establish only a rudimentary baseline for communication of organizational information privacy practices. In order to facilitate communication of organizational information privacy practices, the goal of this research is to answer the research question: What information should organizations communicate to consumers with respect to organizational information privacy practices in consumer information systems?

To answer the research question, we develop an ontology of the information relevant for communication of organizational information privacy practices (RECIPE ontology). An ontology is useful to inform communication of organizational information privacy

[5] Within the scope of this work, the term consumer information system refers to any socio-technical system open to consumers in which information technology is employed to process information. Consumer information systems are a suitable research context because such systems depend on voluntary use and organizations can use attention to information privacy as one potential lever to make their information systems more attractive to consumers than information systems of competitors.

practices because ontologies capture domain knowledge, enable analysis and reuse of domain knowledge, and are useful to share and communicate a common understanding (Noy and McGuinness 2001). The RECIPE ontology constitutes nomothetic design knowledge (Baskerville et al. 2015) for a class of artifacts where instantiations are virtually non-existent in today's consumer information system environments—the class of artifacts facilitating substantive communication of organizational information privacy practices. The RECIPE ontology can inform diverse undertakings concerned with communication of organizational information privacy practices (eg, design of privacy notices, specification of certification schemes, or assessments and comparisons of organizational information privacy practices). Knowledge of the information relevant for communication of organizational information privacy practices is a prerequisite for development of relevant and purposeful artifacts intended to communicate organizational information privacy practices.

I selected extant knowledge on privacy notices in research and practice as primary data source for this study because privacy notices are natural language descriptions of organizational information privacy practices and a prevalent, fundamental tool for providing the information relevant for communication of organizational information privacy practices. Although describing organizational information privacy practices in privacy notices posted on company websites gained popularity already in the late 1990s and early 2000s (Ciocchetti 2007), many privacy notices still do not achieve their core objective of communicating organizational information privacy practices to consumers, as attested by an abundant body of literature (eg, Jensen and Potts 2004, Liu and Arnett 2002, Meinert et al. 2006, Milne and Culnan 2002, Miyazaki and Fernandez 2000, Sunyaev et al. 2015, Vail et al. 2008). Trying to convince consumers of their commitment to information privacy without subjecting themselves to substantial commitments in the letter of the law, organizations seem to employ privacy notices as a strategic tool rather than a communication tool that offers the information relevant to consumers (Schwaig et al. 2005).

The primary contribution of this research is the development of nomothetic design knowledge in the form of the RECIPE ontology that captures the information relevant for communication of organizational information privacy practices. Without knowledge of the information relevant for substantive organizational information privacy communication, one cannot arrive at reliable conclusions related to effective designs for organizational information privacy communication, for example, with respect to matters like amount of information to be offered or suitable means for presentation (McDonald and Cranor 2008, Metzger 2006). Improved knowledge of the information relevant for substantive organizational information privacy communication enables the tailoring of related efforts in research and practice to consumer needs so that consumers may ultimately be empowered to make informed decisions with respect to consumer information system adoption and use. Hence, consumers can be enabled to become active and confident participants of future consumer information system environments. The results establish a baseline for the content of substantive organizational information privacy communication in information privacy–sensitive domains (eg, health IT) where it is especially relevant to address consumers' information privacy concerns in order to make effective use of information systems (Agaku et al. 2014). From a methodological standpoint, establishment of a common understanding of the information relevant for substantive organizational information privacy communication is useful to make research on organizational information privacy communication comparable across research projects and domains and to guide downstream research efforts like design of information privacy assurances (eg, Garrison et al. 2012) or machine-interpretable representation and communication of organizational information privacy practices (Antón, Bertino, et al. 2007).

5.2 Related Research

5.2.1 Ontologies

Ontologies have been used in diverse disciplines, most notably Philosophy and Computer Science, and there is no commonly agreed-on definition for ontologies (Guarino 1997, Smith and Welty 2001, Spyns et al. 2002). Within the scope of this manuscript, we adopt the definition of Guarino: "An ontology is an explicit, partial account of the intended models of a logical language" (Guarino 1997, p. 298). Accordingly, the RECIPE ontology specifies the content relevant for substantive organizational information privacy communication (Noy and McGuinness 2001).

The core uses of ontologies are communication, system engineering, and interoperability (Uschold and Gruninger 1996). Due to the variety of purposes for ontology development, extant ontologies can be classified on a continuum ranging from simple, informal catalogs to complex, formal logical languages (Guarino et al. 2009, Smith and Welty 2001). In line with the research objective to identify the information relevant for substantive organizational information privacy communication, the intended use of the RECIPE ontology is interhuman communication. Hence, the developed ontology requires some degree of formalism to represent hierarchical relationships between categories of relevant information (ie, content aspects) but the focus is on structuring, representing, and communicating a general model (March and Smith 1995) of the information relevant for organizational information privacy communication in consumer information systems that is tailored to be interpretable by humans and not machines.

5.2.2 Fair Information Practice Principles

Fair information practice principles (FIPP) can be considered the global, guiding standard for organizational information privacy communication. FIPP were developed as a response to the rise of automated data-processing in the 1960s and can be traced back to two separate efforts by the US Federal Department of Health Education and Welfare (HEW) and the Organisation for Economic Cooperation and Development (OECD) to establish a code of conduct for privacy-attentive information practices (Ciocchetti 2007). Definitions of the HEW and OECD FIPP are listed in Table 17 in the Appendix. While the HEW FIPP, Openness, Disclosure, Secondary Use, Correction, and Security, are more concise (US Federal Department of Health Education and Welfare 1973), the OECD FIPP subsume the HEW principles and add the additional principles of Collection Limitation and Accountability (Organisation for Economic Cooperation and Development 1980). A consolidated list of the seven FIPP set forth by the HEW and the OECD is presented in Table 15.

FIPP serve as foundation for various information privacy research efforts (Smith et al. 2011). In the privacy notice literature, FIPP are often used to assess the quality of privacy notices (Milne and Culnan 2002). Thorough implementation of FIPP would also result in useful organizational information privacy communications. FIPP establish, in principle, a code of conduct for information practices and the Disclosure principle requires that consumers get informed about the information practices.

However, FIPP have two key short comings, which render them inadequate for guiding design of organizational information privacy communications. First, FIPP lack level of detail, which makes them unsuitable to ascertain what information is missing from organizational information privacy communications (Milne and Culnan 2002). For example, privacy notices often lack information on organizational information privacy practices not carried out (Pollach 2007). Omitting information is undesirable for organizations because consumers tend to assume negative organizational intentions if organizational information privacy practices remain unknown (Oulasvirta et al. 2014). Second, communication of organizational information privacy practices is not concerned with privacy

Table 15. Consolidated definitions of fair information practice principles. Adapted from US Federal Department of Health Education and Welfare (HEW; 1973) and Organisation for Economic Cooperation and Development (OECD; 1980).

Fair Information Practice Principles	Sources
Openness: *There must be no personal-data record-keeping systems whose very existence is secret.*	HEW: Openness; OECD: Openness
Collection Limitation: *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*	OECD: Collection Limitation
Disclosure: *There must be a way for an individual, to find out what information about her is in a record and how it is used.*	HEW: Disclosure; OECD: Openness, Individual Participation
Secondary Use: *There must be a way for an individual to prevent information about her obtained for one purpose from being used or made available for other purposes without her consent.*	HEW: Secondary Use; OECD: Purpose Specification, Use Limitation
Correction: *There must be a way for an individual to correct or amend a record of identifiable information about her.*	HEW: Correction; OECD: Individual Participation
Security: *Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.*	HEW: Security; OECD: Data Quality, Security Safeguards
Accountability: *A data controller should be accountable for complying with measures which give effect to the principles stated above.*	OECD: Accountability

attentiveness or consumer friendliness of organizational information privacy practices—organizational information privacy practices do not need to be fair in order to be communicated. Thus, an ontology of the information relevant for communication of organizational information privacy practices must go beyond FIPP and offer a higher level of detail without prescribing actual manifestations of organizational information privacy practices.

5.2.3 Privacy Notices

Privacy notices are the prevalent tool for communication of organizational information privacy practices and, hence, extant knowledge on privacy notices in research and practices is the primary data source for this research. Privacy notices are notices posted on organizational web sites that introduce the organization and describe organizational information privacy practices. The purpose of privacy notices is to address the uncertainty inherent to online interactions between consumers and organizations by communicating the organizational information privacy practices to consumers (Pollach 2006). Communication of organizational information privacy practices reduces uncertainty and information asymmetry and reduces barriers to consumers' liking of IT offerings by fostering perceived behavioral control (Oulasvirta et al. 2014, Pavlou 2002). As a consequence, organizations and consumers can engage in fruitful, mutually beneficial relationships (Culnan and Armstrong 1999).

Extant research on privacy notices focuses mostly on privacy notice availability (eg, Johnson-Page and Thatcher 2001), privacy notice comprehensibility (eg, Graber et al. 2002, Jensen and Potts 2004), consumers' motivation for reading privacy notices (eg, McDonald and Cranor 2008, Milne and Culnan 2004), privacy notice representation (eg, Kelley et al. 2010, McDonald et al. 2009, Vail et al. 2008), or behavior and intentions as consequences of access to privacy notices (eg, Lowry et al. 2012, Tsai et al. 2011, H. Xu et al. 2011). With respect to privacy notice content, extant research is focused on compliance with selected requirements for privacy notice content like FIPP (eg, LaRose and Rifon 2006, Rains and Bosch 2009, Schwaig et al. 2006) or content mandated by government regulation (eg, Beldad et al. 2009, Hooper and Vos 2009), assesses what content is provided in privacy notices (eg, Liu and Arnett 2002, Pollach 2007, Rizk et al. 2010), or elicits consumer perceptions of privacy notice content (eg, McGrath 2011, Metzger 2006). A few studies focus on prescription of privacy notice content. These studies are however limited in scope and focus on interpretation and consolidation of pertinent regulation (eg, Ciocchetti 2007, Fang 2010, Yee and Korba 2013) or implications of technological innovations (eg, Kubis 2010, Strickland and Hunt 2005).

The diversity of extant research on privacy notices attests to the relevance of organizational information privacy communication but lacks a thorough consolidation of the relevant information to be offered. With this research, I close this gap and lay a foundation for future research working towards substantive organizational information privacy communications that are actually of use to consumers. Organizational information privacy communications can only be deemed useful if they offer the information consumers are looking for.

5.2.4 Simplified Model of Organizational Information Privacy Communication

To focus the research efforts on the research objective of identifying the information relevant for organizational information privacy communication, I formulated an abstraction of organizational information privacy communication in consumer information systems as the research context—the Simplified Model of Organizational Information Privacy Communication (Figure 15). The Simplified Model of Organizational Information Privacy Communication is focused on two stakeholder groups essential to communication of organizational information privacy practices—organizations and consumers. Organizations are essential because their information privacy practices are communicated. Consumers are essential because organizational information privacy practices are communicated to consumers.

We take the perspective of a single arbitrary organization embedded in a consumer information systems network of interchangeable IT offerings. To communicate organizational information privacy practices in a substantive way—and ideally stand out from the crowd—this organization is faced with the challenge of satisfying the information requests issued by consumers that are concerned with organizational information privacy practices. Satisfying the information requests is challenging due to the heterogeneity of consumers. The heterogeneity of consumers is induced by the nature of information privacy, which is context-dependent and subject to individual, cultural, and situational influences (Acquisti et al. 2015, Miltgen and Peyrat-Guillard 2014, Smith et al. 2011).

Since organizations are usually catering to large groups of consumers, it is unfeasible to satisfy each information request separately. Instead, organizations have to rely on predefined responses to information requests (eg, privacy notices or seals). The prevalent approaches to satisfy information privacy–related consumer demands are trust signaling (Lee et al. 2005) and uncertainty reduction (Pollach 2006). In this research, we focus on uncertainty reduction through communication of organizational information privacy practices. Moreover, we focus on development of a general model of the actual information to be provided (the RECIPE ontology), which allows the organization to employ an arbitrary orchestration of means facilitating information presentation and information retrieval aligned with the characteristics of the targeted consumers and features offered by available technology. The RECIPE ontology constitutes a metaspecification for the content of predefined organizational responses to any information request issued by consumers without imposing restrictions on aspects like message formatting, message redundancy, means for communication available, the number of messages required to convey the response, or actual manifestations of organizational information privacy practices.

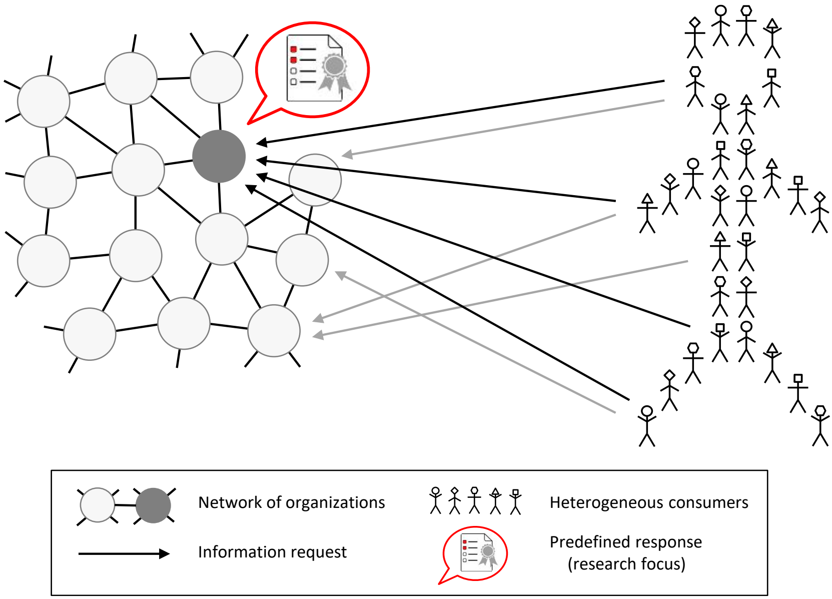


Figure 15. Illustration of the Simplified Model of Organizational Information Privacy Communication. In essence, information privacy communication requires well crafted predefined responses of organizations to future information requests issued by consumers with respect to organizational information privacy practices.

5.3 Methods

In line with the goal to develop an ontology of the information relevant for substantive organizational information privacy communication, that is, a nomothetic model of the content relevant for substantive organizational information privacy communication (March and Smith 1995), the research approach is based on the design science research paradigm (Gregor and Hevner 2013, Venable et al. 2016). Design science research is a research paradigm concerned with the development of socio-technical artifacts (Gregor and Hevner 2013). For development of the RECIPE ontology, I focused on topical relevance (ie, aboutness) because other dimensions of affective relevance (cognitive, situational, and socio cognitive relevance) are too dependent on consumer characteristics or situational circumstances (Cosijn and Ingwersen 2000). I leveraged extant knowledge in research and practice for identification of information topically relevant for organizational information privacy communication.

All ontology build and refinement phases employ the following ontology development process: First, I identified information relevant for communication of organizational information privacy practices by reviewing research or practice resources (eg, published privacy policies, pertinent articles). Once identified, new content aspects are assigned a unique identifier, annotated with a description, and added to the RECIPE ontology. If any ambiguities or inconsistencies are identified, they are resolved through corresponding revisions of the ontology (eg, removal of duplicates, rearrangement of content aspects, or refinement of identifiers and descriptions). To reduce complexity and ease interpretation, modification, and use of the RECIPE ontology, the ontology is structured as a monohierarchy—every node has only one parent, except for the root node, which has no parent by definition (Smith and Ceusters 2010). The root node (tier-0) is *Content*. Nodes on deeper tiers increase level of detail and refine their parents. For example, nodes on tier-1, the tier below the root node, group relevant information by consumers' main information privacy concerns, information collected, rationale for collection, handling of information, and offered information privacy controls (Ackerman et al. 1999, Antón et al. 2010, Earp et al. 2005). Relations between nodes represent 'is_a' relations (Smith 2004). For example, the relation *InformationCollectionTypeContent→IdentifierContent* represents that content aspects referring to the collection of identifiers offer information on what information is collected.

5.3.1 First Design Cycle—Initial Version of the RECIPE Ontology

In the first design cycle, I focused on incorporation of knowledge from practice. I derived the initial version of the RECIPE ontology from the Platform for Privacy Preferences Project (P3P; Reagle and Cranor 1999). P3P is a domain-specific language for privacy notices that can be used to construct machine-readable representations of organizational information privacy practices. I reviewed the P3P specification (Cranor et al. 2006), extracted all P3P language elements representing content topically relevant for substantive organizational information privacy communication, and added them to the ontology. The ontology was complemented through formative evaluation (Venable et al. 2016). At first, two experts from the domains of medicine and law reviewed the ontology for completeness and comprehensibility. Afterwards, I used the refined ontology to assess the privacy notice content of mobile health (mHealth) apps available on the Android and iOS app stores (Sunyaev et al. 2015). mHealth app privacy notices were chosen because of the high sensitivity of health information, which makes attention to information privacy particularly important (Rindfleisch 1997). In each app store, we selected the 300 most-frequently rated apps for privacy notice review and tested whether the ontology covered the content offered in all app-related privacy notices. The sample yielded 62 app-related privacy notices (Android: 31; iOS: 31), which were independently reviewed by a doctoral student and me. Reliability assessment with Janson's and Olsson's ı—a multivariate extension of Cohen's κ for multiple judges on the same scale (Janson and Olsson 2001)—led to an 'almost perfect' (Landis and Koch 1977) agreement score of ı=0.94.

The evaluation in the first design cycle demonstrates that the employed version of the RECIPE ontology was useful to capture the information provided in the reviewed mHealth app privacy notices. However, many content aspects included in the RECIPE ontology were only addressed by a few privacy notices or not addressed in any privacy notice (Sunyaev et al. 2015), which led to the conclusion that extant privacy notices are not an informative resource to obtain a detailed understanding of the information relevant for substantive organizational information privacy communication. Consequently, I conducted a second design cycle to further improve and refine the RECIPE ontology.

5.3.2 Second Design Cycle—Strengthening of Topical Relevance

In the second design cycle, I incorporated knowledge from the scientific knowledge base and conducted a literature review as a further formative evaluation step to strengthen topical relevance.

Literature Search. The literature review was conducted to refine the RECIPE ontology based on extant literature. The goal of the literature review was to identify and consolidate organizational information privacy practices topically relevant for organizational information privacy communication. To focus the literature search on pertinent articles, I developed a two-part search string. The first part of the search string is designed to match articles dealing with privacy notices and the second part of the search string reduces the matches to articles dealing with the content of privacy notices. I restricted the literature search to matches in title, abstract, or keywords. A database search was conducted to include a wide range of outlets and cover a wide range of domains. However, I restricted the search to literature databases focused predominantly on journals and conferences relevant for information systems research because this study was conducted in the domain of information systems research. Chosen databases were EBSCO (Academic Search Complete, Business Search Complete, Medline), ProQuest, AISeL, and ScienceDirect. Figure 16 presents an overview of the literature review. Table 18 in the appendix lists the search strings formatted in the syntax of the different databases. Articles were retrieved in September 2014.

Literature Screening. We screened all articles based on title, keywords, and abstracts. All articles that were duplicates, not written in English, not peer-reviewed research papers, or that did not yield any input on organizational information privacy practices topically relevant for communication of organizational information privacy practices were excluded from further assessment. Literature screening was independently performed by the author and a doctoral student. To reduce the likelihood of false positives, I only excluded articles if both researchers independently identified a reason for exclusion of the article. All remaining articles were read in detail to identify organizational information privacy practices topically relevant for communication of organizational information privacy practices.

Literature Analysis. After initial training rounds to clarify the coding scheme and resolve any misunderstandings, the author and a doctoral student independently assessed 72 of the 101 remaining articles. The coding scheme was iteratively improved and the final version corresponds to the content aspects listed in Table 19. Reliability assessment with Janson's and Olsson's ı (Janson and Olsson 2001) led to a substantial

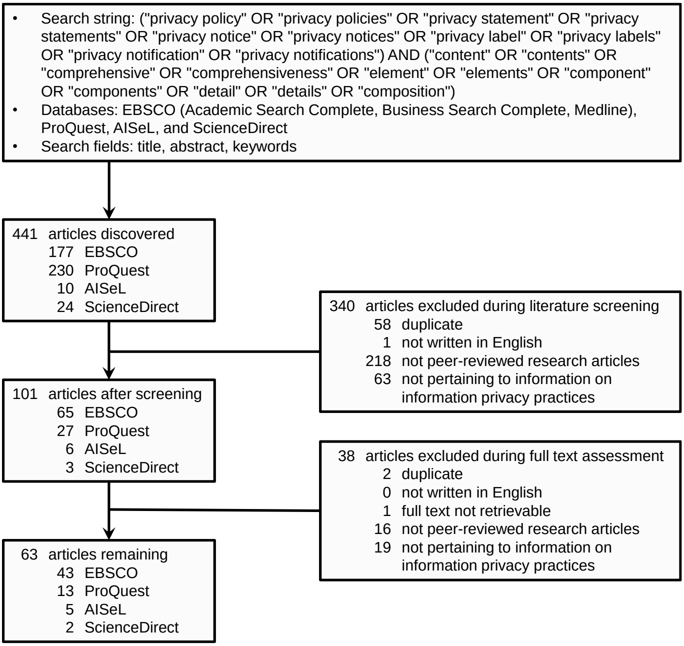

• Search string: ("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifications") AND ("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition")
• Databases: EBSCO (Academic Search Complete, Business Search Complete, Medline), ProQuest, AISeL, and ScienceDirect
• Search fields: title, abstract, keywords
441 articles discovered
177 EBSCO
230 ProQuest
10 AISeL
24 ScienceDirect
340 articles excluded during literature screening
58 duplicate
1 not written in English
218 not peer-reviewed research articles
63 not pertaining to information on information privacy practices
101 articles after screening
65 EBSCO
27 ProQuest
6 AISeL
3 ScienceDirect
38 articles excluded during full text assessment
2 duplicate
0 not written in English
1 full text not retrievable
16 not peer-reviewed research articles
19 not pertaining to information on information privacy practices
63 articles remaining
43 EBSCO
13 ProQuest
5 AISeL
2 ScienceDirect

Figure 16. Overview of literature review.

(Landis and Koch 1977) and satisfactory agreement score of ı=0.74. Because reliability of assessments was demonstrated, the remaining 29 articles were assessed by the author alone. The researchers coded (Braun and Clarke 2006) all content aspects mentioned and looked especially for content aspects still missing in the RECIPE ontology and for any other indications for need for revisions of the ontology (eg, refinement of descriptions). Conflicts and ambiguities in assessments were resolved through discussions.

Applicability of the RECIPE Ontology to the Wikipedia Privacy Notice. As a final artificial, summative evaluation step (Venable et al. 2016), I applied the RECIPE ontology to assess the content of an exemplary artifact aiming to communicate organizational information privacy practices. I selected the Wikipedia privacy notice (Wikimedia Foundation 2014) as exemplary artifact for the final evaluation step.

Wikipedia is a strongly frequented web site. Hence, the Wikipedia provider, the Wikimedia Foundation, should have enough resources to craft a privacy notice that effectively communicates organizational information privacy practices. With respect to other highly frequented web sites, a unique characteristic of Wikipedia is that Wikipedia is a community project—the organization is community-driven. In terms of the Simplified

Model of Organizational Information Privacy Communication, the Wikipedia privacy notice basically constitutes a predefined response crafted by consumers to potential information requests issued by consumers. This constitutes a core advantage with respect to communication of organizational information privacy practices. A community-driven organization is more likely to know what consumers want to know than other organizations, especially, if the community is large. Moreover, Wikipedia is a crowd-sourcing project (Howe 2006). The whole encyclopedia is created by a self-organizing community of volunteers. Hence, consumer satisfaction is crucial because Wikipedia depends on consumers to add content, improve offered service, and administer the web site. A further reason to select the Wikipedia privacy notice as sample tool for the final evaluation step was that the privacy notice actually implies purposeful communication as a core objective: "We believe that information-gathering and use should go hand-in-hand with transparency." (Wikimedia Foundation 2014)

The goal of the final evaluation step is to test whether the RECIPE ontology is comprehensive and whether the content aspects are topically relevant. To test comprehensiveness, I tested whether the RECIPE ontology can capture the organizational information privacy practices addressed by the Wikipedia privacy notice. To test topical relevance of the RECIPE ontology content aspects, I checked whether the content aspects in the RECIPE ontology are mentioned in the Wikipedia privacy notice. Any content aspects not mentioned in the Wikipedia privacy notice were reviewed for topical relevance.

5.4 The RECIPE Ontology

A large fraction of the articles discovered in the literature search assesses information offered in artifacts communicating organizational information privacy practices (mostly privacy notices) against predefined assessment catalogues or coding schemes (42.9%, n=27). Assessment catalogues and coding schemes are often derived from FIPP and amended with few organizational information privacy practices selected by authors. Other articles elicit what information is offered by artifacts communicating organizational information privacy practices (12.7%, n=8) or develop normative prescriptions for information to be offered by artifacts communicating organizational information privacy practices (15.9%, n=10). Another category of articles focuses on consumer perceptions (eg, utility of offered information, missing information) of artifacts communicating organizational information privacy practices (11.1%, n=7). Table 16 gives an overview of the different article categories.

During the literature analysis, we identified 132 content aspects. The maximum depth of the hierarchy is 5. Figure 17 gives an overview of the ontology. Table 19 in the appendix outlines the hierarchy, lists all content aspects with a detailed description, states how often a content aspect was mentioned by articles in the sample, and indicates during which stage of the research approach the content aspect was added. Table 20 in the appendix gives an overview of the articles in the final literature sample. Table 20

Table 16. Discovered articles by article category.

Article category	Category description	Articles, N (%)
Content Assessment	Articles assessing the information offered by artifacts (eg, privacy notices, privacy seals) that communicate organizational information privacy practices against a predefined coding scheme.	27 (42.9)
Content Prescription	Articles making normative prescriptions what information should be offered in artifacts (eg, privacy notices, privacy seals) that communicate organizational information privacy practices.	10 (15.9)
Content Analysis	Articles examining what information is offered by artifacts (eg, privacy notices, privacy seals) that communicate organizational information privacy practices.	8 (12.7)
Consumer Perception	Articles studying consumer perceptions of artifacts (eg, privacy notices, privacy seals) that communicate organizational information privacy practices.	7 (11.1)
Other	Other articles focus on issues like design of artifacts that communicate organizational information privacy practices or consumer preferences for information on organizational information privacy practices.	11 (17.5)

lists all 63 articles with a brief outline of the article aims and the number of content aspects mentioned. During the literature analysis, we coded whether content aspects were deemed relevant or irrelevant for communication of organizational information privacy practices. However, none of the articles in the sample characterize any content aspects as irrelevant. Hence, all content aspects deliberately mentioned in articles were considered relevant for organizational information privacy communication. Content aspects were, for example, coded as relevant for communication of organizational information privacy practices if articles state that consumers should be informed about them, use them in coding schemes, state that consumers are concerned about them, or if articles report that content aspects were deemed relevant in pertinent legal proceedings. We only excluded content aspects that appeared to be incidentally mentioned in sample articles. The following sections outline the main content aspects of the RECIPE ontology.

Metainformation is the only main content aspect that captures organizational characteristics not directly related to organizational information privacy practices. Metainformation refers to information privacy–related characteristics of organizations. This is, for instance, the name of the organization, contact information, laws the organization complies with, and information privacy–related seals.

Information collection content aspects capture what information is collected (type) and how information is collected (sensors). Information collection type is subdivided into content aspects capturing identifiers (eg, financial identifiers, governmental identifiers), operational information (eg, user navigation, location), personal information (eg, demographics, preferences) and information form (eg, audio, text). Information collection sensors are specified by content aspects like environment sensors (eg, camera, Bluetooth), location sensors (eg, GPS, network connection), or software use sensors (eg, cookies, surveys).

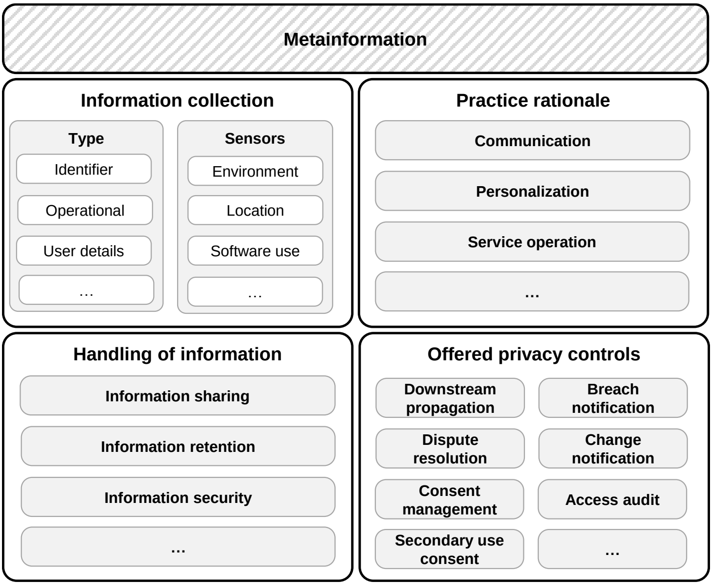


Figure 17. Partial overview of the RECIPE ontology.

Content aspects referring to handling of information are subdivided into content aspects related to information sharing (eg, with advertisers or other consumers), information retention (eg, in accordance with legal requirements), information security (during transfer, processing, and storage), and information storage (eg, on consumer device or in the cloud).

Practice rationale content aspects capture for what purposes organizational information privacy practices are carried out. The main subdivision of practice rationale content aspects is collection for communication (eg, marketing, communication with other users), service provision (eg, payment, physical delivery of goods), personalization (eg, tailoring, profiling), public welfare (eg, research, government services), and collection for technical details (eg, account or session management).

Content aspects addressing offered information privacy controls capture information system features and organizational processes that allow for or support consumers in exercising individual control with respect to information privacy. This entails whether consumers are enabled to review accesses to their information, how consumers are notified if information privacy was breached (eg, occurrence of breach, nature of breach, and remedies offered and carried out), whether consumers are notified if organizational information privacy practices change (eg, collection of further information or for additional purposes), whether consumers can review past specifications of organizational information privacy practices and are informed according to which organizational information privacy practices their information is treated (eg, information privacy practices current at information collection or current information privacy practices), how consumers can review and change given consents, what means are offered for dispute resolution (eg, settlement through customer service, courts, or an independent organization), what remedies are offered for justified disputes (eg, rectification or money), to what degree the organization practices downstream propagation of consumer actions (eg, will information also be deleted in backup tapes and databases of third parties, if the consumer deletes it in the organization's consumer information system), where the organization sets the boundaries for information privacy management (eg, compliance with information requests by law enforcement or control of privacy practices of subsidiaries), how organizations monitor compliance with intended privacy practices (eg, automated monitoring, regular independent or internal audits), whether consent must be given prior to secondary uses of consumer information, and how consumers can access submitted information (eg, view, correct, delete, download).

5.5 Evaluation—Applicability of the RECIPE Ontology to the Wikipedia Privacy Notice

The RECIPE ontology captures all statements in the Wikipedia privacy notice (Wikimedia Foundation 2014) that relate to organizational information privacy practices. A mapping of all statements in the Wikipedia privacy notice to the RECIPE ontology is available from the author upon request. Statements not captured by the RECIPE ontology refer to aspects like privacy notice structure or definitions.

While the Wikipedia privacy notice addresses a majority of content aspects in the RECIPE ontology, a few content aspects included in the RECIPE ontology are not addressed in the Wikipedia privacy notice. Metainformation content aspects not addressed are minimum user age and information privacy–related certifications. However, both are topically relevant. Information privacy–related certifications foster trust by signaling that offered information on organizational information privacy practices is approved by an independent organization (LaRose and Rifon 2006). Specifying a minimum user age signals whether organizational information privacy practices cater to the special information privacy–related needs of children (Bélanger et al. 2013).

With respect to information collection, the Wikipedia privacy notice does not address a few means for information collection (Bluetooth, camera, microphone, near field communication, available wireless networks, fingerprint scanner). However, these are common tools for information collection, especially, for mobile devices; thus, they are topically relevant for organizational information privacy communication (Mylonas et al. 2013). For example, microphones can be used to detect voice commands for applications and available wireless networks can be used to determine consumer location. The Wikipedia privacy notice also does not state whether audio information, government identifiers, purchases, financial information, or health information is collected. Such information is, however, considered sensitive by consumers (Cranor et al. 1999); thus, it is topically relevant. Government identifiers can, for instance, be used for identity theft and purchases are a good predictor for consumer preferences, life style, and other characteristics (Turner and Dasgupta 2003).

With respect to information handling, the Wikipedia privacy notice did not mention whether information is shared with analysts or physical logistics providers and whether information is stored in cloud services, with third party storage providers, or on secondary user devices. These are however also common practices for handling of information with different implications for information privacy; thus, they are topically relevant. For example, third party analysts could infer sensitive information based on consumer information and storage of information in cloud services introduces a whole new set of threats to confidentiality (Nanavati et al. 2014).

Rationale for organizational information privacy practices not addressed in the Wikipedia privacy notice are financial management, sales, processing of payments, physical delivery of goods, delivering the arts, charity, preserving history, and offering health services. Such uses are however either perceived as undesirable or as desirable by consumers; thus, they are topically relevant for organizational information privacy communication (Lee et al. 2008).

Offered privacy controls not addressed in the Wikipedia privacy notice are consent management and downstream propagation of consumer actions. Both are topically relevant for organizational information privacy communication. Since use of consumer information systems often entails numerous occasions where consumers give or revoke implicit or explicit consent for organizational information privacy practices, organizations can support consumers in information privacy management by offering functionality allowing consumers to view and modify all given and revoked consents (Ciocchetti 2007). Organizations can offer additional support through downstream propagation of consumer actions, thereby, relieving consumers of having to track down all copies of information they want updated or deleted (Hossain and Dwivedi 2014).

5.6 Discussion

The RECIPE ontology enables organizations to develop predefined responses to information privacy–related information requests issued by consumers that serve as signal and as incentive (Pavlou et al. 2007). Organizations can signal their quality with respect to information privacy by communicating their organizational information privacy practices and reducing hidden information. Simultaneously, organizations are incentivized to adhere to stated organizational information privacy practices because violating publicly stated organizational information privacy practices makes organizations susceptible to litigation. Hence, crafting predefined responses based on the RECIPE ontology makes consumers not only aware of organizational information privacy practices but is also a testimonial of organizational commitment to adhere to stated organizational information privacy practices.

The RECIPE ontology constitutes a metaspecification of a comprehensive selection of organizational information privacy practices that are topically relevant for organizational information privacy communication. I accounted for topical relevance of the RECIPE ontology content aspects by deriving and consolidating them from extant knowledge in research and practice. Comprehensiveness of the RECIPE ontology was demonstrated through application of the RECIPE ontology to the Wikipedia privacy notice. It is however important to note that comprehensiveness will never be equal to completeness as long as there is technological innovation (eg, new means for information collection or new approaches to foster information privacy control). In its current form, the RECIPE ontology can serve organizations as a starting point to understand what information must be contained in organizational information privacy communications.

Since ontologies can be used as representations of reality they are well suited to account for change. For example, the Wikipedia privacy notice did not address whether health information is collected, although changes in reading patterns of consumers allow, for instance, to infer that consumers or consumer acquaintances were diagnosed with a disease (eg, diagnosis of cancer or diabetes). In the case of Wikipedia, it would likely suffice to briefly outline how such information is handled. For consumer information systems collecting more detailed health information, for instance, information systems for pervasive health (Ruotsalainen et al. 2012), a comprehensive predefined response would likely require more detailed information on collection of health information. In such cases, the RECIPE ontology could be extended based on extant ontologies in the health care domain (Blobel 2011). During assessment of the Wikipedia privacy notice, I extended the RECIPE ontology with an additional ontology capturing stated organizational information privacy practices to not only assess addressed organizational information privacy practices but also capture the stated organizational information privacy practices, for instance, to capture that information is not shared with third party marketing services instead of only capturing that the Wikipedia privacy notice offers information on sharing with third party marketing services. Actual manifestations of organizational information privacy practices are beyond the scope of this manuscript. The extended version of the RECIPE ontology is available from the author upon request.

Salient opportunities for further research are extension of the design knowledge captured by the RECIPE ontology with complementary design knowledge. The RECIPE ontology is one piece for the information privacy puzzle and captures, in terms of the Simplified Model of Organizational Information Privacy Communication, a nomothetic model of the information to be offered in organizations' predefined responses to information privacy–related information requests issued by consumers and allows for context-specific adaptation and extension. Further research is necessary to explore how to present and communicate the information and how to account for further dimensions of relevance (Cosijn and Ingwersen 2000). For example, to account for situational relevance, organizations' predefined responses must be able to support consumers in diverse tasks (eg, get an overview of organizational information privacy practices or find out whether and how a certain information privacy practice is carried out). To factor in cognitive relevance, organizations' predefined responses have to account for differences in individual consumer characteristics (eg, differences in familiarity with the organization or differences in extant individual knowledge).

With increasing complexity of organizational information privacy practices, the utility of static privacy notices rapidly decreases because organizational information privacy communication entails communication of much information and reading of privacy notices is time-consuming (McDonald and Cranor 2008). Albeit deficient with respect to information presentation and information retrieval, privacy notices are still the most prevalent tool for organizational information privacy communication that I could identify in the current consumer information systems landscape. Privacy notices are, however, only a suitable response to information requests for a detailed and complete description of organizational information privacy practices. In other cases, interactive representations of organizational information privacy practices seem more appropriate. Organizations could, for example, use ontology visualization methods (Katifori et al. 2007) to present consumers with an initial overview of organizational information privacy practices and also allow them to drill down to retrieve information of interest. An alternative approach is offered by natural language user interfaces (Hirschberg and Manning 2015), which can provide consumers with desired information on organizational information privacy practices in response to voice commands. This could prove particularly useful for mobile phones, where presentation of privacy notices is difficult due to limited screen estate. In addition, current smartphones already offer quite sophisticated natural language user interfaces (eg, Siri on the iOS platform).

