The Differences in Data Sensitivity Perceptions among Private and Workplace Health Apps: A Delphi Study

Maren Billmann
Department of Informatics
Technical University of Munich
Garching, Bavaria, Germany
maren.billmann@web.de

Jens Grossklags
Department of Informatics
Technical University of Munich
Garching, Bavaria, Germany
jens.grossklags@in.tum.de

Markus Boehm
Department of Informatics
Technical University of Munich
Garching, Bavaria, Germany
markus.boehm@in.tum.de

Helmut Krcmar
Department of Informatics
Technical University of Munich
Garching, Bavaria, Germany
krcmar@in.tum.de

ABSTRACT

Data are crucial for tailoring health apps to personal needs. Nonetheless, a users' privacy and security need to be preserved, particularly since health technologies are able to gather a broad range of data over a long time period. In order to guarantee an appropriate level of security and privacy, the perceptions of end users need to be evaluated to enhance adoption of the technologies. In this paper, we conduct a Delphi study to gain insights into the perception of certain data elements used in popular health apps. As health apps are now commonly used both privately and at the workplace, both are compared in this study. As input for the Delphi study, an exploratory market analysis has been utilized. Our work reveals a mismatch between the perception of sensitivity of data and the usage rate of common health apps. Additionally, variations have been identified between the private and corporate health context, providing implications for both practice and theory.

CCS CONCEPTS

• Information systems~Mobile information processing systems • Security and privacy~Privacy protections

KEYWORDS

mHealth, Perceived data sensitivity, Workplace health, Delphi study

DPH' 19, November 20–23, 2019, Marseille, France.
© 2019 Copyright is held by the owner/author(s). Publication rights licensed to the Association for Computing Machinery.
This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in Proceedings of 9th International Digital Public Health Conference (DPH'19), November 20–23, 2019, Marseille, France. ACM, New York, NY, http://dx.doi.org/10.1145/3357729.3357741.
ACM ISBN 978-1-4503-7208-4/19/11…$15.00.

ACM Reference format:

Maren Billmann, Jens Grossklags, Markus Boehm, Helmut Krcmar. 2019. The Differences in Data Sensitivity Perceptions among Private and Workplace Health Apps: A Delphi Study. In *Proceedings of 9th International Digital Public Health Conference (DPH'19), November 20–23, 2019, Marseille, France.* ACM, New York, NY. https://doi.org/10.1145/3357729.3357741

1. INTRODUCTION

Health app business developers utilize various types of data to provide comprehensive and personalized support to their customers. In principle, the more meaningful data elements are gathered, the more sophisticated an app can be [1, 2]. Through the addition of attractive functionalities, users are enticed to provide different kinds of data, including data that are perceived to be sensitive by users. These data include, for instance, demographic information, but also automatically gathered data using in-app permissions without users' direct input. Additionally, sensitive health data is typically requested (whether collected via sensors or by user input) [3]. This rather broad collection of data might violate the perceived privacy of users, because it is often impossible for users to control data collection and usage of data. For example, data elements that are not required for the functionality of an app might be gathered and shared with third-party entities [4, 5]. At the same time, potential privacy and security measures established by the providers are not meaningfully communicated to the end user [6]. The incomplete knowledge of users on how data is being processed, is exacerbated by the low attention of the users to permissions, due to the large number of requests for data access; leading to a state known as notice-and-consent or warning fatigue [7]. Introducing effective privacy measures and ways to communicate these measures to end users are, therefore, key to protect individuals.

In order to evaluate which privacy measures are appropriate for certain types of data, data sensitivity perception of individual data elements needs to be determined to complement the generic

implementation of security standards. Categorization of data is already available for sensitive data on a regulatory level. For instance, the European Commission (EC) defines in its General Data Protection Regulation (GDPR) personal data and certain measures to ensure data privacy and security for this type of data. However, it is unclear to which extent this categorization reflects the data sensitivity perceptions of end users with respect to health data and thus whether adhering to such regulations leads to more confidence of the end-user in the handling of data. Additionally, it has been suggested that the context and information about the health app provider (or brand) might have an influence on the perception of privacy [8, 9], but this has not yet been studied in detail. For instance, one study evaluated the willingness to share data for electronic medical records and revealed that willingness to share differs among various types of recipients of the data. It revealed that there is not even one recipient type with whom all participants would share all data [10]. Additionally, a recent study among older participants showed differences of sharing preferences according to the type of recipient of data as well as among different demographic characteristics of the individuals, e.g., age or education [11].

Due to its popularity for public health, mHealth has also started to be used for workplace health promotion (WHP) [12]. Compared to other forms of WHP, apps are advantageous due to their non-dependence on location and 24-hour availability, which enables the integration of private and work life. Additionally, directly tailored feedback and self-monitoring through real-time tracking and visualization of progress are appreciated by many users [13]. In a workplace with a diverse workforce, it is further considered as a cost-effective option due to its possibility to personalize and integrate various (niche) programs [14]. Potential differences in the perception of privacy and security between these contexts however ought to be considered [15]. Unique characteristics of the workplace, such as the limited number of potential participants, peer pressure, and trust in the employer as well as perceived data usage, might further influence data privacy perception and trust in the app. As perceived data sensitivity has an influence on the acceptance of mobile health applications (mhealth) and willingness to share data [16], the perception of data sensitivity of individual data elements needs to be studied in various contexts.

