Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2014 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2014

Assessment Instrument for Privacy Policy Content: Design and Evaluation of PPC

Tobias Dehling
Department of Information Systems, University of Cologne, Cologne, Germany., dehling@wiso.uni-koeln.de

Fangjian Gao
Department of Information Systems, University of Cologne, Cologne, Germany., gao@wiso.uni-koeln.de

Ali Sunyaev
Department of Information Systems, University of Cologne, Cologne, Germany., sunyaev@wiso.uni-koeln.de

Assessment Instrument for Privacy Policy Content: Design and Evaluation of PPC

Tobias Dehling
University of Cologne, Germany

Fangjian Gao
University of Cologne, Germany

Ali Sunyaev[1]
University of Cologne, Germany

ABSTRACT

Privacy policies are notices posted by providers and intended to inform users about privacy practices. However, extant research shows that privacy policies are often of poor quality and do not address users' concerns. In this paper, we design and develop PPC – a privacy policy content assessment instrument to support assessments of whether offered privacy policy content provides comprehensive information addressing users' privacy concerns. PPC is developed based on extant research, standards, and guidelines. Application of PPC to 62 privacy policies of mHealth apps available in iOS and Android demonstrates utility of PPC and suitability of PPC as assessment instrument for privacy policy content. Contributions of our research are twofold: For research, we conduct improvement design science research contributing to design theory on assessment of privacy policy content. For practice, potential applications of PPC are support in privacy policy development and identification of deficiencies in offered privacy policies. In addition, through evaluation of PPC, we reveal an insufficient current state of mHealth app privacy policy content.

Keywords: *information security, information privacy, privacy policy, privacy practices, privacy policy content, P3P, mHealth, health IT*

[1] Corresponding author: sunyaev@wiso.uni-koeln.de

INTRODUCTION

Today's online environment consists of a multitude of offerings that present information to users, consume user information, process user information, and tailor presented information according to user characteristics and preferences. Users are concerned with privacy issues related to IT offerings and want to control access to their information (Khalid et al. 2014). Without support, users cannot be expected to gauge fit of IT offerings with their preferences and expectations, especially, when it comes to complex concepts like privacy.

For the scope of this paper, we adapt the tripartite model of privacy introduced by Tavani and Moor (2001), which consists of a concept of privacy, management of privacy, and justification for privacy. In addition, we focus only on information privacy (Clarke 1999) and not on other facets of privacy (e.g., physical privacy). Privacy is conceptualized as protection from intrusion and restricted access to information (Tavani 2007; Tavani and Moor 2001). Privacy is managed through external control (e.g., enforcement of laws) and individual control (e.g., choice, consent, and correction).[2] Justification for privacy is that leakage of sensitive, personal information, or risk thereof, can cause harm to users (Dehling et al. 2014; Rindfleisch 1997). A central principle for establishing privacy in online contexts is the publicity principle: "Rules and conditions governing private situations should be clear and known to the persons affected by them"(Moor 1997, p. 32). If providers do not obey the publicity principle, users cannot know providers privacy practices and are thus prevented from managing their privacy through individual control: Without knowledge of privacy practices, users can obviously neither exert choice, consent, nor correction in a meaningful way.

[2] See Tavani and Moor (2001) for a detailed discussion.

Privacy policies are notices provided by providers and a common tool to inform users on privacy practices. However, extant research shows that privacy policies are often of poor quality and do not address users' needs: Privacy policies are often unspecific, do not provide the information users are looking for (Earp et al. 2005), and do not address a common selection of content aspects (McDonald et al. 2009). Providers seem to freely choose which aspects to address and which to leave out (Sunyaev et al. 2014). If privacy policies do not offer content covering the information users are looking for, they cannot attain there objective of informing users about privacy practices. Consequently, users are unlikely to be able to exert individual control or to manage their privacy (Tavani 2007). An instrument for assessment of privacy policy content can guide creation of privacy policies, evaluate offered privacy policies, and alleviate the aforementioned problems. However, to the best of our knowledge, there are no detailed guidelines for assessment of privacy policy content.