5.7 Conclusions

For many organizations, the dominant strategy for accounting for information privacy in consumer information systems seems to be mitigation of information privacy concerns. However, such approaches often result in treatment of symptoms instead of a search for viable solutions. As a result, consumer information systems are stuck in a vicious cycle of introduction of new technology, assimilation and exploration of new technology, heightened public concern about privacy, implementation of reactive privacy legislation, and introduction of new technology (Turner and Dasgupta 2003). The RECIPE ontology supports organizations in hopping off the bandwagon and to embrace information privacy instead of mere mitigation of information privacy concerns. The RECIPE ontology supports organizations in communicating their organizational information privacy practices to consumers and, thereby, in differentiating themselves from their competitors in a web of exchangeable consumer information systems. Hence, organizations can build on the RECIPE ontology to increase their attractiveness to consumers by reducing uncertainty and increasing perceived behavioral control. Features offered by many consumer information systems are often easily copied; effective organizational information privacy communication is not.

5.8 References

Ackerman MS, Cranor LF, Reagle J (1999) Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. 1st ACM Conference on Electronic Commerce. (ACM, Denver, CO, USA), 1–8.

Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and Human Behavior in the Age of Information. Science 347(6221):509–514.

Agaku IT, Adisa AO, Ayo-Yusuf OA, Connolly GN (2014) Concern About Security and Privacy, and Perceived Control over Collection and Use of Health Information are Related to Withholding of Health Information from Healthcare Providers. Journal of the American Medical Informatics Association 21(2):374–378.

Almatarneh A (2011) Privacy Implications for Information and Communications Technology (ICT): The Case of the Jordanian E-Government. Journal of International Commercial Law & Technology 6(3):151–164.

Antón AI, Bertino E, Li N, Yu T (2007) A Roadmap for Comprehensive Online Privacy Policy Management. Communications of the ACM 50(7):109–116.

Antón AI, Earp JB, Young JD (2010) How Internet Users' Privacy Concerns Have Evolved Since 2002. IEEE Security & Privacy 8(1):21–27.

Ashrafi N, Kuilboer JP (2005) Online Privacy Policies: An Empirical Perspective on Self-Regulatory Practices. Journal of Electronic Commerce in Organizations 3(4):61–74.

Bansal G, Zahedi FM, Gefen D (2015) The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern. European Journal of Information Systems 24(6):624–644.

Baskerville RL, Kaul M, Storey VC (2015) Genres of Inquiry in Design-Science Research: Justification and Evaluation of Knowledge Production. MIS Quarterly 39(3):541–564.

de Beaufort Wijnholds H, Little MW (2001) Regulatory Issues for Global E-Tailers: Marketing Implications. Academy of Marketing Science Review 2001(1):1–12.

Bélanger F, Crossler RE, Hiller JS, Park JM, Hsiao MS (2013) POCKET: A Tool for Protecting Children's Privacy Online. Decision Support Systems 54(2):1161–1173.

Beldad AD, De Jong M, Steehouder MF (2009) When the Bureaucrat Promises to Safeguard your Online Privacy: Dissecting the Contents of Privacy Statements on Dutch Municipal Websites. Government Information Quarterly 26(4):559–566.

Berger CR, Calabrese RJ (1975) Some Explorations in Initial Interaction and Beyond: Toward a Developmental Theory of Interpersonal Communication. Human Communication Research 1(2):99–112.

Blobel B (2011) Ontology Driven Health Information Systems Architectures Enable pHealth for Empowered Patients. International Journal of Medical Informatics 80(2):e17–e25.

Braun V, Clarke V (2006) Using Thematic Analysis in Psychology. Qualitative Research in Psychology 3(2):77–101.

Bulgurcu B, Cavusoglu H, Benbasat I (2010) Understanding Emergence and Outcomes of Information Privacy Concerns: A Case of Facebook. ICIS 2010 Proceedings. (St. Louis, MO, USA).

Cai X, Gantz W, Schwartz N, Wang X (2003) Children's Website Adherence to the FTC's Online Privacy Protection Rule. Journal of Applied Communication Research 31(4):346–362.

Cha J (2011) Information Privacy: A Comprehensive Analysis of Information Request and Privacy Policies of Most-Visited Web Sites. Asian Journal of Communication 21(6):613–631.

Ciocchetti CA (2007) E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors. American Business Law Journal 44(1):55–126.

Clarke R (1994) The Digital Persona and its Application to Data Surveillance. The Information Society 10(2):77–92.

Clarke R (2006) A Pilot Study of the Effectiveness of Privacy Policy Statements. BLED 2006 Proceedings. (AIS, Bled, Slovenia).

Cosijn E, Ingwersen P (2000) Dimensions of Relevance. Information Processing & Management 36(4):533–550.

Cottrill CD (2011) Location Privacy: Who Protects? Journal of the Urban & Regional Information Systems Association 23(2):49–59.

Cranor L, Dobbs B, Egelman S, Hogben G, Humphrey J, Langheinrich M, Marchiori M, et al. (2006) The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. Retrieved (March 3, 2017), http://www.w3.org/TR/2006/NOTE-P3P11-20061113.

Cranor LF, Reagle J, Ackerman MS (1999) Beyond Concern: Understanding Net Users' Attitudes about Online Privacy. AT&T Labs-Research Technical Report, TR 99.4.3. (MIT Press, Cambridge, MA, USA).

Culnan MJ (2000) Protecting Privacy Online: Is Self-Regulation Working? Journal of Public Policy & Marketing 19(1):20–26.

Culnan MJ, Armstrong PK (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science 10(1):104–115.

Culnan MJ, Williams CC (2009) How Ethics can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches. MIS Quarterly 33(4):673–687.

Desai M, Lodge D, Gates M, Wolvin M, Louer G (2012) The FTC Privacy Report: What the Report Means and How You can get Ahead of Enforcement Trends by Implementing Best Practices Now. International Journal of Mobile Marketing 7(2):26–36.

Earp JB, Antón AI, Aiman-Smith L, Stufflebeam WH (2005) Examining Internet Privacy Policies Within the Context of User Privacy Values. IEEE Transactions on Engineering Management 52(2):227–237.

Faja S, Trimi S (2006) Influence of the Web Vendor's Interventions on Privacy-Related Behaviors in e-Commerce. Communications of the Association for Information Systems 17(1):27.

Fang Y (2010) The Death of the Privacy Policy: Effective Privacy Disclosures after In Re Sears. Berkeley Technology Law Journal 25(1):671–700.

Garrison L, Hastak M, Hogarth JM, Kleimann S, Levy AS (2012) Designing Evidence-Based Disclosures: A Case Study of Financial Privacy Notices. Journal of Consumer Affairs 46(2):204–234.

Graber MA, D'Alessandro DM, Johnson-West J (2002) Reading Level of Privacy Policies on Internet Health Web Sites. The Journal of Family Practice 51(7):642–645.

Gregor S, Hevner AR (2013) Positioning and Presenting Design Science Research for Maximum Impact. MIS Quarterly 37(2):337–355.

Guarino N (1997) Understanding, Building and Using Ontologies. International Journal of Human-Computer Studies 46(2–3):293–310.

Guarino N, Oberle D, Staab S (2009) What is an Ontology? Studer R, Staab S, eds. Handbook on Ontologies. (Springer, Berlin, Germany), 1–17.

Hanseth O, Lyytinen K (2010) Design Theory for Dynamic Complexity in Information Infrastructures: The Case of Building Internet. Journal of Information Technology 25(1):1–19.

Hirschberg J, Manning CD (2015) Advances in Natural Language Processing. Science 349(6245):261–266.

Hong T, McLaughlin ML, Pryor L, Beaudoin CE, Grabowicz P (2005) Internet Privacy Practices of News Media and Implications for Online Journalism. Journalism Studies 6(1):15–28.

Hooper A, Bunker B, Rapson A, Reynolds A, Vos M (2007) Evaluating Banking Websites Privacy Statements-A New Zealand Perspective on Ensuring Business Confidence. PACIS 2007 Proceedings. (AIS, Auckland, New Zealand).

Hooper T, Evans TB (2010) The Value Congruence of Social Networking Services-A New Zealand Assessment of Ethical Information Handling. The Electronic Journal Information Systems Evaluation 13(2):121–131.

Hooper T, Vos M (2009) Establishing Business Integrity in an Online Environment. Online Information Review 33(2):343–361.

Hossain MA, Dwivedi YK (2014) What Improves Citizens' Privacy Perceptions Toward RFID Technology? A Cross-Country Investigation Using Mixed Method Approach. International Journal of Information Management 34(6):711–719.

Howe J (2006) The Rise of Crowdsourcing. Wired Magazine. Retrieved (March 9, 2012), http://www.wired.com/wired/archive/14.06/crowds.html.

Janson H, Olsson U (2001) A Measure of Agreement for Interval or Nominal Multivariate Observations. Educational and Psychological Measurement 61(2):277–289.

Jensen C, Potts C (2004) Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. (ACM, New York, NY, USA), 471–478.

Johnson-Page GF, Thatcher RS (2001) B2C Data Privacy Policies: Current Trends. Management Decision 39(4):262–272.

Katifori A, Halatsis C, Lepouras G, Vassilakis C, Giannopoulou E (2007) Ontology Visualization Methods—A Survey. ACM Computing Surveys 39(4):10:1-10:43.

Kaupins GE, Reed D (2012) New Media Usage and Privacy Policies of Newspaper Websites of the Baltic States. Current Issues of Business & Law 7(1):27–45.

Kelley PG, Cesca L, Bresee J, Cranor LF (2010) Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. SIGCHI Conference on Human Factors in Computing Systems. (ACM, New York, NY, USA), 1573–1582.

Kim S, Yi SH (2010) Is Privacy at Risk when Commercial Websites Target Primary School Children? A Case Study in Korea. Children & Society 24(6):449–460.

Kubis KE (2010) Google Books: Page by Page, Click by Click, Users Are Reading Away Privacy Rights. Vanderbilt Journal of Entertainment & Technology Law 13(1):217–254.

Kuzma J (2010) An Examination of Privacy Policies of US Government Senate Websites. Electronic Government, an International Journal 7(3):270–280.

Kuzma J (2011) Empirical Study of Privacy Issues among Social Networking Sites. Journal of International Commercial Law and Technology 6(2):74–85.

Landis JR, Koch GG (1977) The Measurement of Observer Agreement for Categorical Data. Biometrics 33(1):159–174.

Langenderfer J, Cook DL (2004) Oh, What a Tangled Web we Weave: The State of Privacy Protection in the Information Economy and Recommendations for Governance. Journal of Business Research 57(7):734–747.

LaRose R, Rifon N (2006) Your Privacy is Assured - Of Being Disturbed: Websites With and Without Privacy Seals. New Media & Society 8(6):1009–1029.

Lee BC, Ang L, Dubelaar C (2005) Lemons on the Web: A Signalling Approach to the Problem of Trust in Internet Commerce. Journal of Economic Psychology 26(5):607–623.

Lee DH, Im S, Taylor CR (2008) Voluntary Self-Disclosure of Information on the Internet: A Multimethod Study of the Motivations and Consequences of Disclosing Information on Blogs. Psychology and Marketing 25(7):692–710.

Liu C, Arnett KP (2002) Raising a Red Flag on Global WWW Privacy Policies. The Journal of Computer Information Systems 43(1):117–127.

Lowry PB, Moody G, Vance A, Jensen M, Jenkins J, Wells T (2012) Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues for Online Consumers. Journal of the American Society for Information Science and Technology 63(4):755–776.

Magi TJ (2010) A Content Analysis of Library Vendor Privacy Policies: Do They Meet Our Standards? College & Research Libraries 71(3):254–272.

March ST, Smith GF (1995) Design and Natural Science Research on Information Technology. Decision Support Systems 15(4):251–266.

Martin KD, Borah A, Palmatier RW (2017) Data Privacy: Effects on Customer and Firm Performance. Journal of Marketing 81(1):36–58.

McDonald AM, Cranor LF (2008) The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 4(3):540–565.

McDonald AM, Reeder RW, Kelley PG, Cranor LF (2009) A Comparative Study of Online Privacy Policies and Formats Goldberg I, Atallah M, eds. Lecture Notes in Computer Science 5672:37–55.

McGrath L (2011) Social Networking Privacy: Important or Not? Interdisciplinary Journal of Contemporary Research In Business 3(3):22–28.

McRobb S (2006) Let's Agree to Differ: Varying Interpretations of Online Privacy Policies. Journal of Information, Communication and Ethics in Society 4(4):215–228.

McRobb S, Rogerson S (2004) Are they Really Listening?: An Investigation into Published Online Privacy Policies at the Beginning of the Third Millennium. Information Technology & People 17(4):442–461.

Meinert DB, Peterson DK, Criswell JR, Crossland MD (2006) Privacy Policy Statements and Consumer Willingness to Provide Personal Information. Journal of Electronic Commerce in Organizations 4(1):1–17.

Metzger MJ (2006) Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure. Communication Research 33(3):155–179.

Milne GR, Culnan MJ (2002) Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys. Information Society 18(5):345–359.

Milne GR, Culnan MJ (2004) Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices. Journal of Interactive Marketing 18(3):15–29.

Miltgen CL, Peyrat-Guillard D (2014) Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries. European Journal of Information Systems 23(2):103–125.

Miyazaki AD, Fernandez A (2000) Internet Privacy and Security: An Examination of Online Retailer Disclosures. Journal of Public Policy & Marketing 19(1):54–61.

Mundy DP (2006) Customer Privacy on UK Healthcare Websites. Medical Informatics and the Internet in Medicine 31(3):175–193.

Mylonas A, Meletiadis V, Mitrou L, Gritzalis D (2013) Smartphone Sensor Data as Digital Evidence. Computers & Security 38(0):51–75.

Nanavati M, Colp P, Aiello B, Warfield A (2014) Cloud Security: A Gathering Storm. Communications of the ACM 57(5):70–79.

Noy NF, McGuinness DL (2001) Ontology Development 101: A Guide to Creating Your First Ontology. Retrieved (August 25, 2014), http://protege.stanford.edu/publications/ontology_development/ontology101-noy-mcguinness.html.

O’Connor P (2003) What Happens to my Information if I Make a Hotel Booking Online: An Analysis of On-Line Privacy Policy Use, Content and Compliance by the International Hotel Companies. Journal of Services Research 3(2):5–28.

Organisation for Economic Cooperation and Development (1980) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Recommendation by the Council of the OECD. Retrieved (June 25, 2013), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm . Archived at: http://www.webcitation.org/6Y7eE1Q3m.

Oulasvirta A, Suomalainen T, Hamari J, Lampinen A, Karvonen K (2014) Transparency of Intentions Decreases Privacy Concerns in Ubiquitous Surveillance. Cyberpsychology, Behavior, and Social Networking 17(10):633–638.

Papacharissi Z, Fernback J (2005) Online Privacy and Consumer Protection: An Analysis of Portal Privacy Statements. Journal of Broadcasting & Electronic Media 49(3):259–281.

Pavlou PA (2002) What Drives Electronic Commerce? A Theory of Planned Behavior Perspective. Academy of Management Proceedings:A1–A6.

Pavlou PA, Liang H, Xue Y (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. MIS Quarterly 31(1):105–136.

Peslak AR (2005) Internet Privacy Policies: A Review and Survey of the Fortune 50. Information Resources Management Journal 18(1):29–41.

Pollach I (2006) Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions. Journal of Organizational and End User Computing 18(1):23–49.

Pollach I (2007) What’s Wrong With Online Privacy Policies? Communications of the ACM 50(9):103–108.

Proctor RW, Ali MA, Vu KPL (2008) Examining Usability of Web Privacy Policies. International Journal of Human-Computer Interaction 24(3):307–328.

Rains SA, Bosch LA (2009) Privacy and Health in the Information Age: A Content Analysis of Health Web Site Privacy Policy Statements. Health Communication 24(5):435–446.

Reagle J, Cranor LF (1999) The Platform for Privacy Preferences. Communications of the ACM 42(2):48–55.

Rindfleisch TC (1997) Privacy, Information Technology, and Health Care. Communications of the ACM 40(8):92–100.

Rizk R, Gürses SF, Günther O (2010) SNS and 3rd Party Applications Privacy Policies and their Construction of Privacy Concerns. ECIS 2010 Proceedings. (AIS, Pretoria, South Africa).

Robles-Estrada C, Vargas-Barraza JA, Sepúlveda-Núñez MDDC (2006) Are Privacy Issues Important in Mexican Online Markets? An Empirical Investigation into Published Online Privacy Statements of Mexican Web Sites. BLED 2006 Proceedings. (Bled, Slovenia).

Roeber B, Rehse O, Knorrek R, Thomsen B (2015) Personal Data: How Context Shapes Consumers’ Data Sharing with Organizations from Various Sectors. Electronic Markets 25(2):95–108.

Ruotsalainen PS, Blobel BG, Seppälä AV, Sorvari HO, Nykänen PA (2012) A Conceptual Framework and Principles for Trusted Pervasive Health. Journal of Medical Internet Research 14(2):e52.

Savirimuthu J (2013) Smart Meters and the Information Panopticon: Beyond the Rhetoric of Compliance. International Review of Law, Computers & Technology 27(1–2):161–186.

Schuele K (2005) Privacy Policy Statements on Municipal Websites. Journal of Government Financial Management 54(2):20–29.

Schwaig KS, Kane GC, Storey VC (2005) Privacy, Fair Information Practices and the Fortune 500: The Virtual Reality of Compliance. SIGMIS Database 36(1):49–63.

Schwaig KS, Kane GC, Storey VC (2006) Compliance to the Fair Information Practices: How Are the Fortune 500 Handling Online Privacy Disclosures? Information & Management 43(7):805–820.

Shalhoub ZK (2006) Content Analysis of Web Privacy Policies in the GCC Countries. Information Systems Security 15(3):36–45.

Smith B (2004) Beyond Concepts: Ontology as Reality Representation. Proceedings of the International Conference on Formal Ontology and Information Systems. (IOS Press, Turin, Italy), 73–84.

Smith B, Ceusters W (2010) Ontological Realism: A Methodology for Coordinated Evolution of Scientific Ontologies. Applied Ontology 5(3–4):139–188.

Smith B, Welty C (2001) Ontology: Towards a New Synthesis. Proceedings of the International Conference on Formal Ontology and Information Systems. (ACM, Ogunquit, ME, USA), 3–9.

Smith HJ, Dinev T, Xu H (2011) Information Privacy Research: An Interdisciplinary Review. MIS Quarterly 35(4):989–1015.

Spyns P, Meersman R, Jarrar M (2002) Data Modelling versus Ontology Engineering. ACM SIGMod Record 31(4):12–17.

Stanaland AJS, Lwin MO, Leong S (2009) Providing Parents with Online Privacy Information: Approaches in the US and the UK. Journal of Consumer Affairs 43(3):474–494.

Stitilis D, Malinauskaite I (2013) Evaluation of Legal Data Protection Requirements in Cloud Services in the Context of Contractual Relations with End-Users. Socialines Technologijos 3(2):390–414.

Strickland LS, Hunt LE (2005) Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions. Journal of the American Society for Information Science and Technology 56(3):221–234.

Sunyaev A, Dehling T, Taylor PL, Mandl KD (2015) Availability and Quality of Mobile Health App Privacy Policies. Journal of the American Medical Informatics Association 22(e1):e28–e33.

Sunyaev A, Schneider S (2013) Cloud Services Certification. Communications of the ACM 56(2):33–36.

Suominen H (2012) Towards an International Electronic Repository and Virtual Laboratory of Open Data and Open-Source Software for Telehealth Research: Comparison of International, Australian and Finnish Privacy Policies. Studies in Health Technology and Informatics 182:153–160.

Tavani HT (2007) Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy. Metaphilosophy 38(1):1–22.

Timpson S, Troutman M (2009) The Importance of a Layered Privacy Policy on all Mobile Internet Sites and Mobile Marketing Campaigns. International Journal of Mobile Marketing 4(1):57–61.

Tsai JY, Egelman S, Cranor L, Acquisti A (2011) The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Information Systems Research 22(2):254–268.

Turner EC, Dasgupta S (2003) Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals. Information Systems Management 20(1):8–18.

Unruh HK, Bowen DJ, Meischke H, Bush N, Wooldridge JA (2004) Women’s Approaches to the Use of New Technology for Cancer Risk Information. Women & Health 40(1):59–78.

US Federal Department of Health Education and Welfare (1973) Records, Computers and the Rights of Citizens: Report of the Secretary’s Advisory Committee on Automated Personal Data Systems. Chapter III. Safeguards for Privacy. Retrieved (April 24, 2015), https://epic.org/privacy/hew1973report/c3.htm . Archived at: http://www.webcitation.org/6Y1gDPqTf.

Uschold M, Gruninger M (1996) Ontologies: Principles, Methods and Applications. Knowledge Engineering Review 11(2):93–136.

Vail MW, Earp JB, Antón AI (2008) An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies. IEEE Transactions on Engineering Management 55(3):442–454.

Venable J, Pries-Heje J, Baskerville R (2016) FEDS: A Framework for Evaluation in Design Science Research. European Journal of Information Systems 25(1):77–89.

Weitzman ER, Cole E, Kaci L, Mandl KD (2011) Social but Safe? Quality and Safety of Diabetes-Related Online Social Networks. Journal of the American Medical Informatics Association 18(3):292–297.

Wikimedia Foundation (2014) Wikimedia Foundation Privacy Policy. Retrieved (May 9, 2015), http://wikimediafoundation.org/wiki/Privacy_policy . Archived at: http://www.webcitation.org/6YOlcGEUD.

Wisniewski P, Islam A, Richter Lipford H, Wilson DC (2016) Framing and Measuring Multi-Dimensional Interpersonal Privacy Preferences of Social Networking Site Users. Communications of the Association for Information Systems 38(1):235–258.

Wu KW, Huang SY, Yen DC, Popova I (2012) The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust. Computers in Human Behavior 28(3):889–897.

Xu H, Dinev T, Smith HJ, Hart PJ (2011) Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems 12(12):798–824.

Yee GOM, Korba L (2013) Personal Privacy Policies. John R. Vacca, ed. Computer and Information Security Handbook. (Morgan Kaufmann, Boston, MA, USA), 773–792.

Zhang X, Toru S, Kennedy M (2007) A Cross-Cultural Analysis of Privacy Notices of the Global 2000. Journal of Information Privacy and Security 3(2):18–36.

5.9 Appendix

Table 17. Fair information practice principles definitions of the US Federal Department of Health Education and Welfare (HEW; 1973) and the Organisation for Economic Cooperation and Development (OECD; 1980)

	Label	Definition
HEW	Openness	There must be no personal-data record-keeping systems whose very existence is secret.
	Disclosure	There must be a way for an individual, to find out what information about him is in a record and how it is used.
	Secondary Use	There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
	Correction	There must be a way for an individual to correct or amend a record of identifiable information about him.
	Security	Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.
OECD	Collection Limitation	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
	Data Quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.
	Purpose Specification	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
	Use Limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification principle except: a) with the consent of the data subject; or b) by the authority of law.
	Security Safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification, or disclosure of data.
	Openness	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
	Individual Participation	An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
	Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above.

Table 18. Generic search string and database syntax–specific search strings employed for the literature search.

#	String
1	*Generic search string:* ("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifications") AND ("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition")
2	*EBSCO (Academic Search Complete, Business Search Complete, Medline), ProQuest:* (((TI("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifications")) OR (SU("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifications")) OR (AB("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifications"))) AND ((TI("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition")) OR (SU("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition")) OR (AB("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition"))))
3	*AISeL:* (((title:("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifications")) OR (subject:("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifications")) OR (abstract:("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifications"))) AND ((title:("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition")) OR (subject:("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition")) OR (abstract:("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition"))))
4	*ScienceDirect:* ((tak("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifications")) AND (tak("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition")))

Table 19. All content aspects identified in this study except for the root content aspect (Content). The column 'Hierarchy' indicates the hierarchy. For the sake of clarity, higher tiers, which have many child content aspects, are indicated with the initial of the top content aspect and lower tiers, which have only a small number of child content aspects are indicated with ascending numbers. Accordingly, aspects with more hierarchy indicators are deeper in the hierarchy.

Hierarchy			Content aspect	Added	#articles	Description
H			HandlingOfInformationContent	P3P review	63	Captures how the information system handles information
H	1		InformationRetentionContent	P3P review	29	Information retention practices of the organizational information system provider
H	2		InformationSecurityContent	App review	58	High-level information on information security measures
H	2	1	SecurityDuringProcessingContent	App review	0	Information security measures protecting information during processing
H	2	2	SecurityDuringStorageContent	App review	25	Information security measures protecting information at rest
H	2	3	SecurityDuringTransferContent	App review	12	Information security measures protecting information in transfer
H	3		InformationSharingContent	P3P review	61	Captures with whom information is shared
H	3	1	SharingWithAdvertiserContent	App review	15	Information sharing with third party offering advertising services within the organizational information system or on their own
H	3	2	SharingWithAggregatorContent	Lit review	0	Information sharing with information aggregators (ie, entities that compile data bases, which are usually drawn from various information sources to be, for example, sold for marketing purposes)
H	3	3	SharingWithAnalystContent	App review	4	Information sharing with third party running analysis services for the organization (eg, compilation of usage statistics)
H	3	4	SharingWithDeliveryContent	P3P review	2	Information sharing with third parties performing physical delivery services
H	3	5	SharingWithGovernmentContent	P3P review	10	Information sharing with government agencies
H	3	6	SharingWithOtherUsersContent	App review	12	Information sharing with other users of the information system
H	3	7	SharingWithProviderAgentsContent	P3P review	22	Information sharing with agents that process information only on behalf of the organization
H	3	8	SharingWithPublicContent	P3P review	7	Information sharing with the public
H	3	9	SharingWithUnrelatedContent	P3P review	52	Information sharing with unrelated third parties not involved in service provision
H	3	10	SharingWithConsumerAuthorizedContent	App review	3	Information sharing with third parties authorized by the consumer
H	4		InformationStorageContent	App review	27	Captures where information is stored

H	4	1		CloudStorageContent	App review	1	Information stored in the cloud
H	4	2		LocalStorageContent	App review	2	Information stored on the consumer device accessing the information system
H	4	3		OtherConsumerDeviceStorageContent	App review	0	Information stored on a secondary consumer device (eg, flash drive)
H	4	4		ProviderStorageContent	App review	3	Information stored within the organization's domain
H	4	5		ThirdPartyStorageContent	App review	0	Information stored by a third-party storage service
I				InformationCollectionContent	App review	62	Captures what and how information is collected
I	1			InformationCollectionSensorContent	App review	53	Sensors used to collect information and the sources of collected information
I	1	1		EnvironmentSensorContent	App review	1	Sensors collecting information on the device (the consumer) environment
I	1	1	1	BluetoothSensorContent	App review	0	Discover contactable Bluetooth-enabled devices
I	1	1	2	CameraContent	App review	1	Collect images or videos made with the device camera
I	1	1	3	MicrophoneContent	App review	0	Collect sound recordings made with the microphone of the device
I	1	1	4	NearFieldCommunicationContent	App review	0	Record consumer actions (eg, payments) conducted via Near Field Communication (NFC)
I	1	2		LocationSensorContent	App review	8	Sensors for location information
I	1	2	1	GpsSensorContent	App review	2	Global Positioning System (GPS) location of consumer client devices
I	1	2	2	NetworkConnectionSensorContent	App review	3	Location coordinates based on cell towers or other network identifiers (eg, IP address)
I	1	2	3	WiFiSensorContent	App review	1	Location coordinates based on available WiFi networks
I	1	3		UserSensorContent	App review	0	Sensors collecting information on the consumer
I	1	3	1	FingerprintScannerContent	App review	0	Collection of consumers’ fingerprint with fingerprint scanner
I	1	4		SoftwareUseSensorContent	Lit review	42	Sensors collecting information on software use or perception
I	1	4	1	AdwareContent	Lit review	1	Collection through adware installed on consumer client devices
I	1	4	2	CookiesContent	P3P review	39	Collection through cookies
I	1	4	3	SurveysContent	P3P review	8	Collection with surveys or questionnaires
I	1	4	4	TrackingSoftwareContent	Lit review	2	Collection with tracking software installed on consumer client devices

I	1	4	5	WebBeaconContent	Lit review	0	Tracking of consumer activity through web beacons (eg, what information system content was accessed)
I	2			InformationCollectionTypeContent	P3P review	60	Type of collected information
I	2	1		InformationFormatContent	Lit review	0	Different formats of collected information
I	2	1	1	AudioInformationContent	Lit review	0	Collection of audio information
I	2	1	2	ImageInformationContent	Lit review	0	Collection of images or photos
I	2	1	3	MetaDataContent	Lit review	0	Collection of metainformation (information on information; eg, geo tags in photos)
I	2	1	4	TextInformationContent	Lit review	0	Collection of textual information
I	2	1	5	VideoInformationContent	Lit review	0	Collection of videos
I	2	2		IdentifierContent	App review	50	Collection of consumer identifiers
I	2	2	1	FinancialIdentifierContent	App review	21	Financial identifiers (eg, bank account or credit card number)
I	2	2	2	GovernmentIdentifierContent	P3P review	23	Government-issued identifiers (eg, social security number)
I	2	2	3	NameContent	Lit review	0	Collection of consumers’ full names (not usernames)
I	2	2	4	OnlineContactContent	P3P review	32	Information that allows to contact the consumer on the internet
I	2	2	5	PhysicalContactContent	P3P review	28	Information that allows to contact the consumer in the physical world (eg, postal address)
I	2	2	6	OwnUniqueIdentifierContent	P3P review	14	Identifiers issued by the organization information system provider for purposes of consistently identifying consumers (eg, usernames)
I	2	3		OperationalContent	App review	44	Information collected for information system operation
I	2	3	1	CommunicationsContent	P3P review	23	Words and expressions contained in the body of a communication (eg, emails, bulletin board postings, and chat room entries)
I	2	3	2	InteractionContent	P3P review	14	Information actively generated from or reflecting explicit interactions with an organizational information system (eg, queries to a search engine or logs of account activity)
I	2	3	3	LocationContent	P3P review	14	Information that identifies consumers' current physical location (eg, GPS positions)
I	2	3	4	NavigationContent	P3P review	23	Information passively generated by information system use (eg, information retrieved and time spent)
I	2	3	5	OnlineContactsContent	P3P review	8	Online contact information of other consumers to facilitate communication

I	2	3	6	PurchasesContent	P3P review	20	Information actively generated by purchases conducted within the information system
I	2	4		ConsumerDetailsContent	App review	47	Information on the consumer
I	2	4	1	DemographicsContent	P3P review	29	Demographic and socioeconomic information
I	2	4	2	FinancesContent	P3P review	22	Information on consumers' finances (eg, account balance and payment or overdraft history)
I	2	4	3	HealthContent	P3P review	23	Information about consumers' physical or mental health, sexual orientation, and use of or inquiry into health care services or products
I	2	4	4	IdeologicalContent	P3P review	9	Affiliations with groups (eg, religious organizations, trade unions, professional associations, and political parties)
I	2	4	5	PreferencesContent	P3P review	30	Information about consumers' likes and dislikes (eg, favorite color)
I	2	4	6	UserDeviceContent	P3P review	19	Information about consumers' client devices (eg, IP address, domain name, browser type, or operating system)
M				MetaInformationContent	App review	45	Content aspects that are not directly related to information privacy practices but still topically relevant for organizational information privacy communications
M	1			CertificationContent	App review	27	Certifications of the information system or the organization
M	2			ContactContent	Lit review	21	Contact information of the organization
M	3			EffectiveDateContent	Lit review	0	Date from which the stated information privacy practices are in effect
M	4			FollowedGuidelinesContent	App review	6	Guidelines the organization follows
M	5			FollowedLawsContent	App review	14	Laws with which the organization or the information system is compliant
M	6			LastUpdateContent	Lit review	12	Date of the last time the stated information privacy practices were updated
M	7			MinimumUserAgeContent	Lit review	0	Outlines the targeted age group (especially important to ascertain whether children are targeted)
M	8			ProviderNameContent	Lit review	17	Name and related information on the organization
O				OfferedPrivacyControlContent	App review	55	Captures offered information privacy controls
O	1			AccessAuditContent	App review	5	Enable consumers to retrieve access logs for their information
O	2			BreachNotificationContent	App review	7	Captures how consumers are notified about breaches of information privacy

O	2	1	BreachNatureContent	App review	0	Notification about what was breached
O	2	2	BreachOccurenceContent	App review	1	Notification that a breach occurred
O	2	3	BreachRemediesContent	App review	0	Notification about remedies offered for breach
O	3		ChangeHistoryContent	Lit review	0	Information on past information privacy practices and performed changes
O	4		ChangeGovernanceContent	Lit review	0	Explains how changes in information privacy practices reflect on already collected information
O	5		ChangeNotificationContent	P3P review	15	Notification about changes of information privacy practices
O	6		ConsentManagementContent	P3P review	0	Illustrates all consents, explicit and implicit, and enables consumers to revoke and modify given consents
O	7		DisputeRemedyContent	P3P review	16	Remedies offered for justified disputes regarding information privacy practices
O	8		DisputeResolutionContent	P3P review	28	Means offered for resolving disputes regarding information privacy practices
O	9		DownstreamPropagationContent	Lit review	5	Describes how changes to information, especially consumer-made corrections and deletions of information, are communicated with and propagated to any third party with which the information was shared
O	10		PrivacyManagementBoundariesContent	App review	20	Captures the boundaries for information privacy management (eg, information requests by law enforcement or control over information privacy practices of subsidiaries)
O	11		PrivacyPracticeMonitoringContent	Lit review	21	Describes how the actual information privacy practices of the organization are monitored
O	11	1	AutomatedMonitoringContent	Lit review	1	Automated monitoring of information privacy practices (eg, by some software)
O	11	2	IndependentMonitoringContent	Lit review	10	Monitoring of information privacy practices by an independent party
O	11	3	InternalMonitoringContent	Lit review	5	Monitoring of information privacy practices by the organization
O	12		SecondaryUseConsentContent	Lit review	10	Describes how consumers are contacted for affirmative consent (opt-in) prior to any secondary use (ie, use of consumer information for any purpose other than for which it was collected)
O	13		UserAccessContent	App review	50	Captures the permissions that consumers have to access collected information

P			PracticeRationaleContent	P3P review	62	Captures the purposes for which information privacy practices are performed
P	1		CommunicationContent	App review	46	To provide communication features
P	1	1	ContactContent	P3P review	34	Contacting consumers without previous request by consumers
P	1	2	FeedbackContent	P3P review	5	Responding to the consumer (eg, respond to consumer query)
P	1	3	MarketingContent	P3P review	38	Advertising, marketing, or promotion purposes
P	1	4	UserCommunicationContent	P3P review	2	Facilitating communication between consumers
P	2		OfferedServiceContent	App review	44	To provide services offered by the information system
P	2	1	FinancialManagementContent	P3P review	2	Banking and financial management
P	2	2	HealthProductsContent	P3P review	2	To offer products or services that relate to consumers’ physical or mental health
P	2	3	PaymentContent	P3P review	0	Payment and transaction facilitation (the organization is processing the payment)
P	2	4	PhysicalDeliveryContent	P3P review	1	Physical delivery of a product
P	2	5	SalesContent	P3P review	7	Conducting a business transaction with the consumer (eg, completing a sale)
P	3		PersonalizationContent	App review	41	Personalization of the information system
P	3	1	IndividualAnalysisContent	P3P review	29	To determine the habits, interests, or other characteristics of consumers and combine them with identified information for research, analysis, and reporting
P	3	2	IndividualDecisionContent	P3P review	7	To determine the habits, interests, or other characteristics of individuals and combine them with identified information to make a decision that directly affects that individual
P	3	3	PseudoAnalysisContent	P3P review	20	To determine the habits, interests, or other characteristics of consumers for research, analysis, and reporting based on pseudonymous identifiers
P	3	4	PseudoDecisionContent	P3P review	1	To determine the habits, interests, or other characteristics of individuals to make a decision that directly affects that individual based on pseudonymous identifiers
P	4		PublicWelfareContent	App review	11	To contribute to public welfare
P	4	1	ArtsContent	P3P review	0	For delivering the arts (eg, music, literature, and movies)
P	4	2	CharityContent	P3P review	0	For charitable purposes

P	4	3	EducationContent	P3P review	0	For educational purposes
P	4	4	GovernmentContent	P3P review	10	For online government services (eg, voter registration)
P	4	5	HistoricalContent	P3P review	1	For the purpose of preserving social history
P	4	6	ResearchContent	P3P review	5	To support research projects
P	5		ServiceOperationContent	App review	27	To operate the information system
P	5	1	CoreFunctionalityContent	P3P review	14	To conduct and support activities for which information was provided
P	5	2	AdministrationContent	P3P review	6	For information system administration
P	5	3	DevelopmentContent	P3P review	11	To enhance, evaluate, or review the information system
P	5	4	LegalObligationsContent	P3P review	8	To fulfill duties enforced by law (eg, court proceedings) or for other legal purposes
P	6		TechnicalDetailsContent	App review	22	For technical purposes
P	6	1	AccountManagementContent	P3P review	15	For consumer account management
P	6	2	SessionManagementContent	P3P review	9	To keep track of sessions and application states

Table 20. Brief overview of all articles in the final sample of the literature review, including the article category, and the number of content aspects mentioned in the article.