However, at present, there is a lack of knowledge about users' willingness to share and the perception of sensitivity of specific data elements and permissions in health apps. Most studies only measure perception of data security and privacy in general, but do not evaluate the differences among the individual data elements [17]. This knowledge could, however, be used by app developers to limit sensitive data usage or communicate effectively on the handling of these perceived sensitive data. As a result, users would have more trust in the app providers and might even increase usage as they are capable to make an informed decision. Due to the fact, that trust of employees is an essential value for companies, the perception of data sensitivity in the workplace is particularly crucial.

Hence, the aim of this study is to determine which of the data elements common in popular health apps are perceived as sensitive and to compare private-use and WHP apps. To this end, the following research question is asked: **Which data elements and permissions are considered as sensitive in the context of health apps used privately and in the workplace?**

We proceed as follows. In Section 2 more background on data privacy in mHealth is given. Following that, the used methods and results of the study are described in detail in Sections 3 and 4. At last, the results are discussed and set into context of its methodological limitations as well as previous studies. The paper closes with a conclusion section.

2. DATA PRIVACY IN MHEALTH

Due to the sensitivity of health data and the increase in the number of data elements included in health technology, data privacy is becoming increasingly important and needs more attention [18], particularly for apps that gather comprehensive data, including the continuous tracking of various parameters over a long period of time (e.g., nutrition intake, location tracking, physical activity, social interactions) [19]. Additionally, the lack of transparency of data usage for the user is further enlarged, because data is likely handled by stakeholders other than the app provider or medical staff. Apart from these challenges, users are often not sufficiently educated about the gathered data, privacy and security measures, making it difficult for the end user to foresee data security and privacy consequences [6]. A survey study reports that 68% of the respondents were worried about privacy and 69% about the security of health information. In particular, they were worried about identity theft, embarrassment, and financial loss [20].

However, studies also show that there is a paradox between the perception of data and the actual usage. People are troubled about data usage, while these concerns are not fully reflected in observable behavior or behavioral change [8, 9]. Behavioral intention and actual behavior are thus deviating. Several studies studied the phenomenon of the so-called privacy paradox and tried to find explanations. One is that through distraction users are not consciously evaluating a given decision-making situation; instead an affective reaction is caused [21, 22]. Furthermore, warning fatigue is argued to lead to acceptance of data usage without an informed decision-making deliberation [7]. For example, in a study on Android permissions, it was shown that customization of warnings could potentially be effective, as the concerns about permissions and data usage have different underlying reasons [7]. Therefore, understanding the perceptions of individual users about certain data elements and permissions is key to improve user-directed communication.

As such, knowledge about data awareness and perceptions of security and privacy ought to be emphasized more in the future [23]. Such detailed knowledge might further trigger changes on the developers' side, which could eventually lead to a higher

uptake and trust of health apps, leading potentially to positive health effects. Even though data sensitivity seems to be directly related to behavior, often studies do not investigate underlying sub-constructs of sensitivity [4, 16]. Additionally, research has not focused on differences between individual data elements or permissions, but rather evaluates very general types of perceptions in various situations.

Also, the workplace needs to be considered separately, especially as users might perceive certain data elements differently when giving them to their employers. A study has demonstrated the mediating role of trust in the provider regarding the association between perceived personalization and privacy concerns on acceptance intention [2]. This means, users who have increased privacy concerns often seem not to trust providers. On the other hand, if users perceive a higher degree of personalization, they seem to trust a provider more [2]. Jimenez et al. further explain that in the workplace sector, experts strive to gain insights into the workforce and potential focus areas for future WHP. But, on the other hand, they need to consider potential violations of trust due to the misuse of the provided information [15]. In order to maximize functionality, while enhancing perceived privacy, an identification of data elements that are perceived to be sensitive and a detailed categorization are necessary.

3. METHODS

A Delphi design was applied to evaluate the perceived sensitivity of commonly used data elements and permissions in health apps while comparing the private and WHP settings. As a basis for the Delphi study the most frequently requested data elements and permissions in health apps as determined by an exploratory market analysis were used. Additionally, experts on workplace health and data security were consulted to create a realistic scenario for the users.

3.1 Market analysis

An exploratory market analysis of health apps used by German end users was carried out, focusing on **data elements and permissions** requested by those health apps. It included privately used apps and WHP apps. More specifically, we evaluated the most popular mobile applications in the two largest Android and iOS app stores. Regarding the analysis of privately used apps, we downloaded the 30 most popular apps in the category Health & Fitness' in the iOS app store and the Google Play store for Android. Only apps available in Germany were considered. However, English-language apps were included if they were popular in the German app stores. In the second step, both app stores were searched for WHP apps. Since no specific category exists for this area, search terms were defined (E.g., workplace health or "Betriebliches Gesundheitsmanagement" [German]). All apps that were free of charge and were not otherwise restricted were downloaded. When downloading the app, the permissions required were documented. These permissions are requested in Android apps at the time of download (for versions older than 6.0). In Android Versions 6.0 or newer, and also in iOS, permissions are requested when they are required for the first time [24]. In order to cover all permissions required during the usage, an older Android version was used. After installation and during initial usage, requested data elements were documented. If needed, user profiles were created to use the apps and analyze the data contained therein. Only data elements requested when using the app for the first time were in the scope of the analysis. Requested data elements that occurred at later points of time were outside the scope of our study. All results were summarized in a data analysis file, and the frequency of usage of specific data in health apps was calculated. The most frequently requested data and permissions were included in the Delphi study.

