USEFUL PRIVACY POLICY CONTENT - RESEARCH OUTLINE AND FIRST RESULTS

Research in Progress

Gao, Fangjian, University of Cologne, Germany, gao@wiso.uni-koeln.de
Dehling, Tobias, University of Cologne, Germany, dehling@wiso.uni-koeln.de
Sunyaev, Ali, University of Cologne, Germany, sunyaev@wiso.uni-koeln.de

Abstract

Mobile health (mHealth) applications (apps) can offer a variety of functionality to support users in health- and medical-related issues. However, users’ privacy concerns impede users’ willingness to share information. This reduces the potential benefits (e.g., chronic disease management, medical intervention support, or medication management) that can be gained from mHealth apps. Our research aims to identify useful privacy policy content that can address users’ privacy concerns before, during, and after the use of mHealth apps. By consolidating privacy concerns and requirements from extant standards, research, and guidelines, we develop a privacy content catalogue containing 121 potentially useful privacy policy content aspects. After analyzing privacy policy content of 600 widely-used iOS and Android mHealth apps, we identify an insufficient status quo of extant privacy policies provided on the current mHealth app market. As next steps, we will implement a Real-Time Delphi study and conduct focus groups to evaluate and revise our content catalogue. With our research, we aim to improve the utility of mHealth app privacy policies for app users, and assist app providers in providing privacy policies addressing users’ concerns.

Keywords: mHealth, Mobile Health, Application, App, Privacy, Privacy Policy, Privacy Notice.

1 Introduction

mHealth is a subset of eHealth (Mechael, 2009). Istepanian et al. define mHealth as “mobile computing, medical sensor, and communications technologies for health care” (Istepanian et al., 2004). mHealth has the potential to alleviate global health burdens due to rising dissemination of smartphones and other mobile devices, standardized and easy access to cloud or internet services, and the possibility of cheap global deployment of apps (Anthes, 2012; d’ Heureuse et al., 2012; Muñoz, 2010). mHealth apps can offer a variety of functionality requiring access to different kinds of information and supporting patients in different ways. mHealth apps provide for instance functionality for weight management, tracking of medication regimens, physician patient communication, management of chronic diseases, or support of medical interventions.

Since mHealth apps have access to sensitive, private health information, a focus on information security and privacy is warranted (Dehling and Sunyaev, 2014). Patients deem access to health information and related services beneficial; however, they are concerned with security and privacy issues and want to control access to their information (Pyper et al., 2004; Simon et al., 2009). Information security and privacy concerns impede patients’ willingness to share information (Bélanger and Crossler, 2011) and thus also the potential benefits that can be gained from mHealth apps (Sunyaev and Chorny, 2012). mHealth apps can only offer more general services or cannot be used at all if users are not willing to share their health information, for instance, with personal health records.
Privacy policies for mHealth apps have the potential to alleviate such concerns, if designed with sufficient quality; they can be used to convey the privacy practices (e.g., collection, use, and sharing of information) of mHealth apps (Jensen and Potts, 2004; Kelley et al., 2009; Milne and Culnan, 2004). In practice, the content offered by privacy policies is unspecific, does not fit users’ actual use of the app, and users are often confused with technical terms (Kelley et al., 2009; Pollach, 2007). Moreover, privacy policies are often designed as legal safeguards to protect providers from lawsuits instead of properly informing users about mHealth app privacy practices (Kelley et al., 2009).

In this paper, we focus on privacy policy content provided for mHealth apps. Our research is guided by the research following question: What useful content should be provided by mHealth app privacy policies so that app users can be informed of app privacy practices? In the context of this paper, privacy policy content is considered as useful if it is able to address users’ mHealth-related privacy concerns before, during, and after use of the related mHealth app. In order to answer the research question, we consolidate privacy concerns and requirements addressed in extant literature, and gather expert and user opinions to identify, revise, and evaluate useful privacy policy content for mHealth apps. In addition, we assess app privacy policies to shed some light on the status quo of privacy policies provided on the current mHealth app market.

The reminder of this paper is structured as follows: Section 2 provides an overview of our research approach. Section 3 presents the preliminary research results. Afterwards, our next research steps are described in Section 4. Finally in Section 5, this paper is concluded with research contributions, suggestions for future research, and potential implications.