Our research aims at closing this gap through design and development of PPC – a privacy policy content assessment instrument. PPC is designed to accomplish two goals. The first goal of PPC is to support assessments of whether offered privacy policy content provides comprehensive information on privacy practices. The second goal is to capture privacy practices stated in assessed privacy policies. PPC can thus be applied to assess whether privacy policies are suitable for enabling users to exert individual control (Tavani 2007).

We assess utility and completeness of privacy policy content aspects by applying PPC to 62 privacy policies of widely-used mobile health (mHealth) applications (apps). mHealth apps leverage various wireless technologies to provide health-related information and services on diverse mobile devices (Istepanian et al. 2004). Users, albeit deeming access to health information and related services beneficial, are however concerned with information security and privacy issues

(Khalid et al. 2014). Since information security and privacy concerns impede users' willingness to share information (Anderson and Agarwal 2011), they also lessen potential benefits to be reaped from mHealth apps. Novelty and associated uncertainty of mHealth app use and the high stakes involved, make mHealth apps an auspicious domain for research on privacy policy content. If users were provided with the information required to gauge information security and privacy practices of mHealth apps, they would be more likely to use mHealth apps and to share personal information in order to benefit from enhanced offerings tailored to their needs – an important step towards realization of the promising potential of mHealth apps to transform and improve the health care environment (Steinhubl et al. 2013).

RESEARCH DESIGN

We followed the Design Science Research paradigm (Gregor and Hevner 2013) and employed a two-step research approach. In the first step, we developed an artifact (i.e., PPC) for the assessment of privacy policy content. In the second step, we evaluated utility and completeness of PPC by applying it to 62 privacy policies of mHealth apps available in the official app stores of the two major mobile platforms – iOS (Apple 2014) and Android (Google 2014a). The tripartite model of privacy (Tavani 2007; Tavani and Moor 2001) was employed as kernel theory for PPC and serves as basis and explanation for our design (Gregor and Jones 2007).

Identification of Privacy Policy Content Aspects

According to the tripartite model of privacy, privacy policies need to offer comprehensive information addressing users' privacy concerns. Users' privacy concerns are however neither static nor identical for all users: Individual and cultural differences lead to differences in privacy concerns (Miltgen and Peyrat-Guillard 2014), while online offerings and privacy policies are globally accessible. Privacy is moreover context-specific (Smith et al. 2011). Hence, users look for different

information, process information differently, and act differently depending on context and contextual clues (Lowry et al. 2012). Therefore, we sacrifice parsimony for comprehensiveness to make the assessment of privacy policy content useful for diverse sets of users in various online situations and contexts. Moreover, PPC leverages a hierarchical, modular structure reflecting users' core privacy concerns: information collected, rationale for collection, handling of information, and offered privacy controls (Ackerman et al. 1999; Antón et al. 2010; Earp et al. 2005). The hierarchical, modular structure of PPC facilitates its adaptability to diverse research scopes and domains, and fosters analysis of privacy policy content on different levels of detail.

The core of PPC is a catalogue of privacy policy content aspects offering information on providers' privacy practices. We established our catalogue of privacy policy content aspects based on extant research, standards, and guidelines to incorporate results of different domains and perspectives related to privacy policy content. We chose privacy policy content covered by the platform for privacy preferences project (P3P, Cranor et al. 2006) as foundation for the content catalogue. P3P is a framework that can be used to construct machine-readable representations of providers' privacy practices (Reagle and Cranor 1999). The P3P specification addresses a wide selection of privacy policy content aspects to facilitate representation of a wide variety of privacy practices (Lämmel and Pek 2013). However, the P3P specification does not directly offer a ready-to-use list of privacy policy content aspects since it only specifies a domain-specific language for privacy policies. Therefore, we analyzed the P3P specification to identify the privacy policy content aspects for PPC and enriched them with additional aspects identified in extant research, standards, and guidelines (Ackerman et al. 1999; Antón et al. 2010; Carrión et al. 2012; Council of the European Communities 1995; Federal Trade Commission 2013; Google 2014b; Health on the Net Foundation 2010; Milne and Culnan 2002; United States Congress 1974). Redundancies and

missing aspects were identified and resolved through an iterative process consisting of multiple revisions of the content aspect catalogue and group discussions of the latest version with all authors. Once satisfied with the result, the catalogue was reviewed by two independent researchers from the domains of medicine and law to ensure comprehensiveness and clarity. All identified ambiguities and resulting changes were subsequently resolved and implemented.