3.2 Delphi Methodology

The Delphi methodology is used to reach group consensus without biases resulting from group discussions and interpersonal influences [25]. In this study, the Delphi methodology was executed in two independent groups (one for the private app context and one for WHP app context), with 20 different German working adults in each group. Participants were asked to rank all data elements requested in popular health apps according to their perceived sensitivity. In order to not influence the decision of participants, no definition of sensitivity was given. The approach thus simulates the practical adoption of an app from a personal perspective. Apart from gathering knowledge on first impressions about data sensitivity of individual data items, as quantitative research would do, the Delphi method adds information about the degree of certainty of the categorization based on the stability of the answers of the users. Additionally, qualitative comments gained throughout the Delphi study provide insights into the reasoning of our participants.

The first group was asked to imagine using a health app **for private use** that requires specific data elements and permissions. The apps Runtastic and Lifesum were mentioned as examples in the description. The second group was asked to imagine that their **employer** had offered them a health app. In order to make the scenario as realistic as possible, it was described that employers only receive anonymous reports on the app data. This assumption was based on an interview with a security expert of an IT company, in which the expert clarified, that health data are usually not allowed to be stored or used by employers based on German law. The same data elements and permissions were presented as in the private group. The scenarios were pre-tested, iteratively shortened and rewritten to add clarity. The first round (August 2017) was executed via an online questionnaire tool. General demographic questions were added to gain additional information about the participants' characteristics. Additionally, all data and permissions were listed and participants were asked to rank these terms according to their level of sensitivity. In the following rounds, the participants received an individual data sheet containing their own answers from the previous round, the average (AVG) ranking of the data in their group, and the associated standard deviation (SD). The meaning and

interpretation of the values were described. Users were asked to evaluate the ranking by the group, rethink their personal answers, and comment on their own ranking.

Due to the different use cases of a Delphi study, no standard measure for consensus exists [26]. In some studies, thresholds such as 50% or 75% agreement are stated. Others stop after a certain number of rounds [27]. Hence, our implicit goal at the start of the study was that 50% of the participants confirm the ranking of the group. The study was continued for three rounds until near-consensus was reached. The third round was completed in February 2018. However, it became obvious that small variations in the order would persist simply due to the high number of terms included in this Delphi study. Therefore, consensus was defined based on the comments made by the participants and the decrease of standard deviation in the groups. This is in line with other studies stating that "the moderator should stop the rounds when the criteria for consensus are achieved, when results become repetitive, or when an impasse is reached" [28].

Apart from the evaluation of the ranking, two researchers coded all comments of the participants in order to grasp individual opinions and arguments. The coding was done using agreed and predefined codes as well as codes defined during the coding. The main codes were

- Code 1: Comment arguing towards sensitivity
- Code 2: Comment arguing against sensitivity
- Code 3: General comment that did not include a concrete argument on sensitivity (e.g.: "I agree with the group)

Afterwards, the comments were coded concerning the content and predefined codes. The most prevalent codes were general accessibility, combination of data, identification, inference of other information, likelihood of misuse, and usability. For this analysis, the comments coded as 3 were excluded. The intercoder reliability was calculated for both coding steps and for each group (see Table 5). Cross-tables were created using SPSS to evaluate the comments. If disagreement concerning the coding occurred, there were discussions in order to reach an agreement.

4. RESULTS

In total, 72 apps were evaluated. 31 WHP apps and 41 general health or life-style apps were found and analyzed. Due to access restrictions (e.g., company email address, or a code were required), some WHP apps needed to be excluded.

Data elements: On average, apps requested 5.5 data elements, with 2.9 types being required/compulsory elements. The maximum number of data elements requested was 18. When comparing app groups, private apps required on average 7.0 data elements in total, whereas WHP apps only requested 3.1 types of data on average. Weight, gender, age, email address, first and last name, and height were demanded by more than 61% of the private apps.

Table 1. Data elements frequently requested in private and workplace health apps

Requested Data	Total	% Apps	WHP Apps	Private Apps
Weight	40	56%	6	34
Gender	39	55%	7	32
Age	36	51%	9	27
Email address	36	51%	11	25
First and surname	33	46%	8	25
Height	30	42%	5	25
Goals	21	30%	2	19
Calorie intake	17	24%	1	16
Steps taken per day	13	17%	3	10
Location/address	13	17%	3	10
Profile picture	12	17%	2	10
Level of fitness	10	15%	1	9
Sorts of sport	9	13%	0	9
Nickname	7	10%	5	2
Water (cups per day)	6	8%	2	4
Sleep data	5	7%	1	4
Activity during work	5	7%	1	4
BMI	5	7%	1	4
Body measurements	4	6%	1	3
Perception of stress	3	4%	3	0
Body fat	3	4%	1	2
Education & profession	3	4%	2	1
Heart Rate	3	4%	3	0
Equipment (shoes, bike)	3	4%	0	3
Contact information	3	4%	0	3
Phone number	2	3%	2	0
Relationship status	2	3%	1	1
Health interests	2	3%	2	0
Emotional status	1	1%	1	0
Step size	1	1%	0	1
Shoe size	1	1%	0	1
Income	1	1%	1	0
Blood group	1	1%	1	0
Ethnical group	1	1%	1	0

In the workplace context, a different picture emerged. Here, email address was most often requested, but only by 35% of the WHP apps. We hypothesize that this rather reserved data usage in the WHP context might be explained by more extensive control on data usage, for instance by employee representatives and the employees themselves. During the evaluation process, it became apparent that when entering the individual data elements, the app developers mostly did not give any information about how and why this information is requested or needed. Additionally, often the users did not get a chance to test or even look at the app without first agreeing to data access. When considering data elements labeled as sensitive by the GDPR [29], 60% of the private apps asked for at least four different kinds of such data (for example, age, gender, name and email address). For WHP apps, this number dropped to just above 25% of the apps. The requested data elements are shown in Table 1.

