An Information Privacy Risk Index for mHealth Apps

Thomas Brüggemann[1], Joel Hansen[1], Tobias Dehling[2], and Ali Sunyaev[2]

[1] University of Cologne, Albertus-Magnus-Platz 1, 50931 Köln, Germany
mail@thomasbrueggemann.com, joel.hansen@pass-on.de
[2] University of Kassel, Mönchebergstraße 19, 34109 Kassel, Germany
tdehling@uni-kassel.de, sunyaev@uni-kassel.de

Abstract. While the mobile application (app) market, including mobile health (mHealth) apps, is flourishing, communication and assessment of information privacy risks of app use has, in contrast, found only cursory attention. Neither research nor practice offers any useful and widely accepted tools facilitating communication and assessment of information privacy risks. We conduct a feasibility study and develop a prototypical instantiation of an information privacy risk index for mHealth apps. The developed information privacy risk index offers more detailed information than privacy seals without suffering from the information overload and inconsistent structure of privacy policies. In addition, the information privacy risk index allows for seamless comparison of information privacy risk factors between apps. Our research adds to the transparency debate in the information privacy domain by illustrating an alternative approach to communication of information privacy risks and investigating a promising approach to enable users to compare information privacy risks between apps.

Keywords: information privacy, risks, mhealth, mobile health, privacy enhancing technologies, usable privacy

1 Introduction

In recent years, the growth of the consumer electronics market has seen a boost through the introduction of smartphones and tablet computers [17]. More and more users are now installing a variety of different applications (apps) on their mobile devices [2]. Among those apps are apps offering information and consultation on medication and other health-related topics [9] making mobile health care (mHealth) possible [17, 18]. mHealth apps allow users, for example, to monitor health-related issues, understand specific medical conditions, or to achieve fitness goals [2]. By entering private and personal health information (e.g., medication intake, disease history, or blood values), users often expose sensitive personal information when using mHealth apps [14, 18, 19]. In return, users receive a tailored app experience offering relevant health-related information and functionality [11]. In the past, personal health information was managed and stored solely in hospitals. Today, it is also collected and managed by mHealth apps and over the internet. Therefore, it is critical to protect users' personal information in order to reduce information privacy risks [17, 18].

The risk to users is that personal health-related information can be misused [30]. Due to the fast growth of the mHealth app market, it is increasingly difficult to assess information privacy risks for each individual mHealth app [9]. Moreover, app providers offer only sparse and vague information on how personal user information is treated or stored. Users have to rely on privacy policies or information privacy seals [7] to acquire relevant information about privacy risks of mHealth apps. But privacy policies lack a standardized format [2], are typically written in formal legalese [23] and hard to understand for the majority of users [25]. Privacy seals aim at providing information about security and privacy of web services by issuing certificates [7]. Privacy seals fail at communicating details about the actual information privacy risks to users [7] and may not have an effect on user information disclosure at all [15]. Consequently, it is challenging for users to evaluate processing of their information by mHealth apps and to compare different apps with respect to information privacy before or while using mHealth apps. The required privacy information is either not available, hidden in legal language or not comprehensible for an averagely educated person [10].

We conduct a feasibility study on how to communicate information privacy risks in a clearer and more detailed way than privacy policies or privacy seals do. We identify six information privacy risk factors by downloading mHealth apps from the iOS and Android app stores and surveying them with respect to their information privacy risks. The six information privacy risk factors concern the input of personal information, sharing targets of collected personal information, a secure data connection, the ability to login to an app, use of analytics and advertising, and reasonableness of information collection [1]. The information privacy risk factors help to communicate the information privacy risks of individual mHealth apps to users more efficiently [26] and to improve the comparability between apps with respect to information privacy. We combine the information privacy risk factors into a factor weight equation [27] and represent the resulting information privacy risk score in a prototypical instantiation of a graphical user interface. The information privacy risk score and the graphical user interface are designed to enable users to better comprehend information privacy risks across multiple apps by providing a standardized communication medium for information privacy risk factors [22].