Reference	Category	Article aims	#content aspects
(Ciocchetti 2007)	Content prescription	Proposes a new federal law designed to make electronic privacy notices more effective	82
(Mundy 2006)	Content assessment	Analyzes privacy notices on popular UK healthcare-related web sites to determine the extent to which consumers' information privacy is protected	63
(Rizk et al. 2010)	Content analysis	Studies the information privacy concerns of social networking site providers with respect to consumers and other stakeholders to understand how these topics are related to each other in the documents, and studies the construction of the different roles, responsibilities and accountabilities assigned to the different stakeholders	60
(Beldad et al. 2009)	Content assessment	Dissects the contents of privacy notices on municipal websites and determines whether the contents of privacy notices on Dutch municipal websites coincide with the significant provisions in the Dutch law 'Wet Bescherming Persoonsgegevens'	59
(Magi 2010)	Content assessment	Assesses whether library resource vendors collect consumer information and handle that information in accordance with information privacy standards articulated by the library profession and the information technology industry	58

(O’Connor 2003)	Content assessment	Assesses whether hotel web sites collect personal information and what reassurances they give customers about what will be done with their personal information, whether hotel web sites display privacy notices and conform to international norms, whether hotel web sites make use of trust marks or privacy seals, and whether hotel web sites conform to their stated privacy policies	58
(Desai et al. 2012)	Content prescription	Reviews enforcement actions of the Federal Trade Commission, especially, as they relate to the commissions recently released Privacy Report and provides a set of practical tips and best practices to assist businesses in staying aligned with emerging trends in consumer information privacy protection	57
(Kubis 2010)	Content prescription	Proposes a solution to the information privacy concerns raised by services like Google Books	57
(Stitilis and Malinauskaite 2013)	Content assessment	Analyzes the compliance with basic principles of data protection in selected consumer-oriented cloud service contracts and highlights the adequate level of data protection in the contracts	56
(Cha 2011)	Content assessment	Investigates the depth of personal information that web proprietors collect from consumers in conjunction with the privacy notices of their sites	56
(Hooper and Evans 2010)	Content assessment	Analyzes the terms of use and privacy notices of six social networking sites against the agreed national values on information handling promulgated in the New Zealand Privacy Act of 1993	55
(Hooper and Vos 2009)	Content assessment	Examines the extent to which New Zealand business web sites conform to the provisions of the New Zealand Privacy Act of 1993	53
(LaRose and Rifon 2006)	Content assessment	Examines whether website proprietors are tacitly following a theory of privacy behavior that assumes that website proprietors have an interest in collecting consumer information and that consumer disclosure of personal information is often the currency of exchange to obtain the desired outcomes at a website	52
(Pollach 2006)	Content analysis	Examines systematically what data handling practices companies engage in, which ones they do not engage in, and whether they fail to address important areas of concern to consumers	51
(Liu and Arnett 2002)	Content assessment	Examines web sites of the Global 500 and shows that different countries greatly vary in their use of privacy notices on their web sites and their use of seal programs as visible signs of attention to information privacy concerns	50
(Hong et al. 2005)	Content assessment	Explores the information collection practices and privacy notices of online news sites	49
(Ashrafi and Kuilboer 2005)	Content assessment	Examines information privacy issues in the context of fair information practices and how they are perceived and practiced by the top 500 interactive companies in the United States	47

(Proctor et al. 2008)	Consumer perception study	Examines the types of information solicited by different categories of web sites and whether consumers are able to comprehend a sites privacy notice to reveal whether the requested information varies within and between different categories of sites and whether it is necessary for the site to complete a transaction or provide a service	47
(Robles-Estrada et al. 2006)	Content assessment	Explores and analyzes the content of 120 privacy notices from online companies established in Mexico to address all information privacy dimensions that seem to be important in online environments	46
(Papacharissi and Fernback 2005)	Content analysis	Evaluates the overall efficacy of privacy notices and focuses on the language, format, information privacy reassurances, complexity of legal and technical terms, and perceived statement credibility	45
(Kim and Yi 2010)	Content analysis	Enquires how commercial sites targeting children endeavor to protect personal information and how children face the possibility of personal information exposure on the web, and discusses a plan to reduce the risk of information privacy invasion	45
(Hooper et al. 2007)	Content analysis	Explores whether information privacy principles might be applied as a basis for assessing banking websites for responsible business practices in electronic commerce	43
(Cottrill 2011)	None	Attempts to provide a clear review of the methods by which information privacy protection may take place at the levels of law, technology, and management	43
(Rains and Bosch 2009)	Content assessment	Reports a content analysis of the privacy notices from 97 general reference health web sites that was conducted to examine the ways in which visitors' information privacy is constructed by health organizations	43
(Bulgurcu et al. 2010)	Consumer perception study	Investigates what consumers' perceived information privacy issues are in an online social networking site, what triggers consumers' attribution of an informational practice to an information privacy issue, and what are outcomes of consumers' perceived information privacy issues	43
(Almatarneh 2011)	Content assessment	Assesses and evaluates the level to which the privacy of personal information is maintained and protected in Jordan	42
(Langenderfer and Cook 2004)	None	Examines different regulatory mechanisms that protect information privacy and their strengths and weaknesses	42
(McRobb and Rogerson 2004)	Content assessment	Surveys privacy notices to reach a better understanding of privacy notices on the internet and the interplay between these notices and other factors	42
(Culnan 2000)	Content assessment	Assesses the extent to which 361 consumer-oriented commercial Web sites post disclosures that describe their information practices and whether these disclosures reflect fair information practice principles	40

(Peslak 2005)	Content assessment	Provides a background on internet privacy, summarizes prior internet privacy studies, updates and expands on internet privacy studies, and proposes an expanded factor analysis as a guide for future studies	39
(Hossain and Dwivedi 2014)	Consumer concerns	Explores the catalysts of perceived privacy taking RFID as a representative technology and applying it in national applications	39
(Schuele 2005)	Content assessment	Assesses the degree to which cities address issues of information privacy on their web sites	38
(Stanaland et al. 2009)	Content assessment	Examines how differences in regulatory information privacy environments manifest in privacy information offered to parents on children's web sites in the US and UK	37
(Savirimuthu 2013)	None	Clarifies the content and application of data protection and privacy rights and outlines a policy framework that will address the lack of specificity on how innovation and information privacy issues can be better calibrated	37
(Pollach 2007)	Content analysis	Investigates why privacy notices fail to effectively communicate data handling practices	36
(Milne and Culnan 2002)	Content assessment	Addresses methodological issues related to using surveys of online privacy notices in the public policy process to evaluate the voluntary posting of privacy notices and the extent to which these disclosures are based on fair information practice principles	35
(H. Xu et al. 2011)	Consumer perception study	Explores the link between individual information privacy perceptions and institutional information privacy assurances	35
(Meinert et al. 2006)	Consumer perception study	Examines the willingness of individuals to provide various types of information based on varying levels of protection offered by privacy notices	35
(Kuzma 2011)	Tool-supported privacy feature crawl	Analyzes the level of information privacy protection among 60 major online social networks throughout the world	34
(McGrath 2011)	Consumers' content preferences	Gathers information about the importance of privacy notices and their contents on social networking web sites	33
(Faja and Trimi 2006)	Consumer concerns	Attempts to answer the question of whether having more information privacy–related elements in a web site results in better perceptions of information privacy which in turn would result in a greater willingness to disclose information and to buy from the site	33
(Schwaig et al. 2006)	Content assessment	Examines the information privacy practices and policies of the Fortune 500 in order to assess how well their privacy notices adhere to fair information practice principles, develops a way to analyze the maturity level of firms with respect to their information privacy disclosure, and determines the extent and substance of online privacy disclosure among the largest and most influential US firms	32
(Kuzma 2010)	Content assessment	Analyses the level of information privacy protection among 50 US Senate web sites	32

(Cai et al. 2003)	Content prescription	Examines the amount and types of personal information collected from children online in October 2000, approximately two years after COPPA was passed by Congress and six months after implementation, and assesses the degree to which website providers complied with COPPA rules	31
(Strickland and Hunt 2005)	Content prescription	Investigates whether the public understands RFID technologies and the manner in which personally identifiable information may be collected, maintained, used, and disseminated and whether the public consents to these information practices	30
(Schwaig et al. 2005)	Content analysis	Examines the reasons for firms to invest organizational resources in a consumer protection mechanism that consumers rarely access and the reasons why researchers rely on compliance to fair information practice principles as a measure of whether or not self-regulation is working and as a surrogate for consumer protection	30
(Yee and Korba 2013)	Content prescription	Presents two semi-automated approaches for obtaining personal privacy notices for consumers	29
(Clarke 2006a)	Content assessment	Evaluates privacy notices against a normative template in order to assess the extent to which they are likely to represent effective protection of information privacy	29
(Zhang et al. 2007)	Content assessment	Examines the leading international companies' online privacy notices, particularly of firms that are on Forbes' Global 2000 list	29
(Kaupins and Reed 2012)	Content analysis	Examines how new media and privacy notices have penetrated the top twelve online newspaper websites in the Baltic States (Estonia, Latvia, and Lithuania)	29
(Metzger 2006)	Consumer perception study	Explores how characteristics of online vendors and consumers interact with web site communications to affect consumer behavior online	29
(Fang 2010)	Content prescription	Discusses a case where the privacy notice offered by the US retailer Sears was determined to be deceptive by the Federal Trade Commission and recommends five measures for effective privacy disclosures	28
(Shalhoub 2006)	Content assessment	Evaluates the contents of privacy notices from a sample of Gulf Cooperation Council companies engaged in electronic commerce transactions	26
(de Beaufort Wijnholds and Little 2001)	None	Explores legal and environmental issues with respect to information privacy, security, taxation, and liability	25
(Timpson and Troutman 2009)	Privacy notice design	Investigates the lack of real standards or specifications as to how privacy notices should be issued and what specific content should be included	21
(McRobb 2006)	Consumer perception study	Investigates how readers understand the meaning of a small set of privacy notices	20
(Suominen 2012)	Content prescription	Aims to better understand the requirements for using health data in research internationally by comparing international, Australian, and Finnish frameworks	18

(Garrison et al. 2012)	Privacy notice design	Identifies barriers to consumer understanding of privacy notices and develops an alternative privacy notice design that consumers could more easily understand and use	17
(Wu et al. 2012)	Impact quantitative	Investigates why consumers with different cultures react differently to the content of various privacy notices which may influence their trust or willingness to provide personal information	16
(Weitzman et al. 2011)	Content assessment	To foster informed decision-making about health social networking by patients and clinicians, the authors evaluate the quality and safety of social networking sites' policies and practices	12
(Unruh et al. 2004)	Content prescription	The objectives of this study were to identify women's preferences for receiving online breast cancer risk information, to identify barriers to accessing this information, and to identify differences in these factors between internet consumers and non-consumers	9
(Tavani 2007)	Content prescription	Articulates a definition of information privacy that can serve as a foundation for a theory of information privacy and shows how this theory enables online privacy notices that are clear transparent and consistent	7
(Tsai et al. 2011)	Consumer perception study	Determines whether a more prominent display of privacy information will cause consumers to incorporate information privacy considerations into their online purchasing decisions	4

6 Meaningful Organizational Information Privacy Communication in Consumer Information Systems

Authors: Tobias Dehling, Ali Sunyaev

Abstract: This study explores how to make organizational information privacy communication in consumer information systems meaningful. Organizational information privacy practices remain largely opaque to consumers because extant organizational information privacy communications provide either too abstract, too much, or too specific information. We advance extant research on information privacy communication by conceptualizing design of meaningful organizational information privacy communication in form of an information systems design theory for transparent communication of information privacy practices (TIPP theory), which is informed by two kernel theories from the domains of interpersonal communication and educational psychology—Uncertainty Reduction Theory and Cognitive Load Theory. In essence, organizations aiming to establish transparency of organizational information privacy practices must balance comprehensiveness of communicated information and avoidance of cognitive overload. The information systems design knowledge and the insights captured in the TIPP theory put common organizational practices, such as posting privacy notices or privacy seals, into question.

Keywords: information privacy communication, organizational information privacy practices, consumer information systems, transparency, information systems design theory, information privacy

6.1 Introduction

Privacy[6] is a prevailing challenge only intensified during the Information Age (Mason 1986). An unresolved question impeding organizations from accounting for privacy in consumer information systems[7] is how to make organizational privacy communication—that is, exchange of information about privacy practices between organizations and their customers—meaningful. With the concept meaningful organizational privacy communication, we refer to communication between organizations and consumers that enables consumers to comprehend the meaning of communicated information and satisfies consumers' information needs with respect to organizational information privacy practices in consumer information systems.

[6] Within the scope of this work we focus on information privacy and not on other facets of privacy, such as bodily, spatial, or behavioral privacy (Koops et al. 2016). For the sake of brevity, we use the term privacy synonymous to information privacy throughout this manuscript.

[7] Within the scope of this work, the term consumer information system refers to any socio-technical system open to consumers in which information technology is employed to process information. Consumer information systems are a suitable research context because such systems depend on voluntary use and organizations can use attention to information privacy as one potential lever to make their information systems more attractive to consumers than information systems of competitors.

Organizational privacy communication has been approached by two dominant literature streams. On the one hand, organizational, legal, and public policy scholars focus predominantly on uniform, normative solutions to make information on organizational privacy practices available to consumers in a consistent and controllable way—the communication generalization stream. Communication approaches proposed, investigated, and refined by the communication generalization stream are usually concerned with privacy notices or privacy seals (eg, Garrison et al. 2012, Milne and Culnan 2002, 2004, Miyazaki and Krishnamurthy 2002, Pollach 2006). On the other hand, computer science scholars focus predominantly on specialized tools that target specific information needs and may also work without organizational involvement—the communication specification stream. Communication approaches proposed, investigated, and refined by the communication specification stream focus on dedicated and isolated information needs, such as identifying select matches and mismatches between organizational privacy practices and consumer preferences (eg, Bélanger et al. 2013, Tsai et al. 2011), revealing undisclosed privacy practices (eg, Bal et al. 2015, Balebako et al. 2013), or facilitating privacy management (eg, Abiteboul et al. 2015, Xu, Crossler, et al. 2012).

Both streams attest to the importance of organizational privacy communication since they focus on making information on organizational privacy practices available to consumers. Yet, neither generalized privacy communication nor specific privacy communication is meaningful due to inadequacy to account for the contextual nature of privacy (Miltgen and Peyrat-Guillard 2014, Nissenbaum 2009, Smith et al. 2011, Xu, Teo, et al. 2012). Generalized privacy communication usually does not provide the information consumers are interested in (Earp et al. 2005). Even if generalized privacy communications, such as privacy notices, offered all the information of interest to costumers in all contexts, they would require too much effort for information retrieval to be of use to consumers (McDonald and Cranor 2008). Specific privacy communication, on the other hand, is too specialized to be of use in diverse contexts. Requiring consumers to keep track of and become accustomed with the wide range of specialized tools required to satisfy information needs will, for most consumers, result in too high demands on digital literacy and privacy literacy (Acquisti et al. 2015, Park 2013).

In this work, we advance extant research on organizational privacy communication by conceptualizing a design space for organizational privacy communication that bridges the communication generalization and the communication specification stream. We envision organizational privacy communication as a continuum of design alternatives for communication of organizational privacy practices. On the one end of the continuum, communication approaches are focused on general communication demonstrating compliance with generic norms, such as fair information practice principles (Organisation for Economic Cooperation and Development 1980, US Federal Department of Health Education and Welfare 1973). On the other end of the continuum, communication approaches are focused on specialized tools for identification and communication of actual privacy practices and often offered in a way beyond the control of organizations. To establish a foundation for organizational privacy communication that is meaningful and suitable to account for the contextual nature of privacy, we focus on the design of organizational privacy communication across the privacy communication continuum, that is, communication that establishes transparency of organizational privacy practices. We answer the following research question:

> *How to design components of consumer information systems that communicate organizational privacy practices in a meaningful way?*

To answer the research question, we develop an information systems design theory (*TIPP theory*[8]) capturing what to build to establish transparency of organizational privacy practices—an individual's subjective perception of being informed about relevant organizational privacy practices (Eggert and Helm 2003)—and why. To inform *TIPP theory* development, we predominantly drew from the shortcomings and strengths of existing approaches to organizational privacy communication and extant literature yielding insights on the information relevant to establishing transparency of organizational privacy practices. The *TIPP theory* constitutes prescient knowledge (Corley and Gioia 2011) that captures the core characteristics of meaningful organizational privacy communication and opens up a whole new spectrum of intermediate opportunities between the end points of the privacy communication continuum.

Our research contributes to the scientific knowledge base in three main ways. First, extant research on transparency employs the concept ambiguously and is, for instance, focused on examining individual perceptions related to transparency (eg, Awad and Krishnan 2006), quantitative operationalization of transparency (eg, Schnackenberg and Tomlinson 2016), design processes fostering transparency (eg, Nussbaumer et al. 2012), or types of organizational transparency (eg, Hultman and Axelsson 2007). Our research complements extant research on transparency by introducing a conceptualization of transparency of organizational privacy practices and focusing on characterization of the design product (Gregor and Jones 2007)—that is, components of consumer information systems for meaningful communication of organizational privacy practices that makes organizational privacy practices transparent to consumers. Second, prior research employed the concept of privacy practices ambiguously, for example, concordance with selections of fair information practice principles, privacy-related organizational practices, or protective consumer behavior (Bélanger and Crossler 2011). In this manuscript, we consolidate extant literature on organizational privacy practices and identify the privacy practices relevant for transparency of organizational privacy practices. Finally, we bridge extant literature streams on privacy communication and develop an information systems design theory for organizational privacy communications that are virtually non-existent in today's information systems landscape: the class of organizational privacy communications establishing transparency of organizational privacy practices.

[8] The TIPP theory is an information systems design theory capturing design knowledge on what to build to establish transparency of organizational information privacy practices in consumer information systems and why. We refer to the TIPP theory with the acronym TIPP. In all other cases, 'transparency of organizational privacy practices' is written out in full.

This manuscript proceeds as follows. First, we review relevant extant research and clarify the concepts important for the development of information systems design theory. Second, we present the individual components of the developed information systems design theory. This manuscript concludes with a discussion of the implications to theory and practice.

6.2 Research Background

6.2.1 Organizational Privacy Communication

Extant research on organizational privacy communication yields limited guidance for the design of meaningful organizational privacy communication. This shortcoming can be attributed to the vagueness and variety of employed privacy conceptualizations (Smith et al. 2011). Extant privacy conceptualizations are either too broad and not instructive or too narrow, such that important facets of privacy are neglected (Solove 2002). Common privacy conceptualizations follow, for example, a rights-based, a control-based, or a market-based view (Smith et al. 2011, Solove 2002, Tavani 2007). Privacy conceptualizations following a rights-based view stipulate that everyone has a right to keep select information out of the public eye (Warren and Brandeis 1890). Control-based privacy conceptualizations advocate for giving individuals control over collection and use of information (Westin 1967). Those following a market-based view postulate that individuals can trade information in exchange for other goods and that privacy can be governed by market mechanisms (Laudon 1996). Such diverging conceptualizations yield limited input for design of meaningful organizational privacy communication for five main reasons.

First, it is difficult to identify clear boundaries between information that should be private and that should not be private. For example, health information can, on the one hand, reveal intimate and personal details about individuals and should be kept private. On the other hand, health information also yields valuable insights for public health research and should be available for research (Horvitz and Mulligan 2015, Rindfleisch 1997). Second, privacy spans entities and levels of society (Bélanger and Crossler 2011, Conger et al. 2013). For example, information commonly known within one's family may be considered private within one's circle of friends and vice versa. Third, privacy is subject to contextual influences (Miltgen and Peyrat-Guillard 2014, Smith et al. 2011, Xu, Teo, et al. 2012). Individuals are, for instance, more likely to disclose information in informal settings than in formal settings (John et al. 2011). Fourth, everyone has a different intuitive conceptualization of privacy shaped through one's interactions with society (Laufer and Wolfe 1977). Consequently, it is difficult to negotiate acceptable privacy practices between involved parties (eg, consumer and organization) due to different internal conceptualizations of privacy (Greenaway et al. 2015, Schwaig et al. 2013). Finally, organizational information processing is complex, can hardly be traced, and is often conducted under secrecy, making assessments of impacts on privacy difficult (Acquisti et al. 2015, Solove 2001).

Instead of focusing on satisfying diverging privacy conceptualizations, we elaborate a different approach to account for privacy in consumer information systems—that is, focusing on meaningful organizational privacy communication that establishes transparency of organizational privacy practices. Establishing transparency of organizational privacy practices allows consumers to ascertain whether organizational privacy practices align with their privacy conceptualizations and enables organizations, by showcasing acquiescence to privacy norms or what compromises they offer, to differentiate from competitors that employ more deceptive strategic responses to privacy norms (Oliver 1991). We communicate our results in the form of an information systems design theory to clearly conceptualize transparency of organizational privacy practices and to outline what to build for meaningful organizational privacy communication.

6.2.2 Information Systems Design Theory

Information systems design theory "shows the principles inherent in the design of an IS artifact that accomplishes some end, based on knowledge of both IT and human behaviour" (Gregor and Jones 2007, p. 322). The essence of information systems design theory is prescriptive knowledge specifying abstract artifacts suitable to achieve metarequirements through a metadesign (Gregor and Jones 2007, Kuechler and Vaishnavi 2012, Walls et al. 1992). The metarequirements specify the design purpose or goal. The metadesign outlines an abstract representation of the focal features of the class of artifacts to be developed.

To formulate the *TIPP theory*, we use the components proposed by Gregor and Jones (2007). The first component (constructs) captures the entities of interest in information systems design theory. The second component (purpose and scope) outlines the goal, metarequirements, and boundary conditions. The third component (justificatory knowledge) refers to theories supporting the information systems design theory by informing and explaining the design rationale. The fourth component (principles of form and function) defines "the structure, organization, and functioning of the design product or design method" (Gregor and Jones 2007, p. 325). The fifth component (artifact mutability) specifies how the metadesign accounts for artifact evolution and adaptation to context. The sixth component (testable propositions) presents propositions focusing on how the metadesign fulfills the metarequirements and to what degree the design objectives are fulfilled. The seventh component (principles of implementation) offers guidance and support for instantiating the developed information systems design theory. The eighth component (expository instantiation) presents an illustrative instantiation of the theory to ease communication.

6.3 Information Systems Design Theory for Transparency of Organizational Privacy Practices

6.3.1 Constructs

Privacy Practices. Two salient perspectives on privacy practices are individual privacy practices and organizational privacy practices (Bélanger and Crossler 2011). Individual privacy practices are concerned with privacy-related consumer actions (eg, sharing or withholding of information, tracking of information flows, or consent management). The present research is concerned with organizational privacy practices, that is, organizational practices that are concerned with information collection and use, the protection of information from intrusion, the restriction of access to information, and the facilitation of privacy management (Tavani 2007).

Transparency of Organizational Privacy Practices. Transparency is "an individual's subjective perception of being informed about the relevant actions and properties of the other party" (Eggert and Helm 2003, p. 103). Analogously, transparency of organizational privacy practices is an individual's subjective perception of being informed about the relevant organizational privacy practices of the other party.

Relevance is not an unequivocal concept and manifests in various ways. Different facets of relevance can be categorized into algorithmic and affective dimensions of relevance (Cosijn and Ingwersen 2000). Within the scope of this research, we focus on affective relevance.[9] Affective relevance focuses on subjective perceptions of relevance (eg, relations between information needs or tasks at hand and offered information). Affective relevance ensures that communicated information is not off-topic and that consumers are not overburdened with information unnecessary for the tasks they are performing (eg, informing consumers with devices configured to not accept cookies about cookie policies). Meaningful organizational privacy communication must thus communicate all information on organizational privacy practices perceived as relevant by consumers and account for peculiarities induced by the situational contexts of individual consumers.

6.3.2 Purpose and Scope

The *TIPP theory* is focused on consumer information systems. The purpose of the *TIPP theory* is to facilitate meaningful communication of organizational privacy practices. Figure 18, adapted to the information systems context from the Organon Model of Language (Bühler 2011, p. 35), illustrates the scope of the *TIPP theory*. The *TIPP theory* constitutes a metaspecification of what to build for meaningful organizational privacy communication. Instantiations of the *TIPP theory* are thus information system components or stand-alone information systems for organizational privacy communication.

[9] Algorithmic relevance focuses on information retrieval through algorithms.

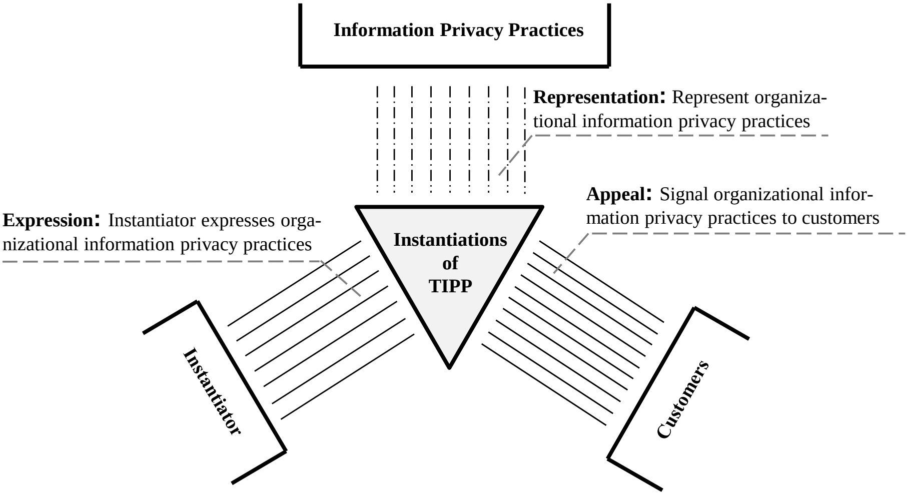

Information Privacy Practices
Representation: Represent organizational information privacy practices
Appeal: Signal organizational information privacy practices to customers
Expression: Instantiator expresses organizational information privacy practices
Instantiations of TIPP
Instantiator
Customers

Figure 18. Scope of the TIPP theory (triangle). The TIPP theory is focused on meaningful communication of organizational privacy practices to consumers. Adapted from the Organon Model of Language (Bühler 2011, p.35).

Consumer information systems usually cater to large consumer bases. Accordingly, it is unfeasible to satisfy consumers' privacy information needs on a per-query basis. Instead, privacy communications constitute upfront responses to unknown information requests of consumers. *TIPP instantiators* prepare precompiled bundles of information and present them to consumers. *TIPP instantiations* cater to consumers in diverse situations and with different individual characteristics (Smith et al. 2011) so that the provision of a wide range of information is required to satisfy the different information demands. Hence, the first metarequirement is as follows:

> ***Metarequirement 1:*** *Consumer information systems aiming to establish transparency of organizational privacy practices must offer a comprehensive selection of information on organizational privacy practices (comprehensiveness).*

Although comprehensiveness[10] is a reasonable fit for the needs of the entire consumer base, comprehensiveness is not a goal in itself. Although communication of a comprehensive selection of information is required to account for the diversity of consumers' information needs, communication of too much information leads to information overload (Cowan 2014). Consequently, to reduce the amount of information consumers must process, transparency of organizational privacy practices requires that no infor-

[10] It is important to note that comprehensiveness will never be equal to completeness as long as technological innovation exists (eg, new methods for information collection or new approaches to foster privacy management).

mation unrelated to privacy practices is offered (eg, information on general privacy management skills, such as disabling cookies in web browsers). The second metarequirement is as follows:

> ***Metarequirement 2:*** *Consumer information systems aiming to establish transparency of organizational privacy practices must offer only topically relevant information (topical relevance).*

Comprehensiveness and topical relevance focus on the useful expression and representation of organizational privacy practices but do not promote appeals of interest to consumers. As in any information searching context, consumers will be interested in obtaining information on privacy practices if they are confronted with an anomalous state of knowledge, for example, an absence of desired knowledge or inconsistencies in their knowledge.[11] Anomalous states of knowledge can be remedied by satisfying resulting information needs (eg, determining whether a privacy practice is carried out or not carried out). To satisfy information needs, consumers shift among information-seeking strategies (eg, searching for information, acquiring information, comparing information) until they have fulfilled or abandoned their search goals (Xie 2000). Accordingly, organizational privacy communication promoting appeals of interest to consumers must foster affective relevance by being flexible and interactive so that changes in consumers' information needs over time and across different consumers can be accounted for (Rouse and Rouse 1984). The third metarequirement is as follows:

> ***Metarequirement 3:*** *Consumer information systems aiming to establish transparency of organizational privacy practices must adapt information presentation to consumers' information needs (interactivity).*

6.3.3 Justificatory Knowledge

How and why *TIPP instantiations* are capable of meaningful organizational privacy communication can be explained by two theories from the domains of interpersonal communication (Uncertainty Reduction Theory; Berger and Calabrese 1975) and educational psychology (Cognitive Load Theory; Kalyuga 011, Sweller 1988). Uncertainty Reduction Theory explains what information needs to be communicated by *TIPP instantiations* (Berger and Calabrese 1975). Initial interactions between two strangers are characterized by a high degree of uncertainty. Both parties strive to reduce uncertainty to restrict the realm of likely possibilities and improve the understanding and predictability of the other's behavior. Once uncertainty is sufficiently reduced, both parties can assess whether the other behaves in an acceptable way and want to continue the relationship or whether they rather discontinue the relationship. In short, "increases in uncertainty level produce decreases in liking; decreases in uncertainty level produce increases in liking" (Berger and Calabrese 1975, p. 107). With respect to meaningful organizational privacy communication, Uncertainty Reduction Theory reinforces the

[11] More formally, an anomalous state of knowledge is "a recognized anomaly in the user's state of knowledge concerning some topic or situation and that, in general, the consumer is unable to specify precisely what is needed to resolve that anomaly" (Belkin et al. 1982, p. 62).

comprehensiveness metarequirement. Uncertainty with respect to organizational privacy practices must be sufficiently reduced so that consumers feel informed. Therefore, *TIPP instantiations* must offer a comprehensive selection of information to cater to the different information needs of all consumers.

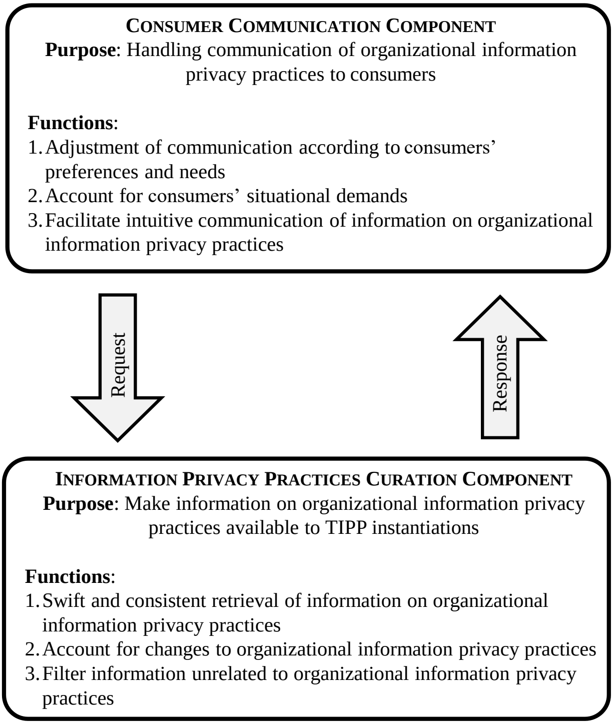
Cognitive Load Theory complements Uncertainty Reduction Theory by explaining how communication can meet the preferences and information-processing capabilities of consumers. Originally, Cognitive Load Theory is concerned with fostering understanding and learning by deriving implications for instructional design based on a model of the human cognitive architecture (Paas and Ayres 2014, Sweller et al. 1998). Cognitive Load Theory is a good fit for the *TIPP theory* because meaningful organizational privacy communication requires that consumers understand organizational privacy practices. Cognitive Load Theory is based on a model of the human cognitive architecture comprising constrained working memory and unlimited long-term memory. All understanding and learning occurs in the working memory, which can handle only a small number of information elements simultaneously (Paas and Ayres 2014). Once novel knowledge is understood and learned, it is stored in the long-term memory. The long-term memory can store an unlimited amount of knowledge with an arbitrary level of complexity (Sweller et al. 1998). The long-term memory allows humans to perform complex information acquisition tasks because knowledge can be recalled and consumes only a single element of working memory capacity, thereby freeing cognitive resources.

Cognitive resources are consumed by two types of cognitive load, intrinsic load and extraneous load (Kalyuga 2011). Intrinsic load is determined by the number and interactions of elements relevant to information acquisition tasks and individual expertise (van Merriënboer and Sweller 2005). Extraneous load constitutes noise irrelevant to information-processing tasks at hand and impedes understanding by wasting cognitive resources. Accordingly, organizational privacy communication can be improved if only topically relevant information is communicated. The second metarequirement supported by Cognitive Load Theory is that *TIPP instantiations* must be interactive. Effective designs for fostering understanding focus on reducing extraneous load and maintaining intrinsic load at levels that harness working memory capacity but do not overload it (van Merriënboer and Sweller 2010). Hence, *TIPP instantiations* must cater to the tasks consumers want to perform and must communicate information pertaining only to current tasks of consumers. Therefore, *TIPP instantiations* must be interactive to be able to adapt to consumers' tasks that vary over time and with individual differences (Rouse and Rouse 1984).

6.3.4 Principles of Form and Function

We propose an abstract architecture for *TIPP instantiations* that comprises two main components (Figure 19). The INFORMATION PRIVACY PRACTICES CURATION COMPONENT[12] is dedicated to the management of information on organizational privacy practices and

[12] To distinguish component names from the rest of the text, component names are formatted in small caps.



Consumer Communication Component

Purpose: Handling communication of organizational information privacy practices to consumers

Functions:

1. Adjustment of communication according to consumers' preferences and needs
2. Account for consumers' situational demands
3. Facilitate intuitive communication of information on organizational information privacy practices

Information Privacy Practices Curation Component

Purpose: Make information on organizational information privacy practices available to TIPP instantiations

Functions:

1. Swift and consistent retrieval of information on organizational information privacy practices
2. Account for changes to organizational information privacy practices
3. Filter information unrelated to organizational information privacy practices

Figure 19. Proposed abstract architecture for TIPP instantiations. TIPP instantiations require two main components. One component is required to maintain and curate information on organizational privacy practices. A second component is required to effectively facilitate communication of information privacy practices to consumers.

interfaces with instantiators. The Consumer Communication Component is dedicated to communicating organizational privacy practices to consumers in an interactive way.

Information Privacy Practices Curation Component. The purpose of the Information Privacy Practices Curation Component is to make information on organizational privacy practices available. Successful management of the required information in the Information Privacy Practices Curation Component requires at least three functions. First, the information must be retrievable in a swift and consistent way. Communication of organizational privacy practices can hardly be considered transparent if responses to information requests take too long or if responses are inconsistent. Second, management of information on organizational privacy practices must account for changes to organizational practices that evolve over time. Changes to organizational practices can also change organizational privacy practices. Organizational privacy communication cannot be considered transparent if outdated information is communicated. Third, irrelevant information must be filtered out. Maintenance of information consumes resources. To avoid unnecessary performance overhead, *TIPP instantiations* should only maintain information actually pertaining to organizational privacy practices.

Consumer Communication Component. The purpose of the CONSUMER COMMUNICATION COMPONENT is the communication of organizational privacy practices to the consumer base. For meaningful organizational privacy communication, the CONSUMER COMMUNICATION COMPONENT must implement at least three functions. First, communication must adapt to consumers' preferences and needs. Inflexible forms of communication are ineffective for satisfying consumers' information needs because consumers would be overburdened with irrelevant information and could only be offered limited support for identifying the information of interest to them. Second, communication of organizational privacy practices must account for situational demands. Consumers need to perform different tasks to satisfy their information needs. For example, consumers may want to compare the privacy practices of similar organizations during product selection, understand why an organization is collecting certain information when interacting with organizations, or obtain support for deletion of their information when it is no longer required. Third, organizational privacy practices must be communicated in an intuitive way. Obtaining information on organizational privacy practices is usually not the primary objective of consumers and likely to be perceived as a burden. Hence, *TIPP instantiations* need to present information in a way that suits the type of communicated information and consumers' preferences for information presentation.

6.3.5 Artifact Mutability

TIPP instantiations can be freely extended by instantiators to overcome new challenges or to offer other desired functionality. Further functions could, for instance, be added to increase automation of the INFORMATION PRIVACY PRACTICES CURATION COMPONENT or account for special requirements of individual *TIPP instantiations*. Additional functionalities monitoring information flows and checking them against rule sets derived from intended organizational privacy practices could, for example, be implemented to improve the alignment of intended and actual organizational privacy practices and decrease dependence on the knowledge of *TIPP instantiators*. The usability of the CONSUMER COMMUNICATION COMPONENT could be improved with enhanced functionality for supporting visually handicapped consumers or better information presentation on devices with small screens.

6.3.6 Principles of Implementation

The INFORMATION PRIVACY PRACTICES CURATION COMPONENT can be implemented with three modules. First, a central repository for organizational privacy practices can ensure swift and consistent retrieval of required information. Required information could be compiled prior to information requests and would be readily available. Consistency of information would be ensured as there is only a single source of information. Second, update functionality for the repository can be implemented to account for changes in organizational practices. Third, an ontology of organizational privacy practices can be used to remove irrelevant information. Checking information added or updated in the repository against an ontology would identify instances in which information does not pertain to organizational privacy practices.

The CONSUMER COMMUNICATION COMPONENT can be implemented with three modules. First, tailoring capabilities can ensure adaptation to consumers' preferences and needs (Germonprez et al. 2007). Consumers could be enabled to configure consumer interfaces to present the information and features that consumers are interested in. In addition, consumer preferences could be learned based on consumer behavior so that interfaces can be automatically adapted to inferred consumer preferences and needs. Second, different sets of features offered by *TIPP instantiations* can be compiled into ready-made configurations for supported tasks. Third, different presentation modes (eg, text, tables, lists, charts, graphs, animations) can be implemented and then combined as desired by consumers to support intuitive communication.

6.3.7 Expository Instantiation—TIPP Ontology

To illustrate the *TIPP theory*, we developed an ontology serving as a metaspecification of the information relevant for meaningful organizational privacy communication. Ontologies have been used in diverse disciplines, notably, philosophy and computer science, and there is no commonly agreed-on definition for ontologies (Guarino 1997, Smith and Welty 2001, Spyns et al. 2002). We adopt the definition of Guarino: "An ontology is an explicit, partial account of the intended models of a logical language" (1997, p. 298). The concepts in the *TIPP ontology* outline content relevant for organizational privacy communication. We refer to the concepts in the *TIPP ontology* as content aspects. For the sake of clarity and parsimony, the relationships among content aspects represent only hierarchical relationships.

We used major privacy concerns, information collection, handling of information, rationale for organizational privacy practices, and offered privacy controls (Ackerman et al. 1999, Antón et al. 2010, Earp et al. 2005) to guide the hierarchical structure of the *TIPP ontology*. Privacy concerns are useful for structuring the *TIPP ontology* because privacy concerns are a proxy for the information consumers want to obtain with respect to privacy.

To develop the *TIPP ontology,* we derived an initial version from the Platform for Privacy Preferences Project (P3P; Reagle and Cranor 1999). P3P is a domain-specific language that can be used to construct machine-readable representations of organizational privacy practices. We reviewed the P3P specification (Cranor et al. 2006), extracted all P3P elements representing content aspects, that is, referring to organizational privacy practices, and added them to the *TIPP ontology*. Based on the initial, P3P-based *TIPP ontology*, we assessed the organizational privacy practices described in privacy notices[13] of mobile health (mHealth) apps to further identify and refine content aspects.

[13] Although privacy notices are not effective in communicating organizational privacy practices, they are the most prevalent approach offered by extant knowledge in research and practice. Accordingly, we complemented the TIPP ontology based on extant privacy notices and privacy notice research.