Permissions: Since detailed information about the permissions used on the app was only available for Android, we focused our analysis on this part of the overall sample. Android requires the developers to list only certain permissions in the overview for the user, leading to a high number of permissions being used but not shown to the user at the download (but listed in detail in the app store). For the evaluated Android apps, only 33% of the utilized permissions are shown to the users before the app is adopted. Usage of photos, files, media, and storage is the most common permission category. In 'others', apps nearly always request permission to use network connection and prevent the phone from sleeping. Identity, contact information, camera, WiFi connect, and location information are used by more than one-third of the evaluated health apps. No differences between WHP and private apps can be recognized in terms of which permissions were requested. However, WHP apps appear to request on average fewer permissions than private apps. Due to the low number of apps included, this was not statistically tested. However, this would be an interesting aspect for future work.

4.1 Delphi study

The data found in the most commonly downloaded health apps were considered as items for the Delphi study. However, in order to avoid overwhelming the participants with too many terms and data, some had to be excluded. In particular, data elements were excluded when they were only requested once as optional by the health apps. Additionally, some unspecific data were excluded based on users' feedback (e.g., contact information). Finally, 27 data items were included. Permissions were chosen using a similar process. For the Delphi study, only permissions presented to app users (as previously discussed) were included. All permissions and data elements were pre-tested with few employees to test for understandability and comprehensiveness of the list. Some adjustments were made upon. Afterwards, we recruited 20 participants for each group. All participants had agreed beforehand to participate in the study. All were German employees from various companies with at least one year of working experience. Demographics are listed in Table 2.

Table 2. Demographic characteristics of the participants

Group characteristics	Private	Workplace
Average age	37.1	38.1
Female (N)	10	8
Use health apps at least from time to time (N)	12	11
Average perception of health status (1-100)	79	83.75
Working for 8 or more years (N)	12	10
Do not have an academic degree (N)	5	2
Working in an IT field	8	8

For each of the two groups, 19 participants completed the whole study (in the group for private health apps one person dropped out in round 2; in the group for workplace health apps one participant dropped out in round 3). The groups can be considered as equally distributed according to the Mann-Whitney-U test for age, gender, education, profession, health app usage and perceived health (sig. values between .156 for health and .757 for age).

It took the participants three rounds to achieve near-consensus. However, changes in the ranking between the rounds were small. That is, the ranking of the permissions stood relatively stable in all three rounds, providing a clear result for sensitivity. More specifically, the standard deviation in the group using a private app dropped from 1.8 to 1.3 to 1.0 for permissions. For the requested data elements, a drop from 6.5 in the first round to 4.3 in the second round to 3.4 in the third round was identified. The standard deviation for permissions in the group for workplace health apps dropped from 1.7 to 1.3 to 1.0. For the requested data elements, the standard deviation dropped from 6.9 to 5.1, and finally to 4.2 in the last round.

In the group for private health apps in the last round, on average (based on all data elements) 41.9% gave the exact identical ranks to the individual data elements. On average 68.4% gave the rank with +/-1. For the workplace group, on average 47.1% gave the exact rank and 67.5% accepted the rank with +/-1. Since only small adjustments to the ranking were made between the second and the third round, the study was considered completed. Additionally, participants stated that they were indifferent about the exact ranks for some data elements. Some participants brought forward a broader categorization of the data elements, such as identifying data elements, health-related data, and other data. Within these categories, the ranking was argued to be less important. The final results are shown in Tables 3 and 4. In order to increase readability, both tables are ordered according to the ranking of the private group.

Inspecting the process and the final results more closely, it appears for both groups that personal data that could identify a person are ranked more sensitive than other data elements (including health data). Within the group of a WHP app, the ranking is slightly different to the private group. Name, email address, phone number, location, and profile picture held the top ranks, including all personal data. Ranks 6 and 7 in the group for workplace health apps (relationship status and emotional state) are not considered as personal data by the GDPR; however, they are perceived as sensitive.

Taken together, most of the personal data are ranked among the six most sensitive data elements in both groups. Further, and perhaps quite surprisingly, *participants ranked data elements that include identification as more sensitive compared to health data.* Only the data elements of emotional status, body measurements, and sleep data were ranked among the 10 most sensitive data elements in both groups. For the private app group, stress perception was also among the top 10. For the workplace group, weight was additionally among the top 10. The ranking of the permissions also showed differences between the groups.

Table 3. Ranking of data elements and permissions: Private group (most sensitive at the top)

Data	Difference *	Ranking	AVG	SD
First- and surname	-0.2	1	2.5	4.4
Phone number	0.7	2	3.2	3.9
Location/address	0.1	3	4.8	4.6
Profile picture	1.4	4	5.1	5.3
Emotional state	3.1	5	5.9	2.3
Email address	-3.5	6	6.3	3.4
Body measurements e.g. arm span, legs	2.5	7	7.9	1.3
Relationship status	0.5	8	8.2	4.5
Stress perception	2.2	9	8.8	3.7
Sleep data	0.2	10	9.6	3.5
Body fat	0.7	11	11.1	2.8
Education & profession	2.3	12	12.2	4.1
Calories intake	0.3	13	13.6	3.3
Weight	-3.5	14	13.9	2.1
Activity during work	3.7	15	14.5	4.4
Heart rate	2.7	16	15.0	3.7
Health goals	-2.3	17	16.1	2.1
Age	-0.5	18	17.3	3.3
Level of fitness	-1.8	19	18.1	3.3
Health interests	-1.1	20	18.6	3.1
Steps (measured using a pedometer)	3.3	21	20.4	3.5
Gender	-0.5	22	20.9	4.2
Height	-2.5	23	21.6	3.2
Nickname	-4.0	24	23.2	4.1
Sorts of sports	-0.3	25	23.2	3.1
Water intake (number of drank glasses)	-1.3	26	24.9	2.7
Equipment (e.g. shoes, bikes)	-0.4	27	25.4	2.9
Permissions				
Access to contacts	0.5	1	1.7	1.3
Access to device ID and call information	1.9	2	2.1	0.7
Access to pictures/ media/ files	-1.6	3	3.1	1.1
Access to camera	0.7	4	4.5	1.2
Connection with social media (Facebook, Twitter)	0.0	5	4.7	1.4
Access to GPS	-1.8	6	5.1	1.2
Connection to gadgets and tracking apps	0.2	7	6.7	0.4
* calculation: average of group for workplace health apps minus average of the group for private health apps				