2 Communication of Information Privacy Risks

Privacy risks in the mHealth app context have been subject to various studies. Privacy risk assessment has been studied from different angles and various attempts were made to communicate privacy risks to users [2]. As users expose sensitive personal information when using mHealth apps [24], there is a vital need for accurate communication of information privacy risks. Currently, app providers' information privacy practices are predominantly communicated via their privacy policies.

The content of privacy policies of mHealth apps has been analyzed and evaluated, revealing that many popular apps do not provide privacy policies useful to users. The availability of privacy policies for mHealth apps has improved in recent years, but privacy policies are still difficult to comprehend for an averagely educated audience [10]. Users often agree to the privacy policies of popular apps on a basis of common trust [29] because reading them is highly time consuming [21]. Such user behavior does not foster user comprehension and understanding of information privacy risks, instead, it promotes exactly the opposite. Privacy seals represent an alternative approach, but can be misinterpreted. Users conclude, for instance, that a privacy seal indicates a high protection of personal information without paying attention to the service characteristics actually certified [20]. As a result, users may prefer web sites of providers featuring a privacy seal, even though there is no difference in privacy protection. Consequently, privacy seals can promote situations where users are misled in comparisons of online offerings with respect to information privacy risks. Even though studies have developed suggestions for enhancement [16, 23], privacy policies and privacy seals cannot be considered effective tools for communication of information privacy risks of mHealth apps to users.

Other studies identified information privacy risks by downloading the apps. With this approach, information privacy risk factors, such as an insecure data transfer, geographic location and phone identifier leakage were identified [1, 14, 5, 4, 3, 6]. These information privacy risk factors are mostly of a technical nature. Although the identification of information privacy risks has been enhanced through this procedure, attention to communication of identified information privacy risks is limited. In our study, we take a step further by downloading a sample of mHealth apps and identifying as well as analyzing information privacy risk factors of these apps. As a new and promising approach for communication of information privacy risks to users, we develop an information privacy risk index that communicates information privacy risk scores for mHealth apps through a publicly accessible graphical user interface.

3 Development of the Information Privacy Risk Index

Our study is based on a dataset of the 300 most often rated apps from the Google PlayStore and the 300 most often rated apps from the Apple AppStore in the app store categories 'Medical' and 'Health & Fitness'. Since our research approach requires the installation of the apps on our mobile devices, we excluded all apps not available free of charge (124 apps). The free apps are potentially more prone to information privacy violations than paid apps: The revenue model of free apps is often built around displaying personalized advertisements to users based on collected user information [1]. We downloaded every app available to our smartphones and identified six information privacy risk factors based on the

Table 1. Personal information that had to be entered in the apps in our survey clustered in categories and assigned with their factor scores for the information privacy risk index equation

Category	Members of Category	Factor Scores
Medication intake	Pills / recipes, medication dosage	0.147
Vital values	Blood pressure, heart rate, blood sugar, blood values etc.	0.147
Diseases	Kind of disease	0.118
Symptoms	All acute, chronic, relapsing or remitting symptoms. For example: mood changes, rashes, swellings	0.118
Life status specs	Pregnancy, lifestyle (activity), smoking habits	0.106
Address	Country, state, street	0.088
Body specs	Weight, height, body frame, body fat, temperature etc.	0.082
Family	Medical condition of children or ancestors, family size	0.059
Medical appointments	Date, doctor	0.053
Food intake	Calories, diet plan, drinks	0.035
Workout / Activities	goals, steps, distance covered / GPS tracking	0.029
Personality test	Questions about own behavior in certain situations	0.012
Sleep metrics	Sleep sound, dream description	0.006

resulting dataset and the information privacy risk factors proposed by Ackerman [1] and He, Dongjing, et al. [14].