Finally, we conducted a literature review to refine the *TIPP ontology*. The content analyses were independently conducted by the first author and a doctoral student. Conflicts in assessments were resolved through discussion. The second author was consulted to resolve remaining disputes. Once identified, new content aspects were assigned a unique identifier, annotated with a description, and added to the *TIPP ontology*. Any encountered ambiguities or inconsistencies were resolved through corresponding revisions of the *TIPP ontology* (eg, removal of duplicates, rearrangement of content aspects, and refinement of identifiers and descriptions). The following sections outline the main content aspects. Figure 20 provides an overview of the *TIPP ontology*. Table 22 in the appendix lists all content aspects with their descriptions. A detailed report on *TIPP ontology* development and an interactive representation of the *TIPP ontology* encoded in Web Ontology Language is available from the authors upon request.

Metainformation. Metainformation contains content aspects capturing organizational characteristics not directly related to organizational privacy practices. Metainformation refers to the privacy-related characteristics of organizations, including the name of the organization, contact information, laws with which the organizational privacy practices comply, and privacy-related certifications or seals.

Information Collection. Information collection content aspects capture what information is collected (type) and how information is collected (sensors). The information collection type is subdivided into content aspects capturing identifiers (eg, financial identifiers and governmental identifiers), operational information (eg, user interface navigation and consumer location), personal information (eg, demographics and preferences), and information format (eg, audio and text). Information collection sensors are specified by content aspects such as environment sensors (eg, camera and Bluetooth), location sensors (eg, Global Position System (GPS) and network connection), or software-use sensors (eg, cookies and surveys).

Handling of Information. Content aspects referring to the handling of information are subdivided into content aspects related to information sharing (eg, with advertisers and with other consumers), information retention (eg, in accordance with legal requirements), information security (during transfer, processing, and storage), and information storage (eg, on consumer device and in the cloud).

Practice Rationale. Practice rationale content aspects capture the purposes for which privacy practices are performed. The main categories of practice rationale content aspects are collection for communication (eg, marketing and responding to consumer inquiries), service provision (eg, payment and physical delivery of goods), personalization (eg, tailoring and consumer profiling), public welfare (eg, research and government services), and collection for technical details (eg, account management and session management).

Offered Privacy Controls. Content aspects addressing offered privacy controls capture organizational offerings that allow for or support consumers in exercising privacy control, including how consumers are notified if privacy is violated (eg, occurrence of

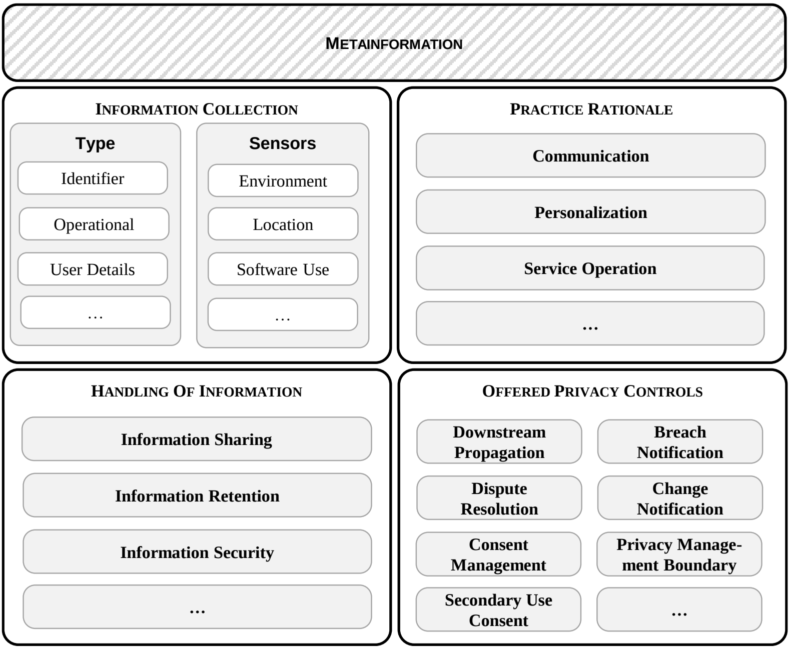


Figure 20. Partial overview of the TIPP ontology content aspects.

breach, nature of breach, and remedies offered and carried out), whether consumers can review past specifications of organizational privacy practices and are informed about which practices their information is treated under (eg, organizational privacy practices current at information collection or current organizational privacy practices), to what degree downstream propagation of consumer actions is practiced (eg, will information also be deleted in the backup tapes and databases of third parties if the consumer deletes it), and how organizations monitor compliance with intended privacy practices (eg, automated monitoring and regular independent or internal audits).

6.3.8 Testable Propositions

The purpose of this section, is to make the design knowledge captured in the *TIPP theory* and the design rationale for *TIPP instantiations* more explicit in form of testable propositions. As a foundation, we first describe the underlying concepts of transparency of organizational privacy practices with respect to *TIPP instantiation design quality*, their laws of interaction, and the possible states of *TIPP instantiations* (Dubin 1978).

Fulfillment of requirements can be represented on a scale ranging from not addressed at all over fulfilled to overfulfilled. *TIPP instantiations,* thus, account for a metarequirement in an optimal way when it is reflected in their design as much as necessary but no additional resources are expended. To what degree a requirement has to be fulfilled is determined by contextual factors beyond the scope of the *TIPP theory*, such as complexity of information flows, perceived sensitivity of collected information, and consumers' associated privacy needs. Accordingly, fulfillment of the *TIPP metarequirements* can be represented as a relational concept determined by perceived need for the metarequirement in relationship with the implementation extent of the metarequirement. Consequently, within the scope of the *TIPP theory*, the relevant underlying concepts of transparency of organizational privacy practices, are perceived need for comprehensiveness, perceived need for topical relevance, perceived need for interactivity, comprehensiveness implementation extent, topical relevance implementation extent, and interactivity implementation extent. Consequently, *TIPP instantiations* can be in four states. First, design of *TIPP instantiations* is optimal if all perceived needs for metarequirements equal the respective implementation extents. Second, *TIPP instantiations* will be unsuited for meaningful organizational privacy communication if at least one perceived need for a metarequirement is greater than the respective implementation extent. Third, if at least one perceived need for a metarequirement is less than the respective implementation extent, *TIPP instantiations* are better than they have to be. This is not undesirable with respect to establishment of transparency of organizational privacy practices but constitutes a state where organizational resources are wasted. Fourth, *TIPP instantiations* are unsuitable for meaningful organizational privacy communication and waste organizational resources if at least one perceived need for a metarequirement is greater than the respective implementation extent and at least one other perceived need for a metarequirement is less than the respective implementation extent.

A naïve approach to improving design of *TIPP instantiations* would be to elicit the perceived needs for the metarequirements and then implement them to a corresponding extent. This will however fail for two reasons. First, perceived needs will not be static due to the evolving and contextual nature of privacy (Antón et al. 2010, Nissenbaum 2009). Second, perceived needs and implementation extents interact with each other so that changes in implementation extents will invalidate prior need assessments. There are four salient laws of interaction. First, increases in comprehensiveness implementation extent reduce topical relevance implementation extent because provision of more information makes it more likely that irrelevant information is provided. Second, increases in comprehensiveness implementation extent increase perceived need for interactivity because more tasks are supported if more information is provided. Accordingly, more interactive features are required to adapt communicated information to current tasks of consumers. Third, increases in interactivity implementation extent decrease perceived need for topical relevance because interactivity simplifies retrieval of relevant information. Fourth, increases in topical relevance implementation extent decrease perceived need for interactivity because there is reduced need for filtering irrelevant information or identifying relevant information. Figure 21 depicts the underlying concepts of *TIPP instantiation design quality* including the laws of interaction.

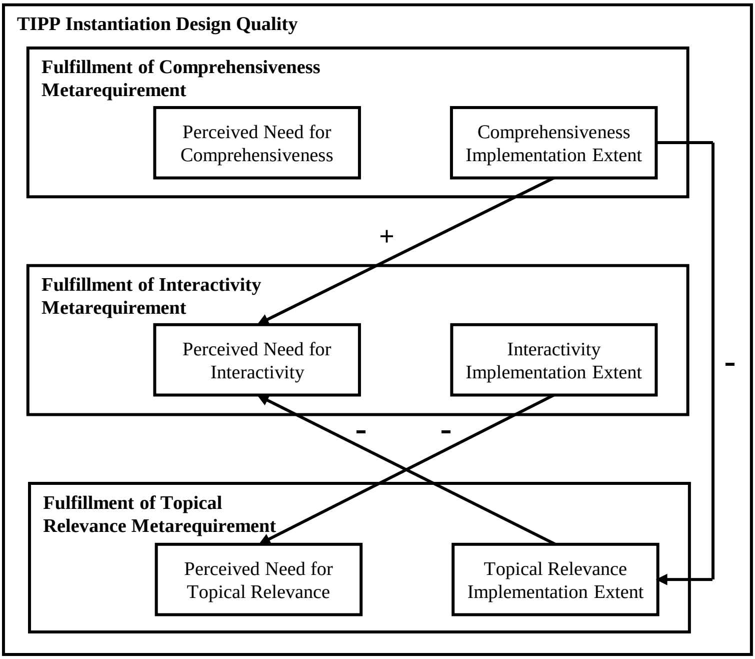

TIPP Instantiation Design Quality
Fulfillment of Comprehensiveness Metarequirement
Perceived Need for Comprehensiveness
Comprehensiveness Implementation Extent
+
Fulfillment of Interactivity Metarequirement
Perceived Need for Interactivity
Interactivity Implementation Extent
-
-
-
Fulfillment of Topical Relevance Metarequirement
Perceived Need for Topical Relevance
Topical Relevance Implementation Extent

Figure 21. Underlying concepts of TIPP instantiation design quality including their laws of interaction.

The laws of interaction support the argument that *TIPP instantiations* can be suitable to establish transparency of organizational privacy practices if they fulfill the comprehensiveness metarequirement and account for lacking topical relevance implementation extent by reducing perceived need for topical relevance through overfulfilling the interactivity metarequirement. However, also satisfying the topical relevance metarequirement will result in better designed *TIPP instantiations* because *TIPP instantiators* must maintain and communicate less information, which saves resources. In addition, more attention can be given to interactivity features supporting consumers in shaping and satisfying their information needs because the offered interactivity features do not have to remedy the lack of topical relevance. Hence, P1 and P2:

> ***P1:*** *Organizational privacy communications that do not fulfill the topical relevance metarequirement will be perceived as transparent if they fulfill the comprehensiveness metarequirement and remedy the lack of topical relevance through overfulfillment of the interactivity metarequirement.*
>
> ***P2:*** *Organizational privacy communications that fulfill all TIPP metarequirements (comprehensiveness, topical relevance, and interactivity) will be better designed than organizational privacy communications that fulfill the comprehensiveness metarequirement and overfulfill the interactivity metarequirement.*

Over time, design quality of *TIPP instantiations* will decrease because perceived needs for metarequirements change. Consumers will, for example, become accustomed with or desensitized to certain organizational privacy practices so that perceived needs for metarequirements will decrease (Solove 2002), which results in overfulfillment of metarequirements and, consequently, waste of resources. On the other hand, technological advances (eg, new sensors for information collection or new means for information analytics) will create new demands for support in information acquisition tasks or provision of information so that perceived needs for metarequirements will increase, which results in metarequirements no longer being fulfilled, thus, rendering organizational privacy communication no longer meaningful. Hence, P3 and P4:

> ***P3:*** *Design quality of organizational privacy communications decreases over time because of changes of perceived needs for metarequirements resulting in overfulfillment or nonfulfillment of metarequirements.*
>
> ***P4:*** *Decreasing time where organizational privacy communications are not in an optimal state requires constant elicitation and assessment of perceived needs for metarequirements and consequent adaption of implementation extents.*

Although it is rational to increase metarequirement implementation extents only until perceived needs for metarequirements are met to avoid unnecessary implementation efforts, decreasing implementation extents in case of decreasing perceived needs for a metarequirement may not be the best approach. First, resources required for continuing operation and maintenance may be marginal and negligible in contrast to implementation efforts for decreasing implementation extents. Second, perceived needs for metarequirements may increase again in the future. Third, some consumer segments or privacy needs may have been missed during assessment of perceived needs for metarequirements so that offered features are still useful to some consumers. Hence, P5 and P6:

> ***P5:*** *When perceived need for a metarequirement is greater than the respective implementation extent, the implementation extent should be increased to obtain meaningful organizational privacy communications.*
>
> ***P6:*** *When perceived need for a metarequirement is less than the respective implementation extent, it is only beneficial to decrease the implementation extent in such situations where associated costs for instantiation operation outweigh additional implementation efforts.*

Operationalizing the *TIPP theory* or measuring the fulfillment of *TIPP metarequirements* is beyond the scope of this work. To illustrate that operationalization of the *TIPP theory* is theoretically feasible, we present the following illustrative example. Straightforward measurements for the fulfillment of the comprehensiveness, topical-relevance, and interactivity metarequirement are the percentage of *TIPP content aspects* covered by organizational privacy communications, the percentage of offered information that cannot be mapped to *TIPP content aspects*, and the percentage of information-seeking strategies (Xie 2000) supported by *TIPP instantiations*, respectively. For illustrative purposes, we assess the fulfillment of *TIPP metarequirements* on a binary scale (Not Fulfilled, Fulfilled) for abstract approaches that may be considered *TIPP instantiations*. The results are presented in Table 21 along with a ranking by suitability for establishing transparency of organizational privacy practices. *TIPP instantiations* that fulfill all metarequirements are deemed most suitable for establishing transparency of organizational privacy practices. If the amount of provided information is comprehensive enough, lack of topical relevance can be remedied with interactive features (eg, filtering of irrelevant information). *TIPP instantiations* that adequately address topical relevance and only one other metarequirement are considered partially suitable for establishing transparency of organizational privacy practices because they either promote information overload or fail to provide information desired by consumers, which reduces the number of supported information acquisition tasks. All other instantiations are considered unsuitable for establishing transparency of organizational privacy practices because they fail to provide necessary information or good support for information retrieval and are unlikely to satisfy consumers' information needs.

6.4 Discussion

We conceptualize a design space for meaningful organizational privacy communication in form of an information systems design theory for transparency of organizational privacy practices. Meaningful organizational privacy communication must balance offering access to a comprehensive selection of information and avoiding cognitive overload by focusing on topical relevance and interactivity. Common organizational privacy practices that must be addressed in organizational privacy communication are captured in the *TIPP ontology*, which can be seamlessly adapted to the specific requirements and peculiarities of individual instantiations of the *TIPP theory*. Related research concerned with organizational privacy communication is mostly focused on building and evaluating individual tools that address specific threats (eg, blocking tools or opt-out tools) or on testing and critiquing extant tools (eg, the effectiveness of privacy notices or seals) (Cranor 2012). The *TIPP theory* takes a step back and contributes to the scientific knowledge base by first establishing more general design knowledge on what to build for meaningful organizational privacy communication.

6.4.1 Limitations

This research has some limitations. First, the *TIPP theory* does not account for special circumstances of individual organizations for the sake of parsimony. For some governmental institutions, transparency of organizational privacy practices might, for example, be impossible because of national security considerations mandating secrecy. Other organizations might be hesitant to establish transparency of organizational privacy practices because they fear losing competitive advantage if organizational practices become known. The *TIPP theory* captures knowledge on what to build for meaningful organizational privacy communication that makes organizational privacy practices transparent

Table 21. Illustrative ranking of potential, abstract TIPP instantiations ranked by suitability for establishing transparency of organizational privacy practices.

Rank	Suitability	Comprehensiveness	Topical relevance	Interactivity	Abstract example for TIPP instantiation
1	Suitable	Fulfilled	Fulfilled	Fulfilled	Interactive, organization-spanning portal of privacy practices[a]
2	Suitable	Fulfilled	Not Fulfilled	Fulfilled	Interactive portal of organizational practices[b]
3	Partial	Not Fulfilled	Fulfilled	Fulfilled	P3P consumer agents[c]
4	Partial	Fulfilled	Fulfilled	Not Fulfilled	Ideal privacy notice[d]
5	Unsuitable	Fulfilled	Not Fulfilled	Not Fulfilled	Overloaded privacy notice[e]
6	Unsuitable	Not Fulfilled	Fulfilled	Not Fulfilled	Privacy seal[f]
7	Unsuitable	Not Fulfilled	Not Fulfilled	Fulfilled	Network traffic analysis visualizer[g]
8	Unsuitable	Not Fulfilled	Not Fulfilled	Not Fulfilled	Typical privacy notice[h]

[a] Such a portal could offer a comprehensive amount of topically relevant information for various consumer information systems in an interactive way.

[b] Such a portal would lack topical relevance because it is focused on organizational practices in general. With high levels of interactivity, it can still be deemed suitable for establishing transparency of organizational privacy practices because organizational privacy practices are a subset of all organizational practices.

[c] P3P consumer agents are ranked third because P3P can be considered quite comprehensive. However, comprehensiveness cannot be considered fulfilled because P3P does not cover some common privacy practices and extensions of P3P are too complicated (Lämmel and Pek 2013).

[d] An ideal privacy notice would present a comprehensive amount of topically relevant information but can only be considered partially suitable for establishing transparency of organizational privacy practices because it lacks interactivity.

[e] An overloaded privacy notice masks topically relevant information with irrelevant information. As this severely impedes information retrieval, an overloaded privacy notice is unsuitable for establishing transparency of organizational privacy practices.

[f] Privacy seals can, by design, convey only a limited amount of information and are thus deemed unsuitable for establishing transparency of organizational privacy practices.

[g] Although network traffic visualizers can present the results of their analyses in an interactive way, they also track a large amount of irrelevant traffic and can address only a few organizational privacy practices. Hence, they are deemed unsuitable for the establishment of transparency of organizational privacy practices.

[h] Privacy notices usually convey only limited and often irrelevant information in a static way and are thus unsuitable for establishing transparency of organizational privacy practices.

and offers insights on how to accomplish this. Understanding why organizations do or do not want to establish transparency of organizational privacy practices is beyond the scope of the *TIPP theory*.

Second, the *TIPP theory* captures contextual influences with perceived needs for metarequirements but does not explicitly consider specific contextual influences, such as the sensitivity of information exchanges or the complexity of information flows, impacting needs for metarequirement fulfillment. Consumers desire different information and want to perform different tasks depending on organizational characteristics. For example, organizations that focus predominantly on information provision (eg, weather forecasts) will most likely have to offer only high-level information to be perceived as transparent with respect to organizational privacy practices. Other organizations collecting sensitive information (eg, health or financial organizations) must likely offer a higher level of detail. Ascertaining the needs for metarequirement implementation for individual instantiations of the *TIPP theory* is left to the domain knowledge and expertise of *TIPP instantiators* and must be determined over time in real-world contexts.

Third, we refrained from including contextual considerations in the testable propositions to make them less convoluted and keep them at the level of abstraction of the overall *TIPP theory*. Derivation of hypotheses from the testable propositions for the purpose of testing the *TIPP theory* (Bacharach 1989) will require careful consideration of the context of the situated consumer information systems under study. For instance, it has to be determined what variables are best suited to operationalize perceived needs for metarequirements and the respective implementation extents with respect to the consumer information systems under study. With our illustrative example for *TIPP theory* operationalization (see Table 21), we illustrate that operationalization of the *TIPP theory* is theoretically possible. What variables and measurements are best suited to test the *TIPP theory* based on hypotheses derived from the testable propositions must however be determined based on the context of the situated consumer information systems under study. The primary purpose of presenting the testable propositions in this manuscript was to make the design knowledge captured in the *TIPP theory* and the design rationale for *TIPP instantiations* more explicit.

Fourth, we did not examine who should build *TIPP instantiations*. Organizations could develop *TIPP instantiations* themselves. *TIPP instantiations* by other stakeholders (eg, governments, privacy advocate groups, or consumer communities) could, however, cover organizational privacy practices across a range of organizations and could prove to be more promising. In addition, the envisioned benefits of *TIPP instantiations* are countered by powerful economic interests and the complexity of today's information flows. It will be hard for any instantiator to obtain the comprehensive amount of information on organizational privacy practices required by *TIPP instantiations*. Moreover, complementary approaches, such as real-time privacy impact assessments (Oetzel and Spiekermann 2014), would be required to ensure that communicated organizational privacy practices align with actual organizational privacy practices carried out by technical and human information system components.

6.4.2 Opportunities for Future Research

Salient opportunities for future research include the testing and extension of the *TIPP theory*. Research cooperation with organizations already attempting to instantiate meaningful privacy communication seems promising. Future research could focus on developing instantiations of the *TIPP theory* in different contexts and extend the *TIPP theory* with further design knowledge tailored to contextual requirements. The *TIPP theory* paints a general picture of what to build for meaningful organizational privacy communication. Future research could explore different approaches to implementing *TIPP instantiations*, for example, leveraging ontology visualization methods (Katifori et al. 2007) or natural language interfaces (Kaufmann and Bernstein 2007). Future research could also develop gold standards for information to be offered or for levels of transparency desired by consumers within the context of certain types of consumer information systems.

6.4.3 Contributions to Theory

This research contributes to the scientific knowledge base in multiple ways. First, we introduce a conceptualization of transparency of organizational privacy practices. Prior literature has developed unspecific instruments to assess transparency (eg, Oulasvirta et al. 2014) and its importance (eg, Awad and Krishnan 2006, Dinev et al. 2013) in quantitative studies or has relied on the intuitiveness of the concept (eg, Fischer-Hübner et al. 2014, Horvitz and Mulligan 2015). Transparency of organizational privacy practices is not concerned with arbitrary information practices or normative claims regarding fair information practices. Instead, meaningful organizational privacy communication must provide consumers with the information they desire in an intuitive way.

Second, we consolidate research concerned with organizational privacy practices and develop the *TIPP ontology* as a metaspecification of the information relevant for organizational privacy communication. Extant research on organizational privacy communication focuses mostly on stated organizational privacy practices (eg, Anthonysamy et al. 2013, O'Connor 2003), coverage of fair information principles (eg, Liu and Arnett 2002, Milne and Culnan 2002), or different selections of organizational privacy practices (eg, Antón, Earp, et al. 2007, Carrión Señor, Fernández-Alemán, et al. 2012, Pollach 2007). The *TIPP ontology* consolidates research on organizational privacy practices into a hierarchical model of common organizational privacy practices.

Third, we introduce the privacy communication continuum as a new lens for privacy research. The privacy communication continuum illustrates that meaningful organizational privacy communication can leverage a whole range of opportunities between general approaches considered in public policy and legal discourse and technical solutions from the computer science domain. Although these endpoints are well studied, the intermediate area of this range remains largely unexplored. Instead of a focus on approaches that regulators and the market have introduced thus far or that rely predominantly on technical solutions, the privacy communication continuum motivates investigation of new approaches that rely, for instance, on social mechanisms. Promising ideas are, for example, supporting individuals in assessing contextual integrity or compliance with social norms (Martin 2016, Nissenbaum 2009) or developing privacy review systems similar to consumer review systems for products (Jiang and Guo 2015).

Fourth, we develop design knowledge for meaningful organizational privacy communication. The *TIPP theory* constitutes a metaspecification of the interface communicating organizational privacy practices conducted in organizations' inner environment to external environments (Simon 1996). In essence, organizational privacy communication can be considered meaningful if it establishes transparency of organizational privacy practices by offering a comprehensive set of topically relevant information in an interactive way.

Fifth, the *TIPP theory* captures knowledge on how organizations can account for privacy in consumer information systems in a more versatile manner than extant approaches offering only narrow support for satisfying consumers' privacy needs. The

TIPP theory offers guidance how organizations can account for differences in consumers' privacy needs during electronic interactions. The contested and complex nature of privacy (Mulligan et al. 2016, Solove 2002) makes it unlikely that organizations can satisfy consumers' privacy needs with a universally applicable solution. The *TIPP theory* addresses this problem by proposing a flexible, adaptive approach to organizational privacy communication.

6.4.4 Practical Implications

From a practical standpoint, the *TIPP theory* offers insights that bring common organizational practices, such as posting privacy notices and privacy seals, into question. Neither privacy seals nor privacy notices seem suitable to establish transparency of organizational privacy practices. Indeed, privacy seals, for instance, TRUSTe (Benassi 1999), convey only limited information and are static. In practice, privacy notices are often not comprehensive, are bloated with irrelevant legalistic boilerplate (Milne and Culnan 2004), and remain static text documents that cannot adapt to consumers' privacy information needs. New approaches must be developed for making organizational privacy communication meaningful. The *TIPP theory* can be used to communicate organizational privacy practices in a meaningful way. This would allow organizations to differentiate themselves from competitors by implementing more consumer-friendly privacy practices. Today, organizational privacy practices remain largely opaque to consumers. The *TIPP theory* presents on approach to change this situation and transform organizational privacy practices into a tangible quality attribute of organizations by fostering holistic attention to privacy practices, stimulating internalization of privacy, and allowing for enough flexibility to account for contextual influences (Wijen 2014).

6.4.5 Conclusion

Today, the best way for organizations to protect themselves from the risks and undesirable consequences of perceived privacy violations is to ensure that consumer information is not shared in the first place. However, this would render most of the benefits to be redeemed in the Social Age moot and most business models pointless. A more promising approach to establish a sustainable, mutually beneficial consumer information systems landscape is to pay genuine attention to privacy and enable consumers by design to judge what they are getting themselves into—that is, to integrate components for meaningful organizational privacy communication into consumer information systems.

6.5 References

Abiteboul S, André B, Kaplan D (2015) Managing Your Digital Life. Communications of the ACM 58(5):32–35.

Ackerman MS, Cranor LF, Reagle J (1999) Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. 1st ACM Conference on Electronic Commerce. (ACM, Denver, CO, USA), 1–8.

Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and Human Behavior in the Age of Information. Science 347(6221):509–514.

Anthonysamy P, Greenwood P, Rashid A (2013) Social Networking Privacy: Understanding the Disconnect from Policy to Controls. IEEE Computer 46(6):60–67.

Antón AI, Earp JB, Vail MW, Jain N, Gheen CM, Frink JM (2007) HIPAA's Effect on Web Site Privacy Policies. IEEE Security & Privacy 5(1):45–52.

Antón AI, Earp JB, Young JD (2010) How Internet Users' Privacy Concerns Have Evolved Since 2002. IEEE Security & Privacy 8(1):21–27.

Awad NF, Krishnan M (2006) The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. MIS Quarterly 30(1):13–28.

Bacharach SB (1989) Organizational Theories: Some Criteria for Evaluation. Academy of Management Review 14(4):496–515.

Bal G, Rannenberg K, Hong JI (2015) Styx: Privacy Risk Communication for the Android Smartphone Platform Based on Apps' Data-Access Behavior Patterns. Computers & Security 53(1):187–202.

Balebako R, Jung J, Lu W, Cranor LF, Nguyen C (2013) "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. Proceedings of the Ninth Symposium on Usable Privacy and Security. SOUPS '13. (ACM, New York, NY, USA), 12:1–12:11.

Bélanger F, Crossler RE (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly 35(4):1017–1041.

Bélanger F, Crossler RE, Hiller JS, Park JM, Hsiao MS (2013) POCKET: A Tool for Protecting Children's Privacy Online. Decision Support Systems 54(2):1161–1173.

Belkin NJ, Oddy RN, Brooks HM (1982) ASK for Information Retrieval: Part I. Background and Theory. Journal of Documentation 38(2):61–71.

Benassi P (1999) TRUSTe: An Online Privacy Seal Program. Communications of the ACM 42(2):56–59.

Berger CR, Calabrese RJ (1975) Some Explorations in Initial Interaction and Beyond: Toward a Developmental Theory of Interpersonal Communication. Human Communication Research 1(2):99–112.

Bühler K (2011) Theory of Language: The Representational Function of Language (John Benjamins Publishing Co, Amsterdam / Philadelphia).

Carrión Señor I, Fernández-Alemán JL, Toval A (2012) Are Personal Health Records Safe? A Review of Free Web-Accessible Personal Health Record Privacy Policies. Journal of Medical Internet Research 14(4):e114.

Conger S, Pratt JH, Loch KD (2013) Personal Information Privacy and Emerging Technologies. Information Systems Journal 23(5):401–417.

Corley KG, Gioia DA (2011) Building Theory about Theory Building: What Constitutes a Theoretical Contribution? Academy of Management Review 36(1):12–32.

Cosijn E, Ingwersen P (2000) Dimensions of Relevance. Information Processing & Management 36(4):533–550.

Cowan N (2014) Working Memory Underpins Cognitive Development, Learning, and Education. Educational Psychology Review 26(2):197–223.

Cranor L, Dobbs B, Egelman S, Hogben G, Humphrey J, Langheinrich M, Marchiori M, et al. (2006) The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. Retrieved (March 3, 2017), http://www.w3.org/TR/2006/NOTE-P3P11-20061113.

Cranor LF (2012) Necessary but not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. Journal on Telecommunications and High Technology Law 10:273–307.

Dinev T, Xu H, Smith JH, Hart P (2013) Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts. European Journal of Information Systems 22(3):295–316.

Dubin R (1978) Theory Building (Collier Macmillan Publishers, London, UK).

Earp JB, Antón AI, Aiman-Smith L, Stufflebeam WH (2005) Examining Internet Privacy Policies Within the Context of User Privacy Values. IEEE Transactions on Engineering Management 52(2):227–237.

Eggert A, Helm S (2003) Exploring the Impact of Relationship Transparency on Business Relationships: A Cross-Sectional Study among Purchasing Managers in Germany. Industrial Marketing Management 32(2):101–108.

Fischer-Hübner S, Angulo J, Pulls T (2014) How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used? Hansen M, Hoepman JH, Leenes R, Whitehouse D, eds. Privacy and Identity Management for Emerging Services and Technologies. (Springer Berlin Heidelberg), 77–92.

Garrison L, Hastak M, Hogarth JM, Kleimann S, Levy AS (2012) Designing Evidence-Based Disclosures: A Case Study of Financial Privacy Notices. Journal of Consumer Affairs 46(2):204–234.

Germonprez M, Hovorka D, Collopy F (2007) A Theory of Tailorable Technology Design. Journal of the Association for Information Systems 8(6):351–367.

Greenaway KE, Chan YE, Crossler RE (2015) Company Information Privacy Orientation: A Conceptual Framework. Information Systems Journal 25(6):579–606.

Gregor S, Jones D (2007) The Anatomy of a Design Theory. Journal of the Association for Information Systems 8(5):312–335.

Guarino N (1997) Understanding, Building and Using Ontologies. International Journal of Human-Computer Studies 46(2–3):293–310.

Horvitz E, Mulligan D (2015) Data, Privacy, and the Greater Good. Science 349(6245):253–255.

Hultman J, Axelsson B (2007) Towards a Typology of Transparency for Marketing Management Research. Industrial Marketing Management 36(5):627–635.

Jiang Y, Guo H (2015) Design of Consumer Review Systems and Product Pricing. Information Systems Research 26(4):714–730.

John LK, Acquisti, A, Loewenstein G (2011) Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information. Journal of Consumer Research 37(5):858–873.

Kalyuga S (2011) Cognitive Load Theory: How Many Types of Load Does It Really Need? Educational Psychology Review 23(1):1–19.

Katifori A, Halatsis C, Lepouras G, Vassilakis C, Giannopoulou E (2007) Ontology Visualization Methods—A Survey. ACM Computing Surveys 39(4):10:1-10:43.

Kaufmann E, Bernstein A (2007) How Useful Are Natural Language Interfaces to the Semantic Web for Casual End-Users? Aberer K, Choi KS, Noy N, Allemang D, Lee KI, Nixon L, Golbeck J, et al., eds. The Semantic Web. Lecture Notes in Computer Science. (Springer Berlin Heidelberg), 281–294.

Koops BJ, Newell BC, Timan T, Skorvanek I, Chokrevski T, Galic M (2016) A Typology of Privacy. University of Pennsylvania Journal of International Law 38(2):483–575.

Kuechler W, Vaishnavi V (2012) A Framework for Theory Development in Design Science Research: Multiple Perspectives. Journal of the Association for Information Systems 13(6):395–423.

Lämmel R, Pek E (2013) Understanding Privacy Policies. Empirical Software Engineering 18(2):310–374.

Laudon KC (1996) Markets and Privacy. Communications of the ACM 39(9):92–104.

Laufer RS, Wolfe M (1977) Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues 33(3):22–42.

Liu C, Arnett KP (2002) Raising a Red Flag on Global WWW Privacy Policies. The Journal of Computer Information Systems 43(1):117–127.

Martin K (2016) Understanding Privacy Online: Development of a Social Contract Approach to Privacy. Journal of Business Ethics 137(3):551–569.

Mason RO (1986) Four Ethical Issues of the Information Age. MIS Quarterly 10(1):5–12.

McDonald AM, Cranor LF (2008) The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 4(3):540–565.

van Merriënboer JJG, Sweller J (2005) Cognitive Load Theory and Complex Learning: Recent Developments and Future Directions. Educational Psychology Review 17(2):147–177.

van Merriënboer JJG, Sweller J (2010) Cognitive Load Theory in Health Professional Education: Design Principles and Strategies. Medical Education 44(1):85–93.

Milne GR, Culnan MJ (2002) Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys. Information Society 18(5):345–359.

Milne GR, Culnan MJ (2004) Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don’t Read) Online Privacy Notices. Journal of Interactive Marketing 18(3):15–29.

Miltgen CL, Peyrat-Guillard D (2014) Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries. European Journal of Information Systems 23(2):103–125.

Miyazaki AD, Krishnamurthy S (2002) Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. Journal of Consumer Affairs 36(1):28–49.

Mulligan DK, Koopman C, Doty N (2016) Privacy is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy. Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 374(2083):1–17.

Nissenbaum H (2009) Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press, Stanford, CA, USA).

Nussbaumer P, Matter I, Schwabe G (2012) “Enforced” vs. “Casual” Transparency – Findings from IT-Supported Financial Advisory Encounters. ACM Transactions on Management Information Systems 3(2):11:1–11:19.

O’Connor P (2003) What Happens to my Information if I Make a Hotel Booking Online: An Analysis of On-Line Privacy Policy Use, Content and Compliance by the International Hotel Companies. Journal of Services Research 3(2):5–28.

Oetzel MC, Spiekermann S (2014) A Systematic Methodology for Privacy Impact Assessments: A Design Science Approach. European Journal of Information Systems 23(2):126–150.

Oliver C (1991) Strategic Responses to Institutional Processes. Academy of Management Review 16(1):145–179.

Organisation for Economic Cooperation and Development (1980) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Recommendation by the Council of the OECD. Retrieved (June 25, 2013), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm . Archived at: http://www.webcitation.org/6Y7eE1Q3m.

Oulasvirta A, Suomalainen T, Hamari J, Lampinen A, Karvonen K (2014) Transparency of Intentions Decreases Privacy Concerns in Ubiquitous Surveillance. Cyberpsychology, Behavior, and Social Networking 17(10):633–638.

Paas F, Ayres P (2014) Cognitive Load Theory: A Broader View on the Role of Memory in Learning and Education. Educational Psychology Review 26(2):191–195.

Park YJ (2013) Digital Literacy and Privacy Behavior Online. Communication Research 40(2):215–236.

Pollach I (2006) Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions. Journal of Organizational and End User Computing 18(1):23–49.

Pollach I (2007) What's Wrong With Online Privacy Policies? Communications of the ACM 50(9):103–108.

Reagle J, Cranor LF (1999) The Platform for Privacy Preferences. Communications of the ACM 42(2):48–55.

Rindfleisch TC (1997) Privacy, Information Technology, and Health Care. Communications of the ACM 40(8):92–100.

Rouse WB, Rouse SH (1984) Human Information Seeking and Design of Information Systems. Information Processing & Management 20(1):129–138.

Schnackenberg AK, Tomlinson EC (2016) Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships. Journal of Management 42(7):1784–1810.

Schwaig KS, Segars AH, Grover V, Fiedler KD (2013) A Model of Consumers' Perceptions of the Invasion of Information Privacy. Information & Management 50(1):1–12.

Simon HA (1996) The Sciences of the Artificial 3rd ed. (MIT Press, Cambridge, MA, USA).

Smith B, Welty C (2001) Ontology: Towards a New Synthesis. Proceedings of the International Conference on Formal Ontology and Information Systems. (ACM, Ogunquit, ME, USA), 3–9.

Smith HJ, Dinev T, Xu H (2011) Information Privacy Research: An Interdisciplinary Review. MIS Quarterly 35(4):989–1015.

Solove DJ (2001) Privacy and Power: Computer Databases and Metaphors for Information Privacy. Stanford Law Review 53(6):1393–1462.

Solove DJ (2002) Conceptualizing Privacy. California Law Review 90(4):1087–1155.

Spyns P, Meersman R, Jarrar M (2002) Data Modelling versus Ontology Engineering. ACM SIGMod Record 31(4):12–17.

Sweller J (1988) Cognitive Load During Problem Solving: Effects on Learning. Cognitive Science 12(2):257–285.

Sweller J, van Merriënboer JJG, Paas FWC (1998) Cognitive Architecture and Instructional Design. Educational Psychology Review 10(3):251–296.

Tavani HT (2007) Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy. Metaphilosophy 38(1):1–22.

Tsai JY, Egelman S, Cranor L, Acquisti A (2011) The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Information Systems Research 22(2):254–268.

US Federal Department of Health Education and Welfare (1973) Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Chapter III. Safeguards for Privacy. Retrieved (April 24, 2015), https://epic.org/privacy/hew1973report/c3.htm . Archived at: http://www.webcitation.org/6Y1gDPqTf.

Walls JG, Widmeyer GR, El Sawy OA (1992) Building an Information System Design Theory for Vigilant EIS. Information Systems Research 3(1):36–59.

Warren SD, Brandeis LD (1890) The Right to Privacy. Harvard Law Review 4(5):193–220.

Westin A (1967) Privacy and Freedom (Ig Publishing, New York, NY, USA).

Wijen F (2014) Means versus Ends in Opaque Institutional Fields: Trading off Compliance and Achievement in Sustainability Standard Adoption. Academy of Management Review 39(3):302–323.

Xie HI (2000) Shifts of Interactive Intentions and Information-Seeking Strategies in Interactive Information Retrieval. Journal of the American Society for Information Science 51(9):841–857.

Xu H, Crossler RE, Bélanger F (2012) A Value Sensitive Design Investigation of Privacy Enhancing Tools in Web Browsers. Decision Support Systems 54(1):424–433.

Xu H, Teo HH, Tan BCY, Agarwal R (2012) Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. Information Systems Research 23(4):1342–1363.