## 2 Research Approach

We employ a four-step procedure to derive useful content for mHealth app privacy policies. Figure 1 illustrates our research process in which the four steps are represented as rectangles, and the related input(s) and output of each step as ovals. By now, Step 1 and Step 2 have been completed. Step 3 and Step 4 are in progress. To the best of our knowledge, there is no consensus regarding the content that should be provided by privacy policies to address users’ privacy concerns. Hence, as an initial step (Step 1), we identify potentially useful content aspects by investigating privacy policy standards, extant research, and privacy guidelines (Ackerman et al., 1999; Antón et al., 2010; Carrión et al., 2012; Cranor et al., 2006; Federal Trade Commission, 2012; Health on the Net Foundation, 2010; Federal Trade Commission, 2013). After reviewing and consolidating privacy concerns or requirements addressed in the identified literature, we develop an initial content catalogue containing concrete potentially useful content aspects for mHealth privacy policies.

![Schematic representation of research approach.](image-url)
In Step 2, we assess the privacy policies of 600 widely-used mHealth apps based on the content catalogue from the previous step. Our analysis objects are privacy policies of English language mHealth apps offered in the iOS (itunes.apple.com) as well as Android app store (play.google.com). Apple’s iOS and Google’s Android operating system are becoming the de facto global platforms for mobile Health (d’Heureuse et al., 2012; Istepanian et al., 2004). We start with discovering apps from the Medical and Health & Fitness categories offered in both stores. Then we exclude discovered apps that were not available in English, did not have an English description, or were not health-related (e.g., apps offering wallpapers). During app discovery, we noticed that the app stores offer different information on apps, including apps’ download count or rating count. Download count and rating count are indicators for apps’ success and thus can be used to gauge whether apps are widely-used (d’Heureuse et al., 2012). However, download count information is not available for iOS apps. Thus, we review the rating count information of the discovered apps and select the 300 most-frequently rated mHealth apps from each of the app stores (in total 600 apps). Afterwards, we try to obtain privacy policies of the selected mHealth apps. We use a three-step manual procedure for privacy policy discovery looking for typical locations of privacy policies. First, we check for a privacy policy on the app store web site for the particular app. Then, we check developer’s web page used to advertise and introduce her company and products. Finally, we review the first 30 results of a Google search for the query ‘$APPNAME “privacy” “policy”’. Once a privacy policy is found, we omit the remaining steps.

We discovered that the content of obtained privacy policies could be limited to a 1) ‘single app’, apply to 2) ‘multiple apps’, or pertain to a 3) ‘backend web application’ supporting the app(s), 4) ‘developer homepage’, 5) ‘all developer services’, or seemingly 6) ‘app-unrelated topics’. Accordingly, we defined the six enumerated scope categories, which are mutually exclusive. The definitions of the scope categories are presented in Table 2. Two researchers separately assessed each obtained privacy policy to classify it into one of the six scope categories based on its content scope. Privacy policies that did not focus on a single app, multiple apps, or the related backend web application are unlikely to offer mHealth-app-related useful content for users and thus excluded from the further content assessment. Afterwards, the two researchers separately reviewed and assessed the content of the remaining mHealth privacy policies. By employing the initial privacy policy content catalogue, they assess what parts of the potentially useful privacy policy content aspects from the content catalogue are actually provided by the reviewed mHealth app privacy policies.

To ensure reliability of assessment results, we evaluate the inter-rater agreement of the two researchers. The inter-rater agreement is measured with Janson’s and Olsson’s $\gamma$, a multivariate extension of Cohen’s $\kappa$ for multiple judges on the same scale (Janson and Olsson, 2001). The resulting $\gamma$ value ($\gamma$=0.94) shows that the two researchers reach an “almost perfect” (Landis and Koch, 1977) agreement level. Afterwards, conflicts are resolved through group discussion.

