Understanding Privacy Risk Perceptions of Consumer Health Wearables – An Empirical Taxonomy

Moritz Becker  
*Ludwig-Maximilians-Universitat Munchen  Fakultat fur Betriebswirtschaft, m.becker@bwl.lmu.de*

Christian Matt  
*Universitat Bern Institut fur Wirtschaftsinformatik, matt@bwl.lmu.de*

Thomas Widjaja  
*Universitat Passau, thomas.widjaja@uni-passau.de*

Thomas Hess  
*Ludwig-Maximilians-University Munich, thess@bwl.lmu.de*

Follow this and additional works at: [http://aisel.aisnet.org/icis2017](http://aisel.aisnet.org/icis2017/IT-and-Healthcare/Presentations/12)
Understanding Privacy Risk Perceptions of Consumer Health Wearables
An Empirical Taxonomy

Completed Research Paper

Moritz Becker
LMU Munich
Ludwigstr.28, 80530 Munich
m.becker@bwl.lmu.de

Christian Matt
University of Bern
Engehaldenstr. 8, 3012 Bern
christian.matt@iwi.unibe.ch

Thomas Widjaja
University of Passau
Dr.-Hans-Kapfinger-Str. 12, 94032 Passau
thomas.widjaja@uni-passau.de

Thomas Hess
LMU Munich
Ludwigstr.28, 80530 Munich
thess@bwl.lmu.de

Abstract
Perceived privacy risks are an important factor for the adoption of consumer health wearables. However, little is known about the nature of those risk perceptions. We develop a perceived privacy risk taxonomy, which is derived based on an established numerical approach in biology. We apply a four-step mixed-method taxonomy development process to empirically explore privacy perceptions of consumer health wearables. 60 hours of interviews with two different samples, multidimensional scaling, property fitting, and qualitative data analysis enable us to uncover the structure of the mental perception of respondents' privacy risk perceptions. Our taxonomy reveals that the most relevant dimensions to distinguish consumer health wearables according to the respondents' perceptions of privacy risks refer to the perceived data sensitivity, perceived data variety, and perceived tracking activity. The developed taxonomy helps researchers to enhance the understanding of privacy perceptions of consumer health wearables and provides practitioners with a comprehensive nomenclature.

Keywords: Consumer health wearables, privacy risk perceptions, taxonomy, multidimensional scaling

Introduction

Consumer health wearables arising from the intersection of healthcare, health informatics, and information systems can improve utility for individuals, health professionals, and service providers (Agarwal et al. 2010). As the use of traditional health technologies is often considered to be driven by older individuals, the uptake of consumer health wearables is bimodally distributed (Chiauzzi et al. 2015). As the older group (approx. >55 years) tends to use the devices to improve and monitor their overall health status with respect to diseases, the younger group (approx. <30 years) often aims at enhancing their fitness levels through increased personal health surveillance and social connections with others to be motivated (e.g. Piwek et al. 2016). For both user-groups, the individual becomes a real-time “walking data generator” (McAfee and Brynjolfsson 2012, p. 63), and privacy risks occur by exposing personal health information without awareness or consent (Meingast et al. 2006). A practitioners’ report in 2014
postulated privacy risks as important apprehensions of (potential) users; more than 80% of respondents were worried about that consumer health wearables would invade their privacy (PwC Health Research Institute 2014). This observation seems to hold not only for consumer health wearables (e.g. Lee et al. 2015), since such “poor information privacy practices have been identified in health apps” (Huckvale et al. 2015, p. 1), health websites (e.g. LaRose and Rifon 2007), clinical devices (e.g. Chai et al. 2014).

Literature commonly cited privacy problems as primary barrier to the persistent adoption of health wearables (e.g. Kang et al. 2013; Lee et al. 2015), there is little empirical research into individuals’ privacy perceptions of consumer health wearables (Miltgen et al. 2013). To date, no study offers an integrated, comprehensive conceptualization of perceived privacy risks of consumer health wearables, and there is no empirical evidence of what the main risk dimensions are that affect individuals’ privacy perception. As privacy risks are complex psychological concepts in the individual minds (Dinev et al. 2015), we use a taxonomy approach to structure the heterogeneous privacy perceptions into homogeneous dimensions to compare and analyze different types of consumer health wearables (Doty and Glick 1994). Understanding how individuals’ perceived privacy risks vary across consumer health wearables and identifying the primary dimensions behind this differentiation could „help researchers and designers understand the major dimensions that are critical in their work“ (Alridge and Chatterjee 2015, p. 497).

By developing such a perceived privacy risk taxonomy (i.e. perceptual map) of consumer health wearables, we provide researchers with a full view of the main privacy risk dimensions, uncover the structure of privacy perception (e.g. Dinev et al. 2015) and lay the basis for future research approaches concerning perceived privacy of health technologies. Our study addresses the call for research of Alridge and Chatterjee (2015) to develop a privacy taxonomy concerning health wearables and of Plachkinova et al. (2015, p. 3194) „to examine into more detail the dimensions of the taxonomy, which can be broken into various (privacy) subcategories.” For practitioners our taxonomy provides structure to the area of consumers health wearables from a privacy perspective (Glass and Vessey 1995) and creates a common nomenclature of the main dimensions that drive individuals’ perceived privacy risks concerning consumer health wearables (e.g. Li et al. 2016). Thus our taxonomy can serve as a starting point for developers when deciding on the configuration of a new device, with specific features, biometrical sensors or tracking technologies. Therefore we ask:

What dimensions do individuals use to classify consumer health wearables according to their perceived privacy risks?

As our definition of consumer health wearables exclude medical devices, in which health professionals diagnose and evaluate users’ medical problems (professional health wearables), we investigated a population of consumer health wearables and explored the privacy-related similarities and differences between the devices, focusing on the science of diversity (Posey et al. 2013) rather than that of uniformity (Lee and Baskerville 2003). We apply a rigorous four-step mixed-method approach to empirically investigate individuals’ perceived privacy risks regarding their consumer health wearable and uncover the structure that best represents the mental perception of the respondents’ ratings (Schiffman et al. 1981). As “biology has studied (taxonomies) extensively and developed a number of classification schemes that order the complexity of the living world” (Nickerson et al. 2013, p. 336), our taxonomy development process is based on the numerical approach in biology (Sneath and Sokal 1973), which has already been recognized and applied in information systems research (e.g. Posey et al. 2013). To maximize content validity and generalizability, we conducted two rounds of quantitative and qualitative data collections (Sample 1 N=35; Sample 2 N=21) and analyzed them via multidimensional scaling (MDS), property fitting (ProFit), and qualitative analysis to determine dimensions (i.e. perceived privacy risks) and characteristics in the taxonomy (i.e. perceptual maps). This “set of mathematical techniques (...) enable researchers to uncover the ‘hidden structure’ of data bases” (Kruskal and Wish 1978, p. 5). Perceptual maps visualize this hidden structure in a multidimensional space and therefore allow us to display the functional dimensions that individuals use to classify consumer health wearables according to their privacy risk profiles.