Evaluation of PPC

Privacy policies of current mHealth apps are suffering from low quality (Sunyaev et al. 2014) and constitute thus an appropriate domain for further research on privacy policy content. We applied PPC to privacy policy content of mHealth apps to evaluate utility of PPC and comprehensiveness of identified privacy policy content aspects. Derived from the publicity principle, our main testable proposition (Gregor and Jones 2007) is that PPC supports assessments of whether offered privacy policy content is comprehensive, within the context of online IT offerings. We conducted a naturalistic, ex-post evaluation (Venable et al. 2012) and evaluated whether PPC can be adapted to the domain of analysis and whether mHealth app privacy policy content can be covered with PPC's privacy policy content aspects. The three competing goals for evaluation in design science research are rigor, efficiency, and ethics (Venable et al. 2012). For our evaluation, the main goals are rigor and efficiency because our evaluation involves no human subjects and rigorous, efficient research on privacy policy content is clearly in line with the ethical principles proposed by Myers and Venable (2014). Rigor requires establishment of efficacy and effectiveness (Venable et al. 2012). Hence, we applied our assessment instrument to assess content of actual privacy policies of mHealth apps. To ensure efficiency, we limited our analysis to privacy policies of mHealth apps and conducted the evaluation mainly with two raters.

Privacy policies were taken from the data set collected by Sunyaev et al. (2014), who gathered English language mHealth apps in the official iOS (Apple 2014) and Android (Google 2014a) app stores, and surveyed the 600 most-frequently rated apps (iOS: 300 apps; Android: 300 apps) for privacy policies. For each app we identified the privacy policy by successively checking the app store web site, web pages maintained by the app provider, and Google search results. Only those privacy policies that focus on a backend application, multiple apps, or a single app were included in the content assessment because privacy policies with a scope unrelated to the actual app do not offer information on app-related privacy practices (Sunyaev et al. 2014).

For the content assessment, two raters independently read all privacy policies and annotated statements matching PPC content assessment aspects or attributes with respective identifiers and values. Results of the coding (Hruschka et al. 2004) were subsequently loaded into a database to facilitate identification of discrepancies, inter-rater reliability assessment, and analysis of results. Both raters started with a small random subset of privacy policies. Once finished, arising issues were discussed and resolved, and PPC was improved if necessary. When any errors in raters' assessment were revealed or PPC was updated, both raters started anew with assessment of all privacy policies. With increasing rater proficiency and PPC maturity, the size of the random privacy policy subset was increased until it encompassed all privacy policies. To ensure inter-rater reliability, we employed Janson's and Olsson's ι, a multivariate extension of Cohen's κ for multiple judges on the same scale (Janson and Olsson 2001). Differences, ambiguities, and other issues identified during application of PPC were resolved through group discussions with all authors followed by a revision of PPC, if necessary.

RESULTS

Artifact Description

With pre-defined privacy policy content aspects, PPC enables users to assess whether a privacy policy offers comprehensive content addressing users' privacy concerns. To improve ease of use, structure content aspects to be assessed, and facilitate adaptability, PPC orders privacy policy content assessments aspects hierarchically. Figure 1 presents a schematic representation of PPC. The top-tier consists of abstract, high-level content aspects. Four top-tier content aspects *Information Collected*, *Rationale for Collection*, *Handling of Information*, and *Offered Privacy Controls* represent main user concerns (Ackerman et al. 1999; Antón et al. 2010; Earp et al. 2005) and the fifth top-tier aspect *Meta Information* is not directly related to the privacy policy content and mainly required for execution of the assessment and representation of additional information. Application of PPC requires each rater to assess 121 content assessment aspects per privacy policy.

