Risk Perceptions for Wearable Devices

Anonymous
Some Place

ABSTRACT

Wearable devices bring great benefits but also new potential privacy and security risks that could expose users' activities without their awareness or consent. Effective design of notifications and security controls for wearable devices will require careful foresight to prevent habituation by treating user attention as a scarce resource, which requires understanding which risks have the potential to be most concerning to users. In this paper, we describe a large-scale survey that we conducted to investigate user security and privacy concerns regarding wearable devices. We surveyed 1,782 Internet users about their perceptions of wearable devices, in order to identify risks that are particularly concerning to users. We specifically controlled for the effects of data type and data recipient on the magnitude of perceived risks, while also collecting open-ended concerns. Finally, we compared wearable device risks to those of more familiar technologies. We hope that this work will inform design of future privacy and security controls for wearable devices.

Keywords

Privacy, Security, User Studies, Risk Perception, Ubiquitous Computing, Wearable Devices

1. INTRODUCTION

Wearable technologies, or "wearables," are a $700 million industry [2] that may see significant growth in the near future: one market research company estimates that 52% of technology consumers are aware of wearables and 33% are likely to buy one [6]. With 20% of the general population owning at least one wearable and 10% using it daily [11], wearables are bringing ubiquitous computing to everyday life.

Wearable devices offer many compelling opportunities for benefiting users. For instance, they could enable more natural, human-centered interface experiences and healthier, fitness-data inspired lifestyles. There will likely be many more applications in the future that take advantage of data captured by wearable devices. However, wearable devices also bring new potential privacy and security risks that could expose users' activities without their awareness or consent. Even though wearable technology is currently in early stages, we have already seen manifestations of these risks. For instance, Fitbit's default privacy settings inadvertently exposed information about some of their users' sexual activity [25], resulting in the inadvertent disclosure of sensitive information. Public discomfort toward facial recognition caused Google to prohibit Google Glass applications from using facial recognition [37], and public concerns about privacy may have partly contributed to Google's discontinuation of Glass [15, 47, 35, 14].

Similar privacy [30, 48, 50] and security issues [17, 19] pervade smartphones. Mobile platforms have tried to address the risks by communicating data capture to users. However, many users are habituated to these notifications, because they see them frequently, often for things that they do not care about [20]. Once habituated to seemingly benign privacy and security warnings, users tend to ignore more sensitive warnings that are similarly designed [16].

With the additional capabilities of wearable devices and their increasing popularity, people have expressed interest in being notified before data is captured [13]. However, the possible data types that these devices will be able to capture is likely to dwarf those currently captured by smartphones. Because human attention is a finite resource [7], bombarding users with notifications for every conceivable data capture is likely to be counter-productive as it can lead to user frustration and habituation. Therefore, user concerns need to be investigated so that systems can warn users only about the situations they are likely to care about.

The goal of this work is to gain a better sense of users' privacy concerns when interacting with wearable devices, so that future systems can take these concerns into account when designing privacy notifications. To our knowledge, this is the first large-scale study to investigate user security and privacy concerns for wearable devices. We surveyed 1,782 Internet users about their perceptions of wearable devices and contribute the following:

- We compare users' perceptions of a range of privacy and security risks of wearables. We found that user concern is driven more by the type of data being captured than the recipient of the data.
- We shed light on how users feel about various data recipients. We observed that users make less distinction between sharing data with friends, co-workers, and the general public, compared to sharing with an application's servers (the latter is viewed as less concerning).
- We analyze users' self-reported top concerns regarding wearable devices. The results give a sense of what broad concerns users have, which can be used to guide future research on unexplored use cases.
- We examine how serious users perceive the risks of

wearables to be, compared to risks associated with more familiar technologies. Most of our participants saw wearables' new capabilities as benign, though we suspect that this could be due to a lack of exposure to these newer technologies.

2. RELATED WORK

In this section, we outline previous research that has examined privacy for ubiquitous and wearable computing environments, smartphone privacy and security, as well as user risk perceptions and behaviors.

2.1 Ubiquitous and Wearable Devices

Many authors have emphasized that we are rapidly moving towards a world of ubiquitous sensing and data capture, with ensuing privacy challenges [1, 40, 8]. Many researchers have worked to study how privacy can be preserved in the presence of ubiquitous devices. Examples of such efforts include frameworks to design for privacy [4, 9, 31], protocols for anonymous communication [12], evaluation metrics for privacy [49], and privacy models [26, 28]. However, none of these works attempted to quantify or rank user concern over different privacy risks.

Roesner *et al.* urge the community to address potential concerns for wearable devices before the technologies become widespread [46] and explore the unique and difficult problems these devices present in terms for law and policy [45]. A small-scale interview of how bystanders feel about wearable devices found that bystanders were predominantly split between having indifference and negative reactions to the device, but expressed clear interest in being able to give permission for data to be captured [13]. Our research furthers this goal of communicating risks to users and bystanders.

2.2 Smartphones

Many researchers have attempted to study user concerns about security or privacy issues associated with their smartphones. Research shows that perceptions of risk change based on the particular device being used. Chin *et al.* found that users' attitudes toward security and privacy for smarphones significantly differed from attitudes towards traditional computing systems [10]. How people used their smartphones also differed from how they used other computing systems. Palen *et al.* tracked smartphone users for six weeks and observed radical changes with respect to how they used their devices [41]. People also perceive and behave without a realistic understanding of the risks they are taking. Felt *et al.* examined the Android permission system and found that 17% of participants paid attention to permission requests, and only 3% comprehended what these permissions meant.

Smartphones allow applications to access new types of data. While this tends to benefit users, they do not think of the privacy implications. Lindqvist *et al.* studied a popular location tracking application, and found that people share their location information for gaming, signaling availability to friends, without concern for the privacy implications of broadcasting that information [33]. Tsai *et al.* found that when mobile users get feedback about releasing data, such as who has viewed location information, it greatly impacts future behaviors [53]. However, this type of feedback is not generally provided to users. There are still many unresolved concerns, such as the opaqueness that prevents users from fully understanding how applications are using their data or rogue applications inappropriately accessing data [29, 58].

2.3 User Perceptions and Behaviors

In this paper, we focus on measuring user perceptions of security and privacy risks, as they relate to wearable devices. One limitation of user perceptions is that people do not always have enough information to make privacy-sensitive decisions; even if they do, they often trade off long-term privacy for short-term benefits [3]. Also, actual behavior may deviate from self-reported behaviors [27] and stated privacy preferences [51].

While risk communication for the physical world has been examined for several decades (e.g., [21, 36]), research into effectively communicating computer-based risks has only recently been researched. For example, both Garg *et al.* and Blythe *et al.* show that due to varying perceptions and abilities that correlate with demographic factors, computer-based risk communication should employ some degree of demographic targeting [24, 5]. While this work is likely applicable to wearable computing risk communication, we believe that a better understanding of users' risk perceptions in this domain is warranted, prior to examining risk communication.

3. METHODOLOGY

To obtain a comprehensive list of possible risks that wearable devices might present in the future, we examined the sensors, capabilities, permissions, and applications of the most popular wearable devices on the market. At the time of this study, August 2014, the most popular wearable devices included the Fitbit fitness tracker, which continuously monitors heartbeat, steps taken, and sleep patterns [22, 52]; the Pebble smartwatch, which can take pictures, send texts, show notifications from online, and push notifications to services [42, 56, 44]; and Google Glass [57, 54]. We used these wearable devices, along with other comparable wearable devices on the market, as inspiration to develop a list of security and privacy risks that users might be concerned about.

We designed a survey to gauge what risks users consider to be relevant. Our survey contained two main sections. In one section, we presented participants with several scenarios—something undesirable that might happen with their wearable device—and asked them to rate their level of concern if each scenario were to happen. This was intended to elicit their perception of the severity and impact of the risk. The format of this section was based on Felt *et al.*'s study of user perceptions of security and privacy risks with mobile devices [18]. In the other section, we asked participants to compare the risks and benefits of wearable technologies to those of better-understood technologies, following the same methodology from Fischhoff *et al.*'s seminal study in risk perception [21].

3.1 Motivation

In this section, we describe the two prior works on which we based our survey format: Felt *et al.*'s survey of smartphone-based risks [18] and Fischhoff *et al.*'s survey of more general technology-based risk perceptions [21].