3.1 Identification of Information Privacy Risk Factors

To identify information privacy risk factors and assess all apps in our dataset, we used a four-step procedure: First, we read the description of the app inside the app store to identify possible information privacy risks. App descriptions were assessed for indicators of information-privacy-related input fields. Second, we inspected the screenshots offered in the app store. The screenshots indicate information requested from users by showing text input fields for user information (e.g., medication intakes, disease history, blood values). Third, we downloaded the apps to our smartphones and used them. During app use, we checked the data transfer with the web debugging proxy application *Charles Proxy*[3]. *Charles Proxy* visualizes the HTTP connections the app uses and allows for the identification of data transfers between the app and third parties. Fourth, in an optional step, we read the privacy policy or terms of service to obtain information about the use of personal information. This step was only conducted when a data transfer displayed in the web debugging proxy application remained unclear.

[3] https://www.charlesproxy.com, visited 02/09/2016

Information Sharing Targets (T): We refer to information sharing targets as the target or host destination to which apps send users' personal information. Personal information can be sent directly to the app provider, research projects, social networks, analytics tools and marketing agencies [2]. Some apps may offer data storage and syncing on app providers' remote servers, which leads to a potential information privacy risk for users since, from the user perspective, the data vanishes on a non-traceable and non-retrievable remote server [2, 14].

Personal Information Types (P): During app assessment, we extended the types of personal information input continuously as required. In total, we identified thirteen types of personal information input relevant for our research scope (see Table 1). For the sake of brevity, we only outline the most critical categories below. 'Life status specs' refer to user inputs revealing details about users' lifestyle (e.g., information about a pregnancy or smoking habits). Personal information inputs labeled 'medication intake' capture the amount and kind of medication consumed by the user. 'Vital values' represent health measurements (e.g., blood metrics or heart rate). 'Diseases' and 'Symptoms' are each assigned to single self-explanatory categories that represent the input of disease and symptom information [2, 14]. The types of personal information inputs listed in Table 1 are limited to information inputs required by apps in our dataset. However, the personal information inputs align with the types of mHealth data inputs described by Kumar et al. [19].

Login (L): Furthermore, we distinguished between two assessments for login information. If a login is required [2], a user either has to register via a username or an email address, or otherwise via a social network login (e.g., Facebook). In the case that no login is required, apps were assessed with the value 'none'.

Connection Security (S): We classified data transfers as either an unencrypted or an encrypted HTTP data transmission. In case of an encrypted connection, we could only suspect, which data is actually being transferred.

Unspecific Information Transfer (U): We tested with the proxy application whether apps used click tracking analytics tools or contacted advertisement servers to display advertisement banners. We listed those findings under the information privacy risk factor 'Unspecific Information Transfer'. Due to encryption, we could not assess what personal information is being exchanged with these target hosts and whether transmitted information poses a threat to information privacy.

Reasonable Information Collection (R): For each identified personal information input, we coded the reasonableness of collection of personal information as a binary assessment. Some apps collected, for example, personal information that is not noticeably used by the app so that information collection seems fraudulent.

3.2 Calculation of the Information Privacy Risk Score

Based on the assessments of all apps in our dataset, we developed an algorithm for calculating an information privacy risk score that assigns each app with an information privacy score on a scale between 0.0 and 1.0. A privacy score of 0.0