The top-tier is further refined in disjunct sub-tiers consisting of further content aspects with similar abstraction level, which refine top-tier content aspects with respect to level of detail. Analogously, sub-tiers group related content aspects in further, more detailed sub-tiers. The bottom-tier content aspects have consequently the narrowest focus and the highest level of detail in comparison to higher tiers. The hierarchical layout and disjunct grouping of content aspects ensures adaptability by allowing for arbitrary addition/removal of content aspects on any tier if necessary and refinement of content aspects to any desired level of detail.

Information Collected is refined through three tier-2 content assessment aspects: *Type* represents assessments of what information is collected (e.g., *Identification*). *Sensors* represents assessments of how information is collected. *Sensors* collect for instance information on the user *Location* (e.g., *GPS Location*). *Feature-Specific Information Collection* represents an assessment

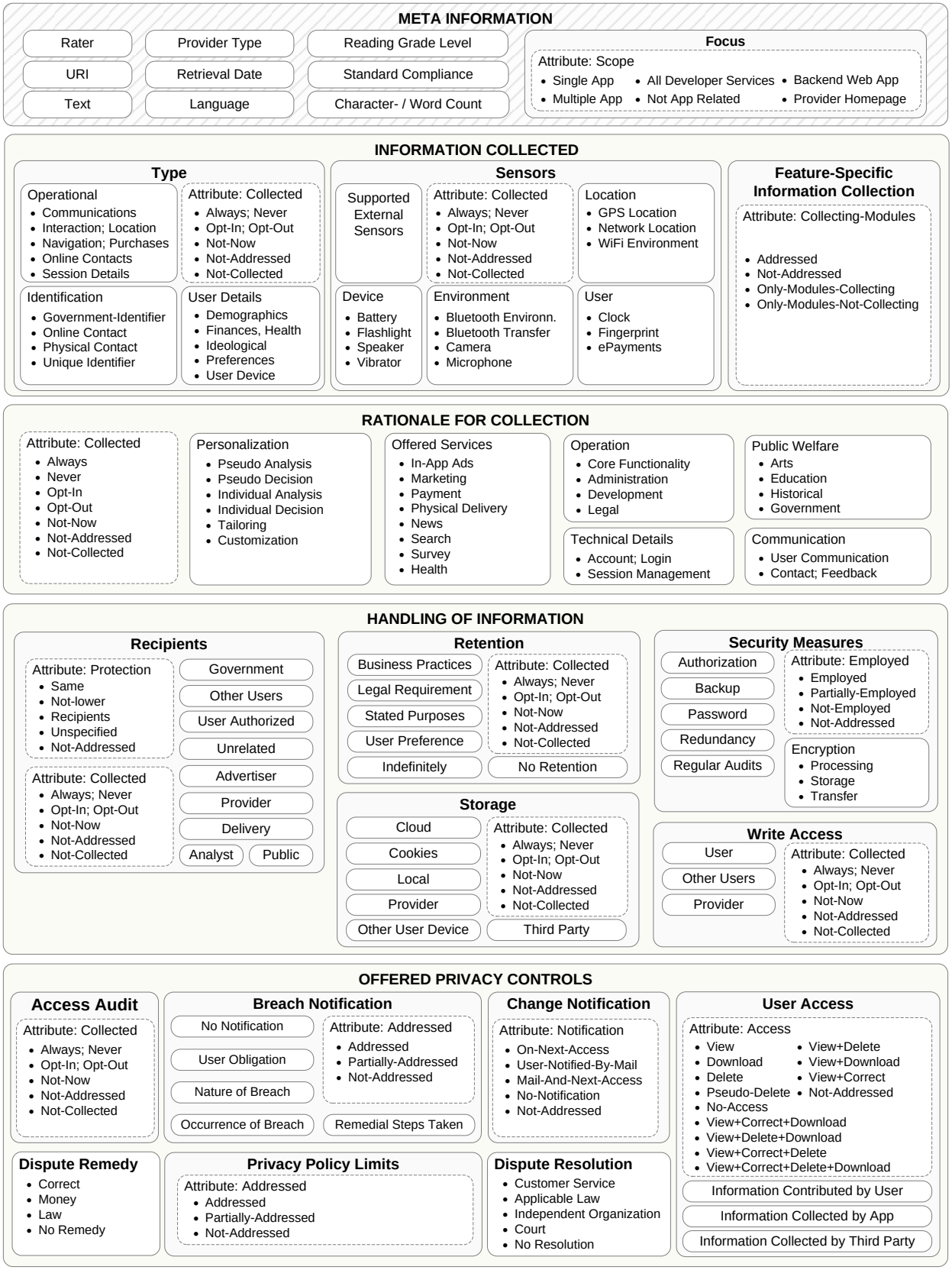

Figure 1: Schematic representation of P2C. (Continuous boxes represent assessment aspects and dashed boxes represent attributes.)

whether privacy policies outline what information is/is not collected by which features. Consider the following example: Users might want to use an application that offers medication information and can also tailor presented information to users' information stored in a personal health record (PHR). In such a case, it would be helpful for users if the privacy policy outlined whether PHR access is mandatory or whether the application can also be used for plain information retrieval without tailoring.

Rationale for Collection is refined through six tier-2 content assessment aspects: *Operation* represents operational purposes for which information is collected (e.g., application *Administration*). *Personalization* represents assessments of stated reasons for collecting information to personalize the application (e.g., employment of *Pseudo Analysis* for general personalization through analysis of aggregated user behavior). *Communication* aggregates content assessments of whether a privacy policy states that information is collected to facilitate communication (e.g., communication between users (*User Communication*)). *Offered Services* refers to assessments of instances where realization of offered services is stated as purpose for information collection (e.g., processing of *Payments*). The two remaining tier-2 content assessment aspects record cases where *Technical Details* (e.g., *Session Management*) or *Public Welfare* (e.g., secondary use for *Educational* purposes) are given as rationale for information collection.