3.1.1 Smartphone Risk Scenarios

Felt *et al.* previously studied the security concerns of smartphone users by conducting a large-scale online survey [18]. Their survey asked 3,115 smartphone users about 99 risk scenarios. Participants were asked how upset they would be if a certain action occurred without their permission. Participants rated each situation on a Likert scale ranging from "indifferent (1)" to "very upset (5)." Our methodology closely follows that study, but with scenarios chosen to shed light on the security and privacy risks of wearable devices.

3.1.2 Technology Risk Perceptions

Fischhoff *et al.* performed a seminal study of the perceived risks surrounding 30 widely used technologies [21]. In their study, participants were asked to separately rate the risks and benefits for these technologies. They told participants to think about all people affected by the technology, and to think about long-term versus short-term risks and benefits. Then, the participants rated these technologies with respect to each other on a numerical scale, being instructed to rate the least risky or least beneficial technology a 10 and scaling the ratings linearly (e.g., a technology with a risk rating of 20 is considered twice as risky as compared to a technology with a risk rating of 10). We apply their methodology to evaluate the perceived risks and benefits of several technologies related to wearable computing and how these technologies compared to more familiar technologies.

3.2 Survey Questions

In our survey, each participant answered 27 questions, across five different sections:

- 2 reading comprehension questions
- 6 questions about wearable computing scenarios
- 2 questions about smartphone scenarios
- 2 Fischhoff-style risk/benefit questions
- 15 demographic questions

We randomized the order participants saw sections of the survey (with the exception of the comprehension and demographic questions, which were always first and last, respectively), as well as the order of questions in each section.

3.2.1 Comprehension Questions

Because participants might be biased to specific companies (e.g., visceral reactions to Google Glass based on popular media stories), we based our questions on a fictitious wearable. Thus, the beginning of the survey introduced participants to the "Cubetastic3000," which was the basis for all questions on wearables risks. We highlighted the capabilities of this device and described use cases:

> *Imagine that you are the proud owner of the Cubetastic3000, a new, high-tech computing device designed to be worn on your head. Imagine also that you wear this device all the time, because it is very lightweight, durable, and convenient.*
>
> *The Cubetastic3000 has the capability to capture video, photos, audio, and biometrics (biological data about you, such as heart rate). Just like other devices today, you can install third-party applications from an app store, and these applications can use the information that the Cubetastic3000 captures.*
>
> *With a wide range of applications and capabilities, your device can do all sorts of things, such as:*
>
> *—measuring heart rate, breathing, and other things to keep track of your fitness level and overall health*
>
> *—look at what you see to provide information about what's around you*
>
> *—allow you to take notes just by telling the device what you need to remember*
>
> *—take videos of you or what you see to share with others*
>
> *—automatically take photos or video so that you can replay events that previously happened*
>
> *—play music that you like for you when it detects that no one is around*
>
> *—infer information about you so you don't need to log in or search for the same thing over and over*
>
> *...and much more!*

To ensure that participants had read and understood this device's capabilities, since it would form the basis for many of our survey questions, we ask them two multiple-choice comprehension questions about the device's capabilities and where it might be worn. We filtered out responses from participants who could not answer these questions.

3.2.2 Wearable Scenarios

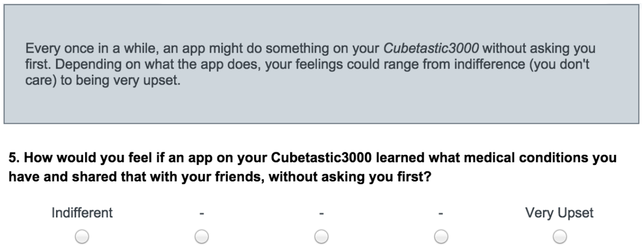
We presented scenarios involving data captured by the Cubetastic3000 and asked participants to rate how upset they would be if a particular type of data (e.g., video, audio, gestures, etc.) were shared without permission with a particular data recipient (see Figure 1). Responses were reported on a 5-point Likert scale (from "indifferent" to "very upset"), following Felt *et al.* [18]. Questions were of the form:

"How would you feel if an app on your Cubetastic3000 learned <data> and shared it with <recipient>, without asking you first?"

We created an initial pool of 288 questions by combining 72 data types (<data>) with 4 data recipients (<recipient>):

- Your work contacts
- Your friends
- The public
- The app's server (but didn't share it with anyone else)

The purpose for using this question format was to determine how upset participants would be if data were inappropriately shared, and the extent to which their reactions were based on the data type and recipient. Each participant answered



Every once in a while, an app might do something on your *Cubetastic3000* without asking you first. Depending on what the app does, your feelings could range from indifference (you don't care) to being very upset.

5. How would you feel if an app on your Cubetastic3000 learned what medical conditions you have and shared that with your friends, without asking you first?

Indifferent	-	-	-	Very Upset
○	○	○	○	○

Figure 1: An example of a wearable scenario question participants saw while taking the survey.

6 questions that were randomly drawn from a pool of 293: the 288 described here, plus 5 that we describe in the next section (Section 3.2.3).

3.2.3 Smartphone Scenarios

We presented participants with a second set of scenarios to control for the type of device being used. Rather than using the previous pool of 288 <data> and <recipient> combinations, we selected 5 scenarios that Felt *et al.* found least and most concerning to their participants [18]:

1. *How would you feel if an app on your <device> vibrated your phone without asking you first?*
2. *How would you feel if an app on your <device> connected to a Bluetooth device (like a headset) without asking you first?*
3. *How would you feel if an app on your <device> unmuted a phone call without asking you first?*
4. *How would you feel if an app on your <device> took screenshots when you were using other apps, without asking you first?*
5. *How would you feel if an app on your <device> sent premium (they cost money) calls or text messages, without asking you first?*

In the previously described section of our survey, <device> was set to "Cubetastic3000" and not every participant received one of these questions (i.e., these 5 questions were among the pool of 293 questions from which participants were randomly assigned 6). In the separate smartphone section of the survey, every participant received exactly two of these questions, where <device> was set to "smartphone." This allowed us to perform controlled comparisons based on whether the same misbehavior was occurring on a smartphone (i.e., a better understood device) or the Cubetastic3000 (i.e., a fictitious wearable device).

3.2.4 Risk and Benefit Assessment

In addition to investigating reactions to particular scenarios, we examined broad perceptions of new technologies and how those compared to perceptions of other understood technologies. We modeled this section after a seminal risk perception study by Fischhoff *et al.* [21], in which participants ranked technologies by their relative risk and benefit to society. We asked participants to perform this exercise for 4 technologies previously examined by Fischhoff *et al.*: handguns, motorcycles, lawnmowers, and electricity. These technologies were chosen to span varying levels of risks and benefits.

Alongside the 4 studied technologies, we asked participants to evaluate one of 20 technologies relevant to wearables: Internet, email, laptops, smartphones, smart watches, fitness trackers, Google Glass, Cubetastic3000, discrete camera, discrete microphone, facial recognition, facial detection, voice recognition, voice-based emotion detection, location tracking, speech-to-text, language detection, heart rate detection, age detection, and gender detection. We asked about familiar technologies such as the Internet, general and specific wearable artifacts, and a range of new capabilities.

To parallel Fischhoff *et al.*'s risk perception study, we gave our participants a similar prompt to numerically express the perceived gross risk/gross benefit over a long period of time for all parties involved. We randomized whether they performed the ranking for risks or benefits first. The prompt is listed in Appendix A. The question format was as follows:

Fill in your <risk/benefit> numbers for the following:

Handguns: ______
Motorcycles: ______
Lawnmowers: ______
<Wearable Technology>: ______
Electricity: ______

3.2.5 Additional Questions

The exit portion of the survey contained demographic questions asking for age, gender, and education. We also asked participants if they owned a wearable device so we could control for prior exposure, and included an open-ended question on what would be the most likely risks associated with wearable devices. We ended with the 10-question Internet Users' Information Privacy Concerns (IUIPC) index [34], so we could control for participants' general privacy attitudes.

3.3 Focus Group

We conducted a one-hour focus group to validate our design, gauge comprehension, and measure fatigue. The focus group began with participants taking the survey. Afterward, we asked participants to give feedback on the format and the content, noting any instructions or questions that were unclear. The focus group concluded with a discussion of possible benefits and risks of wearable devices, in order to brainstorm any additional scenarios to include. Finally, we compensated participants with $30 in cash. We recruited all of our focus group participants from Craigslist. Of the 13 participants, 54% were female, and ages ranged from 18 to 64 ($\mu = 36.1$, $\sigma = 15.3$). Education backgrounds ranged from high school to doctorate degrees, and professions included student, artist, marketer, and court psychologist.