The remaining paper proceeds as follows: In the next section (Theoretical Background) we define and briefly describe consumer health wearables and perceived privacy risk. In the third section (Methodology) we propose the four-step mixed-method methodology, combining quantitative and qualitative techniques. After illustrating the proposed perceived privacy risk taxonomy of consumer health wearables with a hierarchical map (Results) we discuss the developed taxonomy and the primary dimensions behind this
differentiation (Discussion). In the last section (Implications and Limitations), we draw conclusions by presenting implications, limitations, and further research approaches.

**Theoretical Background**

**Defining Consumer Health Wearables**

In the literature, there are various ideas and nomenclature of consumer health wearables, as a specific form of mobile health technologies for private users. Thus, we first clarify what constitutes a consumer health wearable in our sense. According to our definition the three constituting characteristics of a consumer health wearable are: Consumer health wearables are a) designed for private users worn on the body as small digital devices b) with biometrical sensors to continuously generate personal health data c) to be used without the need for health professionals.

First, devices are offered in various shapes, such as wristbands, watches, glasses, or textiles to track, analyze, communicate, and “to monitor the minutiae of our everyday lives” (Newell and Marabelli 2015, p. 3). Despite these differences in functionality and appearance, all devices are seamlessly integrated into the outfit, or directly worn on the body (Berghaus and Back 2015). Being seamlessly integrated in everyday life, consumer health wearables disappear in individuals' minds and can, according to Weiser and Brown (1997), be classified as calm health technologies.

Second, consumer health wearables "have the same fundamental technical properties, i.e., integrated sensors, massive storage and software applications” (Wieneke et al. 2016, p. 3). Especially embedded biometrical sensors can unobtrusively collect human physiological data, such as physical activity with an oximeter or sleep patterns via an accelerometer. For instance, electrodermal sensors can measure stress, and electromyographic sensors can track users’ muscle activities over long periods (Trickler 2013). These biometrical “sensors can be woven or integrated into clothing, accessories, and the living environment, such that health information can be acquired seamlessly and pervasively in daily living” (Zheng et al. 2014, p. 1538).

Third, a small form factor makes devices easier to wear continuously (Piwek et al. 2016) and – in contrast to smartphones, health apps, or health websites – these devices collect human physiological data that usually cannot be accessed in other ways (Meng et al. 2011). Thus, users get personalized, immediate, and goal-oriented feedback (Soar et al. 2005) based on specific tracking data obtained via biometrical sensors. In contrast to digital medicine, clinical wearable technologies (professional health wearables), in which health professionals diagnose and evaluate patients' medical problems by also monitoring human physiological data and needs in real time (Paschou et al. 2013), users of consumer health wearables can independently interact with their device (Varshney 2014). The analysis of user's personal health data is usually done separately by themselves with applications on more powerful devices (tablets, mobile devices, or PCs) (Safavi and Shukur 2014). These applications use advanced data analytics or benchmarking to generate insights about different aspects of individuals’ health status without the need for health professionals involved.

**Perceived Privacy Risks of Consumer Health Wearables**

Consumer health wearables can monitor a range of personal health data and give individuals direct access to their personal health information, which can contribute to their health, facilitate preventive care, and support the management of ongoing illness. But “these benefits will only be achieved, however, if individuals are confident in the privacy of their health-related information” (Kotz et al. 2016, p. 22). Health information privacy “is an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data” (Cohn 2006, p. 1). In contrast to medical health wearables for professional usage or other clinical devices, in which electronic health records are created and managed by healthcare providers (hospitals and other clinical organizations), users of consumer health wearables create and manage their personal health information without the help of physicians (Varshney 2014). Owing to the high sensitivity of such personal health information, privacy aspects have proved to be more important in the context of consumer health wearables than other technological devices (e.g. Chatterjee and Price 2009; Miltgen et al. 2013).
Previous studies primarily use the privacy calculus theory to analyze individuals’ willingness to share personal health information voluntarily if they expect that perceived benefits from data disclosure outweigh the perceived costs (e.g. Anderson and Agarwal 2011; Li et al. 2016). This tradeoff theory has been described as “the most useful framework for analyzing contemporary consumer privacy concerns” (Culnan and Bies 2003, p. 326), but still underscores the risk-control interplay. Both risk and control have been shown to operate as privacy-borne beliefs relating to the potential consequences of personal health information disclosure (Dinev et al. 2013). In the context of consumer health wearables, improper information practices would result in the mining and mapping of personal data to make an individual’s health status more visible. The collected personal health data may be easily analyzed, distributed, and reused, and users perceive a relatively high risk that the provided personal health information is being put into secondary use for unrelated purposes without their knowledge or consent (Li et al. 2016). Thus, the sensitivity of various datasets such as demographics, activities (accelerometers, pedometers, location), or physiologies (electrocardiograms, pulse oximeters, blood glucose meters, and weight scales) in particular have prompted heated discussions about individuals’ perceived privacy risks (Kotz et al. 2016; Piwek et al. 2016). Especially in the context of health wearables for private users, there is very little empirical research on individuals’ privacy perception (Miltgen et al. 2013).