Handling of Information is refined through five tier-2 content assessment aspects: *Recipients* represents stated information sharing practices (e.g., if user-entered information is shared with *Other Users*). *Retention* is comprised of content assessment aspects of stated information retention practices (e.g., retention according to *Legal Requirements*). The content assessment aspect *Security Measures* records statements regarding measures taken to ensure information security. Assessments regarding *Security Measures* remain however quite general (e.g., use of *Backup*

mechanism) since technical implementation details, like the actual algorithms implemented, are not very meaningful to end-users. *Storage* groups content assessment aspects focusing on where information is stored (e.g., in the *Cloud*). *Write Access* captures statements regarding who can insert, update, and delete user-entered information (e.g., the *User*).

Offered Privacy Controls is refined through seven tier-2 content assessment aspects: *Access Audit* captures whether users are offered means for reviewing at which time who assessed what parts of their information. *Breach Notification* records statements regarding notifications in case of privacy infringements (e.g., when the breach occurred (*Occurrence of Breach*)). *Change Notification* represents statements concerned with how users will be informed about modifications of the privacy policy (e.g., whether *Users* are *Notified-by-Mail). Dispute Resolution* and *Dispute Remedy* reflect statements on offered courses of action for resolving disputes regarding the privacy policies (e.g., through an *Independent Organization*) and remedies offered for justified user objections (e.g., *Monetary* remedies). *Privacy Policy Limits* captures whether the privacy policy addresses its boundaries like entities covered by the targeted privacy policy. *User Access* groups content assessment aspects of how users can access information collected on them (e.g., *Information Collected by the Application*).