3.4 Recruitment and Analysis Method

We recruited 2,250 participants over August 7–13, 2014 via Amazon's Mechanical Turk. We restricted participants to those over 18, living in the United States, and having a successful HIT completion rate of 95% or above. We compensated each participant with $1.75 upon successfully completing the survey. Based on incorrect responses to either of the two comprehension questions, we filtered out 366 (16% of 2,250) participants. We filtered out an additional 99 participants (4% of 2,250) due to incomplete responses, and three participants who were under 18, leaving us with a total sample size of 1,782. Of these, 57.9% were male (1,031), 41.0% were female (731), and 20 participants declined to state their genders. Ages ranged from 18 to 73, with a mean of 32.1 (σ = 10.37). Almost half of our participants had completed a college degree or more (49.2% of 1,782), which includes the 219 (12.3% of 1,782) who reported graduate degrees. While our sample was younger and more educated than the U.S. population as a whole, we believe it is still consistent with the U.S. Internet-using population.

In performing our analysis in the next section, we chose to focus on the very upset rate (VUR) of each scenario. The VUR is defined as the percentage of participants who reported a '5' on the Likert scales. We use the VURs rather than the average of all Likert scores for the same reasons as Felt *et al.*: the VUR does not presume that the ratings, ranging from "indifferent" to "very upset," are linearly spaced. Additionally, most people are likely to be upset, at least a little, in all scenarios, because a device is taking action without permission (rating distribution: "1"= 759, "2" = 918, "3" = 1,452, "4"' = 2,421, "5" = 8,344). Thus, the main distinguishing factor of a participant reacting to a given scenario is whether they were maximally upset or not, rather than how upset they were. However, one limitation of this approach is that it only allows us to make *relative* comparisons between scenarios, rather than being able to definitively state how upset people might be if a single scenario were to occur.

We followed Fischhoff *et al.*'s methodology and did not normalize the numerical responses. Rather, we report medians and quartiles, which are not impacted by outliers. For the open-ended question at the end (i.e., additional privacy concerns), two researchers independently coded 1,782 responses, with an initial agreement rate of 89.7%. The researchers discussed and resolved any disagreements so that the final codings reflect unanimous agreement.

4. RESULTS

In this section, we present participants' responses to the various data-sharing scenarios, and how data type, data recipient, and device contributed to their risk perceptions. Next, we discuss participants' risk/benefit assessment of various new technologies relative to well-established technologies. We conclude the section with participants' self-reported concerns about the biggest risks in owning wearable devices.

4.1 Concern Factors

Many factors impact participants' concern levels for each scenario: the data recipient, the data type, and whether or not the scenario occurred on a wearable or a smartphone. We analyze each factor individually, as well as present a statistical model of participants' concerns as a function of all of the factors, including demographic traits.

4.1.1 Data Type

Based on our statistical models (later reported in Section 4.3.2), we observed that the largest effect on participants' VURs stemmed from the type of data being shared; data recipient and device type had weaker impacts on overall VURs. The most and least concerning data types are listed in Table 1, and the full list can be seen in Table 9 in Appendix C.

Participants were most concerned about photos and videos, especially if they contained embarrassing content, nudity, or financial information. As seen in Table 1, photos and videos accounted for five of the top ten concerns, and are almost unanimously considered to be concerning. Information that could be used to impersonate someone (e.g., usernames/passwords for websites), or photos of someone at home, were also among the most concerning data types.

Participants were least concerned about data that could be collected through observations of public behavior, such as demographics (e.g., age, gender, language) or information available to advertisers (e.g., TV shows watched, music on device). As seen in Table 1, participants' responses had a greater amount of variance. This greater variance and overall decreased concern may be because of uncertainty with how the data would be used, or because the financial, social, or physical consequences would be less immediate.

Although certain data is considered unanimously upsetting to have shared, it is interesting to note that no data was considered unanimously non-upsetting to have shared, nor were there any data types that evoked strong disagreement between participants (i.e., bimodal). Generally, the average concern magnitude was inversely correlated with the standard deviation, which suggests the presence of ceiling effects for the most concerning data types. For the complete ranked list of data types in this study, see Appendix **??**.

4.1.2 Data Recipient

There was a statistically significant difference in VUR for data sent to an application's servers compared to data sent to human recipients. On average, 42% of participants stated that they would be "very upset" if their data was shared with only an application's servers, whereas the VURs for friends (70%), work contacts (75%), and the public (72%) were almost double (Table 2). A chi-square test indicated that these differences were statistically significant (Table 3). However, these effect sizes were small: the largest effect was between work contacts and an app's server ($\phi = 0.11$); while the VUR for sharing with work contacts was significantly higher than sharing with friends, the effect size was negligible ($\phi = 0.004$).

We note that this chi-square test violates the assumption of independent observations, since participants responded to multiple scenarios with multiple recipients. But based on the randomization of treatments and large sample size, we do not believe that this significantly impacted our results. Similarly, we are unaware of a more appropriate test, given our data format. Cochran's Q requires binary outcomes (i.e., participants would have had to answer only one question for each data recipient, preventing us from adequately controlling for data type) and a repeated measures ANOVA requires normality (our data was not normally distributed). Nonetheless, we repeated our analysis using only one randomly-selected data point per participant and found that our selected test was robust to this violation. Therefore, we conclude that participants were significantly more concerned about having their data seen by a human versus an application, though differences between specific human groups such as the public, friends, and work contacts were not as significant.

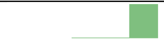
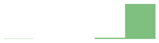
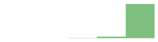
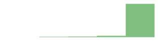
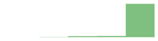
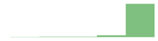
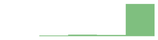
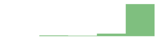
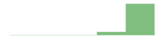
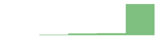
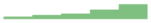
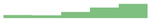
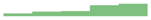
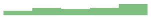
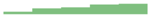
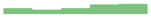
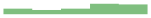
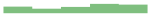
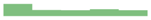
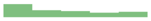
Rank	Data	VUR	σ	Distribution
1	video of you unclothed	95.97%	0.31	
2	bank account information	95.91%	0.35	
3	social security number	94.84%	0.26	
4	video entering in a PIN at an ATM	92.67%	0.47	
5	photo of you unclothed	92.59%	0.46	
6	photo of you that is very embarrassing	91.39%	0.55	
7	username and password for websites	89.55%	0.62	
8	credit card information	88.98%	0.56	
9	video of you that is very embarrassing	88.41%	0.53	
10	photo of you at home	87.50%	0.60	
	⋮			
64	eye patterns (for eye tracking)	40.51%	1.27	
65	exercise patterns	38.66%	1.26	
66	when you are happy or having fun	34.75%	1.27	
67	television shows watched	30.20%	1.40	
68	when you are busy or interruptible	29.50%	1.26	
69	music on device	28.06%	1.43	
70	your heart rate	27.50%	1.40	
71	age	24.29%	1.43	
72	language spoken	15.86%	1.49	
73	gender	15.00%	1.45	

Table 1: The 10 most and least upsetting data types, across all recipients. For the complete list of all data types across all recipients, see Appendix C.

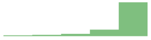
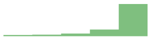
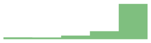
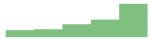
Rank	Recipient	VUR	sigma	Distribution
1	Work Contacts	75.16%	0.94	
2	Public	72.41%	0.98	
3	Friends	69.47%	1.02	
4	App's Server	42.28%	1.15	

Table 2: The overall upset rate for all recipients.

Recipients	χ^2	p-value	n	ϕ
Work-App	565.910	<0.0001	5,083	0.111
Public-App	481.776	<0.0001	5,1988	0.093
Friends-App	381.653	<0.0001	5,096	0.075
Friends-Work	20.39	<0.0001	5,037	0.004
Friends-Public	5.41	<0.0200	5,142	0.001
Work-Public	5.00	<0.0253	5,129	0.001

Table 3: Results of a chi-square test to examine VUR based on data recipient, across all data points.

We do not claim that there are no distinctions between the friends, public, and work contact recipients. People are more comfortable sharing certain data types with certain human data recipients. For instance, participants were significantly uncomfortable sharing if they were lying, nervous, or stressed to work contacts compared to the rest of the data recipients. Participants were much more comfortable sharing phone use and products purchased with an application server than with human recipients. Table 12 Appendix C shows the complete VUR and rankings of all data types by recipient.