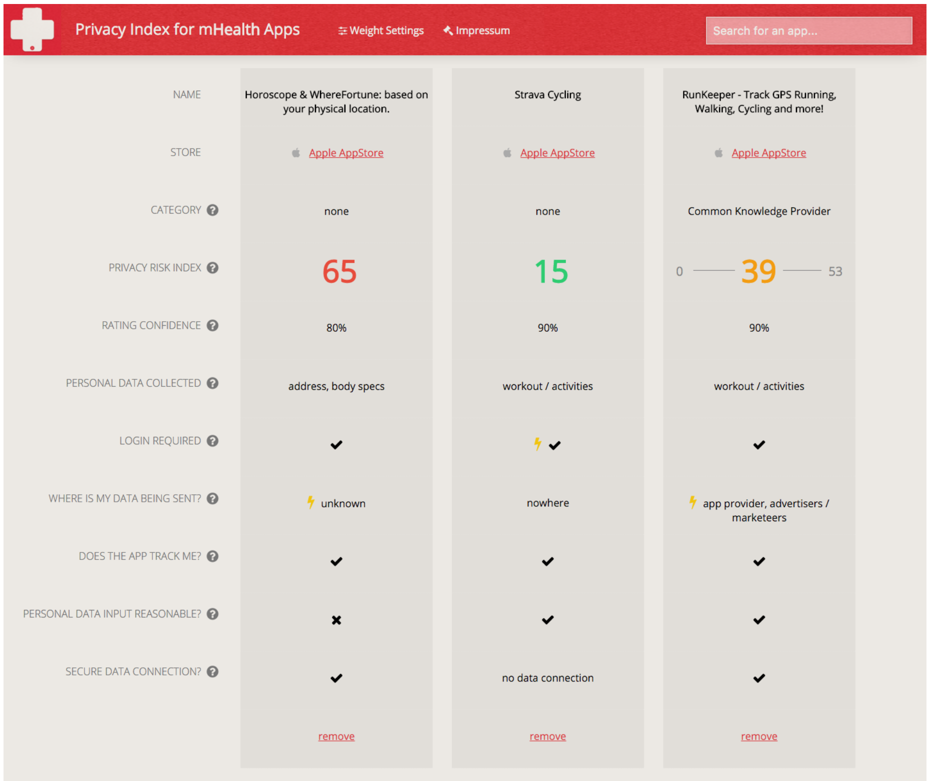
indicates that the app poses no information privacy risk according to our app assessment. A privacy score of 1.0 on the other hand represents a strong information privacy risk. The information privacy risk score is the result of a factor weight equation based on the six information privacy risk factors we identified during app assessment. Triantaphyllou et al. [27] promote the use of a factor weight equation[4] as a decision making support tool. A factor weight equation is a suitable foundation for the information privacy risk index because the information privacy risk index serves as a decision support tool for app users. Additionally, using a simple factor weight equation makes the method of calculating the information privacy score comprehensible for possible future end-users. We determined default weights for the information privacy risk factors based on the risk assessment weights that Ackerman [1] proposed. Usually the reliability and validity of measures (such as the weights in our factor weight equation) are determined in research under controlled laboratory conditions [19]. To remedy this, the prototypical implementation of the information privacy risk index allows users to either use the default weights or to set their own weights [13].

$$\begin{aligned} PrivacyRiskScore_{App} = T_{App} * w(T) + P_{App} * w(P) + \\ L_{App} * w(L) + S_{App} * w(S) + U_{App} * w(U) + R_{App} * w(R) \end{aligned} \tag{1}$$

where: T = Information Sharing Targets, P = Personal Information Types, L = Login, S = Connection Security, U = Unspecific Information Transfer, R = Reasonable Information Collection, w(T)+w(P)+w(L)+w(S)+w(U)+w(R) = 1

Scoring Model After setting the weights for each information privacy risk factor, we developed the scoring models for each individual information privacy risk factor. For the binary information privacy risk factors connection security (S), unspecific information transfer (U) and reasonable information collection (R) no further scoring is necessary. As a special case, the information privacy risk factor connection security (S) will only be set to 1.0, if the connection is unencrypted and personal information is transmitted and the encryption of the connection is of no relevance [19]. For the information privacy risk factor information sharing targets (T), we assigned default scoring values based on our discussion of relative importance in contribution to information privacy risks of mHealth app use. These values can be freely adapted by users. The scoring model for the information privacy risk factor personal information types (P) is slightly more elaborate. A single app can ask for multiple categories of personal information input and the scoring model would need to sum up the scores for each existing category to calculate the final score for personal information types (P). In total, we identified 13 types of personal information input but the maximum number of personal information input types identified for a single app was 5. This would lead to a single app never reaching the maximum score of 1.0. To remedy this, a correction factor is applied to the final privacy risk score.