To capture more detailed information and stated privacy practices, content assessment aspects are assigned attributes, as applicable. Attributes are basically sets of more detailed assessments or of possible manifestations of privacy practices. Figure 1 depicts all used attributes in dashed boxes, possible values they can be set to, and the content assessment aspects to which they are assigned. In total eight different attributes are used to facilitate more detailed assessments of how content aspects are addressed. Three attributes (*Addressed*, *Collecting Modules*, and *Scope*) are used for more detailed assessments of privacy policies content aspects, beyond binary assessments

of addressed/not-addressed. The remaining five attributes (*Access*, *Collected*, *Employed*, *Notification*, and *Protection*) capture stated privacy practices. *Access* is, for instance, assigned to the User Access sub-content aspects and records the permissions (e.g., view, correct, delete, and/or download) users have for accessing information contributed by them, collected by the provider, or collected by a third party (e.g., an advertising network). *Collected* is the most frequently used attribute and captures whether information collection or a certain privacy practice is mandatory, optional, or not performed. Multiple attributes can be assigned to a single content aspect. The sub-content assessment aspects of Recipients (e.g., Advertiser or Public) are, for instance, assigned the attributes *Collected* and *Protection*. *Protection* assesses how information is protected by data recipients: A third party receiving information can, for example, be bound by the same privacy policy as the provider, their own privacy policy (recipients), or an own privacy policy that does not yield lower protection than the providers' privacy policy (not-lower).

Evaluation of PPC

We evaluate PPC's utility and comprehensiveness through application to 62 privacy policies of most-frequently rated mHealth apps. With a score of ι=0.94, inter-rater reliability assessment with Janson's and Olsson's ι leads to an "almost perfect"(Landis and Koch 1977) agreement. The content assessment shows that content provided in all assessed mHealth app privacy policies can be covered by content aspects of PPC. This indicates a high degree of comprehensiveness of PPC's privacy policy content aspects and implies that PPC is a suitable assessment instrument for comprehensiveness of privacy policy content.

Our assessment results reveal that privacy policies of mHealth apps are in a bad state of health and unlikely to provide sufficient information addressing privacy concerns. Due to page limitations, we can only give a short overview of our assessment results. The 62 privacy policies

fail to address many content aspects. While the high-level top tier content assessment aspects insinuate coverage of content aspects in over 85% of assessed privacy policies, deficiencies of mHealth app privacy policy content are revealed through traversal of the content assessment aspect hierarchy. For instance, some content aspects, like *Sensors*, *Write Access*, and *Dispute Resolution*, are only addressed by less than a fifth of discovered privacy policies. Furthermore, no privacy policy addresses whether users are enabled to audit accesses to their information (*Access Audit*), whether and how they are informed about breaches of privacy (*Breach Notification*), or what remedies are offered to rectify or compensate for justified user objections (*Dispute Remedy*). A further major deficiency is that privacy policies only seldom state what practices are not implemented and what information is not collected so that users' are left in uncertainty with respect to the unaddressed aspects. In short, current privacy policies of mHealth apps are unsuitable to achieve their objective of informing users about privacy practices.

DISCUSSION AND CONCLUSION

PPC is an assessment instrument that supports holistic, comprehensive, and structured assessments of privacy policy content. Application of PPC to assess privacy policy content of 62 mHealth apps shows utility of PPC and demonstrates comprehensiveness of PPC's privacy policy content aspects. In terms of the eight components of the design theory specification framework by Gregor and Jones (2007), PPC contributes to design theory on assessment of privacy policy content as follows: PPC focuses on the information offered by privacy policy content, other aspects like comprehensibility are beyond the scope of PPC. The main constructs employed are statements, content assessment aspects, attributes and privacy practices. Privacy policies consist of statements that convey privacy practices carried out by the respective information system or its provider. Content assessment aspects capture the results of assessments. Attributes are employed, as