4.1.3 Device

Recall that each participant answered 2 questions drawn from a set of 5 regarding their reactions to smartphone misbehaviors. To compare these misbehaviors with misbehaviors on the Cubetastic3000, we included these same 5 questions amongst the pool of 293 Cubetastic3000 scenarios, only modifying the device type. In this manner, while all 1,782 participants received 2 smartphone questions, there were 159 participants who received at least one of these questions in relation to the Cubetastic 3000. Across all participants, the VUR was 46.7% (of 1,782) when describing smartphones,

Misbehavior	Cubetastic3000	Smartphone
All	58.79%	46.67%
Vibration	14.81%	6.14%
Bluetooth	44.12%	19.86%
Unmuted Call	87.10%	58.44%
Screenshot	52.78%	55.74%
Premium Calls/Texts	86.49%	91.94%

Table 4: VURs for the five questions about device misbehaviors described in Section 3.2.3, contrasting smartphones with the Cubetastic3000.

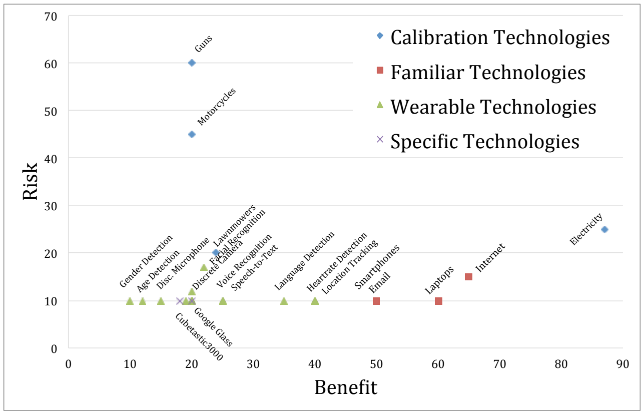


Figure 2: Participants' median risk-benefit ratings of technologies examined by Fischhoff *et al.* [21], which we used for calibration, alongside familiar technologies (e.g., laptops, the Internet, etc.), wearable technologies, as well as two specific wearable devices (Google Glass and the Cubetastic3000).

whereas the VUR increased to 58.8% (of 159) when describing these same misbehaviors on the Cubetastic3000. The VURs for both devices for all 5 questions are in Table 4.

To ensure independence of observations, we performed a Mann-Whitney U test to compare participants' average VURs for the Cuebtastic3000 scenarios (i.e., 159 participants) to the remaining participants' average VURs for the smartphone scenarios (i.e., 1,623 participants). This difference was statistically significant ($U = 108,664.0$ with $p < 0.0005$), however, the effect size was very small ($r = 0.08$). Because of this small effect size, we did not further reduce our statistical power by separately comparing each of the 5 misbehaviors. We conclude that while in general users are likely to be more wary of misbehaviors occurring on wearable devices than smartphones, the difference is likely negligible. The entire effect may be due to participants' increased familiarity with smartphones, and therefore may disappear as they increasingly encounter more wearable devices.

4.2 Risk and Benefit Rankings

We asked participants to rate new capabilities related to wearable technologies (e.g., facial recognition) in terms of their risks and benefits. We also asked them to do this for technologies with which they were likely to be more familiar (e.g., smartphones and laptops) in addition to two examples of specific wearable devices, Google Glass and the fictitious Cubetastic3000. To calibrate our results, we also asked about four well-established technologies studied by Fischhoff *et al.* [21]. We found that participants generally rated technologies related to wearables as being low-risk comparatively to other technologies (Figure 2). Tables 10 and 11 in Appendix C shows participants' median, quartiles, and distributions of risks and benefit ratings for all technologies. We found that the calibration technologies, which were more familiar to the participants, were all rated as the most risky.

As a group, participants rated more familiar technologies as more beneficial. We believe this is the result of exposure to these technologies—most people use these technologies daily and therefore see what the benefits of these technologies are. It is true that people perceive unfamiliar technologies as less beneficial at the moment, but this will change as the use of these technologies evolve and adoption increases. Most calibration technologies, with the exception of electricity, were seen as lower benefit than the others. However, Google glass and Cubetastic3000 were about equally beneficial, and gender and age recognition were less beneficial.

Of the wearable technologies, the riskiest technologies included facial recognition, the Internet, and discrete cameras, whereas the remainder of the technologies were seen as having minimal, equivalent risk levels (i.e., a median of "10"). We did not test the differences in risk between the different wearable-related technologies for statistical significance, but given their minimal spread compared to the calibration options, the differences appears to be negligible. Interestingly, privacy risks were perceived as being comparable to physical risks; for instance, the capacity for facial detection on a wearable device was perceived as being almost as risky as interacting with a lawnmower.

Participants were prompted to rate technologies with respect to all considerations (see Appendix A), including risk of physical harm to bystanders, financial cost, distress, misuse, or impact on public, personal, and private life. Participants may have still evaluated the risks with an emphasis toward physical risk and without an emphasis on privacy risk. Among the five presented options, the wearable-related one is the only one without some physical risk scenario, and physical risk is a clear, tangible risk.

We examined participants' perceptions, and therefore responses may not be reflective of actual risks or benefits. However, they also reflect the general public's exposure to these technologies and show that people perceive specific risks and benefits. We suspect that the similarity in assessments between the various wearable technologies are because most people are not consciously aware of the possibilities and that performing this experiment longitudinally may yield more interesting results, as these technologies become pervasive (and more familiar to participants).

4.3 Open-Ended Concerns for Wearables

We captured participants' general reactions to wearable devices as a whole by asking the following open-ended question:

What do you think are the most likely risks associated with wearable devices?

Concern	Responses	Frequency
Privacy	452	25.32%
Being Unaware	275	15.40%
Health Risk	191	10.70%
Safety	185	10.42%
Social Impact	157	8.80%
Financial Cost	151	8.46%
Security	144	8.07%
Accidental Sharing	69	3.87%
Miscellaneous	57	3.19%
None	51	2.86%
Social Stigma	39	2.18%
False Information	33	1.85%
Don't know	31	1.74%
Aesthetics	19	1.06%
Don't care	11	0.62%

Table 5: The most common open-ended risks associated with owning a wearable device.

This question was asked along with demographics questions (but before any IUIPC questions, which asked a lot of direct privacy-related questions, to avoid biasing the recipients). The participants were presented with a blank box to write in, with no character limit to their open-ended responses.

Table 5 shows common user concerns related to wearable devices. Appendix B details the responses categorized in each coding label. Most are related to privacy and security, but this open-ended data gives a sense of what broad categories of concerns are most relevant to users. This can be used to guide research in unexplored use cases.

In addition to privacy and security in the general sense, significant concerns included being unaware of what the device is collecting, doing, or which information it is using (Being Unaware). Other concerns were orthogonal to privacy, such as long-term health effects caused from wearing the device such as cancer from EMF waves (Health), safety hazards from wearing the device, such as distractions that cause car accidents (Safety), resulting changes in social behaviors, such as dependence on devices or spending less time with loved ones (Social Impact), the high financial cost of buying, replacing, or caring for the device (Financial).

4.3.1 Demographic Factors

The biggest demographic predictor of participants' decisions to rate a scenario as very upsetting was their self-reported level of general privacy concerns, as determined by the IUIPC scale [34]. A Spearman correlation yielded a statistically significant effect between average IUIPC scores and VUR ($\rho = 0.446$, $p < 0.0005$), which suggests responses to questions were mostly based on privacy preferences. Additionally, we observed that age was a significant predictor of VUR ($\rho = 0.121$, $p < 0.0005$). We suspect that the effect of age is due to the significant correlation between age and IUIPC scores ($\rho = 0.188$, $p < 0.0005$); others have observed that older individuals tend to be more privacy protective [55].

Parameters	χ^2	*df*	QIC
(Intercept)	423.96	1	13,209.1
(Intercept)	207.07	1	12,551.49
IUIPC (covariate)	368.5	1	
Gender (covariate)	6.30	1	
(Intercept)	411.66	1	12,458.86
Data Recipient	599.72	3	
(Intercept)	418.02	1	11,382.75
Data Type	1,141.40	71	
(Intercept)	66.18	1	9,609.65
Data Recipient	617.25	3	
Data Type	1,288.51	71	
IUIPC (covariate)	105.73	1	
Gender (covariate)	9.74	1	
IUIPC × Gender	8.33	1	

Table 6: Goodness-of-fit metrics for various binary logistic models of our data using general estimating equations to account for repeated measures. The columns represent the Wald test statistic for each parameter and the overall Quasi-Akaike Information Criterion (QIC) for each model. Each parameter listed was statistically significant at $p < 0.005$.