6.6 Appendix

Table 22. All content aspects included in the TIPP ontology. The column 'Hierarchy' indicates the hierarchy. For the sake of clarity, higher tiers, which have many child content aspects, are indicated with letters and lower tiers, which have only a small number of child content aspects are indicated with ascending numbers. Aspects with more hierarchy indicators are deeper in the hierarchy.

Hierarchy				Content aspect	Description
H				HandlingOfInformation	Captures how information is handled
H	1			InformationRetention	Information retention practices
H	2			InformationSecurity	Information security measures
H	2	1		SecurityDuringProcessing	Information security measures during processing
H	2	2		SecurityDuringStorage	Information security measures for information at rest
H	2	3		SecurityDuringTransfer	Information security measures during transfer
H	3			InformationSharing	Captures with whom information is shared
H	3	1		SharingWithAdvertiser	Information sharing with third party advertiser
H	3	2		SharingWithAggregator	Information sharing with data aggregators
H	3	3		SharingWithAnalyst	Information sharing with third party analyst
H	3	4		SharingWithDelivery	Information sharing with physical delivery services
H	3	5		SharingWithGovernment	Information sharing with government agencies
H	3	6		SharingWithOtherConsumers	Information sharing with other consumers
H	3	7		SharingWithProviderAgents	Information sharing with provider agents
H	3	8		SharingWithPublic	Information sharing with the public
H	3	9		SharingWithUnrelated	Information sharing with unrelated third parties
H	3	10		SharingWithConsumerAuthorized	Information sharing with consumer-authorized third parties
H	4			InformationStorage	Captures where information is stored
H	4	1		CloudStorage	Data stored in the cloud
H	4	2		LocalStorage	Data stored on primary consumer device
H	4	3		OtherConsumerDeviceStorage	Data stored on a secondary consumer device
H	4	4		ProviderStorage	Data stored within the organizations domain
H	4	5		ThirdPartyStorage	Data stored by a third-party storage service
I				InformationCollection	Captures what and how information is collected
I	1			InformationCollectionSensor	Sources of collected information
I	1	1		EnvironmentSensor	Sensors collecting data on consumer environment
I	1	1	1	BluetoothSensor	Discover contactable Bluetooth-enabled devices
I	1	1	2	Camera	Collect images/videos made with the device camera
I	1	1	3	Microphone	Collect recordings made with device microphone
I	1	1	4	NearFieldCommunication	Record consumer actions (eg, payments) via NFC
I	1	2		LocationSensor	Sensors for location information
I	1	2	1	GpsSensorContent	Global Positioning System (GPS) device location
I	1	2	2	NetworkConnectionSensor	Location based on cell towers or network identifiers
I	1	2	3	WiFiSensor	Location coordinates based on available WiFi networks
I	1	3		ConsumerSensor	Sensors collecting information on the consumer
I	1	3	1	FingerprintScanner	Collection of fingerprints with fingerprint scanner
I	1	4		SoftwareUseSensor	Sensors collecting information on software use
I	1	4	1	AdwareContent	Collection through adware installed on the device
I	1	4	2	CookiesContent	Collection through cookies
I	1	4	3	SurveysContent	Collection with surveys or questionnaires
I	1	4	4	TrackingSoftware	Collection with tracking software installed on device

I	1	4	5	WebBeaconContent	Tracking of consumer activity through web beacons
I	2			InformationCollectionType	Type of collected information
I	2	1		InformationFormat	Different formats of data collected
I	2	1	1	AudioInformation	Collection of audio data
I	2	1	2	ImageInformation	Collection of image/photo data
I	2	1	3	MetaData	Collection of metadata (data on data)
I	2	1	4	TextInformation	Collection of textual data
I	2	1	5	VideoInformation	Collection of video data
I	2	2		Identifier	Collection of consumer identifiers
I	2	2	1	FinancialIdentifier	Financial identifiers (eg, bank account number)
I	2	2	2	GovernmentIdentifier	Government-issued identifiers
I	2	2	3	Name	Collection of consumers' full names (not user names)
I	2	2	4	OnlineContact	Information to contact consumers on the internet
I	2	2	5	PhysicalContact	Information to contact consumers in the physical world
I	2	2	6	OwnUniqueIdentifier	Information system provider–issued identifiers
I	2	3		Operational	Information collected for information system operation
I	2	3	1	Communications	Words contained in the body of a communication
I	2	3	2	Interaction	Data reflecting interactions with an information system
I	2	3	3	Location	Consumers' physical location (eg, GPS position data)
I	2	3	4	Navigation	Data passively generated by information system use
I	2	3	5	OnlineContacts	Online contact information of other consumers
I	2	3	6	Purchases	Information on purchases conducted
I	2	4		ConsumerDetails	Information on the consumer
I	2	4	1	Demographics	Demographic and socioeconomic data
I	2	4	2	Finances	Information on consumers' finances
I	2	4	3	Health	Information about consumers' health
I	2	4	4	Ideological	Affiliations with groups (eg, religious groups)
I	2	4	5	Preferences	Information about consumers' likes and dislikes
I	2	4	6	ConsumerDevice	Information about consumers' client devices
M				MetaContent	Content aspects not directly related to privacy practices
M	1			Certification	Certifications of the organization
M	2			Contact	Contact information of the organization
M	3			EffectiveDate	Date information privacy practices are in effect from
M	4			FollowedGuidelines	Guidelines the information system provider followed
M	5			FollowedLaws	Laws the organization is compliant with
M	6			LastUpdate	Date of last update of stated privacy practices
M	7			MinimumConsumerAge	Outlines the targeted age group (eg, children)
M	8			ProviderName	Name of provider organization
O				OfferedPrivacyControl	Captures offered privacy controls
O	1			AccessAudit	Enables to retrieve access logs for information
O	2			BreachNotification	Captures how privacy breach notifications are made
O	2	1		BreachNature	Notification about what was breached
O	2	2		BreachOccurence	Notification that a breach occurred
O	2	3		BreachRemedies	Notification about remedies offered for breach
O	3			ChangeHistory	Information on past information privacy practices
O	4			ChangeGovernance	Effects of practice updates on collected information
O	5			ChangeNotification	Notification about changes of privacy practices
O	6			ConsentManagement	Management of all consents, explicit and implicit

O	7		DisputeRemedy	Remedies offered for justified privacy disputes
O	8		DisputeResolution	Means offered for resolving privacy disputes
O	9		DownstreamPropagation	Propagation of information updates to data recipients
O	10		PrivacyManagementBoundaries	Boundaries for information privacy management (eg, information requests by law enforcement)
O	11		PrivacyPracticeMonitoring	Monitoring of organizational privacy practices
O	11	1	AutomatedMonitoring	Automated monitoring of information privacy practices
O	11	2	IndependentMonitoring	Information privacy practices monitoring by third party
O	11	3	InternalMonitoring	Information privacy practices monitoring by provider
O	12		SecondaryUseConsent	Contacting of consumers prior to any secondary use
O	13		ConsumerAccess	Consumer permissions to access collected information
P			PracticeRationale	Purposes privacy practices are performed for
P	1		Communication	To provide communication features
P	1	1	Contact	Responding to the consumer (eg, to consumer query)
P	1	2	Feedback	Contacting consumers without previous requests
P	1	3	Marketing	Advertising, marketing, or promotion purposes
P	1	4	ConsumerCommunication	Facilitating communication between consumers
P	2		OfferedService	To provide services offered by the information system
P	2	1	FinancialManagement	Banking and financial management
P	2	2	HealthProducts	To offer products related to consumers' health
P	2	3	Payment	Payment and transaction facilitation
P	2	4	PhysicalDelivery	Physical delivery of a product
P	2	5	Sales	Conducting a business transaction with the consumer
P	3		Personalization	Personalization of the information system
P	3	1	IndividualAnalysis	Determine individual user characteristics for analysis
P	3	2	IndividualDecision	Determine individual user characteristics for tailoring
P	3	3	PseudoAnalysisContent	Determine general user characteristics for analysis
P	3	4	PseudoDecision	Determine general user characteristics for tailoring
P	4		PublicWelfare	To contribute to public welfare
P	4	1	Arts	For delivering the arts (eg, music, and movies)
P	4	2	Charity	For charitable purposes
P	4	3	Education	For educational purposes
P	4	4	Government	For online government services (eg, voter registration)
P	4	5	Historical	For the purpose of preserving social history
P	4	6	Research	To support research projects
P	5		ServiceOperation	To operate the information system
P	5	1	CoreFunctionality	To conduct activities for which data were provided
P	5	2	Administration	For information system administration
P	5	3	Development	To enhance, evaluate, or review the information system
P	5	4	LegalObligations	For duties enforced by law or other legal purposes
P	6		TechnicalDetails	For technical purposes
P	6	1	AccountManagement	For consumer account management
P	6	2	SessionManagement	To keep track of sessions and application states

7 Consumer Archetypes for Organizational Information Privacy Communication

Authors: Tobias Dehling, Manuel Schmidt-Kraepelin, Ali Sunyaev

Abstract: Although subject to public debate for decades, normative standards have not resulted in the emergence of effective organizational information privacy communication. This study takes a bottom-up perspective and explores consumer preferences for organizational information privacy communication to establish a foundation for development of organizational information privacy communication that not only fulfills normative standards but also addresses the information privacy preferences of consumers. We elicit consumers' information privacy information needs with a scenario-based online survey with 909 participants. Consumer archetypes are identified with an agglomerative community detection analysis and characterized based on five latent variables identified through exploratory factor analysis. We identify a total of nine consumer archetypes with diverse information privacy information needs. Our findings add to the evidence that organizational information privacy communication development solely based on normative standards is not effective. Based on the diversity of the information privacy information needs of the identified consumer archetypes, we propose a refined view on organizational information privacy communication that is grounded in Integrative Social Contracts Theory. Contributions of our study are the identification and characterization of consumer archetypes with different information privacy information needs, the proposition of a refined lens on organizational privacy communication that also accounts for the diversity of consumers' information privacy information needs, and the derivation of implications for organizations and policy makers for how to approach organizational information privacy communication in a more effective way.

Keywords: information privacy, information need, privacy communication, community detection, exploratory factor analysis, archetypes, clustering

7.1 Introduction

Many organizations try to address the privacy[14] risks introduced by their consumer information systems[15] through compliance with general, normative privacy standards, such as Fair Information Practice Principles or laws and regulations derived from them (Organisation for Economic Cooperation and Development 1980, US Federal Department of Health Education and Welfare 1973). However, a growing body of research

[14] Within the scope of this work we focus on information privacy and not on other facets of privacy, such as bodily, spatial, or behavioral privacy (Koops et al. 2016). For the sake of brevity, we use the term privacy synonymous to information privacy throughout this manuscript.

[15] Within the scope of this work, the term consumer information system refers to any socio-technical system open to consumers in which information technology is employed to process information. Consumer information systems are a suitable research context because such systems depend on voluntary use so that attention to privacy is a promising lever to make consumer information systems more appealing to consumers.

attests to the contextual nature of privacy (Acquisti et al. 2015). Accordingly, normative standards are of limited value to guide organizational privacy communication because neither can they be detailed enough to offer the information relevant across all contexts nor can their underlying values reflect all the convictions valued by the respective consumer groups (Donaldson and Dunfee 1994, Langenderfer and Cook 2004). Numerous empirical studies illustrate the inadequacy of extant organizational privacy communication by demonstrating, for example, that privacy notices neither offer the information consumers are looking for nor are presented in a form consumers are willing or capable to consume (eg, Earp et al. 2005, Jensen and Potts 2004, McDonald and Cranor 2008), that consumer perceptions of organizational practices do not align with the actual practices (eg, Miyazaki and Krishnamurthy 2002, Vail et al. 2008), or that consumers resort to self-protective and deceptive practices to protect themselves from privacy violations by the information systems they use (eg, Jiang et al. 2013, Son and Kim 2008).

Extant research identified various antecedents for differences in privacy attitudes between consumer groups, such as socio-demographics (eg, Miltgen and Peyrat-Guillard 2014, Rodríguez-Priego et al. 2016), privacy literacy (eg, Park 2013), situational cues (eg, John et al. 2011), sensitivity of collected information (eg, Bansal et al. 2010), industries of information system providers (eg, Hsu 2006), or perceived intrusiveness of information flows (eg, Sutanto et al. 2013). Although these studies underscore the diversity of contextual influences that shape the consumer groups whose privacy preferences organizational privacy communication has to satisfy, they stay rather mute on the concrete groups, and their respective privacy preferences, consumer information systems are confronted with. In this study, we aim to extend extant research on consumer privacy preferences by establishing an overview of consumer groups with respect to their privacy information needs[16] in consumer information systems.

A fundamental challenge for allowing consumers to assess whether organizational privacy practices align with their privacy preferences is to provide consumers with the right information on organizational privacy practices. Accordingly, we focus on characterizing consumer groups by their privacy information needs. Our study is based on an online survey on general privacy information needs. As outlined above, privacy information needs are dependent on a wide array of influences that will have different effects on different consumers in different situations. To make our findings relevant across a wide range of contexts, we focus on general privacy information needs that are independent of a particular situated consumer information system, instead of situational privacy information needs that are contextualized to specific consumer information systems in specific use situations. Focusing on general privacy information needs allows us to identify general patterns of consumer groups (consumer archetypes). The primary research question answered in this manuscript is: What are the consumer archetypes with respect to privacy information needs in consumer information systems?

[16] With the term privacy information needs we refer to consumers' wishes to be informed whether certain organizational practices perceived as relevant for privacy are being exercised by a consumer information system or not.

Our research contributes to the scientific knowledge base by identifying consumer archetypes with different privacy information needs. Extant research on consumer archetypes with respect to privacy is concerned with the empirical testing of different constructs that may influence consumer groups or with partitioning consumers based on privacy attitudes, privacy behaviors, or demographic characteristics, most notably, the Westin partitioning into Fundamentalists, Pragmatists, and Unconcerned (Kumaraguru and Cranor 2005). This study complements these efforts by partitioning consumers based on privacy information needs, which serves as foundation for more comprehensive conceptualizations of the privacy information needs that organizational privacy communication must cater to.

The remainder of this manuscript is structured as followed. First, we briefly review related research on privacy partitionings. Second, we describe the methods employed for data collection with the online survey and the community detection analysis. Third, we present our findings and conclude with a discussion of the implications for theory and practice.

7.2 Research Background

Extant research offers consumer privacy partitionings from diverse perspectives. However, few partitionings yield insights fostering understanding of consumer preferences for organizational privacy communication. Westin's privacy partitioning was developed to succinctly convey privacy attitude survey results and to keep track over changes in privacy attitudes over time (Kumaraguru and Cranor 2005). Other researchers used consumer archetypes to investigate the nature of privacy concerns (Ackerman et al. 1999, Cranor et al. 1999), to investigate attitudes towards secondary use of information (Culnan 1993), to identify relationships between personalization preferences and privacy attitudes (Zhu et al. 2017) or privacy risks (Lee and Rha 2016), to refine the Westin partitioning for the online context (Sheehan 2002), to map privacy concerns with internet literacy and social awareness (Dinev and Hart 2006b), to map privacy concerns with privacy literacy (Hoofnagle and Urban 2014), to interpret privacy perceptions (Adams and Sasse 1999), or to compare stated privacy preferences to behavioral intentions (Woodruff et al. 2014) or to actual online behavior (Berendt et al. 2005, Jensen et al. 2005, Spiekermann et al. 2001). Other researchers partitioned consumers by privacy-related behaviors, such as privacy management strategies (Lankton et al. 2017, Wisniewski et al. 2017), or used geographical regions to determine differences in privacy preferences (Huang and Bashir 2016, Milberg et al. 1995, Reed et al. 2016).

Partitioning consumers by privacy attitudes or privacy behaviors yields only limited insights to understand how to satisfy consumers' privacy information needs and how consumers' privacy information needs differ. Partitionings of consumers by privacy attitudes or privacy behaviors foster understanding how consumers perceive organizational privacy practices or how they react to it. However, they do not yield substantiated insights into how to improve organizational privacy communication to better meet consumer preferences. Partitionings useful for understanding consumer preferences for organizational privacy communication require a mapping of information system characteristics to consumer preferences. Otherwise, guidance on what information should be conveyed through organizational privacy communication remains unspecific or is distorted by other factors of interest to consumers.

Few studies include specific information system characteristics in privacy partitionings. Hann et al. (2007) partitioned consumers based on consumer perceptions of privacy practices and benefits offered by information systems, which resulted in the archetypes Privacy Guardians, Information Sellers, and Convenience Seekers. Morton and Sasse (2014) partitioned consumers based on desired information cues related to aspects, such as organizational privacy orientation, information use, offered privacy controls, offered benefits, environmental cues, and privacy risks, resulting in the archetypes Information Controllers, Security Concerned, Benefit Seekers, Crowd Followers, and Organizational Assurance Seekers. As a foundation to inform organizational privacy communication, we take a similar approach but focus solely on identifying consumer archetypes and their differences with respect to consumer preferences for information to be included in organizational privacy communication. Our study establishes a foundation for improving organizational privacy communication by identifying consumer archetypes that are only shaped by consumer preferences for organizational privacy communication and not distorted by other factors such as privacy attitudes, perceived benefits of consumer information systems use, preferences for organizational privacy practices, or privacy behaviors. We partition consumers based on their information needs with respect to organizational privacy practices of a consumer information system, that is, privacy information needs.

Information needs differ from other types of needs, such as the physiological need for food, which is a primary human need (Maslow 1943). An information need can be seen as a secondary need that is an instrument to meet a primary need (Hjørland 1997). For example, privacy can be linked to higher primary needs, for instance, status or belonging (Clarke 2006b); the information needs of consumers with respect to organizational privacy practices are secondary needs in order to meet such primary needs. Within the scope of this work, we focus on conscious information needs of consumers with respect to organizational privacy practices. We conceptualize privacy information needs as the wish to be informed whether certain organizational practices perceived as relevant for privacy are being exercised by a consumer information system or not. Deriving consumer archetypes based on privacy information needs, instead of privacy attitudes, privacy behaviors, or manifestations of organizational privacy practices, yields clear implications for guiding organizational privacy communication because it allows to draw conclusions about organizational privacy practices of particular relevance to consumers and reveals differences of privacy information needs between consumer archetypes.

7.3 Methods

7.3.1 Scenario-Based Online Survey

Scenario Development. We chose a scenario-based online survey approach to elicit consumers' privacy information needs because we wanted to identify consumer archetypes based on consumers' general privacy information needs in consumer information systems. Privacy information needs were elicited with illustrative scenarios based on smartphone applications (apps) because they are targeted to consumers, consumers are used to them, and we conducted the survey with a consumer sample. Since we employed a scenario-based approach and did not observe consumer privacy information needs in real situations, the survey elicited privacy information needs on a general level and results should not reflect situational impacts.

To control for situational impacts on consumers' privacy information needs, we initially developed a pool of eighteen scenarios for common types of apps (see Table 26 in the appendix for an overview). The scenarios feature generic descriptions of apps to ensure that survey participants had a similar understanding of the functionality of the app and that results were not biased by brand effects. Finally, we selected four scenarios with different levels of information sensitivity and perceived privacy for our main privacy information needs survey based on a prestudy, which proceeded as follows. First, a short introduction informing participants about smartphone apps in general and the design of the survey was displayed. Afterwards, each participant was assigned to four randomly selected scenarios. For every scenario, Information sensitivity and perceived privacy were measured with items from Dinev et al. (2013) on 7-point Likert scales anchored in 'strongly disagree' and 'strongly agree' (see Table 27 in the appendix). For the purposes of the survey, all items were translated to German. To ensure a high quality of translation, translations were checked by two fellow researchers. A pretest was conducted with eighteen information systems researchers and student assistants to improve the wording of displayed texts, scenario descriptions, and items. Based on the pretest we removed seven scenarios where participants reported privacy and information sensitivity perceptions that were similar to those reported for other scenarios.

The prestudy was conducted online in April 2016. Participants were recruited via social media channels and mailing lists. In total, 172 participants completed the survey. Responses of 27 participants were removed for failing to complete the survey, speeding through the survey, or failing to correctly answer a control question. From the remaining 145 participants, 88 stated their gender as female, 56 as male, and 1 as other. Age groups of participants range from under 18 years old to 65–70 years old (M=31.1; SD=12.8). Cronbach's Alpha for information sensitivity and perceived privacy are 0.8685 and 0.9184, respectively. Information sensitivity and perceived privacy have a strong negative correlation (Pearson r = -0.9816, p < 0.001). Based on the responses on information sensitivity and perceived privacy, we selected four scenarios for the privacy information needs survey, one with high sensitivity, two with medium sensitivity, and one with low sensitivity (Table 23). Table 26 in the appendix lists the prestudy results for all scenarios.

Privacy Information Needs Survey. The privacy information needs survey constitutes the main data collection effort in our study and was designed to elicit consumers' privacy information needs. The survey proceeded as follows. After a short introduction outlining the study purpose and clarifying the central concepts, the survey elicited global privacy concerns and information seeking intention with three items from Malhotra et al. (2004) and three items from Kahlor (2007), respectively, on 7-point Likert scales anchored in 'strongly disagree' and 'strongly agree'. Items were slightly adapted to fit the scope of our study. Then, every survey participant was presented with the description of one scenario randomly selected out of the four scenarios identified in the prestudy. For the respective scenario, the survey elicited participants' privacy information needs with the question: "If you would use such an app, how important would it be for you to be informed about the following aspects?" The aspects listed below the question were focused on different organizational privacy practices. Table 27 in the appendix lists the complete survey instrument. To identify a diverse but parsimonious set of aspects, we reviewed relevant literature on the content of organizational privacy communication (Ciocchetti 2007, Cottrill 2011, Culnan 2000, Desai et al. 2012, Faja and Trimi 2006, Langenderfer and Cook 2004, LaRose and Rifon 2006, Liu and Arnett 2002, Milne and Culnan 2002, Pollach 2006, Schwaig et al. 2006, Stanaland et al. 2009, H. Xu et al. 2011). Subsequently, the selection of aspects was iteratively refined based on feedback collected in the prestudy and the pilot study. Table 29 in the appendix lists the final selection of organizational privacy practices included in our survey.

Listed aspects were organized by major privacy concerns: information collection, handling of information, and offered privacy controls (Ackerman et al. 1999, Antón et al. 2010). Four aspects focused on sensors used for information collection: sensors on the user environment (eg, camera or microphone), location sensors, fingerprint scanners, and sensors for system usage (eg, web beacons or adware). Ten aspects focused on type of information collected: financial identifiers (eg, bank account number), governmental identifiers (eg, social security number), real consumer name, financial information (eg, account balance), consumer interactions with information systems (eg, click streams), purchases conducted by consumers, health-related information, consumer affiliations with groups (eg, political or religious groups), consumer preferences, and characteristics of client devices (eg, operating system or screen resolution). Four aspects focused on handling of information: retention of information, employed security measures, sharing practices, and storage practices. Eleven aspects focused on offered privacy controls: provision of access logs for consumer data, notification practices in case of privacy breaches and changes of organizational privacy practices and about effects of practice changes on already collected information, means offered for management of implicit and explicit consents, propagation of information updates to data recipients, consents for secondary uses of information, means offered to access collected information, and monitoring of organizational privacy practices by automated means, an

Table 23. Results of information sensitivity analysis for the four scenarios selected for the privacy information needs survey with number of respondents (N), mean (M) and standard deviation (SD) values for information sensitivity and perceived privacy ratings (1=low, 7=high) obtained in the survey.

Scenario	Brief description	N	Information sensitivity M (SD)	Perceived privacy M (SD)
Calculator App	An app that supports the consumer to solve simple arithmetic problems.	54	2.40 (1.78)	5.89 (1.40)
Music Streaming App	An app to access a large number of music tracks and stream them to the mobile device.	50	4.05 (1.72)	3.95 (1.60)
Navigation App	An app to help the consumer navigating while driving a car.	44	5.19 (1.79)	3.47 (1.63)
Finance App	An app to access a bank account and make financial transactions.	44	6.09 (1.63)	2.86 (1.96)

independent party, or the consumer information system provider. Participants gave answers on 11-point Likert scales anchored in ‘unimportant’ and ‘very important’. For the purposes of the survey, all items were translated to German. To ensure a high translation quality, translations were checked by two fellow researchers. A pretest was conducted with twelve information systems researchers and student assistants to improve the wording of displayed texts and items.

To further test and refine the survey design and to test the implementation of the community detection algorithm, we conducted a pilot study with 160 participants, which resulted in 134 valid responses because 26 participants failed to complete the survey, sped through the survey, or failed to correctly answer a control question. Participants for the pilot study were recruited over social media channels. After the questionnaire was sufficiently refined, the privacy information needs survey was conducted in March 2017. Participants were recruited with the support of a market research agency. Study participants that successfully completed the questionnaire were remunerated with €0.10 per minute.

7.3.2 Community Detection Analysis

To identify the consumer archetypes, we employed an agglomerative hierarchical community detection algorithm with Euclidean distances (Ward’s method; Ward 1963). Participants with the smallest difference in the variance of their privacy information need responses were iteratively grouped. For the community detection analysis, survey participant responses were standardized to unit variance. Communities and their subcommunities were identified through dendrogram inspection. As a tradeoff between parsimony and expressiveness, archetypes with less than 30 members, with no siblings, or on tiers deeper than tier-3 in the hierarchy were excluded from further analysis. The community detection algorithm was performed with the Scientific Computing Tools for Python (Jones et al. 2001). To validate the resulting communities, we tested whether mean privacy information needs of identified communities had significant positive correlations with reported global privacy concerns and information seeking intentions. The rationale for this was that participants reporting higher privacy concerns or higher information seeking intention should be grouped into clusters with higher privacy information needs.

To characterize differences of identified communities, we conducted an exploratory factor analysis in SPSS. Exploratory factor analysis reveals latent variables accounting for the covariance in observed data. Since our goal was to identify latent variables based on shared variance instead of data reduction and we expected moderate to strong correlations between the latent variables, we employed factor analysis instead of principal component analysis, which does not differentiate between shared and unique variance (Henson and Roberts 2006). Principal axis factoring was used because our data was not normally distributed[17]. Due to the exploratory nature of our study and our goal to identify differences between identified consumer archetypes, we focused on the upper bounds for the number of factors to be retained based on Kaiser's eigenvalue-greater-than-one rule and the scree test (Hayton et al. 2004). To account for correlation between factors, oblique rotation (direct oblimin) with Kaiser normalization was employed (Henson and Roberts 2006). The factor scores of each identified consumer archetype were used to characterize the archetype, coin a descriptive label for each archetype, and to examine the differences between identified consumer archetypes.

7.4 Results

7.4.1 Sample Description

A total of 1,557 participants started the survey, 648 responses were excluded from data analysis because participants failed to complete the survey, sped through the survey, or failed to answer a control question. Responses of 909 participants (female (472, 51.93%), male (435, 47.85%), trans* (2, 0.22%) remained for data analysis. The average questionnaire duration was six minutes. Participant age ranged from less than eighteen to 65-70 years (<18 (5, 0.55%), 18-24 (108, 11.88%), 25-29 (105, 11.55%), 30-34 (83, 9.13%), 35-39 (51, 5.61%), 40-44 (67, 7.37%), 45-49 (92, 10.12%), 50-54 (225, 24.75%), 55-59 (102, 11.22%), 60-64 (64, 7.04%), 65-70 (7, 0.77%)). Most participants had a completed vocational training or a university degree as highest degree (no degree (4, 0.44%), middle school degree (222, 24.42%), high school degree (191, 21.01%), completed vocational training (276, 30.36%), university degree (216, 23.76%)). The majority of participants owned a smartphone (819, 90.1%). Most participants used a smartphone at least daily (hourly (144, 15.84%), several times a day (486, 53.47%), daily (118, 12.98%), several times a week (58, 6.38%), few times a month (20, 2.2%), less than once a month (6, 0.66%), never (74, 8.14%), no response (3, 0.33%)). The majority of participants had less than 10 apps that they regularly used installed on their smartphones (0 apps (134, 14.74%), 1 app (45, 4.95%), 2-3 apps (197, 21.67%), 4-5 apps (238, 26.18%), 6-10 apps (197, 21.67%), 10-15 apps (49, 5.39%), 15-20 apps (21,

[17] Shapiro-Wilk test was significant (p<0.001) for all elicited privacy information needs.

2.31%), >20 apps (19, 2.09%), no response (9, 0.99%)). Survey participants were distributed equally across scenarios (Finance App: 229, 25.19%; Navigation App: 215, 23.65%; Music Streaming App: 228, 25.08%; Calculator App: 237, 26.07%).

Which scenario was presented (Spearman ρ = 0.076, p = 0.023, archetypes ranked by mean privacy information need and scenarios ranked by information sensitivity), level of education (Spearman ρ = -0.009, p = 0.792), smartphone ownership (Spearman ρ = -0.012, p = 0.713), frequency of smartphone use (Spearman ρ = -0.089, p = 0.007), and number of installed smartphone apps (Spearman ρ = -0.067, p = 0.043) had no meaningful or no significant impact on archetypes. Age was weakly correlated with archetypes (Spearman ρ = 0.191, p < 0.001). Global information privacy concern (Spearman ρ = 0.449, p < 0.001) and information seeking intention (Spearman ρ = 0.367, p < 0.001) were moderately correlated with archetypes.

Across all archetypes, consumers are most interested in collection of financial identifiers (M=8.82, Mdn=10, SD=2.48), collection of financial information (M=8.78, Mdn=10, SD=2.51), means offered for consent management (M=8.61, Mdn=10, SD=2.32), logs of accesses to their data (M=8.48, Mdn=10, SD=2.46), information sharing practices (M=8.48, Mdn=10, SD=2.61), and collection of government identifiers (M=8.47, Mdn=10, SD=2.75). Consumers are least interested in use of fingerprint scanners (M=6.8, Mdn=8, SD=3.51), collection of preferences (M=7.11, Mdn=8, SD=3.17), collection of group affiliations (M=7.49, Mdn=9, SD=3.20), use of software use sensors (M=7.55, Mdn=8, SD=2.88), and collection of system interactions (M=7.65, Mdn=9, SD=2.83).

7.4.2 Identified Privacy Information Need Factors

The collected sample is appropriate for exploratory factor analysis. The ratio of cases to variables was greater than 30 to 1. All items have a correlation of at least 0.3 with another item. The KMO Measure of Sampling Adequacy is 0.971 and well beyond the threshold of 0.6. Bartlett's Test of Sphericity was significant ($X^2(406)=24{,}485$, p<0.001). Extracted communalities were greater than 0.6 for 28 items and 0.386 for one item. Five factors have eigenvalues over one. Solutions for three, four, five, and six factors were examined. The five factor solution was selected because the factors could be meaningfully interpreted, all eigenvalues were greater than one, and the scree plot reveals that eigenvalues level off for more than five factors. The items focused on collection of real names and information on the client device have loadings of 0.361 and 0.355, respectively, but were retained because examination of Cronbach's α values reveals convergent validity.

The five factors explained 75% of variance. Due to correlation of factors, the variance explained by the individual factors could not be calculated. The first factor, information sensors (SEN), represents privacy information needs concerned with how information is collected. The second factor, identifier collection (ICO), represents privacy information needs concerned with collection of identifiers and of financial information. The third factor, consumer data collection (CCO), represents privacy information needs concerned with collection of information about consumers. The fourth factor, information handling

(IHD), represents privacy information needs concerned with the handling of information. The fifths factor, privacy controls (PCT), represents privacy information needs concerned with privacy controls offered to consumers. Table 24 presents an overview of factors, loadings, communalities, Cronbach's α values, and rotation sums of squared loadings. Correlations between factors were moderate to strong, ranging from .430 for consumer data collection and information handling to .713 for information handling and privacy controls. Table 28 in the appendix lists all correlations between factors.

7.4.3 Consumer Archetypes by Privacy Information Needs

The community detection algorithm revealed thirteen archetypes across three hierarchy levels. Figure 22 presents an overview of all archetypes. Three archetypes form the top tier of the hierarchy. Six archetypes refine tier-1 archetypes on the second tier. Four archetypes refine tier-2 archetypes on the third tier. In the following, we focus on the nine archetypes that are not further refined by subarchetypes since higher-level archetypes represent aggregations of their subarchetypes. The following paragraphs describe the nine archetypes ordered by increasing mean privacy information need. Figure 23 and Table 25 presents an overview of the privacy information needs for the nine identified archetypes.

Laid-Back Information Seekers comprise 6.49% (59/909) of sample participants. These consumers have very latent privacy information needs. They seldom may want to be informed about some organizational privacy practices. For example, if they interact with potentially insidious consumer information systems. However, they seem to be usually apathetic about organizational privacy practices.

Inspectors of Identifiable Information Collection and Handling comprise 4.40% (40/909) of sample participants. These consumers have overall moderate privacy information needs. Their privacy information needs are highest for collection of identifiers and handling of information. Inspectors of Identifiable Information Collection and Handling appear to be concerned with the appropriate handling of identifiable information and may be interested in obtaining information on further organizational privacy practices if handling of identifiable information is perceived as inappropriate.

Controllers of Identifiable Information Collection and Handling comprise 10.67% (97/909) of sample participants. These consumers have high privacy information needs for collection of identifiers and are also more interested in collection of other information on them and offered privacy controls than Inspectors of Identifiable Information Collection and Handling. Privacy information needs of Controllers of Identifiable Information Collection and Handling seem to be spurred by collection of information that can be linked back to them. In such situations, they are also interested in means offered to control organizational privacy practices.

Information Handling Controllers comprise 6.49% (59/909) of sample participants. These consumers have high privacy information needs for information handling and offered privacy controls. Other organizational privacy practices are only of moderate interest to them. Privacy information needs of Information Handling Controllers appear to be mainly concerned with the handling of information and offered privacy controls independent of the types of information collected.

Table 24. Factor loadings and communalities for privacy information needs and Cronbach's α and rotation sums of squared loadings for factors determined through principle axis factoring with direct oblimin rotation (N=909).

Factor	Item	Factor loading					Communalities	Cronbach α	Rotation sums of squared loadings
		SEN	ICO	UCO	IHD	PCT			
Information sensors (SEN)	Environment	**.752**	.147	-.040	-.001	.018	.687	.845	10.018
	Location	**.731**	-.041	.035	.107	.100	.755		
	Fingerprint	**.630**	-.018	.061	-.027	-.027	.386		
	Software use	**.518**	-.040	.039	.268	.150	.689		
Identifier collection (ICO)	Financial identifier	.058	**.855**	-.066	.084	.002	.806	.890	8.659
	Government identifier	.050	**.773**	.062	.016	.009	.718		
	Real name	.106	**.361**	.107	.134	.246	.607		
	Financial data	-.012	**.680**	.182	.012	.087	.710		
Consumer data collection (CCO)	System interaction	.159	.115	**.421**	.137	.195	.699	.911	8.628
	Purchases	.078	.093	**.465**	.081	.215	.603		
	Health	.022	.347	**.522**	-.040	.094	.663		
	Affiliation	.103	.093	**.724**	.031	-.003	.721		
	Preferences	.070	-.029	**.801**	.064	.001	.734		
	Client device	.071	.178	**.355**	.091	.233	.572		
Information handling (IHD)	Retention	.009	-.082	.072	**.875**	.028	.807	.941	11.046
	Security	-.021	.064	-.054	**.887**	.041	.833		
	Sharing	.017	.116	-.028	**.885**	-.025	.798		
	Storage	.055	-.034	.032	**.864**	-.009	.795		
Privacy controls (PCT)	Access log	.011	.001	.005	.020	**.811**	.699	.962	14.293
	Breach notification	.007	.042	-.090	-.005	**.889**	.749		
	Practice change governance	.041	-.054	.004	.029	**.819**	.704		
	Practice change notification	.084	.055	-.046	.045	**.771**	.750		
	Consent management	.026	.081	-.110	.027	**.824**	.721		
	Downstream propagation	.111	.044	.064	-.016	**.695**	.681		
	Secondary use consent	.072	-.010	-.033	-.091	**.871**	.689		
	Consumer access	-.029	.100	-.029	.083	**.749**	.698		
	Automated practice monitoring	-.063	-.061	.169	.029	**.793**	.716		
	Third-party practice monitoring	-.008	.005	.105	.020	**.734**	.657		
	Practice self-monitoring	-.080	-.054	.135	.079	**.775**	.700		

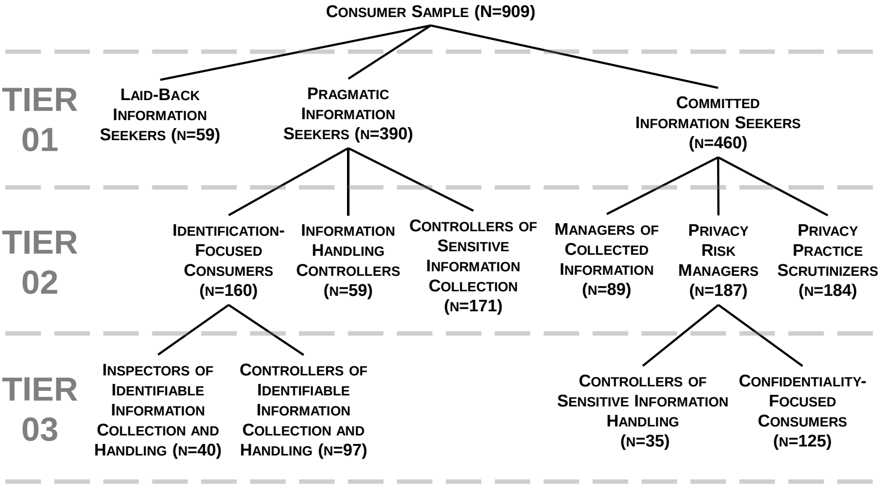

Consumer Sample (N=909)
TIER 01
TIER 02
TIER 03
Laid-Back Information Seekers (n=59)
Pragmatic Information Seekers (n=390)
Committed Information Seekers (n=460)
Identification-Focused Consumers (n=160)
Information Handling Controllers (n=59)
Controllers of Sensitive Information Collection (n=171)
Managers of Collected Information (n=89)
Privacy Risk Managers (n=187)
Privacy Practice Scrutinizers (n=184)
Inspectors of Identifiable Information Collection and Handling (n=40)
Controllers of Identifiable Information Collection and Handling (n=97)
Controllers of Sensitive Information Handling (n=35)
Confidentiality-Focused Consumers (n=125)

Figure 22. Overview of hierarchy of consumer archetypes by privacy information needs and archetype size within our sample. Archetypes on lower tiers in the hierarchy refine their parents. Mean privacy information needs increase from the left side of the tree to the right side of the tree.