The perceived state of privacy is generally determined by an individual’s sense of potential risks when personal health information is revealed (Fusilier and Hoyer 1980; Pavlou 2002). Perceived privacy risks enter individuals’ decision-making processes when situations in this process create uncertainty, discomfort, and/or anxiety (Dowling and Staelin 1994). Adapting the definition of Dinev et al. (2013) to our research, we define perceived privacy risks as a user’s perceived expectation of suffering a negative outcome as a result of personal health data collected by consumer health wearables. We identified three research streams focusing privacy risks and mobile health technologies. The first stream addressed individuals’ senses of privacy when considering the consequences of information disclosure (Culnan and Bies 2003; Fusilier and Hoyer 1980; Pavlou 2002). These studies use perceived privacy risks to predict personal health information disclosure on social networks (Krasnova et al. 2009), websites (Dinev et al. 2013), or activity trackers (Rheingans et al. 2016). The second stream determines perceived privacy risks as a primary barrier to the persistent adoption of consumer health wearables (Kang et al. 2013; Lee et al. 2015; Miltgen et al. 2013). The third stream explores specific factors that affect privacy risks of consumer health wearables, such as information sensitivity (e.g. Dinev et al. 2013), functional congruence (e.g. Motti and Caine 2015), or legislative regulations (e.g. Li et al. 2016). But none of these studies offer an comprehensive treatment of the primary dimensions that affect privacy risks of individuals concerning consumer health wearables (Dinev et al. 2013). Thus, “more work is needed in creating a detailed classification [...] to improve the privacy aspects of (consumer health wearables) and make (individuals) aware of these challenges” (Varshney 2014 p. 24). To address this call for research, we developed a perceived privacy risk taxonomy of consumer health wearables that explores the main perceived privacy risk dimensions and how consumer health wearables vary in these factors.

**Methodology**

A taxonomy’s general purpose is to structure complex heterogeneous objects into homogeneous concepts that can then be analyzed and compared (Doty and Glick 1994). In information systems research, the importance of taxonomies is well recognized (Nickerson et al. 2010). Suitable taxonomies provide structure to an area (Glass and Vessey 1995), reduce the complexity among objects (Nickerson et al. 2013), and lay the basis for future research approaches (Hevner et al. 2004).

In this study, we propose a perceived privacy risk taxonomy that explores the diversity of consumer health wearables. Based on the numerical approach in biology, we investigate a population of consumer health wearables by highlighting and understanding the privacy-related similarities and differences of the devices (McKelvey 1978; McKelvey 1982). In contrast to other approaches for developing health wearable taxonomies (e.g. Alrige and Chatterjee 2015), which used a deductive design science research approach followed by empirical verification (Hevner and Chatterjee 2010; Nickerson et al. 2013), we chose an empirical inductive mixed-method methodology (Mingers 2001; Venkatesh et al. 2013) that involves a combination of MDS, ProFit, and qualitative data analysis. We use this group of data classification techniques (Kruskal and Wish 1978) to empirically understand the perception of individuals regarding their privacy risks concerning consumer health wearables and uncover the structure that best represents...
the mental perceptions of respondents’ ratings (Schiffman et al. 1981). The obtained privacy-related similarity ratings form the foundation for identifying and labeling the functional dimensions underlying this representation with a ProFit analysis (Kruskal and Wish 1978; Schiffman et al. 1981). To understand individuals’ perception, we created perceptual maps by focusing on the science of diversity (Posey et al. 2013). With these perceptual maps, we are able to explore the functional dimensions that individuals use to classify consumer health wearables according to their privacy risk profiles. Previous studies in information systems have successfully used this empirical inductive approach to develop taxonomies in the contexts of sensor positioning (Ji and Zha 2004), wearable device comparisons (Wang 2015), or medical information sources (Bunn 1993). Going forward, we strictly adhere to this established process, which involves four subsequent steps.

<table>
<thead>
<tr>
<th>Used methods</th>
<th>Basis for why each step is requisite</th>
<th>Data basis and procedure addressing this step</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Selection of Consumer Health Wearables</td>
<td>The first step aims at building a record of devices that represents the population of the objects of interest (i.e. consumer health wearables). This record should be as exhaustive as possible in order to cover all existing kinds of consumer health wearables and their induced privacy risk perceptions.</td>
<td>We conducted a market analysis to gain a record of available devices, as well as their fields of application and capabilities. According to other studies (e.g. Berghaus and Back 2015), we used the database of Vandricco (2016). This database provides, to our best knowledge, the most extensive and objective overview of 448 current wearable devices. Applying our understanding of consumer health wearables and verifying that there was sufficient information for analyzing we dismissed 136 devices. According to other taxonomy approaches using MDS, which selected 11% of the entire population as their sample (e.g. Engelbrecht et al. 2016), we choose an equivalent sample ratio (11.2%) and selected randomly 35 consumer health wearables from the remaining 312 devices.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Acquisition of Privacy-related Similarity Ratings (Sample 1)</td>
<td>Researchers should ascertain how the target population perceives the randomly selected objectives (i.e. consumer health wearables) relative to each other (according their privacy risk perceptions).</td>
<td>Our first sample consists of 35 respondents between the ages of 18 to 29 (Sample 1 N=35). We conducted face-to-face interviews (60 -90 minutes) to collect quantitative and qualitative privacy risk perceptions.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Analyzing Quantitative and Qualitative Similarity Ratings Using MDS</td>
<td>Researchers should determine the number of functional dimensions that represent the de facto proximities between the data (i.e. privacy risk perceptions). The number of dimensions and potential labels of the dimension that the target population uses to make the comparisons in step 2, have to be ascertained.</td>
<td>2a) Gathering quantitative privacy risk similarity ratings: The Respondents had to rate each device pair comparison on a 9-point bipolar scale (1 = not at all similar; 9 = very similar). By comparing all possible combinations of devices, we collected 1,190 perceived privacy risk similarity ratings. 2b) Gathering qualitative privacy statements: In the qualitative part, we ask the respondents to reflect on the criteria for their comparison decisions after each judgment. In detail, we ask: “Based on what characteristics do you compare the privacy risk rating?” In total, we collected more than 1,500 qualitative statements.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Mapping and Labeling the Dimensions Using ProFit Analysis (Sample 2)</td>
<td>In the next step researchers should merge the potential dimension labels and the extracted dimensions to form a taxonomy.</td>
<td>3a) We calculate the structure of our respondents’ perceptions using the 1,190 quantitative privacy risk similarity ratings. Following a decompositional MDS approach (Posey et al. 2013), we used the proximity scaling (PROXSCAL) to determine that three dimensions best represented respondents’ privacy risk perceptions of the devices. 3b) We utilized the qualitative statements to extract potential dimension labels. Three researches independently coded more than the 1,500 qualitative statements and created a list of possible attributes. After a multilevel coding process, we ended up with nine potential labels for the three dimensions extracted in step 3a.</td>
</tr>
</tbody>
</table>

Table 2. The Four-step Taxonomy Development Process
After building a set of consumer health wearables (Step 1), we gathered perceived privacy risk similarity ratings from the respondents (Step 2) that form the foundation for extracting the taxonomy’s dimensionality using MDS (Step 3). To label the extracted dimensions, we identified common characteristics based on qualitative data and conducted a ProFit analysis to map these characteristics to the functional dimensions and, in the last step, formalized the taxonomy (Step 4). We will now explain how we conducted these four steps (see Table 1).