Table 4. Ranking of data elements and permissions: Workplace group

Data	Difference *	Ranking	AVG	SD
First- and surname	-0.2	1	2.4	3.9
Phone number	0.7	3	3.9	3.1
Location/address	0.1	4	4.9	3.3
Profile picture	1.4	5	6.6	6.2
Emotional state	3.1	7	9.0	5.3
Email address	-3.5	2	2.8	3.5
Body measurements e.g. arm span, legs	2.5	10	10.5	1.9
Relationship status	0.5	6	8.7	5.0
Stress perception	2.2	11	10.9	3.9
Sleep data	0.2	8	9.8	5.6
Body fat	0.7	12	11.8	3.8
Education & profession	2.3	15	14.5	6.5
Calories intake	0.3	14	13.9	4.6
Weight	-3.5	9	10.4	2.7
Activity during work	3.7	20	18.2	4.6
Heart rate	2.7	19	17.7	5.3
Health goals	-2.3	13	13.8	3.4
Age	-0.5	16	16.9	6.3
Level of fitness	-1.8	17	16.3	2.7
Health interests	-1.1	18	17.5	3.2
Steps (measured using a pedometer)	3.3	26	23.7	1.9
Gender	-0.5	23	20.4	5.4
Height	-2.5	21	19.1	5.0
Nickname	-4.0	22	19.2	5.9
Sorts of sports	-0.3	24	22.9	2.7
Water intake (number of drank glasses)	-1.3	25	23.6	4.7
Equipment (e.g. shoes, bikes)	-0.4	27	25.1	3.6
Permissions				
Access to contacts	0.5	2	2.2	1.3
Access to device ID and call information	1.9	4	3.9	0.7
Access to pictures/ media/ files	-1.6	1	1.5	0.8
Access to camera	0.7	6	5.2	1.2
Connection with social media (Facebook, Twitter)	0.0	5	4.8	1.4
Access to GPS	-1.8	3	3.3	1.3
Connection to gadgets and tracking apps	0.2	7	6.9	0.3
* calculation: average of group for workplace health apps minus average of the group for private health apps				

Additionally, we calculated non-parametric correlations to evaluate the influence of demographics. Older participants seem to rate gender higher than younger participants (-.365; p =.044). But on the other hand, nickname (.496; p =.005) and connection to social media (.342; p =.044) seem to be ranked as less sensitive by the older participants. Differences were further found for health status. Those who perceive their health as better ranked height less and nickname more sensitive. Detailed investigations could be subject to future work.

4.1.1 Qualitative comments

Two researchers conducted the coding of the comments. Intercoder reliability is shown in Table 5. In the group for private health apps, on average 13 participants commented per data element in all three rounds.

Address/location, email address, and profile picture were commented about most often. As expected, for most data elements, more comments were given towards high sensitivity. The exceptions were gender, nickname, and connection to gadgets and tracking apps in the group for private health apps, where more arguments towards non-sensitivity were observed.

In the group for workplace health apps, the most discussed data elements were email address, weight, emotional state, calorie intake, sleep data, and stress perception. On average 10.5 comments were given per data element. In this group, more data elements were discussed controversially. Profession & education, water intake, fitness level, and health interests included an equal number of argumentations in favor and against sensitivity. Relationship status, health goals, gender, height, and nickname attracted slightly more arguments favoring high sensitivity.

Correlations were calculated for demographics and number of comments. It seems as older participants generally stated less comments (-.410; p =.010) and especially less comments against sensitivity (-.414; p =.010)

In the group for private health apps, the arguments most often mentioned were that conclusions are possible about health status (44 comments) and inferences about other data (whereas those two often occurred together). Additionally, identification (30 comments), violation of privacy (27 comments), and likelihood of misuse (14 comments) were frequently mentioned. Moreover, arguments against sensitivity of data elements were often justified with the statement that no conclusions would be possible or that data could be controlled. In the group for workplace health apps, the most often mentioned arguments towards sensitivity were that the combination of data is critical, inferences are possible, as well as identification and violation of privacy. Arguments favoring that data are less sensitive included that there is no possibility of identification and that data are already available to the employer.

When comparing the **arguments among the two groups**, some interesting differences can be reported. For instance, in the group for private health apps, gender was coded three times stating that no inferences are possible. However, in the group for workplace health apps, one mentioned that it: "Depends on the number of colleagues" [1]. The same applied for profession and education. This indicates that a smaller group of potential users seems to change the perception of data sensitivity, because inferences on identity are possible. Generally, identification was mentioned about more data elements in the group for workplace health apps, including height, body measurements and heart rate compared to the private group. One participant of the workplace group for instance stated regarding body measurements that it "can in extreme cases clearly identify a person or limit the possible group of people extremely". For heart rate, one stated the unnecessary usage for employers and possibilities of identification by saying: "[…] For me that is quite critical. What does my employer care about my pulse? Especially since this in itself is not useful information without correlation to other data such as height, weight, gender and can then suddenly but quickly identify a person."