Controllers of Sensitive Information Collection comprise 18.81% (171/909) of sample participants. These consumers are mainly interested in collection of sensitive information and all kinds of offered privacy controls. Other organizational privacy practices are of lesser interest to them. However, their privacy information needs are moderately high or high for all kinds of organizational privacy practices. Controllers of Sensitive Information Collection give the impression to desire protection and appropriate use of their sensitive information and to become interested in a wide range of organizational privacy practices if sensitive information is collected.

Managers of Collected Information comprise 9.79% (89/909) of sample participants. These consumers have moderate privacy information needs for sensors used for information collection. Otherwise, their privacy information needs are high. Managers of Collected Information do not seem to be particularly interested in how consumer information systems obtain their information. Otherwise, they require detailed information on organizational privacy practices and offered privacy controls.

Controllers of Sensitive Information Handling comprise 3.85% (35/90) of sample participants. These consumers have high overall privacy information needs and are particularly interested in the collection of sensitive information, information handling practices, and offered privacy controls. Controllers of Sensitive Information Handling give the impression to be mainly concerned with the protection and use of sensitive information.

Confidentiality-Focused Consumers comprise 13.75% (125/187) of sample participants. These consumers have high overall privacy information needs and are particularly interested in collection of sensitive information and information security and sharing

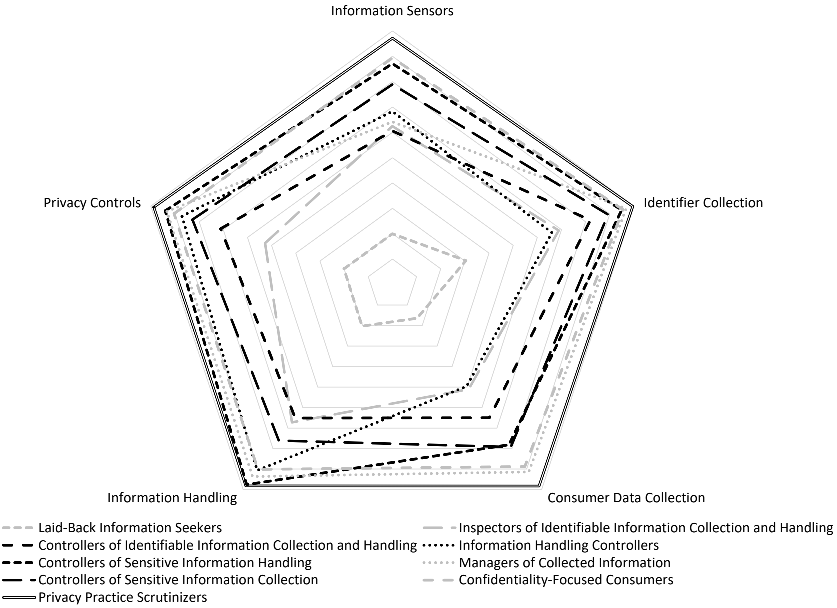


Figure 23. Mean privacy information needs of identified consumer archetypes that are not refined by subarchetypes. The center indicates mean privacy information needs of 0 and the outmost line indicates mean privacy information needs of 10.

practices. Confidentiality-Focused Consumers appear to focus predominantly on what sensitive information is collected, whether it is properly protected, and who has access to it.

Privacy Practice Scrutinizers comprise 20.24% (184/460) of sample participants. These consumers have high privacy information needs for any organizational privacy practice. Privacy Practice Scrutinizers seem to be interested in obtaining as much information on organizational privacy practices as they can.

7.5 Discussion

7.5.1 Implications for Theory and Practice

This study follows a bottom-up approach for knowledge development on organizational privacy communication. With respect to the entire sample, reported privacy information needs are high for all organizational privacy practices. The lowest reported mean privacy information need was 6.8 on a scale from 0–10 for use of fingerprint scanners for information collection. Exploratory factor analysis revealed five factors capturing differences in privacy information needs between consumer archetypes. We identified nine distinct consumer archetypes with diverse privacy information needs that organizational

Table 25. Mean (M), median (Mdn), and standard deviations (SD) for the consumer archetypes not refined by subarchetypes.

	Information sensors M (Mdn, SD)	**Identifier collection M (Mdn, SD)**	**Consumer data Collection M (Mdn, SD)**	**Information handling M (Mdn, SD)**	**Privacy controls M (Mdn, SD)**
Laid-back information seekers	2.00 (0, 3.04)	3.05 (0, 3.87)	1.65 (0, 2.57)	2.03 (0, 2.95)	2.00 (0, 2.83)
Inspectors of identifiable information collection and handling	6.24 (6, 2.64)	6.89 (7, 2.66)	5.11 (5, 2.62)	6.72 (6, 2.30)	5.27 (6, 2.55)
Controllers of identifiable information collection and handling	6.06 (6, 2.57)	8.2 (9, 1.80)	6.5 (7, 2.19)	6.51 (7, 2.15)	7.11 (7, 1.71)
Information handling controllers	6.83 (8, 3.67)	6.61 (9, 4.10)	4.97 (5, 4.14)	9.06 (10, 1.72)	8.72 (10, 2.13)
Controllers of sensitive information collection	7.89 (8, 1.83)	8.93 (9, 1.47)	7.93 (8, 1.95)	7.61 (8, 2.51)	8.28 (8, 1.71)
Managers of collected information	6.41 (8, 3.69)	9.68 (10, 0.97)	9.13 (10, 1.59)	9.37 (10, 1.19)	9.34 (10, 1.43)
Controllers of sensitive information collection and handling	8.71 (9, 1.95)	9.49 (10, 1.14)	7.81 (9, 2.50)	9.76 (10, 0.64)	9.40 (9, 0.96)
Confidentiality-focused consumers	8.93 (9, 1.27)	9.55 (10, 0.86)	8.87 (9, 1.18)	9.01 (9, 1.24)	9.04 (9, 0.96)
Privacy practice scrutinizers	9.71 (10, 0.77)	9.96 (10, 0.26)	9.83 (10, 0.57)	9.82 (10, 0.55)	9.88 (10, 0.49)

privacy communication must cater to. Some consumers exhibit low, moderate, or high privacy information needs across all organizational privacy practices, which aligns with the Westin partitioning in Unconcerned, Pragmatists, and Fundamentalists (Kumaraguru and Cranor 2005). However, other consumers have more refined privacy information needs. Some consumer archetypes exhibit higher privacy information needs for organizational privacy practices related to identifier collection, information handling, offered privacy controls, or combinations thereof. Some consumer archetypes exhibit lesser interests for practices related to information sensors and consumer data collection. Related research demonstrates that diverse influences, such as sensitivity of collected information, situational cues, or socio-demographics (Bansal et al. 2010, John et al. 2011, Miltgen and Peyrat-Guillard 2014), shape consumer groups with different privacy preferences. Our study extends the extant body of knowledge on consumers' privacy preferences by identifying consumer archetypes with different privacy information needs that must be satisfied by effective organizational privacy communication.

Furthermore, this research contributes to the scientific knowledge base by highlighting shortcomings of traditional views on development of technical privacy communications[18]. From a retrospective point of view, technical privacy communications can be considered one outcome of the Information Technology Privacy Cycle. The Information Technology Privacy Cycle (Turner and Dasgupta 2003) captures how the introduction of new information technology and its subsequent increased use will lead to heightened public concern about privacy, finally to the implementation of reactive privacy legislation, and then the cycle starts all over with the introduction of new information technology. New privacy legislation encourages organizations to improve their technical privacy communications which are then presented to consumers (Figure 24A). However, this reoccurring top down process aligns badly with the diversity of the privacy information needs of the consumer archetypes identified in our study. Privacy legislation is not only the outcome of complex and tedious democratic processes influenced by various interest groups but also unlikely to result in prescriptions detailed enough to match the diverse privacy information needs of consumers across all contexts consumer information systems are used in (Langenderfer and Cook 2004). Furthermore, advancing privacy legislation would become even more complex and tedious if all the convictions valued by the respective consumer groups were elicited and incorporated. Our findings indicate that a more flexible and direct development process is required for the emergence of effective organizational privacy communication catering to the diverse privacy information needs of the identified consumer archetypes.

As a first step, we propose a Privacy Communication Circle as a more effective system for development of technical privacy communications (Figure 24B). From this perspective, organizational privacy communication is conceptualized as a circle rearranging itself on a spectrum between vicious and virtuous (Masuch 1985). The circle represents consumer information systems with three components relevant within the scope of this work—organizations, their technical privacy communications, and a set of consumer archetypes. All components reciprocally interact with each other in various ways exemplarily illustrated in the following paragraph[19].

Technical privacy communications are instantiated and maintained by organizations and provide organizations with feedback on their use. Members of consumer archetypes use technical privacy communications and technical privacy communications address privacy information needs of consumer archetypes. Members of consumer archetypes provide organizations with revenue, or compensation claims, and organizations finance the maintenance of the consumer information systems that are used by members of consumer archetypes and signal their actual privacy practices during system use.

[18] With the term technical privacy communications, we refer to any means useful to control or convey information on organizational privacy practices. That may be conventional means such as privacy notices, privacy seals, just-in-time privacy notifications, publishing of source code, or privacy settings but could also be entirely new means for communicating or controlling organizational privacy practices that are tailored to the specific privacy information needs of certain consumer archetypes.

[19] A taxonomy of interactions between the components is beyond the scope of this work.

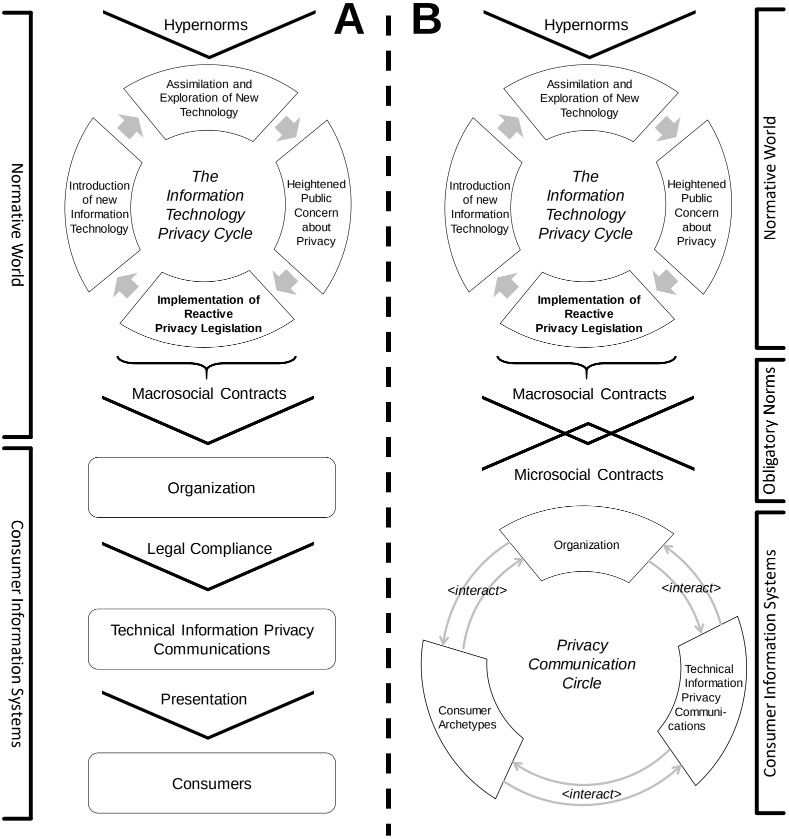

A
B
Hypernorms
Assimilation and Exploration of New Technology
Introduction of new Information Technology
The Information Technology Privacy Cycle
Heightened Public Concern about Privacy
Implementation of Reactive Privacy Legislation
Macrosocial Contracts
Microsocial Contracts
Organization
Legal Compliance
Technical Information Privacy Communications
Presentation
Consumers
Normative World
Consumer Information Systems
Obligatory Norms
Privacy Communication Circle
Consumer Archetypes
Technical Information Privacy Communi-cations
<interact>

Figure 24. (A) Traditional top-down process where organizational privacy communication is predominantly the result of organizational compliance to privacy regulation. (B) Proposed Privacy Communication Circle view on organizational privacy communication where communities of organizations and consumer archetypes interact and create technical privacy communications that reflect their shared values and that align with macro- and microsocial contracts.

Organizational privacy communication can still be influenced by new governmental regulation emerging from the Information Technology Privacy Cycle but the Privacy Communication Circle can also change its effectiveness on its own. Organizational privacy communication will be least effective if the privacy information needs of only one consumer archetype are satisfied. Introduction of additional technical privacy communications will satisfy privacy information needs of more consumer archetypes and increase the effectiveness of organizational privacy communication until the privacy information needs of all relevant consumer archetypes are satisfied. Conversely, changes to organizational privacy practices may render current technical privacy communications inadequate for some consumer archetypes and organizational privacy communication will become less effective.

The utility of the Privacy Communication Circle is supported by Integrative Social Contracts Theory (ISCT; Donaldson and Dunfee 1994, 1995). ISCT is a contractarian framework developed in the field of business ethics. ISCT aims to bridge the gap between universal norms guiding human behavior and the diverse explicit or implicit social norms valued in contextualized communities. Within the scope of ISCT, a community is "a self-defined, self-circumscribed group of people who interact in the context of shared tasks, values, or goals and who are capable of establishing norms of ethical behavior for themselves" (Donaldson and Dunfee 1994, p. 262). Correspondingly, with respect to the Privacy Communication Circle, a community comprises consumer archetypes and organizations in a situation where organizational privacy communication is supported by technical privacy communications. ISCT is based on two types of social contracts. First, macrosocial contracts are hypothetical, normative contracts that govern general economic behavior. Macrosocial contracts specify the rules that all members of a comprehensive society would agree on "when asked what rules they would want applied to them in the context of economic transactions, under the condition that they not know the position they would occupy under the rules" (Donaldson and Dunfee 1995, p. 93). Within the context of the Privacy Communication Circle, privacy legislation emerging from the Information Technology Privacy Cycle can be considered macrosocial contracts. Second, microsocial contracts are implicit contracts representing social norms valued by specific communities and practiced in the real world. Microsocial contracts account for contextual influences by enabling economic actors to develop their own rules governing behavior in distinct communities. Within the context of the Privacy Communication Circle, microsocial contracts capture the agreed-on values within the Privacy Communication Circle. Hence, proposition P1:

> ***P1**: Organizational privacy communication will only be effective if available technical privacy communications reflect the shared values of the contextualized community of organizations and consumer archetypes.*

ISCT distinguishes between two types of microsocial contract norms—authentic norms and obligatory norms. Authentic norms are norms that fulfill the basic conditions to constitute ethical norms and must be "grounded in informed consent buttressed by a right of exit" (Donaldson and Dunfee 1994, p. 262). Furthermore, albeit informed consent must not be explicit, most members of contextualized communities must approve of the norm, disapprove deviance from the norm, and act in accordance with the norm. Transferred to the context of the Privacy Communication Circle, this means that organizational privacy communication will only be viable if all components of the circle permit current privacy communication practices, disfavor deviance from them, perform accordingly, and have the opportunity to exit the community in case of misalignment. Hence, proposition P2:

> ***P2**: Viable organizational privacy communication has to ensure that all involved organizations and consumer archetypes within a contextualized community approve of current privacy communication practices, disapprove deviance from them, act accordingly, and are supported by compatible technical privacy communications and that all involved organizations and consumer archetypes within a contextualized community are enabled to exit the community.*

Authentic norms are also obligatory norms if they fulfill the additional condition of being compatible with hypernorms. Hypernorms "entail principles so fundamental to human existence that they serve as a guide in evaluating lower level moral norms" (Donaldson and Dunfee 1994, p. 265). Hypernorms are norms valued across cultures and ensure that macrosocial contracts do not sanction arbitrary microsocial contracts. With respect to organizational privacy communication, candidate hypernorms are, for example, notice and choice[20], which are fundamental principles enshrined in privacy regulations and standards across the globe (Cate 2010). Accordingly, obligatory norms link the empirical world of norms governing behavior in practice with the normative world governing how actors should and should not behave. Within the context of the Privacy Communication Circle, hypernorms guide, but can also be used to invalidate, privacy legislation emerging from the Information Technology Privacy Cycle and can be used to determine the appropriateness of privacy communication practices in a contextualized community. Accordingly, organizational privacy communication will be most effective if it complies with hypernorms because, otherwise, it will have to be revised at some point in time due to tension with hypernorms. Compliance with privacy regulation can be a useful proxy for hypernorms, which are often hard to identify (Dunfee 2006). Hence, proposition P3:

> ***P3**: Organizational privacy communication should be compliant with hypernorms, or privacy legislation as a proxy for hypernorms, to increase effectiveness by avoiding need for revisions.*

The Privacy Communication Circle is not intended to replace the traditional top-down development process for organizational privacy communication. It rather constitutes a refined lens on organizational privacy communication that also accounts for the diversity of consumers' privacy information needs. ISCT does much more than establishing a bridge between the normative world and contextualized reality. In particular, it constitutes a powerful ethical decision making and norm development framework that is, among other, of interest to the information systems domain (Conger and Loch 2000). Such application of ISCT in the privacy domain is, however, beyond the scope of this manuscript. This manuscript serves as a foundation for design of effective organizational privacy communication by characterizing a central part of the communities relevant in the privacy domain, that is, consumer archetypes.

From a practical standpoint, refinement of the traditional top-down process in form of the Privacy Communication Circle gives rise to the following core insights for managing

[20] The principles of notice and choice require that consumers are informed about organizational privacy practices and enabled to determine for themselves whether they want to be subjected to them.

organizational privacy communication. Organizations that want to improve organizational privacy communication in an effective way should identify the most prevalent consumer archetypes in their consumer base and instantiate technical privacy communications tailored to them. Additionally, technical privacy communications should be designed in such a way that they adapt or can be adapted to specific or changing privacy information needs of consumers. Organizations that want to maintain their current effectiveness of organizational privacy communication should not change their privacy practices in a way that renders their technical privacy communications inadequate. Organizations that want to avoid loss of consumers should introduce suitable technical privacy communications prior to changing their privacy practices. Organizations that want to reduce effort for maintenance of technical privacy communications should reduce privacy practices leading to high or diverging privacy information needs (eg, collection of unnecessary identifiers or extensive sharing practices).

Furthermore, the identified consumer archetypes can be used by practical audiences to better understand the privacy information needs of the consumers they are confronted with and to develop and deploy corresponding technical privacy communications that fit the different contexts their consumer information systems are used in. The identified consumer archetypes could also serve as a foundation for the development of an evaluation framework for the suitability and effectiveness of the ensembles of technical privacy communications deployed by organizations. Such an evaluation framework would also be a useful resource to inform public policy. Finally, the five privacy information needs factors identified with the exploratory factor analysis can be used to inform development of measurement instruments for consumers' privacy information needs or corresponding classification algorithms.

7.5.2 Limitations

This study has some limitations. First, our findings cannot be directly translated to consumer groups of situated consumer information systems. For situated consumer information systems, the size of some consumer archetypes may be negligible. For example, consumer information systems running on air-gapped systems are likely to be predominantly confronted with Laid-Back Information Seekers. Consumer information systems that are only occasionally used will likely not be confronted with many Committed Information Seekers. The goal of our study was to establish an overview of the diversity and range of consumer archetypes with which consumer information system providers may be confronted with. Accordingly, we chose a scenario-based survey approach instead of a situated artifact to avoid omission of archetypes irrelevant for that particular artifact. What consumer archetypes organizational privacy communications should cater to needs to be determined based on the characteristics of the respective situated consumer information system.

Second, we only included a limited subset of privacy information needs in our survey to ensure an acceptable survey duration. Inclusion of more privacy information needs may have increased drop-off rates or response quality. However, this aligns with our study objective of identifying consumer archetypes based on privacy information needs, which requires variety and not comprehensiveness of privacy information needs. To ensure variety, we purposefully elicited privacy information needs for organizational privacy practices organized by major privacy concerns for the privacy information needs survey.

Third, we refrained from breaking the propositions developed based on the Privacy Communication Circle and ISCT down into testable hypotheses (Bacharach 1989). The purpose of the propositions was to capture the main implications of the Privacy Communication Circle and the ISCT perspective on organizational privacy communication. Derivation of hypotheses from the propositions for the purpose of testing the assertions will require careful consideration of the context of the situated consumer information systems under study. For example, it has to be determined what variables are best suited to operationalize concepts such as compliance with hypernorms based on cultural characteristics of consumer information systems under study.

Fourth, the focus on a German sample may have missed some consumer archetypes. However, the diversity of influences on privacy attitudes makes it unlikely that archetypes are only shaped by socio-demographics. Under additional consideration of the focus on general privacy information needs and the sample size, our study design can be deemed suitable to identify the prevalent consumer archetypes.

Fifth, we only elicited whether consumers want to be informed about organizational privacy practices. Thus, our findings yield no insights why consumers want to be informed about organizational privacy practices. For example, some consumers may want to be informed about collection of preferences because they want to be served with tailored applications and others may be concerned about profiling. Still, from the perspective of transparent organizational privacy communication it is inconsequential why consumers want to obtain certain information, the import aspect is what information consumers have to be provided with.

7.5.3 Future Research

Promising avenues for future research include the assessment of current technical privacy communications with respect to suitability for the different consumer archetypes and the development of new designs for technical privacy communications tailored to privacy information needs of consumer archetypes that are not served by existing technical privacy communications. Gold standards for information to be provided to the different consumer archetypes could be developed to aid instantiations of technical privacy communications and to support evaluations of existing technical privacy communications. Furthermore, our exploratory factor analysis could be complemented through confirmatory factor analysis to develop measurement instruments for consumer privacy information needs and classification of consumers by archetypes.

7.5.4 Conclusion

The evolution of normative privacy standards over the past decades fell short in promoting organizational privacy communication satisfying consumers' privacy information needs. As a result, consumer information system providers and consumers are impeded in leveraging the full potential of consumer information systems due to impediments in recognizing the right systems for desired tasks, occurrence of defensive consumer practices, and consumer or regulator backlash once undesirable organizational privacy practices come to light (Choi et al. 2016). The bottom-up approach taken in this study narrows the gap between the normative and the empirical privacy world by revealing the diversity of consumers' privacy information needs, capturing them in consumer archetypes, and unveiling latent variables of consumer privacy information needs. Complementation of normative guidance for organizational privacy communication with a thorough understanding of consumers' privacy preferences may just be the missing impulse for the emergence of truly effective organizational privacy communication.

7.6 References

Ackerman MS, Cranor LF, Reagle J (1999) Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. 1st ACM Conference on Electronic Commerce. (ACM, Denver, CO, USA), 1–8.

Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and Human Behavior in the Age of Information. Science 347(6221):509–514.

Adams A, Sasse MA (1999) Privacy Issues in Ubiquitous Multimedia Environments: Wake Sleeping Dogs or Let Them Lie. Proceedings of Interact '99. (IOS Press, Edinburgh, Scotland), 214–221.

Antón AI, Earp JB, Young JD (2010) How Internet Users' Privacy Concerns Have Evolved Since 2002. IEEE Security & Privacy 8(1):21–27.

Bacharach SB (1989) Organizational Theories: Some Criteria for Evaluation. Academy of Management Review 14(4):496–515.

Bansal G, Zahedi FM, Gefen D (2010) The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online. Decision Support Systems 49(2):138–150.

Berendt B, Günther O, Spiekermann S (2005) Privacy in e-Commerce: Stated Preferences vs. Actual Behavior. Communications of the ACM 48(4):101–106.

Cate FH (2010) The Limits of Notice and Choice. IEEE Security & Privacy 8(2):59–62.

Choi BCF, Kim SS, Jiang ZJ (2016) Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior. Journal of Management Information Systems 33(3):904–933.

Ciocchetti CA (2007) E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors. American Business Law Journal 44(1):55–126.

Clarke R (2006) What's "Privacy"? Retrieved (September 17, 2017), http://www.rogerclarke.com/DV/Privacy.html . Archived at: http://www.webcitation.org/6tXpcLq7f.

Conger S, Loch KD (2000) Invitation to a Public Debate on Ethical Computer Use. SIGMIS Database 32(1):58–69.

Cottrill CD (2011) Location Privacy: Who Protects? Journal of the Urban & Regional Information Systems Association 23(2):49–59.

Cranor LF, Reagle J, Ackerman MS (1999) Beyond Concern: Understanding Net Users' Attitudes about Online Privacy. AT&T Labs-Research Technical Report, TR 99.4.3. (MIT Press, Cambridge, MA, USA).

Culnan MJ (1993) "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. MIS Quarterly 17(3):341–363.

Culnan MJ (2000) Protecting Privacy Online: Is Self-Regulation Working? Journal of Public Policy & Marketing 19(1):20–26.

Desai M, Lodge D, Gates M, Wolvin M, Louer G (2012) The FTC Privacy Report: What the Report Means and How You can get Ahead of Enforcement Trends by Implementing Best Practices Now. International Journal of Mobile Marketing 7(2):26–36.

Dinev T, Hart P (2006) Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. International Journal of Electronic Commerce 10(2):7–29.

Dinev T, Xu H, Smith JH, Hart P (2013) Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts. European Journal of Information Systems 22(3):295–316.

Donaldson T, Dunfee TW (1994) Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory. The Academy of Management Review 19(2):252–284.

Donaldson T, Dunfee TW (1995) Integrative Social Contracts Theory: A Communitarian Conception of Economic Ethics. Economics and Philosophy 11(1):85–112.

Dunfee TW (2006) A Critical Perspective of Integrative Social Contracts Theory: Recurring Criticisms and Next Generation Research Topics. Journal of Business Ethics 68(3):303–328.

Earp JB, Antón AI, Aiman-Smith L, Stufflebeam WH (2005) Examining Internet Privacy Policies Within the Context of User Privacy Values. IEEE Transactions on Engineering Management 52(2):227–237.

Faja S, Trimi S (2006) Influence of the Web Vendor's Interventions on Privacy-Related Behaviors in e-Commerce. Communications of the Association for Information Systems 17(1):27.

Hann IH, Hui KL, Lee SYT, Png IPL (2007) Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. Journal of Management Information Systems 24(2):13–42.

Hayton JC, Allen DG, Scarpello V (2004) Factor Retention Decisions in Exploratory Factor Analysis: A Tutorial on Parallel Analysis. Organizational Research Methods 7(2):191–205.

Henson RK, Roberts JK (2006) Use of Exploratory Factor Analysis in Published Research: Common Errors and some Comment on Improved Practice. Educational and Psychological Measurement 66(3):393–416.

Hjørland B (1997) Information Seeking and Subject Representation (Greenwood Press, Westport, CT, USA).

Hoofnagle CJ, Urban JM (2014) Alan Westin's Privacy Homo Economicus. Wake Forest Law Review 49:261–317.

Hsu CWJ (2006) Privacy Concerns, Privacy Practices and Web Site Categories. Online Information Review 30(5):569–586.

Huang HY, Bashir M (2016) Privacy by Region: Evaluation Online Users' Privacy Perceptions by Geographical Region. Proceedings of the 2016 Future Technologies Conference. (IEEE, San Francisco, CA, USA), 968–977.

Jensen C, Potts C (2004) Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. (ACM, New York, NY, USA), 471–478.

Jensen Carlos, Potts C, Jensen Christian (2005) Privacy Practices of Internet Users: Self-Reports versus Observed Behavior. International Journal of Human-Computer Studies 63(1–2):203–227.

Jiang ZJ, Heng CS, Choi BCF (2013) Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. Information Systems Research 24(3):579–595.

John LK, Acquisti, A, Loewenstein G (2011) Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information. Journal of Consumer Research 37(5):858–873.

Jones E, Oliphant T, Peterson P, et al. (2001) SciPy: Open Source Scientific Tools for Python. Retrieved (July 12, 2017), http://www.scipy.org/.

Kahlor LA (2007) An Augmented Risk Information Seeking Model: The Case of Global Warming. Media Psychology 10(3):414–435.

Koops BJ, Newell BC, Timan T, Skorvanek I, Chokrevski T, Galic M (2016) A Typology of Privacy. University of Pennsylvania Journal of International Law 38(2):483–575.

Kumaraguru P, Cranor LF (2005) Privacy Indexes: A Survey of Westin's Studies (Carnegie Mellon University, Pittsburgh, PA).

Langenderfer J, Cook DL (2004) Oh, What a Tangled Web we Weave: The State of Privacy Protection in the Information Economy and Recommendations for Governance. Journal of Business Research 57(7):734–747.

Lankton NK, McKnight DH, Tripp JF (2017) Facebook Privacy Management Strategies: A Cluster Analysis of User Privacy Behaviors. Computers in Human Behavior 76:149–163.

LaRose R, Rifon N (2006) Your Privacy is Assured - Of Being Disturbed: Websites With and Without Privacy Seals. New Media & Society 8(6):1009–1029.

Lee JM, Rha JY (2016) Personalization–Privacy Paradox and Consumer Conflict with the Use of Location-Based Mobile Commerce. Computers in Human Behavior 63:453–462.

Liu C, Arnett KP (2002) Raising a Red Flag on Global WWW Privacy Policies. The Journal of Computer Information Systems 43(1):117–127.

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

Maslow AH (1943) A Theory of Human Motivation. Psychological Review 50(4):370–396.

Masuch M (1985) Vicious Circles in Organizations. Administrative Science Quarterly 30(1):14–33.

McDonald AM, Cranor LF (2008) The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 4(3):540–565.

Milberg SJ, Burke SJ, Smith HJ, Kallman EA (1995) Values, Personal Information Privacy, and Regulatory Approaches. Communications of the ACM 38(12):65–74.

Milne GR, Culnan MJ (2002) Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys. Information Society 18(5):345–359.

Miltgen CL, Peyrat-Guillard D (2014) Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries. European Journal of Information Systems 23(2):103–125.

Miyazaki AD, Krishnamurthy S (2002) Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. Journal of Consumer Affairs 36(1):28–49.

Morton A, Sasse MA (2014) Desperately Seeking Assurances: Segmenting Users by Their Information-Seeking Preferences. Proceedings of the 12th Annual Conference on Privacy, Security and Trust. 102–111.

Organisation for Economic Cooperation and Development (1980) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Recommendation by the Council of the OECD. Retrieved (June 25, 2013), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm . Archived at: http://www.webcitation.org/6Y7eE1Q3m.

Park YJ (2013) Digital Literacy and Privacy Behavior Online. Communication Research 40(2):215–236.

Pollach I (2006) Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions. Journal of Organizational and End User Computing 18(1):23–49.

Reed PJ, Spiro ES, Butts CT (2016) Thumbs up for Privacy?: Differences in Online Self-Disclosure Behavior Across National Cultures. Social Science Research 59:155–170.

Rodríguez-Priego N, van Bavel R, Monteleone S (2016) The Disconnection Between Privacy Notices and Information Disclosure: An Online Experiment. Economia Politica 33(3):433–461.

Schwaig KS, Kane GC, Storey VC (2006) Compliance to the Fair Information Practices: How Are the Fortune 500 Handling Online Privacy Disclosures? Information & Management 43(7):805–820.

Sheehan KB (2002) Toward a Typology of Internet Users and Online Privacy Concerns. The Information Society 18(1):21–32.

Son JY, Kim SS (2008) Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. MIS Quarterly 32(3):503–529.

Spiekermann S, Grossklags J, Berendt B (2001) e-Privacy in 2nd Generation e-Commerce: Privacy Preferences Versus Actual Behavior. Proceedings of the 3rd ACM Conference on Electronic Commerce. (ACM, New York, NY, USA), 38–47.

Stanaland AJS, Lwin MO, Leong S (2009) Providing Parents with Online Privacy Information: Approaches in the US and the UK. Journal of Consumer Affairs 43(3):474–494.

Sutanto J, Palme E, Tan CH, Phang CW (2013) Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. MIS Quarterly 37(4):1141–1164.

Turner EC, Dasgupta S (2003) Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals. Information Systems Management 20(1):8–18.

US Federal Department of Health Education and Welfare (1973) Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Chapter III. Safeguards for Privacy. Retrieved (April 24, 2015), https://epic.org/privacy/hew1973report/c3.htm . Archived at: http://www.webcitation.org/6Y1gDPqTf.

Vail MW, Earp JB, Antón AI (2008) An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies. IEEE Transactions on Engineering Management 55(3):442–454.

Ward JH (1963) Hierarchical Grouping to Optimize an Objective Function. Journal of the American Statistical Association 58(301):236–244.

Wisniewski PJ, Knijnenburg BP, Lipford HR (2017) Making Privacy Personal: Profiling Social Network Users to Inform Privacy Education and Nudging. International Journal of Human-Computer Studies 98:95–108.

Woodruff A, Pihur V, Consolvo S, Schmidt L, Brandimarte L, Acquisti A (2014) Would a Privacy Fundamentalist Sell Their DNA for $1000...If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences. Symposium on Usable Privacy and Security. (USENIX Association, Menlo Park, CA, USA).

Xu H, Dinev T, Smith HJ, Hart PJ (2011) Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems 12(12):798–824.

Zhu H, Ou CXJ, van den Heuvel WJAM, Liu H (2017) Privacy Calculus and its Utility for Personalization Services in E-Commerce: An Analysis of Consumer Decision-Making. Information & Management 54(4):427–437.

7.7 Appendix

Table 26. Results of scenario sensitivity analysis with number of respondents (N), mean (M) and standard deviation (SD) values for information sensitivity and perceived privacy ratings (1=low, 7=high) obtained in the survey. N/A indicates scenarios eliminated during the pretest.

Scenario	Brief description	N	Information sensitivity M (SD)	Perceived privacy M (SD)
Bookstore App	An app to purchase books online.	N/A	N/A	N/A
Calculator App	An app that supports the user to solve simple arithmetic problems.	54	2.40 (1.78)	5.89 (1.40)
Calendar App	An app to enter appointments in a calendar.	N/A	N/A	N/A
Finance App	An app to access a bank account and make financial transactions.	44	6.09 (1.63)	2.86 (1.96)
Health App	An app that supports the user to correctly take medication.	57	5.80 (1.67)	3.02 (1.69)
Holiday App	An app to book holidays.	57	5.18 (1.68)	3.09 (1.49)
Jogging App	An app to track jogging activities via GPS.	52	5.24 (1.77)	3.13 (1.87)
Messenger App	An app to write and receive short messages with other users.	55	5.43 (1.70)	3.11 (1.50)
Music Streaming App	An app to access a large number of music tracks and stream them to the mobile device.	50	4.05 (1.72)	3.95 (1.60)
Navigation App	An app to help the user navigating while driving a car.	44	5.19 (1.79)	3.47 (1.63)
News App	An app to receive the latest news.	59	3.89 (2.03)	4.60 (1.60)
Photo App	An app to store and edit photos on the user's device.	N/A	N/A	N/A
Public Transport App	An app to receive information on public transport services.	NA	N/A	N/A
Smart Home App	An app to operate all connected smart home devices, for example, heating, lights, cameras, with the mobile device.	N/A	N/A	N/A
Speech Recognition App	An app to operate the device via speech.	57	4.92 (1.74)	3.73 (1.60)
Taxi App	An app to call a taxi to the device's current position.	N/A	N/A	N/A
Water Level App	An app that enables the user to use the device as a tool to measure the water level of objects in the physical world.	51	2.44 (1.84)	5.75 (1.69)
Weather App	An app to receive weather forecasts based on the device's GPS data.	N/A	N/A	N/A

Table 27. Survey instrument of the prestudy and the privacy information needs survey, with the German questions used in the survey and English translations.

Perceived privacy (PP)	
PP1	Ich bin der Meinung, dass ich ausreichend Privatsphäre habe, wenn ich eine solche Smartphone App nutze.
	I feel I have enough privacy when I use such an app.
PP2	Ich fühle mich wohl mit dem Maß an Privatsphäre, das ich habe, wenn ich eine solche Smartphone App benutze.
	I am comfortable with the amount of privacy I have when I use such an app.
PP3	Ich denke meine Privatsphäre bleibt gewahrt, wenn ich eine solche Smartphone App nutze.
	I think my privacy is preserved when I use such an app.
Information sensitivity (IS)	
IS1	Bei einer solchen Smartphone App fühle ich mich nicht wohl bei der Angabe der geforderten Informationen.
	I do not feel comfortable with the type of information such an app requests from me.
IS2	Bei einer solchen Smartphone App finde ich, dass sehr persönliche Informationen über mich gesammelt werden.
	I feel that such an app gathers highly personal information about me.
IS3	Die Informationen, die ich einer solchen Smartphone App zur Verfügung stelle, finde ich schützenswert.
	The information I provide to such an app is very sensitive to me.
Global information privacy concern (GIPC)	
GIPC1	Im Vergleich zu anderen Personen bin ich sensibel in Bezug darauf wie Unternehmen mit meinen Daten umgehen.
	Compared to others, I am more sensitive about the way online companies handle my personal information.
GIPC2	Für mich ist es sehr wichtig, dass meine Privatsphäre nicht durch Unternehmen verletzt wird.
	To me, it is the most important thing to keep my privacy intact from online companies.
GIPC3	Ich sorge mich über aktuelle Bedrohungen für meine persönliche Privatsphäre.
	I am concerned about threats to my personal privacy today.
Information seeking intention (ISI)	
ISI1	Ich plane in Zukunft mehr Informationen über Datenerhebung und -verarbeitung von App-Anbietern einzuholen.
	I plan to seek more information about data collection and processing of app providers in the future.
ISI2	Ich beabsichtige mehr über Datenerhebung und -verarbeitung von App-Anbietern herauszufinden.
	I intend to find out more about data collection and processing of app providers.
ISI3	In Zukunft werde ich versuchen so viele Informationen wie möglich über Datenerhebung und -verarbeitung von App-Anbietern einzuholen.
	In the future, I will try to seek as much information as I can about data collection and processing of app providers.