Selection of Consumer Health Wearables

We conducted a market analysis to gain a record of available devices, as well as their fields of application and capabilities. To cover all existing consumer health wearable types, we sought databases that were as exhaustive as possible to provide us with a comprehensive overview of wearable devices. According to other studies of wearable technologies (e.g. Berghaus and Back 2015), we used the database of vandrico.com, a technology consulting company that catalogs currently available wearable devices (Vandrico 2016). With – at that time 448 devices – this database provides, to our best knowledge, the most extensive and objective overview of current wearable devices. Unfortunately, in our study, it has not been feasible for the respondents to touch and look at real haptic devices; nonetheless, the respondents should be able to experience the device as realistically as possible (Andrade et al. 2015). Thus, we presented the devices using detailed textual information from vandrico.com and the specific product website regarding functionalities, connections, features, or applications of the devices; we also included visual material to deepen our textual explanations of the devices (Ball and Smith 2006). These images provided information that is difficult to present to respondents in textual form only (Wagner 2006). As the original product descriptions from vandrico.com contained relative feature scores to similar devices (e.g. battery, compatibility, connectivity), we blank these scores to avoid a bias of the study participant. Beside the information on vandrico.com, we provided further information for each device and link to the homepage of the company and the product. Applying our understanding of consumer health wearables and verifying that there was sufficient information on every included device on all the websites (vandrico.com, company home page, and device home page), we dismissed 136 devices. To provide an adequate coverage of the diversity of consumer health wearable types, we followed other taxonomy approaches using MDS, which selected 11% of the entire population as their sample (e.g. Engelbrecht et al. 2016), and choose an equivalent sample ratio and selected randomly 35 consumer health wearables from the remaining 312 devices (sample ratio 11,2%). A list of all consumer health wearables with corresponding information (names, Vandrico profiles, and descriptions) is available from the authors upon request.

Acquisition of Privacy-related Similarity Ratings (Sample 1)

For the 35 health wearables for private users, we gathered with “Sample 1” quantitative privacy-related similarity ratings, which are the foundation of extracting the taxonomy’s dimensionality and qualitative statements about these privacy risk perceptions, to label these dimensions. To use MDS, we needed to collect the perceived privacy risk similarity ratings for each consumer health wearable pair. Considering cognitive load, these ratings could not be obtained from each respondent for all pairs owing to the overall sample size. According to other research approaches (e.g. Posey et al. 2013), we asked each respondent to compare the privacy risk perception of one specific device with all remaining ones. To ensure high respondent involvement until the end of the ratings, we conducted one-to-one interviews with each respondent. These interviews took between 60 to 90 minutes each. We used two screens for the interview: On one screen, consumer health wearable descriptions on vandrico.com were presented and the respondents received the links to the product websites and read through them. Therefore, the respondents could use all available information and criteria on these websites to contrast the privacy risks between devices. On the other screen, we noted the quantitative ratings and qualitative statements while sitting next to the respondent.

As the diffusion process of new consumer health wearables can be strongly influenced by individuals’ privacy perception, we consulted both current consumer health wearable users and non-users and try to approximately replicate the adaption ratio of 10% in this age group (Ledger and McCaffrey 2014). Furthermore, the uptake of consumer health wearables is bimodally distributed. The older group (approx. >55 years) usually uses the devices to monitor their overall health status or chronic diseases (e.g.
hypertension). While the younger group (approx. <30 years) tracks their fitness levels and uses their devices for social connections to stay motivated (Chiauzi et al. 2015). As our definition of consumer health wearables excludes medical devices, in which health professionals diagnose and evaluate users’ medical problems (professional health wearables), we decided to concentrate on a younger and healthy population. Consequently, none of our respondents suffer from a chronic disease. Furthermore, our methodology requires extensive knowledge of the respondents in the area of digital technologies and sufficient cognitive capacities to evaluate the devices with their various features. We assume that a younger population would be more suitable to do these similarity ratings as this group is constantly confronted with new technologies and features in their everyday lives (Tsao et al. 2016). In summary, we conducted 35 interviews with respondents between the ages of 18 to 29. A detailed description of “Sample 1” is provided in the appendix (Table 4).

The respondents had to rate each device pair comparison on a 9-point bipolar scale (1 = not at all similar; 9 = very similar). By comparing all possible combinations of devices, we collected 1,190 perceived privacy risk similarity ratings for the quantitative part using MDS. For the qualitative part, the respondents had to reflect on the criteria for their comparison decisions after each judgment. In detail, we asked the respondents, based on what characteristics they compared the devices according to their privacy risk perceptions. Thus, we collected more than 1,500 qualitative statements; we coded these in the next step.

**Analyzing Quantitative and Qualitative Similarity Ratings Using MDS**

In the next step, we needed to determine the number of functional dimensions that represents the de facto proximities between the data. We averaged the perceived privacy risk similarity ratings across all the respondents, making the technique an aggregate MDS approach (Hair et al. 2009). MDS is a group of data classification techniques that are very useful to answer exploratory research questions and help investigators to comprehend how the target population cognitively assesses a topic (Timm 2002). These powerful techniques enabled us to empirically examine the privacy risk perceptions of a population of individuals regarding consumer health wearables. By physically mapping these psychological distances between the device sets that exist collectively in the respondents’ minds (Schiffman et al. 1981), MDS does not rely on a specified variate; reliance on this often introduces researcher bias into exploratory studies (Hair et al. 2009). Following a de-compositional MDS approach (Posey et al. 2013), we used the proximity scaling (PROXSCAL) technique rather than the alternating least-squares (ALSCAL) algorithm in SPSS, because the number of dimensions best representing the perceptual map was unknown beforehand (Young and Hamer 1987). To calculate the structure of our respondents’ perceptions using the similarities, we needed to decide the number of dimensions. We applied Pinkley’s et al. (2005) criteria to determine the dimensionality of MDS. First, we analyzed Kruskal’s (1964) stress index, which states how well the similarity judgments can be matched to a certain dimensionality. Therefore, we conducted a scree test by plotting the stress indexes for six map configurations (Figure 1).