Differences were further found on the perception of misuse. Misuse was mentioned for 10 data elements for the group for private health apps, whereas it was only highlighted for email address, access to GPS, and once for level of fitness in the group for workplace health apps, indicating a degree of trust in the employer. Interestingly, increased usability due to data usage and thus personalization was mentioned more often in the private group compared to the workplace group (nine comments compared to four).

Looking into the **individual data elements and permissions**, further conclusions on different usage behaviors can be detected For instance, the possibility for anonymization was mentioned three times for nickname. One stated that a nickname "is just the anonymization", whereas one other stated that "nickname may also contain the full name like email address and be very sensitive or contain embarrassing / very intimate information (e.g. indication of sexual orientation)".

For email address, participants stated that on the one hand that email addresses "can be anonymized/ changed", on the other hand one stated that "currently it is as important as the physical address and needs to be protected (Spam)" or "critical as it is increasingly used for logins". Violation of privacy was further stated for relationship status and GPS access.

Additionally, users clearly seem to make a difference between data that is needed or makes usage convenient. E.g. for GPS one mentioned "added value is high", or for social media "Saves me from creating new user accounts for new apps. If the requested requests do not go too far I do not have a problem connecting with these accounts, the information is already on Facebook and Co.

[1] Comments shown in this paper were translated from German into English by the authors

anyway and are therefore no longer secret" whereas for name users state that is it not necessary, e.g., "Allows a clear identification and is completely unnecessary for a purely informative app or Sport-app like Runtastic and the data is sensitive". Furthermore, users seem to value if they can decide whether to disclose the information. For the permission to connect with social media one stated "As long as the access is optional I can agree here", whether for the permission to access contacts some stated that "it is a matter of trust of my friends, relatives and all other contacts not to pass on the numbers.".

Table 5. Intercode reliability for the comments

	Private	**Workplace**
Total Comments	598	506
Data element argued to be sensitive		
Agreement in coding	483	379
Disagreement in coding	115	127
Comments stating that data element is sensitive (coded as 1)	189	142
Comments stating that data element is not sensitive (coded as 2)	95	77
Comments do not include argument concerning sensitivity (coded as 3)	314	287
Cohen's Kappa	*.676*	*.584*
Content of comments (excluding those coded as 3)	284	219
Agreement in coding	172	105
Non-agreement in coding	67	39
One researcher did not give a coding	45	75
Cohen's Kappa	*.623*	*.697*

Moreover, comments indicated that often the data element alone was not perceived as sensitive; however, a combination of certain data elements could lead to identification. When evaluating the comments, it further became obvious that different interpretations of 'sensitive' were applied. Some interpreted it as the identification of the person, whereas other kept misuse in mind.

5. DISCUSSION

Even though usage of data and the combination of various data elements might revolutionize the health technology sector [30], the acceptance of end users need to be guaranteed and users should be capable to make informed decisions on data usage sharing. Up until now, it is unclear to what extent the usage of data elements and privacy concerns in health apps influence the intention and actual usage of these apps by end users [17]. Additionally, no categorization of data according to perceived sensitivity by the end users exists, leaving the question open what data should not be requested by app developers and what data elements can users be persuaded to share. Because health apps are being used in the workplace (apart from the private usage), both scenarios were considered to evaluate the influence of the app provider.

When interpreting the results of the Delphi study, further insights into data sensitivity and privacy were gained. First and last names were considered as the most sensitive data, which were requested by many apps in our sample, but it is questionable whether this information is needed. Additionally, in the group for private health apps, the top four data elements in terms of user ranking regarding sensitivity included personal data according to the GDPR definition (first- and surname, mobile phone number, location/address, and profile picture). The group for workplace health apps showed similar results. The first five ranks represent personal data according to the GDPR, further supporting this categorization. Interestingly, health data seem to be in comparison ranked less sensitive by the participants. Apart from these findings, interpretations can be made that the workplace setting leads to more possibilities of identification. More data elements were mentioned to include identification characteristics; in some cases, data such as weight or body measurements could be used for identification (depending on group size). This would support the findings of a study that the app provider (as third-party provider) has an influence on the willingness to share data. However, in that study, data sensitivity of health data seems to be less important than user and usage purpose [31].

Interestingly, different usage behaviors could also be identified by the comments and demonstrate various personal preferences and user behaviors. For instance, the risk of identification from a picture of the person was assumed to have a high sensitivity whereas when the person assumed that a picture without identification can be used (e.g., without the person's face), less sensitivity was reported. The same discussions were found for email address. By educating users on possibilities of (de-) anonymization, the privacy perceptions could thus be improved. Additionally, the combination of some data types seems to be important. Often, the data is not critical per se, but in combination with other data, it is. Also, as discussed in various studies, communication about the usage of data seem to be missing [32], because participants state in the comments that the purpose of data collection and usage is not clear. However, considerations about the added value (increased usability) were also stated by the participants. This supports experts' findings that users generally strive for control over their data, but are open to share data if necessary and if an added value can be expected [33].

A mismatch was further identified between the level of sensitivity and the extent to which the data and permissions are being used in the commonly used apps. For instance, names are used in half of the apps, even though name is considered as most critical by the participants. For the permissions, similar results are revealed. In the group for workplace health apps, access to pictures/files and media is ranked as most sensitive; however, it is being requested by 90% of the apps. Contacts, as ranked most sensitive for the group for private health apps, is required in nearly 40% of the apps.