applicable, to refine content assessment aspects and capture manifestations of privacy practices. Principles of form and function are characterized by the hierarchical and modular design of PPC. Top-level content assessment aspects are refined through more detailed, disjunct lower-level content aspects. Thus, analysis of content assessments aspects on the top-levels offers an overview of assessment results and allows for identification of results warranting more detailed attention. Subsequently, results can be explored in more detail through traversal of the hierarchy. Consideration of artifact mutability is reflected in the hierarchical design allowing for flexibility and adaption of PPC to individual research scopes and domains as well as to incorporate content assessment aspects reflecting relevant technologies, techniques, or threats to privacy emerging in the future. The kernel theory guiding PPC design is the tripartite model of privacy introduced by Tavani and Moor (2001). Accordingly, the main testable proposition is that PPC supports assessments of privacy policy content comprehensiveness in the context of online IT offerings. We test this proposition by demonstrating PPC's utility and sufficiency as assessment instrument through application of PPC to privacy policies of mHealth apps.

Practical contributions of PPC design and development are support of privacy policy development and identification of deficiencies in offered privacy policies. With respect to users, PPC aids in selecting those offerings that fit users' information privacy needs and preferences by facilitating comparisons of individual privacy policies and stated privacy practices: User organizations or users themselves could apply PPC to privacy policies of IT offerings and establish a repository of privacy policy content assessments allowing for comparisons of privacy practices between alternative IT offerings. In addition, through application and evaluation of PPC, we reveal an insufficient current state of mHealth app privacy policy content. This finding highlights the need

for future research and improvement of offered privacy policy content so that privacy policies actually make privacy practices transparent.

In order to sufficiently reduce privacy-related user concerns through privacy policies, content offered in privacy policies must comprehensively offer the information users are looking for. The multifarious, context-dependent nature of privacy makes identification, provision, and assessment of comprehensive privacy policy content a challenging task. PPC addresses this issue, builds on extant research, achieves flexibility and adaptability through a modular, hierarchical design, and constitutes an assessment instrument for privacy policy content. PPC facilitates assessments for privacy policy content and is thus useful for supporting and guiding future efforts towards provision of comprehensive privacy policies that are actually of use to users.

ACKNOWLEDGEMENTS

We would like to thank Kenneth D. Mandl, Harvard Medical School, and Patrick L. Taylor, Harvard Law School, for their helpful comments and advice on clarity and comprehensiveness of the privacy policy content aspect catalogue.

REFERENCES

Ackerman, M. S., Cranor, L. F., and Reagle, J. 1999. "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences," *Proceedings of the 1st ACM Conference on Electronic Commerce*, Denver, USA, November 03-05, 1999, pp. 1–8.

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

Antón, A. I., Earp, J. B., and Young, J. D. 2010. "How Internet Users' Privacy Concerns Have Evolved Since 2002," *IEEE Security & Privacy* (8:1), pp. 21–27.

Apple. 2014. "Apple iTunes App Store," (available at https://itunes.apple.com/us/genre/ios/id36?mt=8; accessed September 26, 2014).

Carrión, S. I., Fernández-Alemán, J. L., and 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), p. e114.

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

Council of the European Communities. 1995. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data," *Official Journal L281 of 11/23/1995*, pp. 31–39.

Cranor, L., Dobbs, B., Egelman, S., Hogben, G., Humphrey, J., Langheinrich, M., Marchiori, M., Presler-Marshall, M., Reagle, J., Schunter, M., Stampley, D. A., and Wenning, R. 2006. "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification," November 13 (available at http://www.w3.org/TR/2006/NOTE-P3P11-20061113/; accessed September 26, 2014).

Dehling, T., Gao, F., Schneider, S., and Sunyaev, A. 2014. "Exploring the Far Side of Mobile Health – Information Security and Privacy of Mobile Health Applications on iOS and Android," *Journal of Medical Internet Research mHealth and uHealth*, doi:10.2196/mhealth.3672.

Earp, J. B., Antón, A. I., Aiman-Smith, L., and Stufflebeam, W. H. 2005. "Examining Internet Privacy Policies within the Context of User Privacy Values," *IEEE Transactions on Engineering Management* (52:2), pp. 227–237.

Federal Trade Commission. 2013. "Mobile Privacy Disclosures: Building Trust through Transparency," Federal Trade Commission, (available at http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf; accessed September 26, 2014).