![Figure 1. Scree Plot of Privacy Risk Perceptions](image-url)
The appropriate configuration is determined on the basis of where (at which configuration) the stress index values begin to form an almost horizontal slope. Ideally, there should be an obvious ‘elbow’ within the scree plot indicating that increasing dimensions (right of the elbow) do not affect stress in any substantial way (Robinson and Bennett 1995; Schiffman et al. 1981). In our case the one-dimensional solution had a stress index of .30 and the two-dimensional solution of .15. For the three-dimensional solution, the index made a considerable drop to .10, suggesting a better fit with the data. The amount of reduced stress leveled off for the four-, five-, and six-dimensional solutions with values of .08, .07, and .06, respectively. Hence, the scree results suggested that the three-dimensional solution provided the most parsimonious and accurate description of the data. Second, we evaluated the stress and squared correlation (RSQ) Index, which describes how much of the variance in the proximity data is accounted for the MDS model, and confirmed the quantity of three functional dimensions (Pinkley et al. 2005).

Following Young and Hamer (1987, p. 205), who assert that the aim is to “select the space with the fewest dimensions and the richest interpretation”; in our view, three dimensions best represent respondents’ mental structures.

After we determined that three dimensions best represented respondents’ perceptions, in the second step, we elicited possible dimension labels. We utilized the qualitative comments to extract the attributes used by the respondents to explain the similarities and differences between the devices concerning their privacy risk perceptions. Following Posey et al. (2013), three researchers independently coded more than the 1,500 qualitative statements and created a list of possible attributes. To arrive at a single list of attributes, we discussed potential differences and merged similar attributes. To determine the relevance of the derived attributes, these three researchers independently counted the occurrences of these attributes in the data and added them up to arrive at a joint ranking. Since the resulting set of attributes must be reduced for feasibility reasons for ProFit analysis (Pinkley et al. 2005), we selected the nine most frequently mentioned attributes, according to Robinson and Bennett (1995) (Table 2).

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Left anchor</th>
<th>Right anchor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data variety (DVA)</td>
<td>A wide variety of data is collected.</td>
<td>A low variety of data is collected.</td>
</tr>
<tr>
<td>Features (FEA)</td>
<td>The device has many features.</td>
<td>The device has few features.</td>
</tr>
<tr>
<td>Fitness focus (FIT)</td>
<td>The device has a fitness focus.</td>
<td>The device has no fitness focus.</td>
</tr>
<tr>
<td>Health focus (HEA)</td>
<td>The device has a health focus.</td>
<td>The device has no health focus.</td>
</tr>
<tr>
<td>Tracking activity (TRA)</td>
<td>Data were permanently tracked.</td>
<td>Data were not permanently tracked.</td>
</tr>
<tr>
<td>Tracking activity (TRA)</td>
<td>The device offers many connections.</td>
<td>The device offers few connections.</td>
</tr>
<tr>
<td>Third parties (EXT)</td>
<td>Third parties have access to the data.</td>
<td>Third parties have no access to the data.</td>
</tr>
</tbody>
</table>

**Table 2. Relevant Attributes from the Qualitative Comments from the Coding Process**

**Mapping and Labeling the Dimensions Using ProFit Analysis (Sample 2)**

To map corresponding labels (qualitative data) to the dimensionality of the respondents’ perceptual maps (quantitative data), in step four, we conducted a ProFit analysis as an objective and rigorous technique that is strongly recommended by leading MDS researchers for dimension labeling (e.g. Kruskal and Wish 1978). Based on multiple regressions, the ProFit analysis determined the respondents’ ratings of possible dimension labels on the devices’ positions in the three-dimensional space. To receive the devices’ values for the extracted attributes (Table 2), we needed to collect an additional round of data. Thus, we conducted a second round of data collection. This second sample (Sample 2) consists of 21 respondents between 20 and 28 years and is presented in detail in the appendix (Table 4). In contrast to the first round of data collection, the respondents had to rate each consumer health wearable concerning all nine attributes on a 7-point bipolar scale. This resulted in more than 700 ratings for each attribute. These ratings allowed subsequent regression analyses for all attributes concerning a device’s location in the perceptual space. We computed one separate regression by using the coordinates of the devices’ positions as independent variables and the attributes as the dependent variables (Robinson and Bennett 1995).
Results

Results of the ProFit Analysis

Table 3 shows the results of these regressions. Three of the nine attributes (FEA, CON, and EXT) had no significant relationship with any dimension resulting from MDS (FEA: F = .21, p = .89; CON: F = .41, p = .74; EXT: F = .09, p = .97); we excluded these in the following process.

Table 3. Results of the Property Fitting Analysis

<table>
<thead>
<tr>
<th>Attribute</th>
<th>R²</th>
<th>F</th>
<th>Dim1</th>
<th>Dim2</th>
<th>Dim3</th>
<th>DVA</th>
<th>TRA</th>
<th>LIF</th>
<th>FIT</th>
<th>HEA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data variety (DVA)</td>
<td>.25</td>
<td>3.45*</td>
<td>.03</td>
<td>-.49**</td>
<td>-.11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tracking activity (TRA)</td>
<td>.24</td>
<td>3.23*</td>
<td>.04</td>
<td>-.05</td>
<td>.48**</td>
<td>.42*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lifestyle focus (LIF)</td>
<td>.34</td>
<td>5.40**</td>
<td>.58***</td>
<td>-.00</td>
<td>-.04</td>
<td>.19</td>
<td>.34*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fitness focus (FIT)</td>
<td>.24</td>
<td>3.18*</td>
<td>.47**</td>
<td>.12</td>
<td>.03</td>
<td>-.05</td>
<td>.31</td>
<td>.61**</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health focus (HEA)</td>
<td>.39</td>
<td>6.77***</td>
<td>-.62***</td>
<td>-.05</td>
<td>-.09</td>
<td>-.02</td>
<td>-.15</td>
<td>-.81*</td>
<td>-.42*</td>
<td></td>
</tr>
<tr>
<td>Data sensitivity (SEN)</td>
<td>.28</td>
<td>3.97*</td>
<td>-.53**</td>
<td>-.01</td>
<td>-.04</td>
<td>.47*</td>
<td>.17</td>
<td>-.37*</td>
<td>-.39*</td>
<td>.52**</td>
</tr>
</tbody>
</table>