While we initially observed an effect on VURs based on whether or not participants claimed to already own wearable devices (57.0% vs. 60.8%, respectively; Mann-Whitney $U = 202,896$, $p < 0.032$), this difference did not remain significant upon correcting for multiple testing (Bonferroni corrected $\alpha = 0.01$). The effect of a participant's gender also did not remain significant upon correcting for multiple testing. We observed no correlation between a participant's education level and VUR.

4.3.2 Regression Models

In order to examine the relative effect of each factor on participants' VURs, we constructed several statistical models to predict whether a participant would be "very upset" with a given scenario based on the data type, data recipient, and their demographic factors (i.e., age, education, gender, and privacy attitudes). We performed binary logistic regressions using generalized estimating equations, which account for our repeated measures experimental design (i.e., each participant contributed multiple data points).

We created several models using two independent variables as predictors: data and recipient. Because the device (i.e., whether they were using the Cubetastic3000 or a smartphone) was only varied for the 5 smartphone misbehaviors listed in Section 3.2.3, we removed these five from our models, which resulted in a total of 72 types of data shared with 4 possible recipients. We also used collected demographic factors as covariates: age, gender, education, wearable device ownership (yes/no), and mean IUIPC score. For each model, we performed Wald's test to examine the model effects attributable to each of these parameters. The only covariates that had an observable effect on our models were gender and participants' IUIPC scores, which also exhibited an interaction effect with each other. Thus, we opted to remove the other covariates from our analysis. Table 6 shows the various models that we examined and the Quasi-Akaike Information Criterion (QIC), which is a goodness-of-fit metric for model selection that also accounts for complexity (lower relative values indicate better fit). As can be seen, the data type was the strongest predictor of VUR. The coefficients for the model with the best fit can be seen in Appendix D.

While these models illustrate the relative weights that users place on information when determining a scenario as truly upsetting, one shortcoming of this approach is its generalizability: the data predictor is categorical and limited to the data that we specifically chose for this study. To make our data set more generalizable to other use cases, we coded each data type in two ways: in terms of broad descriptions of the type of data (e.g., video, audio, etc.) and the type of risk it presents. Two researchers agreed on a codebook and independently coded each of the 72 data types.

The data types fell into the following six possible categories:

1. Photo
2. Video
3. Audio
4. Behavioral Information
5. Biometric Information
6. Demographic Information

While the first three categories are self-explanatory, the latter three categories are all based on different user characteristics. We defined *behavioral information* as observations about the user's activities; *biometric information* as measurements of the user's body; and *demographic information* as non-biometric information about the user's traits.

The risks for each data type fell into the following categories:

1. **Financial:** the loss of money or property.
2. **Image:** the loss of control over one's self-image (e.g., publicizing something embarrassing).
3. **Medical:** the disclosure of medical information.
4. **Physical:** physical harm to the user.
5. **Relationships:** damage to the user's inter-personal relationships.

After independently coding, the researchers met to resolve any disagreements, such that the results reflect unanimity. There was 83% agreement prior to resolution. Cohen's κ was 0.81 for the data categories and 0.75 for the risk categories, both indicating "excellent" agreement [23].

With regard to data types, the most concerning type of data was video (78.0%), which was ranked similarly to photos (76.2%). Next were audio (66.8%) and demographic data (65.4%), followed by behavioral (53.1%) and biometric (46.3%) data. We suspect that demographic data was more concerning because it included information such as a Social Security Number, bank account information, and other financial information. We chose to categorize them as such as they are non-biological descriptors of the user. We were very surprised that biometric information was seen as relatively benign compared to the other broad categories of data. One hypothesis is that since most home users do not use biometric authentication, they may have an inaccurate understanding of the types of systems that might be at risk if biometric data are stolen and abused.

Parameters	χ^2	*df*	QIC
(Intercept)	442.66	1	12,727.42
Risk	405.18	4	
(Intercept)	380.39	1	12,681.86
Data Category	439.45	5	
(Intercept)	256.15	1	12,061.87
Risk	157.84	4	
Data Category	183.90	5	
Risk × Data Category	259.81	8	
(Intercept)	62.65	1	10,406.35
Risk	205.21	4	
Data Category	250.35	5	
Recipient	546.89	3	
IUIPC (covariate)	103.94	1	
Gender (covariate)	9.80	1	
IUIPC × Gender	8.21	1	
Risk × Data Category	303.44	8	
Recipient × Risk	39.14	12	

Table 7: Metrics for additional binary logistic models of our data using general estimating equations to account for repeated measures. The columns represent the Wald test statistic for each parameter and the overall Quasi-Akaike Information Criterion (QIC) for each model. Each parameter listed was statistically significant at $p < 0.005$.

With regard to the presented risks, we observed that average VURs were highest for financial information disclosure (82.0%). Information regarding relationships (69.2%), physical safety (66.4%), and self-image (65.8%) followed. VURs were lowest for medical information disclosure (47.4%). One reason why medical risks were ranked relatively low is that this category broadly covered scenarios involving data about the user's health, but also included more basic medical information, such as age, gender, and emotional state. As mentioned in Section 4.1.1, participants saw these as publicly observable and unconcerning.

Using these two new variables as additional independent variables (and removing the previous data type variable), we created a second set of models. Because these risk categories and mediums are less likely to change over time, models that take these into account are likely to be more useful and less likely to be overfit. What these models show us is that both risk and medium are relatively strong predictors by themselves, and have an even stronger interaction effect. When the data recipient and covariates are added to the model, the resulting goodness-of-fit is not much worse than that of the model using the actual data type. The full model can be found in Appendix E.

5. DISCUSSION

One of the limitations is that our participants might not have interest in or knowledge of wearables and their respective capabilities, since 83% of our participants reported that they do not own a wearable. Participants may be over or underestimating the risk due to unawareness of what can be inferred from the data, not have an idea of how to rate a new technology with respect to familiar ones, or be more influenced by recent events.[1] For instance, biometrics were generally not a concern for our participants, although there are many security and privacy implications [43].

We recruited both wearable users and non-users in order to yield a more representative sample of the general population. We could have easily recruited only wearables owners or people specifically interested in wearables. However, that would have its own biases and limitations. At the time of this writing, about 85% of the general population do not own wearable devices [38, 11], indicating our study is reflective of the current population.

Because of the privacy paradox, participants' stated responses may differ from how they may react to these same scenarios in real life [39, 27]. At the same time, our results do reflect actual perceptions of wearable devices and the associated privacy scenarios involving them. This is an unavoidable, yet important distinction to make with of studies of this nature: our primary goal was to examine perceptions and preferences, so that future systems can be designed with these in mind. We do not expect that such systems will satisfy users in all situations, however, we believe that user-centered design will still be a vast improvement over post hoc approaches (or ignoring user concerns altogether).

Further work can be done to expand various aspects of this study. Investigating more fine-grained data types (e.g., investigating specific instances of location data, versus location data in general) would be a useful endeavor to gain further insight into user perceptions. Adding additional recipients, such as "advertisers" or "acquaintances" may lead to more nuanced results. Additionally, the open-ended concerns are inspiration for future research: addressing the high financial costs of wearables, communicating the reality of health concerns from constant use, creating distraction-free interfaces to prevent safety issues, minimizing negative social impacts of wearable device use, and improving device aesthetics.

Wearables are still in their infancy. Perceptions of situations and capabilities will change rapidly with advancements and increased exposure. However, pursuant to previous studies of smartphone risk perceptions, our participants found embarrassing videos and risks involving financial losses to be the most sensitive, which suggests that these risks should be highlighted by platform developers. Various systems which detect and take actions for sensitive objects in photos and videos will be critical as wearables and other devices become more ubiquitous.

6. REFERENCES

[1] G. D. Abowd and E. D. Mynatt. Charting past, present, and future research in ubiquitous computing. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 7(1):29–58, 2000.

[2] G. Abramovich. 15 mind-blowing stats about wearable technology. `http://www.cmo.com/articles/2014/6/16/Mind_Blowing_Stats_Wearable_Tech.html`. Accessed: 2014-12-19.

[3] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 2:24–30, 2005.

[4] V. Bellotti and A. Sellen. Design for privacy in ubiquitous computing environments. In *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW'93*, pages 77–92. Springer, 1993.