[4] The factor weight equation, as we call it, is often also referred to as the weighted sum model. We decided to us the term factor weight equation because our algorithm distinguishes between factor and weight variables.



NAME	Horoscope & WhereFortune: based on your physical location.	Strava Cycling	RunKeeper - Track GPS Running, Walking, Cycling and more!
STORE	Apple AppStore	Apple AppStore	Apple AppStore
CATEGORY	none	none	Common Knowledge Provider
PRIVACY RISK INDEX	65	15	0 — 39 — 53
RATING CONFIDENCE	80%	90%	90%
PERSONAL DATA COLLECTED	address, body specs	workout / activities	workout / activities
LOGIN REQUIRED	✓	⚡ ✓	✓
WHERE IS MY DATA BEING SENT?	⚡ unknown	nowhere	⚡ app provider, advertisers / marketeers
DOES THE APP TRACK ME?	✓	✓	✓
PERSONAL DATA INPUT REASONABLE?	✗	✓	✓
SECURE DATA CONNECTION?	✓	no data connection	✓
	remove	remove	remove

Fig. 1. Three apps have been selected and are listed in the comparison table view

3.3 Graphical User Interface

The information privacy risk assessment was complemented with a graphical user interface that enables users to make easy assessments of the information privacy risks that an app poses and seamlessly compare the information privacy risk factors of multiple apps. With the graphical user interface, users can get a fast overview about information privacy risks of individual mHealth apps and make a quick decision about selection and use of mHealth apps without having to read complicated privacy policies. The graphical user interface consists of two main views. Initially users are presented a weighting view in which the weights of all information privacy risk factors can be customized. Custom weights are stored in a client side cookie. The second view is the main apps table view. Inter-comparability between apps is achieved by listing the app rating results in a table view next to each other (see Figure 1).Via a search bar, apps can be added to the table view. As soon as apps are added to the table view, information on the information privacy risk factors is displayed. Hovering a table view cell displays a small, black pop-up area offering detailed information on the respective information privacy risk factor. A little yellow bolt icon in front of a table view cell indicates the information privacy risk factor that has the most influence on the information privacy risk score of that app. The information privacy risk score itself is the large, color-coded (green, orange, red) number, which ranges from 0 to 100. This way the user can, in addition to understanding the number value of the information privacy risk score, compare the selected apps with just the glimpse of an eye, by looking at the colors. A click on the score value reveals a detailed view on how the information privacy score calculation was conducted. Dehling et al. [11] proposed the idea of clustering apps by assessments of potential damage through information security and privacy infringements into archetypes. If an app of our dataset is clustered within an archetype, the information-privacy-risk-score cell also displays the numbers of the lowest and highest privacy risk score apps from this archetype. These numbers are clickable in order to add the highest and lowest information privacy risk score apps to the table view. This creates an easy to use, fast and responsive graphical user interface, allowing users to customize the view with instantaneous reaction times [22] and tailor the graphical user interface to their needs [12]. Our graphical user interface is available to the public (https://privacy-risk-mhealth.herokuapp.com) and serves as a first step towards providing a comparison view on apps from the app stores with respect to their information privacy risks.

4 Findings

During the assessment of all 476 apps from our initial dataset, 178 apps were not available for download on the app stores. This reduced our dataset to 298 apps, 147 iOS and 151 Android apps. No apps in our sample have direct data transfers to research project hosts (or host names that we could identify as belonging to research projects) and research data use is only mentioned in three privacy policies. Two apps have data connections to social networks. 63 apps send personal information directly to the app provider. 27 apps potentially sent personal information to advertisers or marketing companies. The data connections potentially transferring personal data established a secure and encrypted HTTP connection within 42 apps, while 28 apps did not encrypt the data connection at all. In 228 cases, we could not identify whether the data connection was encrypted or the app did not send any data at all. 28 apps in our sample request personal information without noticeably using it. 105 apps request personal information and use it to tailor the app experience to users' preferences and needs. 165 apps require no information input at all. 51 apps require a login via username and password or a social media account (e.g., Facebook, Twitter, Google) in order to be able to use the application or to tailor the app experience to the preferences and needs of the individual user.