<table>
<thead>
<tr>
<th>Privacy Policy Scope</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single app</td>
<td>Privacy policy focuses explicitly on the provided single mHealth app.</td>
</tr>
<tr>
<td>Multiple apps</td>
<td>Privacy policy focuses on a group of (similar) apps including the provided mHealth app.</td>
</tr>
<tr>
<td>Backend web application</td>
<td>Privacy policy focuses on a backend web application which belongs to or supports the provided mHealth app.</td>
</tr>
<tr>
<td>Developer homepage</td>
<td>Privacy policy focuses only on the app developer’s or provider’s homepage.</td>
</tr>
<tr>
<td>All developer services</td>
<td>Privacy policy focuses on general services offered by the app provider. The provided mHealth app and/or the app-related services are not explicitly addressed in the privacy policy.</td>
</tr>
<tr>
<td>App-unrelated topics</td>
<td>Privacy policy does not address the provided mHealth app, the app-related services or webpage, or any other services offered by the app provider.</td>
</tr>
</tbody>
</table>

Table 2. Definitions of Privacy Policy Scope Categories.
Table 3. Content categories and exemplary privacy policy content aspects for mHealth apps.

<table>
<thead>
<tr>
<th>Privacy Policy Content Category</th>
<th>Examples of Contained Privacy Policy Content Aspects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to sensor data</td>
<td>Network location; GPS location; Finger print</td>
</tr>
<tr>
<td>Data recipients</td>
<td>Government; Third party analyst; Parties authorized by user</td>
</tr>
<tr>
<td>Data retention</td>
<td>No retention; Retention for stated purpose; Retention based on legal requirement</td>
</tr>
<tr>
<td>Data storage location</td>
<td>On smartphone or tablet; In app provider storage; In the cloud</td>
</tr>
<tr>
<td>Dispute remedies</td>
<td>Rectification of errors; Monetary compensation; Remedies according to law</td>
</tr>
<tr>
<td>Dispute resolution</td>
<td>Through customer service; Through independent organization; Through court</td>
</tr>
<tr>
<td>Employed security measures</td>
<td>Password protection; Backup mechanism; Data transfer encrypted</td>
</tr>
<tr>
<td>Entities with write access to user data</td>
<td>App user; App provider; Third parties</td>
</tr>
<tr>
<td>Functionality that collects information</td>
<td>Modules that collect certain data; Modules that do not collect data</td>
</tr>
<tr>
<td>Kind of information collected</td>
<td>Health-related information; Location information; Demographic information</td>
</tr>
<tr>
<td>Notification of breaches of privacy policies</td>
<td>Nature of breach; Remedial steps to be taken</td>
</tr>
<tr>
<td>Notification of changes of privacy policy</td>
<td>Notification per mail; Notification on next app access; No notification</td>
</tr>
<tr>
<td>Purpose for data collection</td>
<td>Service delivery; Advertising; App administration</td>
</tr>
<tr>
<td>Scope and limits of privacy policy</td>
<td>Limits addressed; Limits partially-addressed; Limits not-addressed</td>
</tr>
<tr>
<td>User access to access audit</td>
<td>Users always have access; Users currently do not have access; Users currently do not and will never have access</td>
</tr>
<tr>
<td>User access to information collected on him</td>
<td>Access to user uploads and entries; Access to data collected by app; Access to data collected by a third party</td>
</tr>
</tbody>
</table>

As next steps, we will refine the initial privacy policy content aspects. In Step 3, we will revise the content catalogue based on expert opinions. Our purpose is to determine, what parts of the privacy policy content aspects derived in Step 1 are regarded to be useful according to opinions of experts from mHealth-related domains. The useful privacy content aspects selected by the experts will be collected with a consensus content catalogue. Moreover, we aim to address additional potentially useful privacy policy content aspects suggested by the experts and, if necessary, add them into the consensus content catalogue. Finally (in Step 4), we will evaluate the content catalogue determined in the previous Step 3. We will conduct focus groups (Krueger, 1998) to identify what parts of privacy policy content aspects in our content catalogue are actually deemed useful by app users. The focus groups will concentrate on the opinions of mHealth app users. The concrete implementation of Step 3 and Step 4 is described in more detail in section ‘Useful Privacy Policy Content for mHealth apps’.

3 Results

Consolidation of privacy policy content addressed in privacy policy standards, extant research, and privacy guidelines resulted in a catalogue of 16 content categories, which are listed in the left column of Table 3. Each category consists of 1 to 35 privacy policy content aspects and, in total, 121 privacy policy content aspects are identified for the privacy policy content catalogue. Examples for privacy policy content aspects contained in each category are also illustrated in Table 3.