***p < .001, **p < .010, *p < .050.

Regarding the remaining six attributes, it seems counterintuitive that four attributes (LIF, FIT, HEA, and SEN) were significantly related to the first dimension. According to the highest regression weights, the first dimension was strongly associated concerning the devices’ health, fitness, and lifestyle focuses (LIF, β = .58; FIT, β = .47; HEA, β = -.62). Further, the sensitivity of the collected data also had a significant relationship and a high regression weight in this analysis (β = .49). This seems reasonable, since consumer health wearables have different main purposes (e.g. lifestyle, fitness or health) and collected various levels of sensitive data along these purposes. Another indicator of the usefulness of this attribute relates to the fact that all four attributes are significantly correlated with each other. SEN and HEA positively correlate to each other (r = .52), and both had negative regression weights to the first dimension; for the attributes LIF and FIT, it is the other way around. We conclude that the dimension’s relationships with these attributes are of opposite signs. Dimension one indicates whether the device has a health focus (high sensitivity) or a fitness/lifestyle focus (low sensitivity). This accounts for the fact that health-focused devices in our population collected more sensitive data than lifestyle-focused or fitness-focused devices. Kenny and Connolly (2016) call this from illness to fitness, while Alrige and Chatterjee (2015) differentiate between monitoring (medical), prevention (fitness), and communication (lifestyle). In sum, the first dimension can be labeled perceived data sensitivity, which ranges from health-focused to fitness-focused and lifestyle-focused devices. While this labeling order is reasonable, it cannot be proved in our dataset; we described the continuum using high vs. low.

In contrast to dimension one, only one attribute had a significant relationship with dimension two. The attribute DVA explains a high amount of variance and has a high regression weight in this analysis (β = .49). Thus, we stated that this attribute appropriately describes dimension two and can be clearly distinguished from the other dimensions. Since we surveyed the associated attribute using the bipolar scale a wide variety of data is collected vs. a low variety of data is collected, we label this dimension perceived data variety; we described the continuum of this dimension using high vs. low.

Only one attribute, TRA, had a significant relationship with dimension three and explains a high amount of variance (β = .48). Thus, we labeled the third dimension perceived tracking activity, on the continuum permanently to not permanently.

These three dimensions (SEN, DVA and TRA) define the spatial space of individuals’ perceptions of privacy risks. Following our MDS approach, each of the 35 randomly selected devices is now located in this perceptual space based on our second round of data collection, where the respondents had to rate each consumer health wearable concerning all nine attributes (Robinson and Bennett 1995). The spatial positions of all 35 devices are illustrated in Figure 2. For readability, the consumer health wearables are numbered from 1 to 35 in this perceptual map (e.g. Jawbone Up Move as HW 1). The letters from A to H
represent the eight different privacy types derived from the three dimensions (data sensitivity, data variety and tracking activity) and their continuums (high vs. low; permanently to not permanently). To illustrate the spatial positions of these eight privacy types (type A to type H) in a comprehensible way we connected the related HWs with lines.

**Figure 2. Individuals’ Perceptual Map of Privacy Risks of Consumer Health Wearables**

Concerning our research question, we can state that the most relevant dimensions to distinguish consumer health wearables according to individuals’ perceptions of privacy risks refer to the perceived sensitivity and variety of the collected data as well as perceived tracking activity. These dimensions are shaped using two extreme points. More specifically, individuals classify consumer health wearables based on their perceived data sensitivity and variety (high vs. low) and whether or not the data are permanently tracked. To account for the privacy type incidence and illustrate the specific characteristics in a comprehensible way, we use a hierarchical map to summarize the respondents’ ratings (Figure 3). To foster a deep understanding of our perceived privacy risk taxonomy, we provide one example from our population of each of these eight privacy types (type A to type H) in the appendix (Table 5).
Figure 1. Privacy Risk Taxonomy of Consumer Health Wearables Illustrated as a Hierarchical Map
Discussion

This study was motivated by the observation that “privacy issues play a critical role in determining individuals’ intention to adopt (consumer health wearables)” (Li et al. 2016, p. 8). Thus, we developed a perceived privacy risk taxonomy to understand the privacy perception of consumer health wearables and the primary dimensions behind this differentiation. We combined quantitative and qualitative techniques to limit the potential for errors of exclusion (Posey et al. 2013; Venkatesh et al. 2013), significant detriments to content validity (Kruskal and Wish 1978) and to reduce potential bias towards subjectivity on the part of the researchers during the analysis (Robinson and Bennett 1995). By focusing on the science of diversity (Posey et al. 2013) rather than that of uniformity (Lee and Baskerville 2003), we investigated a population of consumer health wearables with two different samples (Sample 1 N=35; Sample 2 N=21) and explored the privacy-related similarities and differences between the devices (McKelvey 1978; McKelvey 1982). Our taxonomy revealed that the most relevant dimensions to distinguish consumer health wearables according to the respondents’ perception of privacy risks refer to a) the perceived data sensitivity, b) perceived data variety, and c) perceived tracking activity. Based on these three main dimensions, we differentiated in three-dimensional point cloud eight consumer health wearable privacy types (type A to type H devices) and illustrated our taxonomy as a hierarchical map (Figure 3).

Although various studies that examine factors that affect perceived risks (Culnan and Bies 2003), we know little about the main dimensions that affect the perception of privacy risk concerning consumer health wearables. Therefore, our results targeted this research gap and reveal that the quantity of personal health data causes privacy risks perception and that the sensitivity of the collected personal health data is crucial to individuals. Our first dimension is in accordance with Li et al. (2016, p. 15), who note that “health information sensitivity (has) significant effects on individuals’ perceived privacy risk” and Dinev et al. (2013, p. 308), who “confirm that privacy risk attitudes are grounded in an individual’s values in terms of information sensitivity.” In particular, in the individual mind, fitness and lifestyle-focused devices collected less sensitive personal health data than health-focused devices. This result confirms previous studies, in which researchers reported that individuals found health or medical data much more sensitive than other information such as demographic, lifestyle habits, or purchasing behaviors (Vidmar and Flaherty 1985). It would be interesting to prove whether the continuum ranges from medically to health and from fitness to lifestyle-focused devices concerning the perceived data sensitivity.