Information privacy information needs	
Main question	Bitte geben Sie für die Aspekte jeweils an, wie wichtig es für Sie ist über diese informiert zu werden, wenn Sie die beschriebene Smartphone-App nutzen möchten.
	If you would use such an app, how important would it be for you to be informed about the following aspects?
Information sensors	
Environment	Welche Datenquellen (z. B. Kamera, Mikrofon oder Bluetooth) eingesetzt werden, um Daten aus der Umgebung des Geräts zu erheben.
	Which data sources, for example, camera, microphone, or bluetooth, will be used to collect data from the device environment.
Location	Welche Datenquellen (z. B. GPS) eingesetzt werden, um Standortdaten des Geräts zu erheben.
	Which data sources, for example, GPS, will be used to collect location data.
Fingerprint	Ob der Fingerabdruck des Nutzers / der Nutzerin mithilfe eines im Gerät integrierten Fingerabdruckscanners erhoben wird.
	Whether the user's fingerprint will be acquired through use of an integrated fingerprint scanner in the device.
Software use	Welche Datenquellen (z. B. Cookies, Tracking- oder Werbe-Software) eingesetzt werden, um Daten über die Appnutzung zu erheben.
	Which data sources, for example, cookies, adware, or tracking software, will be used to collect data on the use of the app.
Information collection	
Financial identifier	Ob Finanzidentifikationsdaten erhoben werden (z. B. IBAN oder Kreditkartennummer).
	Whether financial identification data will be collected, for example, IBAN or credit card number.
Government identifier	Ob staatliche Identifikationsdaten erhoben werden (z. B. Sozialversicherungsnummer).
	Whether governmental identification data will be collected, for example, social security number.
Real name	Ob der echte Name des Nutzers / der Nutzerin erhoben wird.
	Whether the user's real name will be saved.
Financial data	Ob Daten über die Finanzen des Nutzers / der Nutzerin erhoben werden (z. B. Kontostand).
	Whether data about the user's financial status will be collected, for example, account balance.
System interaction	Ob Daten, die durch Interaktionen des Nutzers / der Nutzerin mit der Smartphone-App entstehen, erhoben werden (z. B. Suchanfragen oder Accountaktivitäten).
	Whether data generated through user interactions with the smartphone app, for example, search queries or account activities, will be collected.
Purchases	Ob Daten über Einkäufe, die über die Smartphone-App getätigt werden, erhoben werden.
	Whether data is being collected about purchases made via the smartphone app.
Health	Ob gesundheitsbezogene Daten über den Nutzer / die Nutzerin erhoben werden.
	Whether data about the user's health will be collected.

Affiliation	Ob Daten über die Zugehörigkeit des Nutzers / der Nutzerin zu einer Gemeinschaft (z. B. Religionen, politische Parteien) erhoben werden.
	Whether data about the user's affiliation to communities, for example, religions, political party, will be collected.
Preferences	Ob Daten über die Vorlieben und Abneigungen des Nutzers / der Nutzerin erhoben werden (z. B. Lieblingsfarbe).
	Whether data about the user's likes and dislikes will be collected, for example, favorite color.
Client device	Ob Daten über das Gerät des Nutzers / der Nutzerin erhoben werden (z. B. IP-Adresse, Betriebssystem).
	Whether data about the user's device, for example, IP address, operating system, will be collected.
Information handling	
Retention	Welche Verfahren zur Datenaufbewahrung eingesetzt werden (z. B. wie lange Daten aufbewahrt werden).
	How long data is kept.
Security	Welche Sicherheitsmaßnahmen zum Schutz der Daten eingesetzt werden.
	Which security measures are used to protect the data.
Sharing	An wen Daten übertragen werden.
	To whom data is transferred.
Storage	Wo Daten gespeichert werden.
	Where data is stored.
Privacy controls	
Access log	Inwiefern Nutzer/-innen nachverfolgen können, wer auf Daten zugegriffen hat.
	How users can inspect who accessed their data.
Breach notifications	Wie Nutzer-/innen über Datenschutzverletzungen informiert werden.
	How users will be informed about information privacy violations.
Practice change governance	Wie sich Änderungen von Datenerhebung und -verarbeitung auf bereits erhobene Daten auswirken.
	How changes to data collection and processing practices will affect data that was already collected.
Practice change notification	Wie Nutzer/-innen informiert werden, wenn Datenerhebung oder -verarbeitung geändert wird.
	How users will be informed about changes of data collection and processing practices.
Consent management	Welche Einverständniserklärungen ein Nutzer / eine Nutzerin gegeben hat und wie er / sie diese widerrufen kann.
	Which consents users have provided and how they can withdraw them.
Downstream propagation	Wie Daten bei Bedarf (insbesondere bei Korrekturen und Löschungen durch Nutzer/-innen) auch bei Dritten, an die die Daten übermittelt wurden, aktualisiert werden.
	How data updates, especially, in the case of correction and deletion by users, will be communicated to third parties to which the data has been transmitted.
Secondary use consent	Wie Einverständniserklärungen von Nutzern / Nutzerinnen eingeholt werden, wenn bereits gesammelte Daten für einen neuen Zweck genutzt werden sollen.
	How consent is obtained if data will be used for other purposes.

User access	Inwiefern Nutzer/-innen auf über sie erhobene Informationen zugreifen können.
	How users can access their collected data.
Automated practice monitoring	Ob Datenerhebung und -verarbeitung des Anbieters automatisiert (z. B. durch Software) überwacht wird.
	Whether data collection and processing will be monitored automatically, for example, with software.
Third-party practice monitoring	Ob Datenerhebung und -verarbeitung des Anbieters durch eine unabhängige Drittpartei überwacht wird.
	Whether data collection and processing of the provider will be monitored by an independent third-party.
Practice self-monitoring	Ob Datenerhebung und -verarbeitung des Anbieters durch den Anbieter selbst überwacht wird.
	Whether data collection and processing of the provider will be monitored by the provider itself.
App descriptions	
Finance app	Eine solche App ermöglicht es Ihnen von überall auf ihr Konto bei ihrer Bank zuzugreifen und Finanztransaktionen durchzuführen (z. B., Kontostand abfragen, Überweisungen durchführen, Daueraufträge verwalten).
	Such an app allows you to access your bank account from anywhere and carry out financial transactions, for example, query account balance, carry out bank transfers, manage standing orders.
Music streaming app	Eine solche App ermöglicht es Ihnen eine große Auswahl an Musiktiteln auf Ihrem Smartphone abzuspielen. Dabei werden die erforderlichen Daten während des Abspielens aus dem Internet geladen. Außerdem haben Sie die Möglichkeit Ihre Lieblingstitel in Listen zu verwalten.
	Such an app allows you to play a wide range of music tracks on your smartphone. The required data is downloaded from the Internet during playback. You can also manage your favorite songs in lists.
Navigation app	Eine solche App unterstützt Sie bei der Navigation während des Autofahrens. Nachdem Sie eine Zieladresse eingegeben haben, ermittelt die App den besten Weg und navigiert Sie ans Ziel.
	Such an app will help you to navigate while driving. The app determines the best route and navigates you to your destination.
Calculator app	Eine solche App ermöglicht es Ihnen auf Ihrem Smartphone einfache Rechenaufgaben zu lösen. Dabei stehen Ihnen die üblichen Eingabemöglichkeiten, die auch auf einem Taschenrechner zu finden sind, zur Verfügung (z. B. Grundrechenarten, Potenzen, Sinus, Logarithmus etc.).
	Such an app allows you to solve simple computing tasks on your smartphone. Basic input possibilities, which can also be found on a pocket calculator, are available to you, for example, basic calculus, exponentiation, sinus, or logarithm.

Table 28. Factor correlation matrix.

	SEN	**ICO**	**CCO**	**IHD**	**PCT**
Information sensors (SEN)	1				
Identifier collection (ICO)	.529	1			
Consumer data collection (CCO)	.519	.496	1		
Information handling (IHD)	.620	.456	.430	1	
Privacy controls (PCT)	.637	.569	.574	.713	1

Table 29. Mapping of privacy information needs included in the privacy information needs survey to their sources in extant literature. Three privacy information needs (Fingerprint, Practice change government, and Consent management) were added based on participant feedback in the pilot studies and are not mapped to extant literature.

Privacy information need	**Source**													**Brief description**
	(Culnan 2000)	(Liu and Arnett 2002)	(Milne and Culnan 2002)	(Langenderfer and Cook 2004)	(Faja and Trimi 2006)	(LaRose and Rifon 2006)	(Pollach 2006)	(Schwaig et al. 2006)	(Ciocchetti 2007)	(Stanaland et al. 2009)	(H. Xu et al. 2011)	(Cottrill 2011)	(Desai et al. 2012)	
Information sensors (SEN)														
Environment												■		Sensors for user environment (eg, camera)
Location											■	■		Location sensors
Fingerprint														Fingerprint scanners
Software use	■	■	■	■		■	■	■	■	■			■	Trackers of system use (eg, web beacons)
Identifier collection (ICO)														
Financial identifier	■	■	■		■	■							■	Financial identifier (eg, bank account number)
Government identifier	■	■	■	■	■	■			■				■	Governmental identifier (eg, social security number)
Real name	■	■	■	■	■	■			■			■		Consumers' real name
Financial data		■		■	■	■			■			■		Data on consumers' finances
Consumer data collection (CCO)														
System interaction							■		■		■			Consumer system interactions
Purchases				■			■		■					Purchases conducted
Health				■		■			■		■	■		Health-related data
Affiliation						■			■					Affiliations with groups (eg, religious)
Preferences	■	■		■	■	■	■		■			■		Consumers' likes and dislikes
Client device		■				■			■	■	■	■		Details on client device
Information handling (IHD)														
Retention										■		■	■	Information retention practices
Security	■	■	■	■	■	■		■	■	■	■	■	■	Information security measures

Sharing	■	■	■	■	■	■	■	■	■	■	■	■	■	Information sharing practices
Storage		■			■			■	■				■	Information storage practices
Privacy controls (PCT)														
Access log									■					Retrieval of data access logs
Breach notification						■			■					Notifications on privacy breaches
Practice change governance														Effects of practice changes on already collected information
Practice change notification							■	■	■					Notifications on practice changes
Consent management														Management of given consents
Downstream propagation													■	Propagation on information updates to data recipients
Secondary use consent	■	■							■				■	Consent elicitation prior to secondary uses of information
Consumer access	■	■	■	■		■	■	■	■	■	■	■	■	Consumers’ permissions to access information about them
Automated practice monitoring			■											Automated monitoring of practices
Third-party practice monitoring		■	■			■	■				■		■	Practice monitoring by third party
Practice self-monitoring							■							Practice monitoring by provider

8 Complete List of References

Abiteboul S, André B, Kaplan D (2015) Managing Your Digital Life. *Communications of the ACM* 58(5):32–35.

Abraham C, Nishihara E, Akiyama M (2011) Transforming Healthcare with Information Technology in Japan: A Review of Policy, People, and Progress. *International Journal of Medical Informatics* 80(3):157–170.

Abroms LC, Padmanabhan N, Thaweethai L, Phillips T (2011) iPhone Apps for Smoking Cessation: A Content Analysis. *American Journal of Preventive Medicine* 40(3):279–285.

Ackerman MS, Cranor LF, Reagle J (1999) Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. *1st ACM Conference on Electronic Commerce*. (ACM, Denver, CO, USA), 1–8.

Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and Human Behavior in the Age of Information. *Science* 347(6221):509–514.

Adams A, Sasse MA (1999) Privacy Issues in Ubiquitous Multimedia Environments: Wake Sleeping Dogs or Let Them Lie. *Proceedings of Interact '99*. (IOS Press, Edinburgh, Scotland), 214–221.

Agaku IT, Adisa AO, Ayo-Yusuf OA, Connolly GN (2014) Concern About Security and Privacy, and Perceived Control over Collection and Use of Health Information are Related to Withholding of Health Information from Healthcare Providers. *Journal of the American Medical Informatics Association* 21(2):374–378.

Ahern DK, Woods SS, Lightowler MC, Finley SW, Houston TK (2011) Promise of and Potential for Patient-Facing Technologies to Enable Meaningful Use. *American Journal of Preventive Medicine* 40(5 Suppl 2):162–172.

Almatarneh A (2011) Privacy Implications for Information and Communications Technology (ICT): The Case of the Jordanian E-Government. *Journal of International Commercial Law & Technology* 6(3):151–164.

Anderson CL, Agarwal R (2011) The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. *Information Systems Research* 22(3):469–490.

android-market-api (2014) android-market-api. Retrieved (February 14, 2014), http://code.google.com/p/android-market-api . Archived at: http://www.webcitation.org/6NNh225JS.

Anthes G (2012) HTML5 Leads a Web Revolution. *Communications of the ACM* 55(7):16–17.

Anthonysamy P, Greenwood P, Rashid A (2013) Social Networking Privacy: Understanding the Disconnect from Policy to Controls. *IEEE Computer* 46(6):60–67.

Antón AI, Bertino E, Li N, Yu T (2007) A Roadmap for Comprehensive Online Privacy Policy Management. *Communications of the ACM* 50(7):109–116.

Antón AI, Earp JB, Vail MW, Jain N, Gheen CM, Frink JM (2007) HIPAA's Effect on Web Site Privacy Policies. *IEEE Security & Privacy* 5(1):45–52.

Antón AI, Earp JB, Young JD (2010) How Internet Users' Privacy Concerns Have Evolved Since 2002. *IEEE Security & Privacy* 8(1):21–27.

Appari A, Johnson ME (2010) Information Security and Privacy in Healthcare: Current State of Research. *International Journal of Internet and Enterprise Management* 6(4):279–314.

Appelbaum PS (2002) Privacy in Psychiatric Treatment: Threats and Responses. *The American Journal of Psychiatry* 159(11):1809–1818.

Apple (2014a) Apple iTunes App Store. Retrieved (February 14, 2014), https://itunes.apple.com/us/genre/ios/id36?mt=8.

Apple (2014b) Health. Retrieved (July 7, 2014), http://www.apple.com/ios/ios8/health . Archived at: http://www.webcitation.org/6QtK0lqTv.

Ashrafi N, Kuilboer JP (2005) Online Privacy Policies: An Empirical Perspective on Self-Regulatory Practices. *Journal of Electronic Commerce in Organizations* 3(4):61–74.

Avancha S, Baxi A, Kotz D (2012) Privacy in Mobile Technology for Personal Healthcare. *ACM Computing Surveys* 45(1):3:1–3:54.

Awad NF, Krishnan M (2006) The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly* 30(1):13–28.

Bacharach SB (1989) Organizational Theories: Some Criteria for Evaluation. *Academy of Management Review* 14(4):496–515.

Bal G, Rannenberg K, Hong JI (2015) Styx: Privacy Risk Communication for the Android Smartphone Platform Based on Apps' Data-Access Behavior Patterns. *Computers & Security* 53(1):187–202.

Balebako R, Jung J, Lu W, Cranor LF, Nguyen C (2013) "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. *Proceedings of the Ninth Symposium on Usable Privacy and Security*. SOUPS '13. (ACM, New York, NY, USA), 12:1–12:11.

Bansal G, Zahedi FM, Gefen D (2010) The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online. *Decision Support Systems* 49(2):138–150.

Bansal G, Zahedi FM, Gefen D (2015) The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern. *European Journal of Information Systems* 24(6):624–644.

Barak A, Klein B, Proudfoot JG (2009) Defining Internet-Supported Therapeutic Interventions. *Annals of Behavioral Medicine* 38(1):4–17.

Baraniuk RG (2011) More Is Less: Signal Processing and the Data Deluge. *Science* 331(6018):717–719.

Barrows RC, Clayton PD (1996) Privacy, Confidentiality, and Electronic Medical Records. *Journal of the American Medical Informatics Associations* 3(2):139–148.

Baskerville RL, Kaul M, Storey VC (2015) Genres of Inquiry in Design-Science Research: Justification and Evaluation of Knowledge Production. *MIS Quarterly* 39(3):541–564.

de Beaufort Wijnholds H, Little MW (2001) Regulatory Issues for Global E-Tailers: Marketing Implications. *Academy of Marketing Science Review* 2001(1):1–12.

Bélanger F, Crossler RE (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly* 35(4):1017–1041.

Bélanger F, Crossler RE, Hiller JS, Park JM, Hsiao MS (2013) POCKET: A Tool for Protecting Children's Privacy Online. *Decision Support Systems* 54(2):1161–1173.

Beldad AD, De Jong M, Steehouder MF (2009) When the Bureaucrat Promises to Safeguard your Online Privacy: Dissecting the Contents of Privacy Statements on Dutch Municipal Websites. *Government Information Quarterly* 26(4):559–566.

Belkin NJ, Oddy RN, Brooks HM (1982) ASK for Information Retrieval: Part I. Background and Theory. *Journal of Documentation* 38(2):61–71.

Benassi P (1999) TRUSTe: An Online Privacy Seal Program. *Communications of the ACM* 42(2):56–59.

Bender LJ, Yue KRY, To JM, Deacken L, Jadad RA (2013) A Lot of Action, But Not in the Right Direction: Systematic Review and Content Analysis of Smartphone Applications for the Prevention, Detection, and Management of Cancer. *Journal of Medical Internet Research* 15(12):e287.

Berendt B, Günther O, Spiekermann S (2005) Privacy in e-Commerce: Stated Preferences vs. Actual Behavior. *Communications of the ACM* 48(4):101–106.

Berger CR, Calabrese RJ (1975) Some Explorations in Initial Interaction and Beyond: Toward a Developmental Theory of Interpersonal Communication. *Human Communication Research* 1(2):99–112.

Bierbrier R, Lo V, Wu CR (2014) Evaluation of the Accuracy of Smartphone Medical Calculation Apps. *Journal of Medical Internet Research* 16(2):e32.

Blechman EA, Raich P, Raghupathi W, Blass S (2012) Strategic Value of an Unbound, Interoperable PHR Platform for Rights-Managed Care Coordination. *Communications of the Association for Information Systems* 30(1):Article 6.

Blobel B (2011) Ontology Driven Health Information Systems Architectures Enable pHealth for Empowered Patients. *International Journal of Medical Informatics* 80(2):e17–e25.

Blondel VD, Guillaume JL, Lambiotte R, Lefebvre E (2008) Fast Unfolding of Communities in Large Networks. *Journal of Statistical Mechanics: Theory and Experiment* 2008(10):P10008.

Braun V, Clarke V (2006) Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3(2):77–101.

Breton ER, Fuemmeler BF, Abroms LC (2011) Weight Loss-There is an App for That! But does it Adhere to Evidence-Informed Practices? *Translational Behavioral Medicine* 1(4):523–529.

Brüggemann T, Hansen J, Dehling T, Sunyaev A (2016) An Information Privacy Risk Index for mHealth Apps. Schiffner S, Serna J, Ikonomou D, Rannenberg K, eds. *Proceedings of the 4th Annual Privacy Forum*. (Springer International Publishing, Frankfurt (Main), Germany), 190–201.

Bühler K (2011) *Theory of Language: The Representational Function of Language* (John Benjamins Publishing Co, Amsterdam / Philadelphia).

Buitelaar JC (2017) Post-Mortem Privacy and Informational Self-Determination. *Ethics and Information Technology* 19(2):129–142.

Bulgurcu B, Cavusoglu H, Benbasat I (2010) Understanding Emergence and Outcomes of Information Privacy Concerns: A Case of Facebook. *ICIS 2010 Proceedings*. (St. Louis, MO, USA).

Cai X, Gantz W, Schwartz N, Wang X (2003) Children's Website Adherence to the FTC's Online Privacy Protection Rule. *Journal of Applied Communication Research* 31(4):346–362.

California Business and Professions Code (2004) California Online Privacy Protection Act of 2003. *Business and Professions Code Sections 22575-22579*. Retrieved (May 14, 2014), http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579. Archived at: http://www.webcitation.org/6Rv9DRvtC.

Caligtan CA, Dykes PC (2011) Electronic Health Records and Personal Health Records. *Seminars in Oncology Nursing* 27(3):218–228.

Calvillo J, Román I, Roa LM (2013) Empowering Citizens with Access Control Mechanisms to their Personal Health Resources. *International Journal of Medical Informatics* 82(1):58–72.

Campbell JL (2007) Why Would Corporations Behave in Socially Responsible Ways? An Institutional Theory of Corporate Social Responsibility. *Academy of Management Review* 32(3):946–967.

Carrión Señor I, Aleman JLF, Toval A (2012) Personal Health Records: New Means to Safely Handle Health Data? *IEEE Computer* 45(11):27–33.

Carrión Señor I, Fernández-Alemán JL, Toval A (2012) Are Personal Health Records Safe? A Review of Free Web-Accessible Personal Health Record Privacy Policies. *Journal of Medical Internet Research* 14(4):e114.

Cate FH (2010) The Limits of Notice and Choice. *IEEE Security & Privacy* 8(2):59–62.

Cha J (2011) Information Privacy: A Comprehensive Analysis of Information Request and Privacy Policies of Most-Visited Web Sites. *Asian Journal of Communication* 21(6):613–631.

Chan ATS, Cao J, Chan H, Young G (2001) A Web-Enabled Framework for Smart Card Applications in Health Services. *Communications of the ACM* 44(9):76–82.

Chen C, Haddad D, Selsky J, Hoffman JE, Kravitz RL, Estrin DE, Sim I (2012) Making Sense of Mobile Health Data: An Open Architecture to Improve Individual- and Population-Level Health. *Journal of Medical Internet Research* 14(4):e112.

Chen W, Hirschheim R (2004) A Paradigmatic and Methodological Examination of Information Systems Research from 1991 to 2001. *Information Systems Journal* 14(3):197–235.

Chin E, Felt AP, Greenwood K, Wagner D (2011) Analyzing Inter-Application Communication in Android. *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*. MobiSys '11. (ACM, Washington, DC, USA), 239–252.

Choi BCF, Kim SS, Jiang ZJ (2016) Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior. *Journal of Management Information Systems* 33(3):904–933.

Chomutare T, Fernandez-Luque L, Arsand E, Hartvigsen G (2011) Features of Mobile Diabetes Applications: Review of the Literature and Analysis of Current Applications Compared Against Evidence-Based Guidelines. *Journal of Medical Internet Research* 13(3):e65.

Ciocchetti CA (2007) E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors. *American Business Law Journal* 44(1):55–126.

Clarke R (1994) The Digital Persona and its Application to Data Surveillance. *The Information Society* 10(2):77–92.

Clarke R (1999) Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM* 42(2):60–67.

Clarke R (2006a) A Pilot Study of the Effectiveness of Privacy Policy Statements. *BLED 2006 Proceedings*. (AIS, Bled, Slovenia).

Clarke R (2006b) What's "Privacy"? Retrieved (September 17, 2017), http://www.rogerclarke.com/DV/Privacy.html . Archived at: http://www.webcitation.org/6tXpcLq7f.

Collins F (2012) The Real Promise of Mobile Health Apps. *Scientific American* 307(1).

Conger S, Loch KD (2000) Invitation to a Public Debate on Ethical Computer Use. *SIGMIS Database* 32(1):58–69.

Conger S, Pratt JH, Loch KD (2013) Personal Information Privacy and Emerging Technologies. *Information Systems Journal* 23(5):401–417.

Corley KG, Gioia DA (2011) Building Theory about Theory Building: What Constitutes a Theoretical Contribution? *Academy of Management Review* 36(1):12–32.

Cosijn E, Ingwersen P (2000) Dimensions of Relevance. *Information Processing & Management* 36(4):533–550.

Cottrill CD (2011) Location Privacy: Who Protects? *Journal of the Urban & Regional Information Systems Association* 23(2):49–59.

Cowan N (2014) Working Memory Underpins Cognitive Development, Learning, and Education. *Educational Psychology Review* 26(2):197–223.

Cranor L, Dobbs B, Egelman S, Hogben G, Humphrey J, Langheinrich M, Marchiori M, et al. (2006) The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. Retrieved (March 3, 2017), http://www.w3.org/TR/2006/NOTE-P3P11-20061113.

Cranor LF (2012) Necessary but not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. *Journal on Telecommunications and High Technology Law* 10:273–307.

Cranor LF, Reagle J, Ackerman MS (1999) Beyond Concern: Understanding Net Users' Attitudes about Online Privacy. *AT&T Labs-Research Technical Report, TR 99.4.3*. (MIT Press, Cambridge, MA, USA).

Culnan MJ (1993) "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. *MIS Quarterly* 17(3):341–363.

Culnan MJ (2000) Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing* 19(1):20–26.

Culnan MJ, Armstrong PK (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10(1):104–115.

Culnan MJ, Williams CC (2009) How Ethics can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches. *MIS Quarterly* 33(4):673–687.

DeCew JW (2004) Privacy and Policy for Genetic Research. *Ethics and Information Technology* 6(1):5–14.

Dehling T, Sunyaev A (2012a) Information Security of Patient-Centred Services Utilising the German Nationwide Health Information Technology Infrastructure. *3rd USENIX Workshop on Health Security and Privacy*. (USENIX, Bellevue, WA, USA).

Dehling T, Sunyaev A (2012b) Architecture and Design of a Patient-Friendly eHealth Web Application: Patient Information Leaflets and Supplementary Services. *18th Americas Conference on Information Systems*. (AIS, Seattle, WA, USA).

Dehling T, Sunyaev A (2013) Improved Medication Compliance through Health IT: Design and Mixed Methods Evaluation of the ePill Application. *34th International Conference on Information Systems*. (AIS, Milano, Italy).

Dehling T, Sunyaev A (2014a) Information Security and Privacy of Patient-Centered Health IT Services: What needs to be done? *47th Hawaii International Conference on System Sciences*. (IEEE, Big Island, HI, USA), 2984–2993.

Dehling T, Sunyaev A (2014b) Secure Provision of Patient-Centered Health Information Technology Services in Public Networks—Leveraging Security and Privacy Features Provided by the German Nationwide Health Information Technology Infrastructure. *Electronic Markets* 24(2):89–99.

Delgado M (2011) The Evolution of Health Care IT: Are Current U.S. Privacy Policies Ready for the Clouds? *2011 IEEE World Congress on Services*. (Washington, DC USA), 371–378.

Desai M, Lodge D, Gates M, Wolvin M, Louer G (2012) The FTC Privacy Report: What the Report Means and How You can get Ahead of Enforcement Trends by Implementing Best Practices Now. *International Journal of Mobile Marketing* 7(2):26–36.

Dhopeshwarkar RV, Kern LM, O'Donnell HC, Edwards AM, Kaushal R (2012) Health Care Consumers' Preferences Around Health Information Exchange. *The Annals of Family Medicine* 10(5):428–434.

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

Dinev T, Hart P (2006b) Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce* 10(2):7–29.

Dinev T, Xu H, Smith JH, Hart P (2013) Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts. *European Journal of Information Systems* 22(3):295–316.

Donaldson T, Dunfee TW (1994) Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory. *The Academy of Management Review* 19(2):252–284.

Donaldson T, Dunfee TW (1995) Integrative Social Contracts Theory: A Communitarian Conception of Economic Ethics. *Economics and Philosophy* 11(1):85–112.

Donker T, Petrie K, Proudfoot J, Clarke J, Birch MR, Christensen H (2013) Smartphones for Smarter Delivery of Mental Health Programs: A Systematic Review. *Journal of Medical Internet Research* 15(11):e247.

Dorr D, Bonner LM, Cohen AN, Shoai RS, Perrin R, Chaney E, Young AS (2007) Informatics Systems to Promote Improved Care for Chronic Illness: A Literature Review. *Journal of the American Medical Informatics Association* 14(2):156–163.

Dubin R (1978) *Theory Building* (Collier Macmillan Publishers, London, UK).

Dunfee TW (2006) A Critical Perspective of Integrative Social Contracts Theory: Recurring Criticisms and Next Generation Research Topics. *Journal of Business Ethics* 68(3):303–328.

Dünnebeil S, Köbler F, Koene P, Leimeister JM, Krcmar H (2011) Encrypted NFC Emergency Tags Based on the German Telematics Infrastructure. *Proceedings of the 2011 Third International Workshop on Near Field Communication*. (IEEE, Hagenberg, Austria), 50–55.

Dünnebeil S, Sunyaev A, Blohm I, Leimeister JM, Krcmar H (2012) Determinants of Physicians' Technology Acceptance for e-Health in Ambulatory Care. *International Journal of Medical Informatics* 81(11):746–760.

Earp JB, Antón AI, Aiman-Smith L, Stufflebeam WH (2005) Examining Internet Privacy Policies Within the Context of User Privacy Values. *IEEE Transactions on Engineering Management* 52(2):227–237.

Egele M, Kruegel C, Kirda E, Vigna G (2011) PiOS: Detecting Privacy Leaks in iOS Applications. *Proceedings of the Network and Distributed System Security Symposium (NDSS 2011)*. (The Internet Society, San Diego, CA, USA).

Eggert A, Helm S (2003) Exploring the Impact of Relationship Transparency on Business Relationships: A Cross-Sectional Study among Purchasing Managers in Germany. *Industrial Marketing Management* 32(2):101–108.

Ekonomou E, Fan L, Buchanan W, Thüemmler C (2011) An Integrated Cloud-Based Healthcare Infrastructure. *Proceedings of the 3rd IEEE International Conference on Cloud Computing Technology and Science (IEEE CloudCom 2011)*. (IEEE, Athens, Greece), 532–536.

Enck W, Octeau D, McDaniel P, Chaudhuri S (2011) A Study of Android Application Security. *Proceedings of the 20th USENIX Conference on Security*. SEC'11. (USENIX Association, Berkeley, CA, USA), 21–21.

Estrin D, Sim I (2010) Open mHealth Architecture: An Engine for Health Care Innovation. *Science* 330(6005):759–760.

European Commision (2012) *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)* (Brussels, Belgium).

Faja S, Trimi S (2006) Influence of the Web Vendor's Interventions on Privacy-Related Behaviors in e-Commerce. *Communications of the Association for Information Systems* 17(1):27.

Fan L, Buchanan W, Thümmler C, Lo O, Khedim A, Uthmani O, Lawson A, Bell D (2011) DACAR Platform for eHealth Services Cloud. *Proceedings of the 2011 IEEE 4th International Conference on Cloud Computing*. (IEEE, Washington, DC, USA), 219–226.

Fang Y (2010) The Death of the Privacy Policy: Effective Privacy Disclosures after In Re Sears. *Berkeley Technology Law Journal* 25(1):671–700.

Faro S, Lecroq T (2012) Twenty Years of Bit-Parallelism in String Matching. Holub J, Watson BW, Žďárek J, eds. *Festschrift for Bořivoj Melichar*. (Prague Stringology Club, Prague, Czech Republic), 72–101.

Federal Trade Commission (2013) *Mobile Privacy Disclosures Building Trust Through Transparency* (Federal Trade Commission).

Fischer-Hübner S, Angulo J, Pulls T (2014) How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used? Hansen M, Hoepman JH, Leenes R, Whitehouse D, eds. *Privacy and Identity Management for Emerging Services and Technologies*. (Springer Berlin Heidelberg), 77–92.

Food and Drug Administration (2013) *Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff* (Food and Drug Administration).

Forkner-Dunn J (2003) Internet-Based Patient Self-Care: The Next Generation of Health Care Delivery. *Journal of Medical Internet Research* 5(2):e8.

Freifeld CC, Chunara R, Mekaru SR, Chan EH, Kass-Hout T, Ayala Iacucci A, Brownstein JS (2010) Participatory Epidemiology: Use of Mobile Phones for Community-Based Health Reporting. *PLOS Medicine* 7(12):e1000376.

Fu K, Blum J (2013) Controlling for Cybersecurity Risks of Medical Device Software. *Communications of the ACM* 56(10):35–37.

Garber L (2012) The Challenges of Securing the Virtualized Environment. *IEEE Computer* 45(1):17–20.

Garrison L, Hastak M, Hogarth JM, Kleimann S, Levy AS (2012) Designing Evidence-Based Disclosures: A Case Study of Financial Privacy Notices. *Journal of Consumer Affairs* 46(2):204–234.

Germonprez M, Hovorka D, Collopy F (2007) A Theory of Tailorable Technology Design. *Journal of the Association for Information Systems* 8(6):351–367.

Girardello A, Michahelles F (2010) Explicit and Implicit Ratings for Mobile Applications. Fähnrich KP, Franczyk B, eds. *Informatik 2010*. LNI. (GI, Leipzig, Germany), 606–612.

Google (2014a) Google Play App Store. Retrieved (February 14, 2014), https://play.google.com/store/apps.

Google (2014b) The Google Fit SDK. Retrieved (July 7, 2014), https://developers.google.com/fit . Archived at: http://www.webcitation.org/6QtJkTpQE.

Goth Gregory (2012) Analyzing Medical Data. *Communications of the ACM* 55(6):13–15.

Goth Greg (2012) Mobile Security Issues Come to the Forefront. *IEEE Internet Computing* 16(3):7–9.

Graber MA, D'Alessandro DM, Johnson-West J (2002) Reading Level of Privacy Policies on Internet Health Web Sites. *The Journal of Family Practice* 51(7):642–645.

Greenaway KE, Chan YE, Crossler RE (2015) Company Information Privacy Orientation: A Conceptual Framework. *Information Systems Journal* 25(6):579–606.

Gregor S, Hevner AR (2013) Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly* 37(2):337–355.

Gregor S, Jones D (2007) The Anatomy of a Design Theory. *Journal of the Association for Information Systems* 8(5):312–335.

Gritzalis DA (1998) Enhancing Security and Improving Interoperability in Healthcare Information Systems. *Medical Informatics* 23(4):309–323.

Guarino N (1997) Understanding, Building and Using Ontologies. *International Journal of Human-Computer Studies* 46(2–3):293–310.

Guarino N, Oberle D, Staab S (2009) What is an Ontology? Studer R, Staab S, eds. *Handbook on Ontologies*. (Springer, Berlin, Germany), 1–17.

Gürses S (2014) Can You Engineer Privacy? *Communications of the ACM* 57(8):20–23.

Hallam C, Zanella G (2017) Online Self-Disclosure: The Privacy Paradox Explained as a Temporally Discounted Balance Between Concerns and Rewards. *Computers in Human Behavior* 68:217–227.

Hann IH, Hui KL, Lee SYT, Png IPL (2007) Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. *Journal of Management Information Systems* 24(2):13–42.

Hanseth O, Lyytinen K (2010) Design Theory for Dynamic Complexity in Information Infrastructures: The Case of Building Internet. *Journal of Information Technology* 25(1):1–19.

Hayton JC, Allen DG, Scarpello V (2004) Factor Retention Decisions in Exploratory Factor Analysis: A Tutorial on Parallel Analysis. *Organizational Research Methods* 7(2):191–205.

Heitkötter H, Majchrzak TA, Kuchen H (2013) Cross-Platform Model-Driven Development of Mobile Applications with md2. *Proceedings of the 28th Annual ACM Symposium on Applied Computing*. SAC '13. (ACM, Coimbra, Portugal), 526–533.

Henson RK, Roberts JK (2006) Use of Exploratory Factor Analysis in Published Research: Common Errors and some Comment on Improved Practice. *Educational and Psychological Measurement* 66(3):393–416.

d'Heureuse N, Huici F, Arumaithurai M, Ahmed M, Papagiannaki K, Niccolini S (2012) What's App?: A Wide-Scale Measurement Study of Smart Phone Markets. *ACM SIGMOBILE. Mobile Computing and Communications Review* 16(2):16–27.

Hirschberg J, Manning CD (2015) Advances in Natural Language Processing. *Science* 349(6245):261–266.

Hjørland B (1997) *Information Seeking and Subject Representation* (Greenwood Press, Westport, CT, USA).

Hoffmann CP, Lutz C, Ranzini G (2016) Privacy Cynicism: A New Approach to the Privacy Paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10(4).

Hong T, McLaughlin ML, Pryor L, Beaudoin CE, Grabowicz P (2005) Internet Privacy Practices of News Media and Implications for Online Journalism. *Journalism Studies* 6(1):15–28.

Hoofnagle CJ, Urban JM (2014) Alan Westin's Privacy Homo Economicus. *Wake Forest Law Review* 49:261–317.

Hooper A, Bunker B, Rapson A, Reynolds A, Vos M (2007) Evaluating Banking Websites Privacy Statements-A New Zealand Perspective on Ensuring Business Confidence. *PACIS 2007 Proceedings*. (AIS, Auckland, New Zealand).

Hooper T, Evans TB (2010) The Value Congruence of Social Networking Services-A New Zealand Assessment of Ethical Information Handling. *The Electronic Journal Information Systems Evaluation* 13(2):121–131.

Hooper T, Vos M (2009) Establishing Business Integrity in an Online Environment. *Online Information Review* 33(2):343–361.

Horvitz E, Mulligan D (2015) Data, Privacy, and the Greater Good. *Science* 349(6245):253–255.

Hossain MA, Dwivedi YK (2014) What Improves Citizens' Privacy Perceptions Toward RFID Technology? A Cross-Country Investigation Using Mixed Method Approach. *International Journal of Information Management* 34(6):711–719.

Howe J (2006) The Rise of Crowdsourcing. *Wired Magazine*. Retrieved (March 9, 2012), http://www.wired.com/wired/archive/14.06/crowds.html.

Hsu CWJ (2006) Privacy Concerns, Privacy Practices and Web Site Categories. *Online Information Review* 30(5):569–586.

Huang HY, Bashir M (2016) Privacy by Region: Evaluation Online Users' Privacy Perceptions by Geographical Region. *Proceedings of the 2016 Future Technologies Conference*. (IEEE, San Francisco, CA, USA), 968–977.

Huckvale K, Car M, Morrison C, Car J (2012) Apps for Asthma Self-Management: A Systematic Assessment of Content and Tools. *BMC Medicine* 10(1):144.

Hufnagel SP (2009) Interoperability. *Military Medicine* 174(5):43–50.

Hultman J, Axelsson B (2007) Towards a Typology of Transparency for Marketing Management Research. *Industrial Marketing Management* 36(5):627–635.

ISO (2016) *ISO/IEC 27000:2016: Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*

Istepanian RSH, Jovanov E, Zhang YT (2004) Guest Editorial Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-Care Connectivity. *IEEE Transactions on Information Technology in Biomedicine* 8(4):405–414.

Jain AK (2010) Data Clustering: 50 Years Beyond K-Means. *Pattern Recognition Letters* 31(8):651–666.

Janson H, Olsson U (2001) A Measure of Agreement for Interval or Nominal Multivariate Observations. *Educational and Psychological Measurement* 61(2):277–289.

Jensen C, Potts C (2004) Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. (ACM, New York, NY, USA), 471–478.

Jensen Carlos, Potts C, Jensen Christian (2005) Privacy Practices of Internet Users: Self-Reports versus Observed Behavior. *International Journal of Human-Computer Studies* 63(1–2):203–227.

Jiang Y, Guo H (2015) Design of Consumer Review Systems and Product Pricing. *Information Systems Research* 26(4):714–730.

Jiang ZJ, Heng CS, Choi BCF (2013) Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research* 24(3):579–595.

John LK, Acquisti, A, Loewenstein G (2011) Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information. *Journal of Consumer Research* 37(5):858–873.