After reviewing 600 widely-used iOS and Android mHealth apps, we discovered that, in total, only 31% (N=183) of the reviewed apps had privacy policies. On the other hand, iOS mHealth apps were more likely to have privacy policies than Android mHealth apps (38.7% vs. 23.3%, Chi Sq p<0.001). Assessment results of privacy policy content reveal that plenty of potentially useful privacy content aspects (e.g., third parties in category entities with write access to user data, camera in category access to sensor data, and all aspects in category notification of breaches for privacy policies) derived
from privacy policy standards, research, and guidelines are not provided in the reviewed privacy policies at all. On the other hand, some derived privacy policy content aspects are found unlikely to be useful within the scope of mHealth apps. Examples for such privacy policy aspects are gambling in category purpose for information collection, and political in category kind of information collected.

4 Useful Privacy Policy Content for mHealth apps

As described, we aim to refine derived potentially useful privacy policy content aspects in the next two steps. For Step 3, we plan to conduct a Real-Time (RT) Delphi study (Gordon and Pease, 2006) to consolidate expert opinions. RT Delphi is a variant of conventional Delphi. Conventional Delphi is a widely-used tool for applications like forecasting, estimation, or decision making (Green et al., 2011; Landeta, 2006). We chose RT Delphi for Step 3 due to its high efficiency. In contrast to conventional Delphi, RT Delphi does not involve sequential rounds so that its time efficiency can be increased (Gordon and Pease, 2006). Moreover, RT Delphi can simultaneously support asynchronous and synchronous participation in Delphi studies, and offers instant feedback to participants through automation and a web interface.

The potentially useful privacy policy content aspects derived from the previous two research steps (Step 1 and Step 2) will serve as initial input for the RT Delphi study. Each content aspect has a description which defines and explains this content aspect. In addition, each content aspect is assigned with a descriptor that represents the whole content aspect with a short label (e.g., ‘storage local’ for content aspect local on smartphone or tablet in category data storage location). Participants can view all privacy policy content aspects including their descriptions and descriptors. Participants are asked to rate the usefulness of all identified potentially useful content aspects on a Likert scale from one to seven (not useful (1) to very useful (7)). Moreover, participants can also vote on the threshold that determines whether content aspects are included into the resulting consensus privacy policy content catalogue. As soon as a participant has rated a privacy policy content aspect, real-time statistics about ratings as well as the resulting consensus content catalogue are automatically calculated. If a participant’s rating deviates to a certain degree from consensus, she is asked to justify her rating by adding a comment to the rated privacy policy content aspect. Participants can revise their ratings at any time during the RT Delphi phase. Revisions result in automatic reselection of the privacy policy content aspects for the consensus content catalogue.

If participants are missing some privacy policy content aspects for mHealth apps, they can propose additional content aspects. Like the initial privacy policy content aspects, the proposed content aspects will also be rated by all participants. Moreover, participants are also allowed to prompt other raters (more precisely: an anonymous group of raters with the same opinion) for justification of their ratings, ask other participants for clarification of their justification (comments), and comment on other participants’ comments. In this way, we aim to gain additional output from our RT Delphi implementation since the arguments for different positions are also valuable products of RT Delphi (Gordon and Pease, 2006).

To the best of our knowledge, there is no ready-to-use software for RT Delphi that meets our requirements. Therefore, we are developing a free, open-source online application to realize our RT Delphi study. Our development is guided by the theory of tailorable technology design presented by Gemonprez et al. (2007), which enables participants to personalize the application during the RT Delphi study (e.g., participants can edit content descriptions, change descriptors through voting, and personalize their system settings like notification preferences). Afterwards, we will invite experts from mHealth-related domains to take part in our RT Delphi study. The experts include but are not limited to medical professionals, information security and privacy researchers, software developers (health IT and computer science), legal experts, and app end users.
In Step 4, we will evaluate the consensus privacy policy content catalogue resulting from our RT Delphi study. We will conduct focus groups to consolidate user opinions on the consensus content catalogue. Broadly speaking, there are two different user types for applications in Health-IT – patients and healthcare professionals / administrators (Varshney et al., 2013). Our focus groups will concentrate on patients because patients are usually concerned with privacy issues and want to control access to their information (Pyper et al., 2004; Simon et al., 2009). The goal of focus groups is to elicit a range of opinions regarding a certain object of investigation by collecting qualitative data (Krueger, 1998). Focus groups are deemed suitable for Step 4 because they facilitate learning more about app users’ impressions on as well as elicitation of their ideas for improvement of the privacy policy content catalogue resulted from our RT Delphi study. Topic Guide and Questioning Route are two commonly used focus group strategies (Krueger, 1998). In comparison to the Topic Guide, the Questioning Route is a more structured strategy consisting of several types of questions asked in a fixed arrangement. Since it quickly provides precise answers and is easy to analyze, we will employ the Questioning Route strategy. The concrete questions for focus groups will be designed based on the results of the previous Step 3.