The relevance of our second dimension (perceived data variety) confirms and extends the qualitative analysis of Motti and Caine (2015, p. 241), in which “the findings indicate that privacy concerns are not necessarily unique to one specific device or form factor, but are intimately related to the sensors embedded in the device.” Alrige and Chatterjee (2015) also pointed out that the number of different sensors causes the variety of the collected personal health data. Further, we demonstrated that perceptions of privacy risks were influenced by the variety of the collected personal health data. Our illustration of the eight privacy types and the qualitative statements indicated that the number of sensors, sensor type and its invasiveness influences perceived privacy risks. This assumption should be considered in a quantitative approach in further research.

One characteristic in our definition of consumer health wearables is that, personal health data is continuously gathered by biometrical sensors. However, the third dimension of our taxonomy illustrated that individuals distinguish between consumer health wearables more accurately in this aspect. They perceived different tracking activity levels, ranging from permanently to not permanently, even if, according to our definition, all consumer health wearables in our population objectively are capable to gather personal health data continuously. The perception of HW 4 (privacy type D) and HW 29 (privacy type C) illustrates this phenomenon. The device focus of both is very similar (fitness tracker) and individuals perceive for both devices (HW 4 and HW 29) low data sensitivity and high data variety. Although both devices factual continuously gathering personal health data, the perception of the tracking activity is different. As HW 4 is a digital fitness bracelet that can be seamlessly integrating in the everyday life Weiser and Brown (1997) and consequently, the individuals perceive a high tracking activity. In contrast HW 29, a digital sport insole, is only used in combination with a special shoe while training. Consistently, individuals perceive less tracking activity for digital insole (HW 29), although this device continuously gathers personal health data when used similar to the fitness bracelet (HW 4). Our taxonomy illustrated this new nuance between the objective tracking capability of the devices and
Concerning research stream two, to understand the adaption process and foster a successful diffusion, we established a fundamental understanding of perceived privacy risks in the context of consumer health wearables and provided evidence that perceived privacy aspects must be considered in the context of health technologies to understand the adaption process and foster a successful diffusion (Li et al. 2016).

Concerning research stream two, that analyzed privacy aspects as a main barrier in the adoption process,
Understanding Privacy Risk Perceptions of Consumer Health Wearables

Our perceived privacy risk taxonomy provides evidence for the reasons why numerous inconsistencies in findings appeared (e.g. Lee et al. 2015), and why we cannot theorize about the commonalities without first understanding the differences. By developing eight consumer health wearable privacy categories (privacy type A to privacy type H), we created a common nomenclature and answered the call for a systematic overview of health wearables to explore a primary barrier to a persistent adoption (e.g. Varshney 2014). Although individuals likely perceive lower privacy risks when using a privacy type A device compared to a privacy type H device, the de facto correlations between privacy risks and the eight privacy types should be addressed in further research.

Concerning research stream three, that explores specific factors that affect privacy risks of consumer health wearables, we provided an overview of the three main dimensions that individuals use to classify consumer health wearables according to their privacy risks. We uncover individuals’ prioritization of these three dimensions and revealed that the most relevant dimensions to distinguish consumer health wearables according to the respondents’ perception of privacy risks refer to the perceived data sensitivity, followed by perceived data variety, and the perceived tracking activity of the device. Thereby we could enhance the theoretical understanding of the complex mental construct of perceived privacy risks and may form the foundation for various privacy theory-building efforts (e.g. Dinev et al. 2016). The 1,500 collected qualitative statements could serve as a basis for a scale development process for perceived privacy risks in the consumer health wearable context.

Our taxonomy exposes the underlying cognitive dimensions of the mental construct and the interplay between a health technology for private users and privacy dimensions in individuals’ minds. Since our study has an exploratory focus, we did not differentiate, who is using the device and who is collecting the personal health data (e.g. provider, hospital, insurance company). Although – owing to the relatively young sample with likely fewer health insights and chronic illnesses – the generalizability of our findings might be restricted, we provide researchers with rich insights into the complex psychological process of individuals’ perceived privacy risks concerning health technologies. This could serve as a basis for comparing our results with perceptual maps of other health technologies (i.e. professional health wearables) and/or other sharing policies (i.e. physician, insurance company, hospital) and uncover the universal antecedents that influence individuals’ privacy risk perception and the dimensions.

**Practical Implications**

Our taxonomy has a high practical relevance by focusing on individuals’ privacy perceptions of consumer health wearables. We sought to establish a fundamental understanding of perceived privacy that allows providers to develop consumer health wearables in a privacy-focused manner (Motti and Caine 2015). According to the eight privacy device types developers can identify possible target configurations of their future devices. Our proposed perceived privacy risk taxonomy can also be used to segment the market by identifying comparable devices or possible competitors from a privacy perspective.

By developing a taxonomy that is strongly based on perceptual maps, developers can learn which privacy aspects affect individuals in relation to a specific device type. In this sense, the taxonomic efforts highlight the potential difficulties experienced by providers as they seek to enter the market with new devices. We identified the three main dimensions that individuals prioritize in regard to their privacy perception. Until now these dimensions can serve as a guideline for developers when deciding on the configuration of a new device, with specific features, biometrical sensors or tracking technologies. For research and practice, it would be interesting whether and how the privacy perceptions and the perceptual maps of providers of consumer health wearables differ from the perceptual maps of actual and potential users of consumer health wearables. Such a comparison could provide rich insights for developing successful and privacy-friendly devices. Furthermore, confirming a misfit of consumers’ and providers’ perceptual maps of privacy risks could explain the currently still lagging adoption of consumer health wearables in the market (e.g. Kang et al. 2013; Lee et al. 2015).

Finally, using a common nomenclature based on individuals’ perception, our taxonomy provides a comprehensive assessment of recent consumer health wearable devices that can be compared to other mobile health technologies. Developers, providers, and health professionals can discuss the privacy efforts concerning consumer health wearables, can customize their devices along individuals’ privacy perception, and can more efficiently utilize resources so as to develop new devices. In general, our research gives practitioners a full view of recent health wearables for private users “to understand and characterize
privacy disclosure tradeoffs inherent in sharing (health) data, and develop data transformation methods to limit privacy risks” (Kotz et al. 2016, p. 25).