[5] J. Blythe, J. Camp, and V. Garg. Targeted risk communication for computer security. In *Proceedings of the 16th International Conference on Intelligent User Interfaces*, IUI '11, pages 295–298, New York, NY, USA, 2011. ACM.

[6] S. Bogaty. Wearable tech device awareness surpasses 50 percent among us consumers, according to npd. `https://www.npd.com/wps/portal/npd/us/news/press-releases/wearable-tech-device-awareness-surpasses-50-percent-among-us-consumers-according-to-npd/`. Accessed: 2014-12-26.

[7] R. Böhme and J. Grossklags. The security cost of cheap user interaction. In *Proceedings of the 2011 workshop on New security paradigms workshop*, pages 67–82. ACM, 2011.

[8] J. Camp and Y. Chien. The internet as public space: concepts, issues, and implications in public policy. *ACM SIGCAS Computers and Society*, 30(3):13–19, 2000.

[9] L. J. Camp. Designing for trust. In *Trust, Reputation, and Security: Theories and Practice*, pages 15–29. Springer, 2003.

[10] E. Chin, A. P. Felt, V. Sekar, and D. Wagner. Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 1. ACM, 2012.

[11] J. Comstock. Pwc: 1 in 5 americans owns a wearable, 1 in 10 wears them daily. `http://mobihealthnews.com/37543/pwc-1-in-5-americans-owns-a-wearable-1-in-10-wears-them-daily/`. Accessed: 2014-12-19.

[12] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos. Anonysense: privacy-aware people-centric sensing. In *Proceedings of the 6th international conference on Mobile systems, applications, and services*, pages 211–224. ACM, 2008.

[13] T. Denning, Z. Dehlawi, and T. Kohno. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pages 2377–2386. ACM, 2014.

[14] C. Doug Gross. Google glass targeted as symbol by anti-tech crowd - cnn.com, 2014.

[15] J. Dvorak. Rest in peace, google glass: 2012-2014, 2014.

[16] S. Egelman, L. F. Cranor, and J. Hong. You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *CHI '08: Proceeding of The 26th SIGCHI Conference on Human Factors in Computing Systems*, pages 1065–1074, New York, NY, USA, 2008. ACM.

[17] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri.

[1] Recently, stories of exploding batteries were in the news [32], which were explicitly reported as a concern in our open-ended question.

A study of android application security. In *USENIX security symposium*, volume 2, page 2, 2011.

[18] A. P. Felt, S. Egelman, and D. Wagner. I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*, pages 33–44. ACM, 2012.

[19] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. A survey of mobile malware in the wild. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, pages 3–14. ACM, 2011.

[20] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 3. ACM, 2012.

[21] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs. How safe is safe enough? a psychometric study of attitudes towards technological risks and benefits. *Policy sciences*, 9(2):127–152, 1978.

[22] Fitbit.com. Fitbit official site for activity trackers & more, 2014.

[23] J. L. Fleiss, B. Levin, and M. C. Paik. *Statistical Methods for Rates and Proportions*. John Wiley & Sons, Inc., 3rd edition edition, 2003.

[24] V. Garg, L. J. Camp, K. Connelly, and L. Lorenzen-Huber. Risk communication design: Video vs. text. In *Proceedings of the 12th International Conference on Privacy Enhancing Technologies*, PETS'12, pages 279–298, Berlin, Heidelberg, 2012. Springer-Verlag.

[25] K. Hill. Fitbit moves quickly after users' sex stats exposed. `http://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed/`. Accessed: 2014-12-26.

[26] J. I. Hong, J. D. Ng, S. Lederer, and J. A. Landay. Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*, pages 91–100. ACM, 2004.

[27] C. Jensen, C. Potts, and C. Jensen. Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1):203–227, 2005.

[28] X. Jiang, J. I. Hong, and J. A. Landay. Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. In *Ubicomp 2002: ubiquitous computing*, pages 176–193. Springer, 2002.

[29] S. Kane. Your apps are watching you, 2010.

[30] P. G. Kelley, L. F. Cranor, and N. Sadeh. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 3393–3402. ACM, 2013.

[31] M. Langheinrich. Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems. In *Ubicomp 2001: Ubiquitous Computing*, pages 273–291. Springer, 2001.

[32] A. Levin. Exploding lithium batteries riskier to planes: Research, 2014.

[33] J. Lindqvist, J. Cranshaw, J. Wiese, J. Hong, and J. Zimmerman. I'm the mayor of my house: examining why people use foursquare-a social-driven location sharing application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2409–2418. ACM, 2011.

[34] N. K. Malhotra, S. S. Kim, and J. Agarwal. Internet users' information privacy concerns (iuipc): the construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.

[35] Mashable. Woman robbed, assaulted for wearing google glass in a bar, 2014.

[36] M. G. Morgan, B. Fischhoff, A. Bostrom, and C. Atman. *Risk Communication: A Mental Models Approach*. Cambridge University Press, New York, 2001.

[37] E. Morphy. Google glass drops facial recognition (for now). `http://www.forbes.com/sites/erikamorphy/2013/06/02/google-glass-drops-facial-recognition-for-now/`. Accessed: 2014-12-26.

[38] N. News. Are consumers really interested in wearing tech on their sleeves? `http://www.nielsen.com/us/en/insights/news/2014/tech-styles-are-consumers-really-interested-in-wearing-tech-on-their-sleeves.html`. Accessed: 2014-12-19.

[39] P. A. Norberg, D. R. Horne, and D. A. Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1):100–126, 2007.

[40] L. Palen and P. Dourish. Unpacking Privacy for a Networked World. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 129–136. ACM, 2003.

[41] L. Palen, M. Salzman, and E. Youngs. Going wireless: Behavior & practice of new mobile phone users. In *Proceedings of the 2000 ACM conference on Computer supported cooperative work*, pages 201–210. ACM, 2000.

[42] Pebble and P. S. Smartwatch. Pebble smartwatch, 2014.

[43] S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, 1(2):33–42, 2003.

[44] Readwrite.com, 2014.

[45] F. Roesner, T. Kohno, T. Denning, R. Calo, and B. C. Newell. Augmented reality: hard problems of law and policy. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, pages 1283–1288. ACM, 2014.

[46] F. Roesner, T. Kohno, and D. Molnar. Security and privacy for augmented reality systems. *Communications of the ACM*, 57(4):88–96, 2014.

[47] K. Russell. I was assaulted for wearing google glass in the wrong part of san francisco, 2014.

[48] N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, 13(6):401–412, 2009.

[49] J. Scholtz and S. Consolvo. Toward a framework for evaluating ubiquitous computing applications. *Pervasive Computing, IEEE*, 3(2):82–88, 2004.

[50] I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, and H. Borgthorsson. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pages 2347–2356. ACM, 2014.

[51] S. Spiekermann, J. Grossklags, and B. Berendt. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pages 38–47. ACM, 2001.

[52] TIME.com. 26 fitness trackers ranked from worst to first, 2014.

[53] J. Y. Tsai, P. Kelley, P. Drielsma, L. F. Cranor, J. Hong, and N. Sadeh. Who's viewed you?: The impact of feedback in a mobile location-sharing application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, pages 2003–2012, New York, NY, USA, 2009. ACM.

[54] J. Turi. The top 9 wearables you can buy right now, 2014.

[55] H. R. Varian, F. Wallenberg, and G. Woroch. The demographics of the do-not-call list. *IEEE Security & Privacy*, 3(1):34–39, 2005.

[56] T. Verge. The best wearables of ces 2014, 2014.

[57] Wikipedia. Google glass, 2015.

[58] Y. Zhou, X. Zhang, X. Jiang, and V. W. Freeh. Taming information-stealing smartphone applications (on android). In *Trust and Trustworthy Computing*, pages 93–107. Springer, 2011.

APPENDIX

A. FISCHHOFF PROMPTS

We would like to ask you to rate the <risks/benefits> associated with each of the following technologies.

Risks: *Consider all types of risks: the risk of physical harm or death, the risk to others or bystanders, the financial cost of the technology, any distress caused by the technology, what the consequences would be if the technology was misused, any impact on the public, work, or personal life, and other considerations. (e.g. for electricity, consider the risk of electrocution, the pollution caused by coal, the risk that miners need to take to mine the coal, the cost to build the infrastructure to deliver electricity, etc.) Give a global estimate over a long period of time (say, a year) of both intangible and tangible risks.*

Do not consider the costs or risks associated with these items. It is true, for example, that sometimes swimmers can drown. But evaluating such risks is not your present job. Your job is to assess the gross benefits, not the net benefits which remain after the costs and risks are subtracted out.