Johnson ME (2009) Data Hemorrhages in the Health-Care Sector. Dingledine R, Golle P, eds. *Financial Cryptography and Data Security*. Lecture Notes in Computer Science. (Springer-Verlag, Berlin, Heidelberg), 71–89.

Johnson-Page GF, Thatcher RS (2001) B2C Data Privacy Policies: Current Trends. *Management Decision* 39(4):262–272.

Jones E, Oliphant T, Peterson P, et al. (2001) SciPy: Open Source Scientific Tools for Python. Retrieved (July 12, 2017), http://www.scipy.org/.

Kahlor LA (2007) An Augmented Risk Information Seeking Model: The Case of Global Warming. *Media Psychology* 10(3):414–435.

Kaletsch A, Sunyaev A (2011) Privacy Engineering: Personal Health Records in Cloud Computing Environments. *32th International Conference on Information Systems*. (AIS, Shanghai, China).

Kalyuga S (2011) Cognitive Load Theory: How Many Types of Load Does It Really Need? *Educational Psychology Review* 23(1):1–19.

Katifori A, Halatsis C, Lepouras G, Vassilakis C, Giannopoulou E (2007) Ontology Visualization Methods—A Survey. *ACM Computing Surveys* 39(4):10:1-10:43.

Kaufmann E, Bernstein A (2007) How Useful Are Natural Language Interfaces to the Semantic Web for Casual End-Users? Aberer K, Choi KS, Noy N, Allemang D, Lee KI, Nixon L, Golbeck J, et al., eds. *The Semantic Web*. Lecture Notes in Computer Science. (Springer Berlin Heidelberg), 281–294.

Kaupins GE, Reed D (2012) New Media Usage and Privacy Policies of Newspaper Websites of the Baltic States. *Current Issues of Business & Law* 7(1):27–45.

Kelley PG, Cesca L, Bresee J, Cranor LF (2010) Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. *SIGCHI Conference on Human Factors in Computing Systems*. (ACM, New York, NY, USA), 1573–1582.

Khalid H, Shihab E, Nagappan M, Hassan A (2015) What Do Mobile App Users Complain About? A Study on Free iOS Apps. *IEEE Software* 32(3):70–77.

Kim S, Yi SH (2010) Is Privacy at Risk when Commercial Websites Target Primary School Children? A Case Study in Korea. *Children & Society* 24(6):449–460.

Klasnja P, Consolvo S, Choudhury T, Beckwith R, Hightower J (2009) Exploring Privacy Concerns about Personal Sensing. Pervasive ’09. (Springer, Nara, Japan), 176–183.

Koops BJ, Newell BC, Timan T, Skorvanek I, Chokrevski T, Galic M (2016) A Typology of Privacy. *University of Pennsylvania Journal of International Law* 38(2):483–575.

Kotz D (2011) A Threat Taxonomy for mHealth Privacy. *3rd International Conference on Communication Systems and Networks*. (IEEE, Bangalore, India).

Krol K, Preibusch S (2015) Effortless Privacy Negotiations. *IEEE Security & Privacy* 13(3):88–91.

Kubis KE (2010) Google Books: Page by Page, Click by Click, Users Are Reading Away Privacy Rights. *Vanderbilt Journal of Entertainment & Technology Law* 13(1):217–254.

Kuechler W, Vaishnavi V (2012) A Framework for Theory Development in Design Science Research: Multiple Perspectives. *Journal of the Association for Information Systems* 13(6):395–423.

Kumar S, Nilsen W, Pavel M, Srivastava M (2013) Mobile Health: Revolutionizing Healthcare Through Transdisciplinary Research. *IEEE Computer* 46(1):28–35.

Kumaraguru P, Cranor LF (2005) *Privacy Indexes: A Survey of Westin’s Studies* (Carnegie Mellon University, Pittsburgh, PA).

Kuzma J (2010) An Examination of Privacy Policies of US Government Senate Websites. *Electronic Government, an International Journal* 7(3):270–280.

Kuzma J (2011) Empirical Study of Privacy Issues among Social Networking Sites. *Journal of International Commercial Law and Technology* 6(2):74–85.

Lämmel R, Pek E (2013) Understanding Privacy Policies. *Empirical Software Engineering* 18(2):310–374.

Lancichinetti A, Fortunato S (2009) Community Detection Algorithms: A Comparative Analysis. *Physical Review E* 80(5):056117.

Landau S (2015) Control Use of Data to Protect Privacy. *Science* 347(6221):504–506.

Landis JR, Koch GG (1977) The Measurement of Observer Agreement for Categorical Data. *Biometrics* 33(1):159–174.

Landry JP, Pardue JH, Johnsten T, Campbell M, Patidar P (2011) A Threat Tree for Health Information Security and Privacy. Sambamurthy V, Tanniru M, eds. *Proceedings of the 17th Americas Conference on Information Systems*. (AIS, Detroit, MI, USA).

Lane ND, Miluzzo E, Lu H, Peebles D, Choudhury T, Campbell AT (2010) A Survey of Mobile Phone Sensing. *IEEE Communications Magazine* 48(9):140–150.

Langenderfer J, Cook DL (2004) Oh, What a Tangled Web we Weave: The State of Privacy Protection in the Information Economy and Recommendations for Governance. *Journal of Business Research* 57(7):734–747.

Lankton NK, McKnight DH, Tripp JF (2017) Facebook Privacy Management Strategies: A Cluster Analysis of User Privacy Behaviors. *Computers in Human Behavior* 76:149–163.

Lansing J, Schneider S, Sunyaev A (2013) Cloud Service Certifications: Measuring Consumers' Preferences for Assurances. *Proceedings of the 27st European Conference on Information Systems (ECIS 2013)*. (Utrecht, Netherlands), paper 181.

LaRose R, Rifon N (2006) Your Privacy is Assured - Of Being Disturbed: Websites With and Without Privacy Seals. *New Media & Society* 8(6):1009–1029.

Laudon KC (1996) Markets and Privacy. *Communications of the ACM* 39(9):92–104.

Laufer RS, Wolfe M (1977) Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues* 33(3):22–42.

Lee BC, Ang L, Dubelaar C (2005) Lemons on the Web: A Signalling Approach to the Problem of Trust in Internet Commerce. *Journal of Economic Psychology* 26(5):607–623.

Lee DH, Im S, Taylor CR (2008) Voluntary Self-Disclosure of Information on the Internet: A Multimethod Study of the Motivations and Consequences of Disclosing Information on Blogs. *Psychology and Marketing* 25(7):692–710.

Lee JM, Rha JY (2016) Personalization–Privacy Paradox and Consumer Conflict with the Use of Location-Based Mobile Commerce. *Computers in Human Behavior* 63:453–462.

Lewis TL, Wyatt JC (2014) mHealth and Mobile Medical Apps: A Framework to Assess Risk and Promote Safer Use. *Journal of Medical Internet Research* 16(9):e210.

Ley P, Florio T (1996) The Use of Readability Formulas in Health Care. *Psychology, Health & Medicine* 1(1):7–28.

Li C, Li DY, Miklau G, Suciu D (2014) A Theory of Pricing Private Data. *ACM Transactions on Database Systems* 39(4):34:1-34:28.

Li Y (2012) Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework. *Decision Support Systems* 54(1):471–481.

Liccardi I, Pato J, Weitzner DJ (2013) Improving Mobile App Selection through Transparency and Better Permission Analysis. *Journal of Privacy and Confidentiality* 5(2):1–55.

van der Linden H, Kalra D, Hasman A, Talmon J (2009) Inter-Organizational Future Proof EHR Systems: A Review of the Security and Privacy Related Issues. *International Journal of Medical Informatics* 78(3):141–160.

Liu C, Arnett KP (2002) Raising a Red Flag on Global WWW Privacy Policies. *The Journal of Computer Information Systems* 43(1):117–127.

Liu C, Zhu Q, Holroyd KA, Seng EK (2011) Status and Trends of Mobile-Health Applications for iOS Devices: A Developer's Perspective. *The Journal of Systems and Software* 84(11):2022–2033.

Lowry PB, Moody G, Vance A, Jensen M, Jenkins J, Wells T (2012) Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues for Online Consumers. *Journal of the American Society for Information Science and Technology* 63(4):755–776.

Lunshof JE, Chadwick R, Vorhaus DB, Church GM (2008) From Genetic Privacy to Open Consent. *Nature Reviews Genetics* 9(5):406–411.

Magi TJ (2010) A Content Analysis of Library Vendor Privacy Policies: Do They Meet Our Standards? *College & Research Libraries* 71(3):254–272.

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

Mandl KD, Kohane IS (2009) No Small Change for the Health Information Economy. *New England Journal of Medicine* 360(13):1278–1281.

Mandl KD, Mandel JC, Murphy SN, Bernstam EV, Ramoni RL, Kreda DA, McCoy JM, Adida B, Kohane IS (2012) The SMART Platform: Early Experience Enabling Substitutable Applications for Electronic Health Records. *Journal of the American Medical Informatics Association* 19(4):597–603.

March ST, Smith GF (1995) Design and Natural Science Research on Information Technology. *Decision Support Systems* 15(4):251–266.

Martin K (2016) Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics* 137(3):551–569.

Martin KD, Borah A, Palmatier RW (2017) Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing* 81(1):36–58.

Martínez-Pérez B, de la Torre-Díez I, López-Coronado M (2013) Mobile Health Applications for the Most Prevalent Conditions by the World Health Organization: Review and Analysis. *Journal of Medical Internet Research* 15(6):e120.

Martínez-Pérez B, de la Torre-Díez I, López-Coronado M, Herreros-González J (2013) Mobile Apps in Cardiology: Review. *JMIR mHealth uHealth* 1(2):e15.

Martínez-Pérez B, de la Torre-Díez I, López-Coronado M, Sainz-De-Abajo B (2014) Comparison of Mobile Apps for the Leading Causes of Death Among Different Income Zones: A Review of the Literature and App Stores. *JMIR mHealth uHealth* 2(1):e1.

Maslow AH (1943) A Theory of Human Motivation. *Psychological Review* 50(4):370–396.

Mason RO (1986) Four Ethical Issues of the Information Age. *MIS Quarterly* 10(1):5–12.

Masuch M (1985) Vicious Circles in Organizations. *Administrative Science Quarterly* 30(1):14–33.

McDonald AM, Cranor LF (2008) The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society* 4(3):540–565.

McDonald AM, Reeder RW, Kelley PG, Cranor LF (2009) A Comparative Study of Online Privacy Policies and Formats Goldberg I, Atallah M, eds. *Lecture Notes in Computer Science* 5672:37–55.

McGrath L (2011) Social Networking Privacy: Important or Not? *Interdisciplinary Journal of Contemporary Research In Business* 3(3):22–28.

McRobb S (2006) Let's Agree to Differ: Varying Interpretations of Online Privacy Policies. *Journal of Information, Communication and Ethics in Society* 4(4):215–228.

McRobb S, Rogerson S (2004) Are they Really Listening?: An Investigation into Published Online Privacy Policies at the Beginning of the Third Millennium. *Information Technology & People* 17(4):442–461.

Mechael PN (2009) The Case for mHealth in Developing Countries. *Innovations: Technology, Governance, Globalization* 4(1):103–118.

Meinert DB, Peterson DK, Criswell JR, Crossland MD (2006) Privacy Policy Statements and Consumer Willingness to Provide Personal Information. *Journal of Electronic Commerce in Organizations* 4(1):1–17.

Mell P, Grance T (2011) The NIST Definition of Cloud Computing. Retrieved (August 22, 2012), csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Merriam-Webster (2014) Archetype - Definition. Retrieved (July 27, 2014), http://www.merriam-webster.com/dictionary/archetype . Archived at: http://www.webcitation.org/6QdwYwRgI.

van Merriënboer JJG, Sweller J (2005) Cognitive Load Theory and Complex Learning: Recent Developments and Future Directions. *Educational Psychology Review* 17(2):147–177.

van Merriënboer JJG, Sweller J (2010) Cognitive Load Theory in Health Professional Education: Design Principles and Strategies. *Medical Education* 44(1):85–93.

Metzger MJ (2006) Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure. *Communication Research* 33(3):155–179.

Milberg SJ, Burke SJ, Smith HJ, Kallman EA (1995) Values, Personal Information Privacy, and Regulatory Approaches. *Communications of the ACM* 38(12):65–74.

Milne GR, Culnan MJ (2002) Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys. *Information Society* 18(5):345–359.

Milne GR, Culnan MJ (2004) Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices. *Journal of Interactive Marketing* 18(3):15–29.

Milne GR, Rohm AJ, Bahl S (2004) Consumers' Protection of Online Privacy and Identity. *Journal of Consumer Affairs* 38(2):217–232.

Miltgen CL, Peyrat-Guillard D (2014) Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries. *European Journal of Information Systems* 23(2):103–125.

Miyazaki AD, Fernandez A (2000) Internet Privacy and Security: An Examination of Online Retailer Disclosures. *Journal of Public Policy & Marketing* 19(1):54–61.

Miyazaki AD, Krishnamurthy S (2002) Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *Journal of Consumer Affairs* 36(1):28–49.

Mojica IJ, Adams B, Nagappan M, Dienst S, Berger T, Hassan AE (2014) A Large-Scale Empirical Study on Software Reuse in Mobile Apps. *IEEE Software* 31(2):78–86.

Morton A, Sasse MA (2014) Desperately Seeking Assurances: Segmenting Users by Their Information-Seeking Preferences. *Proceedings of the 12th Annual Conference on Privacy, Security and Trust*. 102–111.

Mosa AS, Yoo I, Sheets L (2012) A Systematic Review of Healthcare Applications for Smartphones. *BMC Medical Informatics and Decision Making* 12(1):67.

Mueller B, Urbach N (2017) Understanding the Why, What, and How of Theories in IS Research. *Communications of AIS* forthcoming.

Muessig KE, Pike EC, Legrand S, Hightow-Weidman LB (2013) Mobile Phone Applications for the Care and Prevention of HIV and other Sexually Transmitted Diseases: A Review. *Journal of Medical Internet Research* 15(1):e1.

Mulligan DK, Koopman C, Doty N (2016) Privacy is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 374(2083):1–17.

Mundy DP (2006) Customer Privacy on UK Healthcare Websites. *Medical Informatics and the Internet in Medicine* 31(3):175–193.

Muñoz RF (2010) Using Evidence-Based Internet Interventions to Reduce Health Disparities Worldwide. *Journal of Medical Internet Research* 12(5):e60.

Mylonas A, Meletiadis V, Mitrou L, Gritzalis D (2013) Smartphone Sensor Data as Digital Evidence. *Computers & Security* 38(0):51–75.

Nanavati M, Colp P, Aiello B, Warfield A (2014) Cloud Security: A Gathering Storm. *Communications of the ACM* 57(5):70–79.

Naveh B (2003) JGraphT. Retrieved (February 22, 2013), http://jgrapht.org . Archived at: http://www.webcitation.org/6NYMn4Z4V.

Newman MEJ (2003) The Structure and Function of Complex Networks. *SIAM Review* 45:167–256.

Newman MEJ (2004) Analysis of Weighted Networks. *Physical Review E* 70(5):056131.

Newman MEJ, Girvan M (2004) Finding and Evaluating Community Structure in Networks. *Physical Review E* 69(2):026113.

Nissenbaum H (2004) Privacy as Contextual Integrity. *Washington Law Review* 79:119–157.

Nissenbaum H (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, Stanford, CA, USA).

Noy NF, McGuinness DL (2001) Ontology Development 101: A Guide to Creating Your First Ontology. Retrieved (August 25, 2014), http://protege.stanford.edu/publications/ontology_development/ontology101-noy-mcguinness.html.

Nuseibeh B, Easterbrook S (2000) Requirements Engineering: A Roadmap. *Proceedings of the Conference on The Future of Software Engineering*. ICSE ’00. (ACM, New York, NY, USA), 35–46.

Nussbaumer P, Matter I, Schwabe G (2012) “Enforced” vs. “Casual” Transparency – Findings from IT-Supported Financial Advisory Encounters. *ACM Transactions on Management Information Systems* 3(2):11:1–11:19.

O’Connor P (2003) What Happens to my Information if I Make a Hotel Booking Online: An Analysis of On-Line Privacy Policy Use, Content and Compliance by the International Hotel Companies. *Journal of Services Research* 3(2):5–28.

Oetzel MC, Spiekermann S (2014) A Systematic Methodology for Privacy Impact Assessments: A Design Science Approach. *European Journal of Information Systems* 23(2):126–150.

Oliver C (1991) Strategic Responses to Institutional Processes. *Academy of Management Review* 16(1):145–179.

Organisation for Economic Cooperation and Development (1980) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *Recommendation by the Council of the OECD*. Retrieved (June 25, 2013), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm . Archived at: http://www.webcitation.org/6Y7eE1Q3m.

Oulasvirta A, Suomalainen T, Hamari J, Lampinen A, Karvonen K (2014) Transparency of Intentions Decreases Privacy Concerns in Ubiquitous Surveillance. *Cyberpsychology, Behavior, and Social Networking* 17(10):633–638.

Ozdalga E, Ozdalga A, Ahuja N (2012) The Smartphone in Medicine: A Review of Current and Potential Use among Physicians and Students. *Journal of Medical Internet Research* 14(5):e128.

Ozdemir Z, Barron J, Bandyopadhyay S (2011) An Analysis of the Adoption of Digital Health Records Under Switching Costs. *Information Systems Research* 22(3):491–503.

Paas F, Ayres P (2014) Cognitive Load Theory: A Broader View on the Role of Memory in Learning and Education. *Educational Psychology Review* 26(2):191–195.

Pagano D, Maalej W (2013) User Feedback in the AppStore: An Empirical Study. *Proceedings of the 21st IEEE International Conference on Requirements Engineering*. (IEEE, Rio De Janeiro, Brasil), 125–134.

Pagliari C (2007) Design and Evaluation in eHealth: Challenges and Implications for an Interdisciplinary Field. *Journal of Medical Internet Research* 9(2):e15.

Papacharissi Z, Fernback J (2005) Online Privacy and Consumer Protection: An Analysis of Portal Privacy Statements. *Journal of Broadcasting & Electronic Media* 49(3):259–281.

Park YJ (2013) Digital Literacy and Privacy Behavior Online. *Communication Research* 40(2):215–236.

Pathak A, Hu YC, Zhang M (2012) Where is the Energy Spent Inside my App?: Fine Grained Energy Accounting on Smartphones with Eprof. *Proceedings of the 7th ACM European Conference on Computer Systems*. EuroSys '12. (ACM, Bern, Switzerland), 29–42.

Pavlou PA (2002) What Drives Electronic Commerce? A Theory of Planned Behavior Perspective. *Academy of Management Proceedings*:A1–A6.

Pavlou PA, Liang H, Xue Y (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. *MIS Quarterly* 31(1):105–136.

Pentina I, Zhang L, Bata H, Chen Y (2016) Exploring Privacy Paradox in Information-Sensitive Mobile App Adoption: A Cross-Cultural Comparison. *Computers in Human Behavior* 65:409–419.

Peslak AR (2005) Internet Privacy Policies: A Review and Survey of the Fortune 50. *Information Resources Management Journal* 18(1):29–41.

Petronio S (1991) Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples. *Communication Theory* 1(4):311–335.

Plaza I, Demarzo PMM, Herrera-Mercadal P, García-Campayo J (2013) Mindfulness-Based Mobile Applications: Literature Review and Analysis of Current Features. *JMIR mHealth uHealth* 1(2):e24.

Pollach I (2006) Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions. *Journal of Organizational and End User Computing* 18(1):23–49.

Pollach I (2007) What's Wrong With Online Privacy Policies? *Communications of the ACM* 50(9):103–108.

Proctor RW, Ali MA, Vu KPL (2008) Examining Usability of Web Privacy Policies. *International Journal of Human-Computer Interaction* 24(3):307–328.

Pyper C, Amery J, Watson M, Crook C (2004) Access to Electronic Health Records in Primary Care - A Survey of Patients' Views. *Medical Science Monitor* 10(11):SR17-22.

Rains SA, Bosch LA (2009) Privacy and Health in the Information Age: A Content Analysis of Health Web Site Privacy Policy Statements. *Health Communication* 24(5):435–446.

Raymond ES (2003) *The Art of UNIX Programming* 1st ed. (Addison-Wesley, Boston, MA, USA).

Reagle J, Cranor LF (1999) The Platform for Privacy Preferences. *Communications of the ACM* 42(2):48–55.

Reed PJ, Spiro ES, Butts CT (2016) Thumbs up for Privacy?: Differences in Online Self-Disclosure Behavior Across National Cultures. *Social Science Research* 59:155–170.

Rindfleisch TC (1997) Privacy, Information Technology, and Health Care. *Communications of the ACM* 40(8):92–100.

Rizk R, Gürses SF, Günther O (2010) SNS and 3rd Party Applications Privacy Policies and their Construction of Privacy Concerns. *ECIS 2010 Proceedings*. (AIS, Pretoria, South Africa).

Robles-Estrada C, Vargas-Barraza JA, Sepúlveda-Núñez MDDC (2006) Are Privacy Issues Important in Mexican Online Markets? An Empirical Investigation into Published Online Privacy Statements of Mexican Web Sites. *BLED 2006 Proceedings*. (Bled, Slovenia).

Rodríguez-Priego N, van Bavel R, Monteleone S (2016) The Disconnection Between Privacy Notices and Information Disclosure: An Online Experiment. *Economia Politica* 33(3):433–461.

Roeber B, Rehse O, Knorrek R, Thomsen B (2015) Personal Data: How Context Shapes Consumers' Data Sharing with Organizations from Various Sectors. *Electronic Markets* 25(2):95–108.

Rohm AJ, Milne GR (2004) Just What the Doctor Ordered: The Role of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern. *Journal of Business Research* 57(9):1000–1011.

Romanosky S (2016) Examining the Costs and Causes of Cyber Incidents. *Journal of Cybersecurity* 2(1):121–135.

Rosser BA, Eccleston C (2011) Smartphone Applications for Pain Management. *Journal of Telemedicine and Telecare* 17(6):308–312.

Rothstein MA, Talbott MK (2007) Compelled Authorizations for Disclosure of Health Records: Magnitude and Implications. *The American Journal of Bioethics* 7(3):38–45.

Rouse WB, Rouse SH (1984) Human Information Seeking and Design of Information Systems. *Information Processing & Management* 20(1):129–138.

Ruotsalainen PS, Blobel BG, Seppälä AV, Sorvari HO, Nykänen PA (2012) A Conceptual Framework and Principles for Trusted Pervasive Health. *Journal of Medical Internet Research* 14(2):e52.

Sæther B (1998) Retroduction: An Alternative Research Strategy? *Business Strategy and the Environment* 7(4):245–249.

Savirimuthu J (2013) Smart Meters and the Information Panopticon: Beyond the Rhetoric of Compliance. *International Review of Law, Computers & Technology* 27(1–2):161–186.

Schatz BR, Hardin JB (1994) NCSA Mosaic and the World Wide Web: Global Hypermedia Protocols for the Internet. *Science* 265(5174):895–901.

Schnackenberg AK, Tomlinson EC (2016) Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships. *Journal of Management* 42(7):1784–1810.

Schuele K (2005) Privacy Policy Statements on Municipal Websites. *Journal of Government Financial Management* 54(2):20–29.

Schwaig KS, Kane GC, Storey VC (2005) Privacy, Fair Information Practices and the Fortune 500: The Virtual Reality of Compliance. *SIGMIS Database* 36(1):49–63.

Schwaig KS, Kane GC, Storey VC (2006) Compliance to the Fair Information Practices: How Are the Fortune 500 Handling Online Privacy Disclosures? *Information & Management* 43(7):805–820.

Schwaig KS, Segars AH, Grover V, Fiedler KD (2013) A Model of Consumers' Perceptions of the Invasion of Information Privacy. *Information & Management* 50(1):1–12.

Seneviratne S, Seneviratne A, Mohapatra P, Mahanti A (2014) Predicting User Traits from a Snapshot of Apps Installed on a Smartphone. *SIGMOBILE Mobile Computing and Communications Review* 18(2):1–8.

Shahri AB, Ismail Z (2012) A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS. *Journal of Information Security* 3(2):169–176.

Shalhoub ZK (2006) Content Analysis of Web Privacy Policies in the GCC Countries. *Information Systems Security* 15(3):36–45.

Shea S (1994) Security Versus Access: Trade-Offs are only Part of the Story. *Journal of the American Medical Informatics Association* 1(4):314–315.

Sheehan KB (2002) Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society* 18(1):21–32.

SIL International Linguistics Department (2014) English Wordlists. Retrieved (February 14, 2014), http://www-01.sil.org/linguistics/wordlists/english . Archived at: http://www.webcitation.org/6NS0EItXU.

Simon HA (1996) *The Sciences of the Artificial* 3rd ed. (MIT Press, Cambridge, MA, USA).

Simon SR, Evans JS, Benjamin A, Delano D, Bates DW (2009) Patients' Attitudes Toward Electronic Health Information Exchange: Qualitative Study. *Journal of Medical Internet Research* 11(3):e30.

Slamanig D, Stingl C (2008) Privacy Aspects of eHealth. *3rd International Conference on Availability, Reliability and Security*. ARES'08. (IEEE, Washington, DC, USA), 1226–1233.

Smith B (2004) Beyond Concepts: Ontology as Reality Representation. *Proceedings of the International Conference on Formal Ontology and Information Systems*. (IOS Press, Turin, Italy), 73–84.

Smith B, Ceusters W (2010) Ontological Realism: A Methodology for Coordinated Evolution of Scientific Ontologies. *Applied Ontology* 5(3–4):139–188.

Smith B, Welty C (2001) Ontology: Towards a New Synthesis. *Proceedings of the International Conference on Formal Ontology and Information Systems*. (ACM, Ogunquit, ME, USA), 3–9.

Smith HJ, Dinev T, Xu H (2011) Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* 35(4):989–1015.

Solove DJ (2001) Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review* 53(6):1393–1462.

Solove DJ (2002) Conceptualizing Privacy. *California Law Review* 90(4):1087–1155.

Son JY, Kim SS (2008) Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly* 32(3):503–529.

Song D, Shi E, Fischer I (2012) Cloud Data Protection for the Masses. *IEEE Computer* 45(1):39–45.

Soria-Comas J, Domingo-Ferrer J, Sánchez D, Megías D (2017) Individual Differential Privacy: A Utility-Preserving Formulation of Differential Privacy Guarantees. *IEEE Transactions on Information Forensics and Security* 12(6):1418–1429.

Spiekermann S (2012) The Challenges of Privacy by Design. *Communications of the ACM* 55(7):38–40.

Spiekermann S, Cranor LF (2009) Engineering Privacy. *IEEE Transactions on Software Engineering* 35(1):67–82.

Spiekermann S, Grossklags J, Berendt B (2001) e-Privacy in 2nd Generation e-Commerce: Privacy Preferences Versus Actual Behavior. *Proceedings of the 3rd ACM Conference on Electronic Commerce*. (ACM, New York, NY, USA), 38–47.

Spyns P, Meersman R, Jarrar M (2002) Data Modelling versus Ontology Engineering. *ACM SIGMod Record* 31(4):12–17.

Stanaland AJS, Lwin MO, Leong S (2009) Providing Parents with Online Privacy Information: Approaches in the US and the UK. *Journal of Consumer Affairs* 43(3):474–494.

Steinhubl SR, Muse ED, Topol EJ (2013) Can Mobile Health Technologies Transform Health Care? *JAMA* 310(22):2395–2396.

Stitilis D, Malinauskaite I (2013) Evaluation of Legal Data Protection Requirements in Cloud Services in the Context of Contractual Relations with End-Users. *Socialines Technologijos* 3(2):390–414.

Stoycheff E (2016) Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. *Journalism & Mass Communication Quarterly* 93(2):296–311.

Strickland LS, Hunt LE (2005) Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions. *Journal of the American Society for Information Science and Technology* 56(3):221–234.

Subashini S, Kavitha V (2011) A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications* 34(1):1–11.

Sun Y, Kantor PB (2006) Cross-Evaluation: A New Model for Information System Evaluation. *Journal of the American Society for Information Science and Technology* 57(5):614–628.

Sunyaev A (2013) Evaluation of Microsoft HealthVault and Google Health Personal Health Records. *Health and Technology* 3(1):3–10.

Sunyaev A (2014) Consumer Facing Health Care Systems. *e-Service Journal* 9(2):1–23.

Sunyaev A, Chornyi D (2012) Supporting Chronic Disease Care Quality: Design and Implementation of a Health Service and its Integration with Electronic Health Records. *ACM Journal of Data and Information Quality* 3(2):3:1-3:21.

Sunyaev A, Chornyi D, Mauro C, Krcmar H (2010) Evaluation Framework for Personal Health Records: Microsoft Health Vault vs. Google Health. *Proceedings of the Hawaii International Conference on System Sciences (HICSS 34)*. (IEEE, Kauai, HI, USA).

Sunyaev A, Dehling T, Taylor PL, Mandl KD (2015) Availability and Quality of Mobile Health App Privacy Policies. *Journal of the American Medical Informatics Association* 22(e1):e28–e33.

Sunyaev A, Leimeister JM, Krcmar H (2010) Open Security Issues in German Healthcare Telematics. *Proceedings of the 3rd International Conference on Health Informatics*. (INSTICC, Valencia, Spain), 187–194.

Sunyaev A, Schneider S (2013) Cloud Services Certification. *Communications of the ACM* 56(2):33–36.

Suominen H (2012) Towards an International Electronic Repository and Virtual Laboratory of Open Data and Open-Source Software for Telehealth Research: Comparison of International, Australian and Finnish Privacy Policies. *Studies in Health Technology and Informatics* 182:153–160.

Sutanto J, Palme E, Tan CH, Phang CW (2013) Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Quarterly* 37(4):1141–1164.

Sweller J (1988) Cognitive Load During Problem Solving: Effects on Learning. *Cognitive Science* 12(2):257–285.

Sweller J, van Merriënboer JJG, Paas FWC (1998) Cognitive Architecture and Instructional Design. *Educational Psychology Review* 10(3):251–296.

Tavani HT (2007) Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy. *Metaphilosophy* 38(1):1–22.

Tibély G, Kovanen L, Karsai M, Kaski K, Kertész J, Saramäki J (2011) Communities and Beyond: Mesoscopic Analysis of a Large Social Network with Complementary Methods. *Physical Review E* 83(5):056125.

Timpson S, Troutman M (2009) The Importance of a Layered Privacy Policy on all Mobile Internet Sites and Mobile Marketing Campaigns. *International Journal of Mobile Marketing* 4(1):57–61.

Tsai JY, Egelman S, Cranor L, Acquisti A (2011) The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research* 22(2):254–268.

Tuffs A (2010) Germany Puts Universal Health e-Card on Hold. *BMJ* 340(1):c171.

Turner EC, Dasgupta S (2003) Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals. *Information Systems Management* 20(1):8–18.

Unruh HK, Bowen DJ, Meischke H, Bush N, Wooldridge JA (2004) Women's Approaches to the Use of New Technology for Cancer Risk Information. *Women & Health* 40(1):59–78.

US Federal Department of Health Education and Welfare (1973) Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Chapter III. Safeguards for Privacy. Retrieved (April 24, 2015), https://epic.org/privacy/hew1973report/c3.htm . Archived at: http://www.webcitation.org/6Y1gDPqTf.

Uschold M, Gruninger M (1996) Ontologies: Principles, Methods and Applications. *Knowledge Engineering Review* 11(2):93–136.

Vail MW, Earp JB, Antón AI (2008) An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies. *IEEE Transactions on Engineering Management* 55(3):442–454.

Venable J (2006) A Framework for Design Science Research Activities. Khosrow-Pour M, ed. *Proceedings of the Information Resources Management Association International Conference*. (Idea Group Publishing, Washington, DC, USA), 184–187.

Venable J, Pries-Heje J, Baskerville R (2016) FEDS: A Framework for Evaluation in Design Science Research. *European Journal of Information Systems* 25(1):77–89.

Venkatesh V, Brown SA, Bala H (2013) Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. *MIS Quarterly* 37(1):21–54.

Venkatesh V, Brown SA, Sullivan YW (2016) Guidelines for Conducting Mixed-Methods Research: An Extension and Illustration. *Journal of the Association for Information Systems* 17(7):2.

Viennot N, Garcia E, Nieh J (2014) A Measurement Study of Google Play. *Proceedings of the 2014 ACM International Conference on Measurement and Modeling of Computer Systems*. SIGMETRICS ’14. (ACM, Austin, TX, USA), 221–233.

Vuorinen J, Tetri P (2012) The Order Machine-The Ontology of Information Security. *Journal of the Association for Information Systems* 13(9):695–713.

Wainer J, Campos CJR, Salinas MDU, Sigulem D (2008) Security Requirements for a Lifelong Electronic Health Record System: An Opinion. *Open Medical Informatics Journal* 2:160–165.

Walls JG, Widmeyer GR, El Sawy OA (1992) Building an Information System Design Theory for Vigilant EIS. *Information Systems Research* 3(1):36–59.

Walsh TM, Volsko TA (2008) Readability Assessment of Internet-Based Consumer Health Information. *Respiratory Care* 53(10):1310–1315.

Ward JH (1963) Hierarchical Grouping to Optimize an Objective Function. *Journal of the American Statistical Association* 58(301):236–244.

Warren SD, Brandeis LD (1890) The Right to Privacy. *Harvard Law Review* 4(5):193–220.

Weiss GM, Lockhart JW (2012) The Impact of Personalization on Smartphone-Based Activity Recognition. *Proceedings of the Activity Context Representation Workshop*. (Association for the Advancement of Artificial Intelligence, Toronto, Canada), 98–104.

Weitzman ER, Cole E, Kaci L, Mandl KD (2011) Social but Safe? Quality and Safety of Diabetes-Related Online Social Networks. *Journal of the American Medical Informatics Association* 18(3):292–297.

Weitzman ER, Kaci L, Mandl KD (2010) Sharing Medical Data for Health Research: The Early Personal Health Record Experience. *Journal of Medical Internet Research* 12(2):e14.

West JH, Hall PC, Hanson CL, Barnes MD, Giraud-Carrier C, Barrett J (2012) There’s an App for That: Content Analysis of Paid Health and Fitness Apps. *Journal of Medical Internet Research* 14(3):e72.

Westin A (1967) *Privacy and Freedom* (Ig Publishing, New York, NY, USA).

Whitman ME (2003) Enemy at the Gate: Threats to Information Security. *Communications of the ACM* 46(8):91–95.

Wicker SB (2012) The Loss of Location Privacy in the Cellular Age. *Communications of the ACM* 55(8):60–68.

Wijen F (2014) Means versus Ends in Opaque Institutional Fields: Trading off Compliance and Achievement in Sustainability Standard Adoption. *Academy of Management Review* 39(3):302–323.

Wikimedia Foundation (2014) Wikimedia Foundation Privacy Policy. Retrieved (May 9, 2015), http://wikimediafoundation.org/wiki/Privacy_policy . Archived at: http://www.webcitation.org/6YOlcGEUD.

Wilson DW, Valacich JS (2012) Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. *Proceedings of the Thirty Third International Conference on Information Systems (ICIS 2012)*. (Orlando, FL, USA), paper 101.

Wilson EV (2009) *Patient-Centered E-Health* Wilson EV, ed. (IGI Publications, Hershey, PA, USA).

Wisniewski P, Islam A, Richter Lipford H, Wilson DC (2016) Framing and Measuring Multi-Dimensional Interpersonal Privacy Preferences of Social Networking Site Users. *Communications of the Association for Information Systems* 38(1):235–258.

Wisniewski PJ, Knijnenburg BP, Lipford HR (2017) Making Privacy Personal: Profiling Social Network Users to Inform Privacy Education and Nudging. *International Journal of Human-Computer Studies* 98:95–108.

Wolf JA, Moreau JF, Akilov O, Patton T, English JC, Ho J, Ferris LK (2013) Diagnostic Inaccuracy of Smartphone Applications for Melanoma Detection. *JAMA Dermatology* 149(4):422–426.

Woodruff A, Pihur V, Consolvo S, Schmidt L, Brandimarte L, Acquisti A (2014) Would a Privacy Fundamentalist Sell Their DNA for $1000...If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences. *Symposium on Usable Privacy and Security*. (USENIX Association, Menlo Park, CA, USA).

Wu KW, Huang SY, Yen DC, Popova I (2012) The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust. *Computers in Human Behavior* 28(3):889–897.

Xie HI (2000) Shifts of Interactive Intentions and Information-Seeking Strategies in Interactive Information Retrieval. *Journal of the American Society for Information Science* 51(9):841–857.

Xu H, Crossler RE, Bélanger F (2012) A Value Sensitive Design Investigation of Privacy Enhancing Tools in Web Browsers. *Decision Support Systems* 54(1):424–433.

Xu H, Dinev T, Smith HJ, Hart PJ (2011) Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems* 12(12):798–824.

Xu H, Gupta S, Rosson MB, Carroll JM (2012) Measuring Mobile Users’ Concerns for Information Privacy. *Proceedings of the Thirty Third International Conference on Information Systems (ICIS 2012)*. (Orlando, FL, USA).

Xu H, Teo HH, Tan BCY, Agarwal R (2012) Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. *Information Systems Research* 23(4):1342–1363.

Xu Q, Erman J, Gerber A, Mao ZM, Pang J, Venkataraman S (2011) Identifying Diverse Usage Behaviors of Smartphone Apps. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*. IMC ’11. (ACM, Berlin, Germany), 329–344.

Yau SS, An HG (2011) Software Engineering Meets Services and Cloud Computing. *IEEE Computer* 44(10):47–53.

Yee GOM, Korba L (2013) Personal Privacy Policies. John R. Vacca, ed. *Computer and Information Security Handbook*. (Morgan Kaufmann, Boston, MA, USA), 773–792.

Zhang L, Gupta D, Mohapatra P (2012) How Expensive are Free Smartphone Apps? *SIGMOBILE Mobile Computing and Communications Review* 16(3):21–32.

Zhang R, Liu L (2010) Security Models and Requirements for Healthcare Application Clouds. *Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing*. (IEEE, Miami, FL, USA), 268–275.

Zhang X, Toru S, Kennedy M (2007) A Cross-Cultural Analysis of Privacy Notices of the Global 2000. *Journal of Information Privacy and Security* 3(2):18–36.

Zhu H, Ou CXJ, van den Heuvel WJAM, Liu H (2017) Privacy Calculus and its Utility for Personalization Services in E-Commerce: An Analysis of Consumer Decision-Making. *Information & Management* 54(4):427–437.