Figure 2 shows a histogram of the distribution of information privacy risk scores we calculated for all apps, multiplied by 100 and rounded to the next integer value on the x-axis. The y-axis shows the amount of privacy risk scores in a certain cluster range. The histogram clusters index-values in increments of 5 and clearly shows that the majority of privacy risk scores are below 10. There are

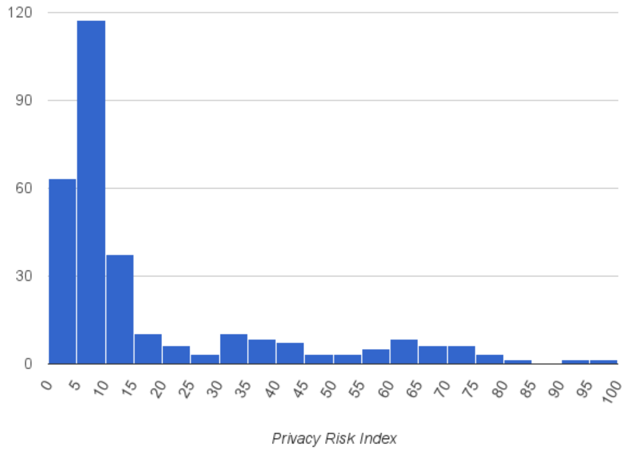


Fig. 2. Histogram of the information privacy risk score distribution

fewer apps with information privacy risk scores above 15. We see two increases in information privacy risk scores at values of 30 to 35 and 60 to 65.

5 Discussion

Our study revealed some interesting findings. 21% of the apps in our dataset collecting personal information collect it without any noticeable use for it. Privacy-attentive apps should only collect information actually used by the app to provide the app functionality or tailor the app to user preferences and needs. Otherwise, information collection appears fraudulent and leaves a negative overall impression of the app. 40% of the apps in our dataset transfer personal information without encryption. Even though use of a secure, encrypted data connection is not visible to users, a secure data connection should always be used by mHealth apps to guarantee confidentiality and integrity of personal data [14, 17]. A reason for the high number of low information privacy risk scores (Figure 2) is the amount of apps that do not collect health information, but rather provide meditation sounds or medical dictionaries.

Overall, our publicly available information privacy risk index demonstrates the feasibility of providing users with an simple-to-use tool to establish an overview of information privacy risks of mHealth apps and compare information privacy risk factors between apps. This constitutes a valuable contribution right between extant approaches that either yield only very general information (i.e., privacy seals) or provide too much information in an inconsistent way impeding information retrieval (i.e., privacy policies). Future research can make use of our feasibility study and develop tools and frameworks to further enhance communication and assessment of information privacy risks.

To scale up app assessment, future research can focus on automating app assessments. For automated app assessments, apps could be automatically downloaded from the app stores, the source code could be decompiled and user inputs and app information handling could be traced within the source code. This would most likely be more feasible for Android apps, due to strict download regulations of the Apple AppStore. To circumvent such issues, the app survey process may be integrated into the app stores by the store providers themselves. The inclusion of the information privacy risk index by app providers bears the risk that information privacy risk factors may not be sufficiently included in the survey of the app stores. Future research could focus on the necessary ruleset to ensure that app providers or other instances include and implement a complete and thorough information privacy survey, for instance, as proposed by the 'Data protection impact assessment' of article 33 of the General Data Protection Regulation [8]. Our concept for a simple information privacy risk communication can also be expanded by considering implications on other important parties such as policy makers and consumer advocates. In this context, future research could also address the development of business models regarding information privacy risk assessment and information privacy risk communication.