Please rate the following technologies below with a number. We know that this might be a bit hard to do, but please try to be as accurate as possible, adjusting the numbers until they feel they are right for you. Start with the least risky technology at 10 and assign higher numbers for the more risky technologies. (For instance, a technology rated 14 is half as risky as a technology rated 28.)

Benefits: *Consider all types of benefits: how many jobs are created, how much money is generated directly or indirectly, how much enjoyment is brought to people, how much a contribution is made to the people's health and welfare, what this technology promotes, and so on. (e.g. for swimming, consider the manufacture and sale of swimsuits, the time spent exercising, the social interactions during swimming, and the sport created around the activity.) Give a global estimate over a long period of time (say, a year) of both intangible and tangible benefits.*

Do not consider the costs or benefits associated with these items. It is true, for example, that electricity also creates a market for home appliances. But evaluating such benefits is not your present job. Your job is to assess the gross risks, not the net risks which remain after the costs and risks are subtracted out.

Please rate the following technologies below with a number. We know that this might be a bit hard to do, but please try to be as accurate as possible, adjusting the numbers until they feel they are right for you. Start with the least beneficial technology at 10 and assign higher numbers for the more beneficial technologies. (For instance, a technology rated 34 is twice as beneficial as a technology rated 17.)

B. CODING LABEL DEFINITIONS

Researchers coded the self reported answers as follows:
Privacy: "privacy," mention of personal details, spying.
Security: "security," mention of malware, hacking.
GPS tracking: "location," "GPS," mention of monitoring.
Being Unaware: mention of using, collecting, and disclosing data without permission.
False information: inaccurate or maliciously false data.
Health Risk: mention of radiation, cancer, or other effects.
Safety: mention of distractions causing car crashes and injuries, violence due to the device, injuries from malfunctions.
Discomfort: mention of eye strain, headache, irritation.
Financial cost: cost of buying or using the device.
Theft: mention of device theft.
Social Impact: mention of dependency, distance from people, changes in decision making, etc.
Social Stigma: mention of judgment, hate, or bystanders.
Aesthetics: mention of fashion or looking dorky.
Miscellaneous: odd comments, uncommon concerns.
None: "None," mention of no threat, or no real concerns
Don't know: "do not know," general confusion
Don't care: " do not care," nonchalant answers

C. CONCERN FACTORS

We show the full, fine-grained results of our survey in this appendix. This includes how participants had ranked each technology in response to the Fischhoff-style questions, the VUR rates for all seventy-two data types, across all recipients and by recipient, and the details of the full regression models used in our analyses.

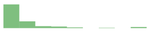
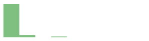
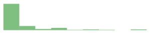
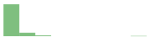
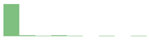
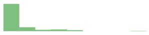
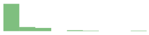
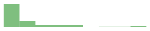
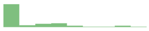
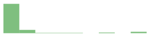
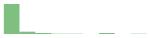
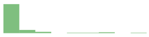
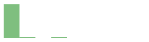
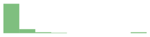
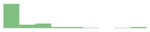
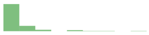
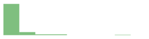
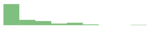
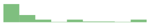
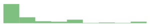
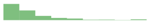
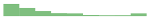
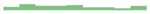
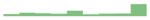
Technology	Q1	Median	Q3	Distribution
Location Tracking	10.0	10.0	20.0	
Speech To Text	10.0	10.0	10.0	
Discreet Microphone	10.0	10.0	20.0	
Smartwatches	10.0	10.0	10.0	
Language Detection	10.0	10.0	10.0	
Laptops	10.0	10.0	15.0	
Smartphones	10.0	10.0	20.0	
Google Glass	10.0	10.0	20.0	
Cubetastic	10.0	10.0	30.0	
Gender Detection	10.0	10.0	13.5	
Voice Recognition	10.0	10.0	15.0	
Voice Based Emotion Detection	10.0	10.0	15.0	
Fitness Trackers	10.0	10.0	10.0	
Age Detection	10.0	10.0	15.0	
Facial Detection	10.0	10.0	25.0	
Email	10.0	10.0	18.0	
Heart Rate Detection	10.0	10.0	10.0	
Discreet Camera	12.0	10.0	30.0	
Internet	15.0	10.0	31.0	
Facial Recognition	17.0	10.0	30.0	
Lawnmower	20.0	12.0	30.0	
Electricity	25.0	15.0	40.0	
Motorcycle	45.0	27.0	70.0	
Handgun	60.0	40.0	100.0	

Table 10: Risk rankings of various technologies in response to the Fischoff-style prompt.

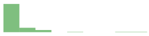
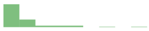
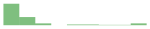
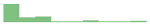
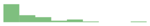
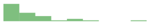
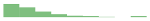
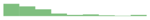
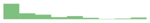
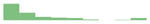
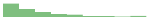
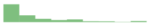
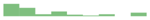
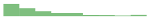
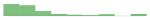
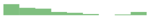
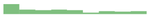
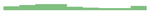
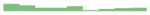
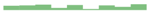
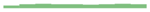
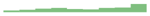
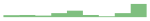
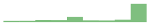
Technology	Q1	Median	Q3	Distribution
Gender Detection	10.0	10.0	15.0	
Age Detection	12.0	10.0	22.0	
Discreet Microphone	15.0	10.0	20.0	
Cubetastic	15.0	10.0	30.0	
Fitness Trackers	18.5	10.0	30.0	
Voice Based Emotion Detection	20.0	10.0	30.0	
Facial Detection	20.0	10.0	34.0	
Discreet Camera	20.0	15.0	30.0	
Google Glass	20.0	12.0	40.0	
Smartwatches	20.0	10.0	35.0	
Motorcycle	20.0	12.0	40.0	
Handgun	20.0	10.0	30.0	
Facial Recognition	22.0	12.5	42.5	
Lawnmower	24.0	15.0	40.0	
Speech To Text	25.0	15.0	40.0	
Voice Recognition	25.0	15.0	40.0	
Language Detection	35.0	15.0	60.0	
Heart Rate Detection	40.0	26.0	65.0	
Location Tracking	40.0	20.0	70.0	
Email	50.0	29.0	77.5	
Smartphones	50.0	30.0	75.0	
Laptops	60.0	40.0	80.0	
Internet	65.0	45.0	100.0	
Electricity	88.0	50.0	100.0	

Table 11: Benefit rankings of various technologies in response to the Fischoff-style prompt.

Rank	Question	VUR	σ	Distribution
1	video of you unclothed	95.97	0.31	
2	bank account information	95.91	0.35	
3	social security number	94.84	0.26	
4	video entering in a PIN at an ATM	92.67	0.48	
5	photo of you unclothed	92.59	0.45	
6	photo of you that is very embarrassing	91.39	0.56	
7	username and password for websites	89.55	0.62	
8	credit card information	88.98	0.56	
9	video of you that is very embarrassing	88.41	0.53	
10	photo of you at home	87.5	0.60	
11	audio recording of work conversations	86.82	0.76	
12	video of entering in a passcode to a door	85.53	0.62	
13	audio recording of phone conversations	85.16	0.61	
14	amount of money you have	84.44	0.61	
15	video of you intoxicated	83.21	0.72	
16	when you have sex	81.95	0.82	
17	how much debt you have	81.12	0.54	
18	video of you at home	81.05	0.60	
19	photo of you intoxicated	78.95	0.82	
20	photo of you at random	78.76	0.85	
21	audio recording of conversations	78.13	0.83	
22	medical conditions	77.7	0.86	
23	video of you at random	76.19	0.59	
24	video of you off-guard	76.0	0.62	
25	photo of your work or workplace	74.62	0.90	
26	username for websites	73.44	0.83	
27	address	72.61	0.86	
28	audio recording you captured	72.55	0.70	
29	photo of you off-guard	72.55	0.77	
30	photo downloaded from internet	71.81	0.90	
31	photo others sent you	71.63	1.03	
32	video others sent you	70.59	0.81	
33	video of your work or workplace	70.54	0.90	
34	fingerprint	70.12	0.86	
35	when you were lying nervous or stressed	69.74	0.91	
36	audio recording of you (voice notes)	69.59	0.91	

Table 8: VUR for all data types (1-36), across all recipients.