**Limitations and Further Research**

First, a key methodological limitation is that respondents’ fatigue can be a strong concern when collecting the paired similarity ratings used by MDS (Posey et al. 2013). Furthermore, the virtual texted-based presentation of a haptic device could influence the perception of privacy. To prevent fatigue and ensure high comprehensibility and involvement until the end of the procedure, we conducted one-to-one interviews with short breaks for the respondents.

Second, the interaction between a wearable device and an individual is complex (Wieneke et al. 2016). We interviewed users and non-users of consumer health wearables to approximately replicate the adoption ratio of 10% in this age group (Ledger and McCaffrey 2014), but previous experiences with other devices could likely play a key role in determining the perceived privacy of a given wearable device. Further research could use our sample of consumer health wearables and the applied four-step mixed-method taxonomy development process MDS approach to compare the perceptual maps of non-users and users.

Third, we have chosen a hierarchical map and a three-dimensional point cloud to illustrate individuals’ perceptual map of perceived privacy risk of consumer health wearables. To examine the distances of the device, further research can conduct a cluster analysis to classify the devices into groups within the predefined space (Timm 2002). Our taxonomy development based on individuals’ imagined interaction with the presented device on the websites and its actual features. Therefore, we evaluated a status quo of the perceived privacy risks concerning the sampled consumer health wearables. The examples of Vuzix Smart Glasses (HW33) and the Apple Watch (HW16) show the subjectivity and transient nature of these risk perceptions. For instance, if smart glasses will be more popular, or smartwatches integrated new apps or cross-connections that may seem more invasive, the privacy risk perceptions will change and consequently the privacy type of the device. A longitudinal study could evaluate these taxonomy changes by exploring the privacy perceptions of specific devices over a period of time or especially after new software and app installations.

Fourth, we conduct the steps 2 and 4 of our methodology with younger people (approx. <30 years) as one target group of the bimodally distributed uptake of consumer health wearables. We assumed that a younger population could possess more extensive knowledge in the area of digital technologies and sufficient cognitive capacities to evaluate the devices as the second target group of older people (approx. >55 years). However, concentrating on the younger group with likely fewer health insights and chronic illnesses, restrict the generalizability of our perceived privacy risk taxonomy. Therefore, it would be interesting to compare our results and especially the developed taxonomy with an older population or individuals with chronic diseases. For instance, researchers could adapt our methodology for clinical technologies or other medical devices (professional health wearables) to explore the privacy perception of individuals (i.e. elderly adult diabetic patients concerning in-home monitoring technologies) and analyze whether additional dimensions of privacy risks emerge (e.g. Chatterjee et al. 2012).
## Appendix

### Table 4. Description of Sample 1 (N=35) and Sample 2 (N=21)

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Sample 1</th>
<th>Sample 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2: Acquisition of Privacy-related Similarity Ratings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4: Mapping and Labeling the Dimensions Using ProFit Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sample Size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>35</td>
<td>21</td>
</tr>
<tr>
<td>Gender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>19</td>
<td>10</td>
</tr>
<tr>
<td>Female</td>
<td>16</td>
<td>11</td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average</td>
<td>24.5</td>
<td>24.9</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Non-User</td>
<td>30</td>
<td>18</td>
</tr>
<tr>
<td>Education Level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>High/Secondary School</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>Bachelor</td>
<td>12</td>
<td>9</td>
</tr>
<tr>
<td>Master</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>PhD</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Employment Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employed</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>Self-employed</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Student</td>
<td>15</td>
<td>6</td>
</tr>
<tr>
<td>Unemployed</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>
### Table 5. Exemplary Instances of the Identified Eight Privacy Types of Consumer Health Wearables

<table>
<thead>
<tr>
<th>Privacy Type</th>
<th>Perceived Characteristics</th>
<th>Devices in this Type</th>
<th>Example Device</th>
<th>Company &amp; Device Name</th>
<th>Link to Product Website (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>-Low data sensitivity</td>
<td>HW 8, HW 17, HW 32</td>
<td>HW 8</td>
<td>Amulyte</td>
<td><a href="http://www.amulyte.com/">http://www.amulyte.com/</a></td>
</tr>
<tr>
<td></td>
<td>-Low data variety</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Not permanently</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>-Low data sensitivity</td>
<td>HW 1, HW 13, HW 18, HW 27</td>
<td>HW 1</td>
<td>Jawbone Up Move</td>
<td><a href="https://jawbone.com/fitness-tracker/upmove">https://jawbone.com/fitness-tracker/upmove</a></td>
</tr>
<tr>
<td></td>
<td>-Low data variety</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Permanently</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>-Low data sensitivity</td>
<td>HW 19, HW 22, HW 24, HW 29, HW 34</td>
<td>HW 29</td>
<td>3L Labs Footlogger</td>
<td><a href="http://footlogger.com:8080/hp_new/footlogger/">http://footlogger.com:8080/hp_new/footlogger/</a></td>
</tr>
<tr>
<td></td>
<td>-High data variety</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Not permanently</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>-Low data sensitivity</td>
<td>HW 4, HW 21, HW 25, HW 26</td>
<td>HW 4</td>
<td>Jawbone Up3</td>
<td><a href="https://jawbone.com/fitness-tracker/up3">https://jawbone.com/fitness-tracker/up3</a></td>
</tr>
<tr>
<td></td>
<td>-High data variety</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Permanently</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>-High data sensitivity</td>
<td>HW 7, HW 10, HW 12, HW 15, HW 28, HW 33</td>
<td>HW 28</td>
<td>Qardio Core</td>
<td><a href="https://www.getqardio.com/qardiocore-wearable-ecg-ekg-monitor-iphone/">https://www.getqardio.com/qardiocore-wearable-ecg-ekg-monitor-iphone/</a></td>
</tr>
<tr>
<td></td>
<td>-Low data variety</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Not Permanently</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>-High data sensitivity</td>
<td>HW 16, HW 30, HW 31</td>
<td>HW 30</td>
<td>LG Gizmopal VC100</td>
<td><a href="http://www.lg.com/us/cell-phones/lg-VC100-Pink-gizmopal">http://www.lg.com/us/cell-phones/lg-VC100-Pink-gizmopal</a></td>
</tr>
<tr>
<td></td>
<td>-Low data variety</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Permanently</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-High data variety</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Not permanently</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-High data variety</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Permanently</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
References


Understanding Privacy Risk Perceptions of Consumer Health Wearables