Google. 2014a. "Google Play App Store," (available at https://play.google.com/store/apps; accessed September 26, 2014).

Google. 2014b. "Android Developer Reference: Permissions," Manifest.permission | Android Developers (available at http://developer.android.com/reference/android/Manifest.permission.html; accessed September 26, 2014).

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

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

Health on the Net Foundation. 2010. "Operational Definition of the HONcode Principles," May 14 (available at http://www.hon.ch/HONcode/Webmasters/Guidelines/guidelines.html; accessed September 26, 2014).

Hruschka, D. J., Schwartz, D., St.John, D. C., Picone-Decaro, E., Jenkins, R. A., and Carey, J. W. 2004. "Reliability in Coding Open-Ended Data: Lessons Learned from HIV Behavioral Research," *Field Methods* (16:3), pp. 307–331.

Istepanian, R. S. H., Jovanov, E., and Zhang, Y. T. 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), pp. 405–414.

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

Khalid, H., Shihab, E., Nagappan, M., and Hassan, A. 2014. "What Do Mobile App Users Complain About? A Study on Free iOS Apps," *IEEE Software*, doi:10.1109/MS.2014.50.

Lämmel, R., and Pek, E. 2013. "Understanding Privacy Policies - A Study in Empirical Analysis of Language Usage," *Empirical Software Engineering* (18:2), pp. 310–374.

Landis, J. R., and Koch, G. G. 1977. "The Measurement of Observer Agreement for Categorical Data," *Biometrics* (33:1), pp. 159–174.

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., and 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), pp. 755–776.

McDonald, A. M., Reeder, R. W., Kelley, P. G., and Cranor, L. F. 2009. "A Comparative Study of Online Privacy Policies and Formats," *Privacy Enhancing Technologies*, Berlin-Heidelberg: Springer, pp. 37–55.

Milne, G. R., and Culnan, M. J. 2002. "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys," *The Information Society* (18:5), pp. 345–359.

Miltgen, C. L., and 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), pp. 103–125.

Moor, J. H. 1997. "Torwards a Theory of Privacy in the Information Age," *ACM SIGCAS Computers and Society* (27:3), pp. 27–32.

Myers, M. D., and Venable, J. R. 2014. "A Set of Ethical Principles for Design Science Research in Information Systems," *Information & Management* (51:6), 801-809.

Reagle, J., and Cranor, L. F. 1999. "The Platform for Privacy Preferences," *Communications of the ACM* (42:2), pp. 48–55.

Rindfleisch, T. C. 1997. "Privacy, Information Technology, and Health Care," *Communications of the ACM* (40:8), pp. 92–100.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989–1016.

Steinhubl, S. R., Muse, E. D., and Topol, E. J. 2013. "Can Mobile Health Technologies Transform Health Care?" *Journal of the American Medical Association* (310:22), pp. 2395-2396.

Sunyaev, A., Dehling, T., Taylor, P. L., and Mandl, K. D. 2014. "Availability and Quality of Mobile Health App Privacy Policies," *Journal of the American Medical Informatics Association*, doi:10.1136/amiajnl-2013-002605.

Tavani, H. T. 2007. "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy," *Metaphilosophy* (38:1), pp. 1–22.

Tavani, H. T., and Moor, J. H. 2001. "Privacy Protection, Control of Information, and Privacy-enhancing Technologies," *ACM SIGCAS Computers and Society* (31:1), pp. 6–11.

United States Congress. 1974. "Privacy Act of 1974," *Pub. L. 93–579, 88 Stat. 1896, 5 U.S.C. ch. 5 § 552a* (available at http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf, accessed September 26, 2014).

Venable, J., Pries-Heje, J., and Baskerville, R. 2012. "A Comprehensive Framework for Evaluation in Design Science Research," *Proceedings of the 7th International Conference on Design Science Research in Information Systems*, Las Vegas, USA, May 14-15, 2012, pp. 423–438.