However, especially in the workplace, where the users cannot decide for an app themselves but need to rely on the employer, data security and privacy should be considered early to enhance trust [15]. When considering the frequencies of requested data elements and permissions, this seems to have partially occurred already. The researchers hypothesize that different aims of implementation are followed. Workplace health experts aim to improve the workforce health, whereas app developers of private apps sell data as part of their business model to provide apps for free. Nonetheless, the developers need to find a way to provide added value to users with minimum data usage and highest security and privacy standards [34]. Additionally, due to the lack of independent and thorough quality assessment, users still have difficulties to make an informed decision about a health app [35].

5.1. Limitations

When considering the findings described above, some limitations need to be considered. Within the market analysis, issues concerning the accessibility of individual apps needs to be mentioned. Especially WHP apps were sometimes not accessible without a corporate account. For the evaluation of the data, only data elements that were requested when using the data for the first time were considered in the analysis; for the permissions, all were considered due to the permission system of Android. Of course, we are aware of the fact that some data might be requested later. Additionally, due to the limited number of data elements that could be incorporated into the study, some specific (health) data elements, that might be perceived as sensitive, might be missing in the study.

For the Delphi Study also, some limitations need to be mentioned. As is usual for studies with individual participants, selection bias might have occurred. Also, even though the Delphi is considered as a method without social interaction, the individual characteristics of the participants are still represented in the comments. For instance, some participants did not give any comments, while others provided lengthy reasonings. Additionally, usually only those deviating from the group gave a reasoning for their rating, thus creating a slight bias in the results. Another limitation that needs to be mentioned in the context of the Delphi study is the comparison of the two individual groups. Usually, Delphi studies consist of just one (type of) study group, while a comparison of groups (similar to experimental treatments), to the researcher's knowledge, has not yet been done before. Therefore, the Delphi studies of the two groups were kept completely separated. Thus, the differences found in the groups have not been proven to be due to the different settings, but might also be explained by the different study groups. Still, as our study is among the first studies to compare the private and workplace settings, it gives an initial indication of the impact of this contextual difference. Additionally, qualitative comments have been considered in order to overcome this limitation.

6. CONCLUSION

The Delphi study reveals that the definitions of personal data by the EC matches the perception of end users. Surprisingly, data for identification seem to be ranked most sensitive, even more sensitive than health-related data.

However, based on the evaluation of the frequency of requested data elements and permissions and the Delphi results, a mismatch was found between the perceived level of sensitivity of the data elements and the usage by the apps (e.g., personal data). Moreover, the results demonstrate that the workplace setting, with its unique characteristics, poses some challenges that differ from the private sector. Prior work already reveals that challenges occur due to high expectations by the users since there is no possibility of individual choice. Our findings further show that participants, when imagining a workplace setting, perceive more data elements as unique identifier. Since the group of potential users is clearly delimited, some markers (e.g., height, weight) can identify a person. On the other hand, some types of data, like profile picture and education, were considered as less critical by the workplace group, because they are already known to the employer. The current WHP apps, however, may already take perceived sensitivity and privacy into account, as the frequency of data elements and permission requests is smaller compared to that in private apps.

On the whole, it can be stated that app developers need to consider the perceptions of data sensitivity of the end users in order to increase participation rates. It is important for developers to balance data gathering for further development of the interventions and for minimizing the data used to provide a high standard of privacy, security, and thus trust among their users. Especially in the workplace sector, trust is crucial for it to be effective and to make a positive impression for the employees. Further developments towards the safe and private use of data are necessary in order to reduce concerns from the end user perspective.

ACKNOWLEDGMENTS

The authors would like to thank all participants of the Delphi study for their contribution as well as the second coder of the comments. The authors would also like to thank the anonymous referees for their valuable comments and helpful suggestions.

REFERENCES

[1] Anett Hoppe, Jenny Knackmuß, Maik Morgenstern, and Reiner Creutzburg. 2017. Privacy Issues in Mobile Health Applications-Assessment of Current Android Health Apps. *Electronic Imaging*, 2017 (6), 76-83.

[2] Xitong Guo, Xiaofei Zhang, and Yongqiang Sun. 2016. The privacy–personalization paradox in mHealth services acceptance of different age groups. *Electronic Commerce Research and Applications*, 16), 55-65.

[3] Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou, Efthimios Alepis, Agusti Solanas, and Constantinos Patsakis. 2018. Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access*, 6), 9390-9403.

[4] Haroon Elahi, Guojun Wang, and Dongqing Xie. 2017. Assessing privacy behaviors of smartphone users in the context of data over-

collection problem: An exploratory study. *IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*.

[5] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. 2011. Android permissions demystified. *Proceedings of the 18th ACM Conference on Computer and Communications Security*. 627-638.

[6] Ali Sunyaev, Tobias Dehling, Patrick L Taylor, and Kenneth D Mandl. 2014. Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, 22 (1), 28-33.

[7] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. *Proceedings of the Eighth Symposium on Usable Privacy and Security*.

[8] Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. 2001. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. *Proceedings of the 3rd ACM Conference on Electronic Commerce*. 38-47.

[9] Alessandro Acquisti, and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3 (1), 26-33.

[10] Kelly Caine, and Rima Hanania. 2012. Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association*, 20 (1), 7-15.

[11] Tae Kyung Kim, and Moon Choi. 2019. Older adults' willingness to share their personal and health information when adopting healthcare technology and services. *International Journal of Medical Informatics*, 126), 86-94.