Our research has some limitations. We were limited mainly in the tracking of personal information transfers. If we were actually able to track what information is transferred, the precision of mHealth app information privacy risk assessments could be improved. Moreover, 178 apps in our dataset were already removed from the app stores and not available for download. And the dataset included several apps of app providers that only differ in their names but not in their functionality (e.g., meditation sound apps). Even though we still examined a large amount of apps, a larger dataset without the redundant apps could be more beneficial for future research. A user study to evaluate the information privacy risk index prototype was not conducted since it exceeded the scope of our study. Lastly, we only examined free apps due to budget restrictions. Future research could also study the information privacy risks of paid apps.

Nevertheless, this study demonstrates the feasibility of an information privacy risk index more informative than privacy seals and better structured than privacy policies. The prototypical instantiation of the information privacy risk index illustrates its utility to obtain an easy-to-use overview of the information privacy risks of mHealth apps and compare information privacy risk factors between different apps. Our research investigates one potential approach to ease the process of selecting the right app out of the overload of mHealth apps available to users [28]. Users can retrieve processed information about information privacy risks of mHealth apps, which increases transparency of information privacy risks of mHealth apps [30]. Consequently, the information privacy risk index can, on the one hand, reduce uncertainty of information use by mHealth apps. On the other hand, the information privacy risk index empowers individual users to make better informed decisions about selection and use of mHealth apps.

References

[1] Linda Ackerman. "Mobile Health and Fitness Applications and Information Privacy". In: *Privacy Rights Clearinghouse, San Diego, CA* (2013).

[2] Rajindra Adhikari, Deborah Richards, and Karen Scott. "Security and Privacy Issues Related to the Use of Mobile Health Apps". In: *Proceedings of the 25th Australasian Conference on Information Systems, 8th - 10th December, Auckland, New Zealand.* ACIS, 2014.

[3] Hazim Almuhimedi et al. "Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging (CMU-ISR-14-116)". In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (2014).

[4] Gökhan Bal, Kai Rannenberg, and Jason Hong. "Styx: Design and Evaluation of a New Privacy Risk Communication Method for Smartphones". In: *ICT Systems Security and Privacy Protection.* Springer, 2014, pp. 113–126.

[5] Gökhan Bal, Kai Rannenberg, and Jason I Hong. "Styx: Privacy Risk Communication for the Android Smartphone Platform Based on Apps' Data-Access Behavior Patterns". In: *Computers & Security* 53 (2015), pp. 187–202.

[6] Rebecca Balebako et al. "Little Brothers Watching You: Raising Awareness of Data Leaks on Smartphones". In: *Proceedings of the Ninth Symposium on Usable Privacy and Security.* ACM. 2013, p. 12.

[7] Patricia Beatty et al. "P3P Adoption on E-Commerce Web Sites: A Survey and Analysis". In: *IEEE Internet Computing* 11.2 (Mar. 2007), pp. 65–71. ISSN: 1089-7801. DOI: 10.1109/MIC.2007.45.

[8] EC European Commission. "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)". In: *COM (2012) 11 final, 2012/0011 (COD), Brussels, 25 January 2012* (2012).

[9] Rocío de la Vega and Jordi Miró. "mHealth: A Strategic Field Without a Solid Scientific Soul. A Systematic Review of Pain-Related Apps". In: *PloS One* 9.7 (2014), e101312. ISSN: 1932-6203.

[10] Tobias Dehling, Fangjian Gao, and Ali Sunyaev. "Assessment Instrument for Privacy Policy Content: Design and Evaluation of PPC". In: *Proceedings of the Pre-ICIS Workshop on Information Security and Privacy.* AIS, Dec. 2014.

[11] Tobias Dehling et al. "Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android". In: *JMIR mHealth and uHealth* 3.1 (2015).

[12] Matt Germonprez, Dirk Hovorka, and Fred Collopy. "A Theory of Tailorable Technology Design". In: *Journal of the Association for Information Systems* 8.6 (2007), pp. 351–367. ISSN: 1536-9323.

[13] Russell E. Glasgow and William T. Riley. "Pragmatic Measures: What They Are and Why We Need Them". In: *American Journal of Preventive Medicine* 45.2 (2013), pp. 237–243. ISSN: 0749-3797.