5 Discussion and Conclusion

In this paper, we present a research in progress that aims to identify useful privacy policy content for mHealth apps. In other contexts, previous studies have already revealed an insufficient situation of extant online privacy policies regarding their availability, readability, or compliance with relevant regulations (e.g., Sheehan, 2005; Jensen and Potts, 2004; Kelley et al., 2009; Pollach, 2007). Our preliminary research results are consistent with results obtained from these studies. The results show an insufficient status quo of the provided privacy policies for the 600 widely-used iOS and Android mHealth apps. Only less than one-third of the 600 apps were found to have privacy policies, in spite of that the Federal Trade Commission (Federal Trade Commission, 2013) recommends app developers to provide privacy policies for mobile apps. In addition, mHealth apps that have privacy policies are suffering from a low quality regarding the provided privacy policy content. More than two-third of the reviewed privacy policies do not focus on the provided app, the app-related multiple apps, or its backend web application. Therefore, the content provided by current privacy policies is unlikely to address users’ privacy concerns about mHealth apps. The above-mentioned findings stress the importance of our future work. In our next steps, we will consolidate expert as well as user opinions to refine our initial privacy policy content aspects.

By providing useful privacy policies that address users’ privacy concerns, mHealth app providers tend to earn more trust from app users; the more trust app users have in an mHealth app, the more likely they are to keep using the app or to recommend it to others (Liu et al., 2005). However, it is surprising that many extant mHealth app privacy policies do not address app users’ privacy concerns and can thus hardly be regarded as useful for app users, as highlighted by our research results. One of the reasons for this phenomenon might be due to a different understanding and thus definition of useful privacy policy content for users between app providers and app users. In future work, researchers could identify the useful privacy policy content for app users from the provider’s perspective. By comparing the identified useful privacy policy content from the provider’s perspective to our research results, researchers could address gaps between the two different perspectives.

Our research can make contributions to both practice and theory. On the practical side, we highlight deficiencies of current mHealth app privacy policies and offer insights on how to make the content of privacy policies a better fit to the needs of mHealth app users. With the identified useful privacy policy content, we also aim to increase the transparency of providers’ privacy practices for app users. Moreover, our work can be used as a foundation for further research like development of industry standards for mHealth privacy policies.
On the theoretical side, our research results can be used by future work to better understand information privacy from the IS perspective. Smith et al. (2011) proposed a macro model – the Antecedent → Privacy Concerns → Outcomes (APCO) model – to provide a concise overview of the relationships between information privacy and other constructs. The APCO model focuses on individuals’ privacy concerns and explains what the antecedents and outcomes of privacy concerns are. An antecedent of privacy concerns is individuals’ privacy awareness (Smith et al., 2011). Privacy awareness reflects the extent to which an individual is informed about organizational privacy practices (Malhotra et al., 2004; Phelps et al., 2001). However, since the APCO model is an overarching model, it does not describe in detail what factors can and how they will influence individuals’ privacy awareness. Our work addresses this gap by focusing on how privacy policies can be used to make privacy practices transparent to users. Our results can serve as foundation for further research aiming at understanding and explaining of privacy awareness. For instance, further research could develop a theory for explaining and predicting privacy awareness (Type IV theory, Gregor, 2006). Such theories could develop explanatory factors and hypotheses to clarify what (privacy policy content) aspects and how these aspects will influence mHealth app users’ privacy awareness. Since we particularly focus on incorporating users’ needs and preferences in our research, our privacy policy content aspects can serve as foundation for deriving such explanatory factors and hypotheses.

mHealth apps are able to support users in health- and medical-related issues; however, users’ high privacy concerns impede potential benefits that can be gained from mHealth apps. mHealth app privacy policies with useful content will address users’ privacy concerns and thus facilitate the use of mHealth apps.

References


Gao et al. / mHealth App Privacy Policy Content