[12] Elsbeth Marieke de Korte, Noortje Wiezer, Joris H Janssen, Peter Vink, and Wessel Kraaij. 2018. Evaluating an mHealth App for Health and Well-Being at Work: Mixed-Method Qualitative Study. *JMIR mHealth and uHealth*, 6 (3), e72.

[13] Anita Dunkl, and Paul Jiménez. 2017. Using smartphone-based applications (apps) in workplace health promotion: The opinion of German and Austrian leaders. *Health Informatics Journal*, 23 (1), 44-55.

[14] Kien Hoa Ly, Kajsa Asplund, and Gerhard Andersson. 2014. Stress management for middle managers via an acceptance and commitment-based smartphone application: A randomized controlled trial. *Internet Interventions*, 1 (3), 95-101.

[15] Paulino Jimenez, and Anita Bregenzer. 2018. Integration of eHealth Tools in the Process of Workplace Health Promotion: Proposal for Design and Implementation. *Journal of Medical Internet Research*, 20 (2).

[16] Moritz Becker, Christian Matt, Thomas Widjaja, and Thomas Hess. 2017. Understanding Privacy Risk Perceptions of Consumer Health Wearables–An Empirical Taxonomy. *Thirty Eighth International Conference on Information Systems*. 12.

[17] Victoria Kisekka, and Justin Scott Giboney. 2018. The Effectiveness of Health Care Information Technologies: Evaluation of Trust, Security Beliefs, and Privacy as Determinants of Health Care Outcomes. *Journal of Medical Internet Research*, 20 (4), e107.

[18] Harsh Kupwade Patil, and Ravi Seshadri. 2014. Big data security and privacy issues in healthcare. *IEEE International Congress on Big data*. 762-765.

[19] David Kotz, Sasikanth Avancha, and Amit Baxi (2009) "A privacy framework for mobile health and home-care systems," in *Proceedings of the first ACM Workshop on Security and Privacy in Medical and Home-care Systems*, Chicago, Illinois, USA, pp. 1-12.

[20] Stacey Pereira, Jill Oliver Robinson, Hayley A Peoples, Amanda M Gutierrez, Mary A Majumder, Amy L McGuire, and Mark A Rothstein. 2017. Do privacy and security regulations need a status update? Perspectives from an intergenerational survey. *PLoS ONE*, 12 (9), e0184525.

[21] Moritz Becker, Susanne Maria Klausing, and Thomas Hess. 2019. Uncovering the privacy paradox: The influence of distraction on data disclosure decisions. *Proceedings of the 27th European Conference on Information Systems (ECIS)*.

[22] Flavius Kehr, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch. 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25 (6), 607-635.

[23] Soumitra S Bhuyan, Hyunmin Kim, Oluwaseyi O Isehunwa, Naveen Kumar, Jay Bhatt, David K Wyant, Satish Kedia, Cyril F Chang, and Dipankar Dasgupta. 2017. Privacy and security issues in mobile health: Current research and future directions. *Health Policy and Technology*, 6 (2), 188-191.

[24] Android Open Source Project. 2018; Permissions, https://developer.android.com/guide/topics/permissions/overview.

[25] Norman C. Dalkey, 1969. The Delphi Method: an experimental study of group opinion, United States Air Force Project Rand,

[26] Elizabeth A Holey, Jennifer L Feeley, John Dixon, and Vicki J Whittaker. 2007. An exploration of the use of simple statistics to measure consensus and stability in Delphi studies. *BMC Medical Research Methodology*, 7 (1), 52.

[27] Ivan R Diamond, Robert C Grant, Brian M Feldman, Paul B Pencharz, Simon C Ling, Aideen M Moore, and Paul W Wales. 2014. Defining consensus: a systematic review recommends methodologic criteria for reporting of Delphi studies. *Journal of Clinical Epidemiology*, 67 (4), 401-409.

[28] Robert Loo. 2002. The Delphi method: a powerful tool for strategic management. *Policing: An International Journal of Police Strategies & Management*, 25 (4), 762-769.

[29] European Commission. 2018; What is personal data?

[30] Connie Chen, David Haddad, Joshua Selsky, Julia E Hoffman, Richard L Kravitz, Deborah E Estrin, and Ida Sim. 2012. Making sense of mobile health data: an open architecture to improve individual-and population-level health. *Journal of Medical Internet Research*, 14 (4).

[31] David Grande, Nandita Mitra, Anand Shah, Fei Wan, and David A Asch. 2013. Public preferences about secondary uses of electronic health information. *JAMA Internal Medicine*, 173 (19), 1798-1806.

[32] Tobias Dehling, Fangjian Gao, Stephan Schneider, and Ali Sunyaev. 2015. Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android. *JMIR mHealth and uHealth*, 3 (1).

[33] Sheridan W Miyamoto, Stuart Henderson, Heather M Young, Amit Pande, and Jay J Han. 2016. Tracking health data is not enough: a qualitative exploration of the role of healthcare partnerships and mHealth technology to promote physical activity and to sustain behavior change. *JMIR mHealth and uHealth*, 4 (1).

[34] Adrian Carter, Jacki Liddle, Wayne Hall, and Helen Chenery. 2015. Mobile phones in research and treatment: ethical guidelines and future directions. *JMIR mHealth and uHealth*, 3 (4).

[35] Stoyan R Stoyanov, Leanne Hides, David J Kavanagh, Oksana Zelenko, Dian Tjondronegoro, and Madhavan Mani. 2015. Mobile app rating scale: a new tool for assessing the quality of health mobile apps. *JMIR mHealth and uHealth*, 3 (1).