[14] He, Dongjing, et al. "Security Concerns in Android mHealth apps". In: American Medical Informatics Association, 2014.

[15] Kai-Lung Hui, Hock Hai Teo, and Sang-Yong Tom Lee. "The Value of Privacy Assurance: An Exploratory Field Experiment". In: *MIS Quarterly* (2007), pp. 19–33.

[16] Patrick Gage Kelley et al. "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach". In: *SIGCHI Conference on Human Factors in Computing Systems, New York, NY, USA*. CHI '10. ACM, 2010, pp. 1573–1582. ISBN: 978-1-60558-929-9. DOI: 10.1145/1753326.1753561.

[17] Jong Tak Kim et al. "Security of Personal Bio Data in Mobile Health Applications for the Elderly". In: *International Journal of Security and Its Applications* 9.10 (2015), pp. 59–70. ISSN: 1738-9976.

[18] David Kotz. "A Threat Taxonomy for mHealth Privacy". In: *3rd International Conference on Communication Systems and Networks*. IEEE, Jan. 2011. ISBN: 1-4244-8952-0. DOI: 10.1109/COMSNETS.2011.5716518.

[19] Santosh Kumar et al. "Mobile Health Technology Evaluation: The mHealth Evidence Workshop". In: *American Journal of Preventive Medicine* 45.2 (2013), pp. 228–236. ISSN: 0749-3797.

[20] Robert LaRose and Nora Rifon. "Your Privacy Is Assured - of Being Disturbed: Websites With and Without Privacy Seals". In: *New Media & Society* 8.6 (2006), pp. 1009–1029.

[21] Aleecia M. McDonald and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies". In: *A Journal of Law and Policy for the Information Society* 4 (2008), pp. 540–565.

[22] Jonathan W. Palmer. "Web Site Usability, Design, and Performance Metrics". In: *Information Systems Research* 13.2 (2002), pp. 151–167. ISSN: 1047-7047.

[23] Irene Pollach. "What's Wrong With Online Privacy Policies?" In: *Communications of the ACM* 50.9 (2007), pp. 103–108.

[24] Andrew J. Rohm and George R. Milne. "Just What the Doctor Ordered: The Role of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern". In: *Journal of Business Research* 57.9 (2004), pp. 1000–1011.

[25] Ali Sunyaev et al. "Availability and Quality of Mobile Health App Privacy Policies". In: *Journal of the American Medical Informatics Association* 22.e1 (2015). PMID: 25147247, e28–e33. ISSN: 1067-5027. DOI: 10.1136/amiajnl-2013-002605.

[26] Herman T. Tavani. "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy". In: *Metaphilosophy* 38.1 (2007), pp. 1–22. ISSN: 1467-9973.

[27] Evangelos Triantaphyllou et al. “Multi-Citeria Decision Making: An Operations Research Approach”. In: *Encyclopedia of Electrical and Electronics Engineering* 15 (1998), pp. 175–186.

[28] Lex van Velsen, Desirée Beaujean, and Julia van Gemert-Pijnen. “Why Mobile Health App Overload Drives Us Crazy, and How to Restore the Sanity”. In: *BMC Medical Informatics and Decision Making* 13.1 (2013), p. 1. ISSN: 1472-6947.

[29] Ran Yang, Yu Jie Ng, and Arun Vishwanath. “Do Social Media Privacy Policies Matter? Evaluating the Effects of Familiarity and Privacy Seals on Cognitive Processing”. In: *Proceedings of the 48th Hawaii International Conference on System Sciences*. Washington, DC, USA: IEEE Computer Society, 2015, pp. 3463–3472. ISBN: 978-1-4799-7367-5.

[30] Fatma Zubaydi et al. “Security of mobile health (mHealth) systems”. In: *Proceedings of the 15th IEEE International Conference on Bioinformatics and Bioengineering (BIBE)*. 2015, pp. 1–5.