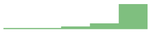
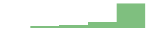
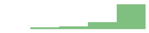
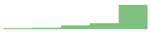
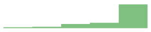
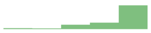
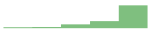
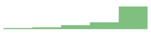
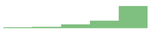
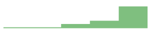
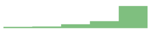
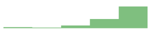
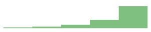
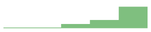
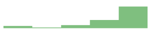
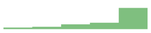
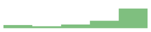
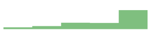
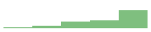
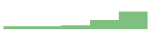
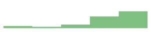
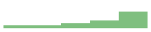
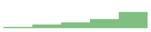
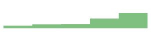
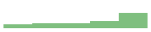
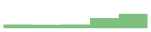
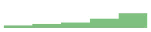
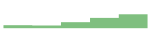
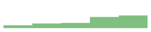
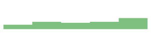
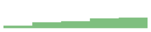
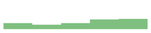
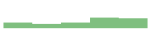
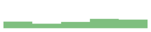
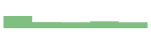
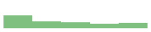
Rank	Question	VUR	σ	Distribution
37	medication taken	69.49	1.01	
38	videos already on device	68.89	0.88	
39	photo of your signature	68.07	0.84	
40	web history	66.44	1.01	
41	photos taken on device	66.21	1.02	
42	home address	65.0	0.97	
43	fine-grained location tracking (+/- cm)	63.51	0.99	
44	photo of people at random	61.94	1.06	
45	video downloaded from the internet	61.49	1.00	
46	when you are alone	61.27	0.99	
47	location tracking (+/- m)	61.24	1.08	
48	videos of people at random	61.04	0.95	
49	where you are currently going	60.87	0.97	
50	recording of sound around you	60.45	0.94	
51	people you spend time with	60.0	1.13	
52	workplace address	58.09	1.16	
53	sounds on device (notifications, etc)	54.4	1.29	
54	phone usage	51.95	1.22	
55	purchased products	50.0	1.09	
56	when you are sick or healthy	48.17	1.27	
57	how close you are to interacting people	46.98	1.12	
58	feelings (based on biometrics)	46.81	1.31	
59	computer usage	44.93	1.16	
60	eating patterns	42.86	1.27	
61	name	42.54	1.40	
62	sleeping patterns	40.56	1.34	
63	eye patterns (for eye tracking)	40.51	1.27	
64	exercise patterns	38.66	1.26	
65	when you are happy or having fun	34.75	1.27	
66	television shows watched	30.2	1.40	
67	when you are busy or interruptible	29.5	1.26	
68	music on device	28.06	1.43	
69	heart rate	27.5	1.40	
70	age	24.29	1.43	
71	language spoken	15.86	1.49	
72	gender	15.0	1.46	

Table 9: VUR for all data types (37-72), across all recipients.

Question	All	Friends	Public	Work	App
video of you unclothed	95% (1)	97% (4)	94% (10)	100% (1)	90% (2)
bank account information	95% (2)	94% (10)	95% (7)	100% (1)	90% (1)
social security number	94% (3)	100% (1)	100% (1)	93% (9)	88% (3)
video entering in a PIN at an ATM	92% (4)	100% (1)	93% (12)	87% (20)	88% (4)
photo of you unclothed	92% (5)	96% (6)	91% (16)	100% (1)	77% (6)
photo of you that is very embarrassing	91% (6)	94% (8)	100% (1)	94% (6)	78% (5)
username and password for websites	89% (7)	96% (5)	95% (9)	94% (7)	64% (14)
credit card information	88% (8)	100% (1)	93% (13)	95% (5)	65% (13)
video of you that is very embarrassing	88% (9)	91% (13)	94% (11)	94% (7)	71% (9)
photo of you at home	87% (10)	85% (19)	96% (5)	93% (10)	71% (10)
audio recording of work conversations	86% (11)	94% (9)	96% (6)	100% (1)	53% (24)
video of entering in a passcode to a door	85% (12)	95% (7)	89% (21)	81% (35)	75% (7)
audio recording of phone conversations	85% (13)	93% (11)	97% (4)	90% (14)	56% (20)
amount of money you have	84% (14)	90% (14)	100% (1)	93% (11)	63% (15)
video of you intoxicated	83% (15)	81% (26)	91% (16)	88% (17)	68% (11)
when you have sex	81% (16)	78% (31)	87% (23)	90% (15)	73% (8)
how much debt you have	81%(17)	85% (19)	90% (20)	87% (22)	59% (18)
video of you at home	81% (18)	87% (16)	86% (24)	89% (16)	60% (17)
photo of you intoxicated	78% (19)	80% (27)	90% (18)	87% (23)	53% (25)
photo of you at random	78% (20)	82% (24)	83% (29)	81% (32)	66% (12)
audio recording of conversations	78% (21)	86% (18)	85% (26)	87% (20)	55% (21)
medical conditions	77% (22)	92% (12)	85% (25)	85% (27)	40% (37)
video of you at random	76% (23)	73% (40)	90% (19)	88% (19)	48% (31)
video of you off-guard	76% (24)	85% (21)	79% (34)	91% (13)	53% (23)
photo of your work or workplace	74% (25)	76% (33)	82% (31)	81% (32)	62% (16)
username for websites	73% (26)	90% (15)	74% (43)	84% (28)	50% (29)
address	72% (27)	62% (50)	93% (14)	81% (31)	51% (28)
audio recording you captured	72% (28)	87% (17)	75% (40)	72% (46)	50% (29)
photo of you off-guard	72% (29)	83% (23)	80% (32)	80% (37)	45% (33)
photo downloaded from internet	71% (30)	79% (29)	76% (38)	86% (25)	32% (47)
photo others sent you	71% (31)	85% (21)	84% (27)	75% (44)	41% (35)
video others sent you	70% (32)	82% (24)	95% (7)	80% (37)	30% (49)
video of your work or workplace	70% (33)	74% (36)	83% (28)	70% (49)	51% (26)
fingerprint	70% (34)	77% (32)	80% (32)	70% (48)	55% (22)
when you were lying nervous or stressed	69% (35)	74% (35)	74% (42)	91% (12)	41% (34)
audio recording of you % (voice notes)	69% (36)	80% (28)	78% (35)	88% (18)	38% (39)
medication taken	69% (37)	79% (29)	73% (44)	81% (34)	37% (40)
videos taken on device	68% (38)	58% (52)	82% (30)	79% (40)	51% (27)
photo of your signature	68% (39)	63% (48)	64% (51)	85% (26)	59% (19)
web history	66% (40)	74% (36)	70% (45)	86% (24)	37% (40)
photos already on device	66% (41)	75% (34)	77% (36)	79% (39)	27% (53)
home address	65% (42)	61% (51)	87% (22)	69% (50)	40% (36)
fine-grained location tracking (+/- cm)	63% (43)	73% (39)	76% (37)	78% (41)	30% (50)
photo of people at random	61% (44)	72% (41)	61% (54)	82% (30)	38% (38)
video downloaded from the internet	61% (45)	63% (47)	75% (40)	82% (29)	33% (45)
when you are alone	61% (46)	51% (55)	69% (46)	80% (36)	35% (43)
location tracking (+/- m)	61% (47)	57% (53)	92% (15)	63% (55)	25% (56)
videos of people at random	61% (48)	63% (49)	75% (39)	71% (47)	28% (52)
where you are currently going	60% (49)	74% (36)	68% (48)	65% (54)	35% (44)
recording of sound around you	60% (50)	71% (42)	64% (50)	75% (43)	35% (42)
people you spend time with	60% (51)	71% (42)	60% (55)	76% (42)	31% (48)
workplace address	58% (52)	69% (45)	64% (49)	57% (61)	46% (32)
sounds on device % (notifications, etc)	54% (53)	70% (44)	59% (56)	66% (52)	22% (58)
phone usage	51% (54)	67% (46)	56% (57)	68% (51)	15% (64)
purchased products	50% (55)	57% (54)	55% (58)	62% (57)	26% (54)
when you are sick or healthy	48% (56)	40% (64)	61% (52)	62% (58)	26% (55)
how close you are to interacting people	46% (57)	50% (57)	61% (53)	51% (62)	13% (66)
feelings (based on biometrics)	46% (58)	50% (57)	55% (58)	63% (56)	18% (61)
computer usage	44% (59)	51% (56)	52% (60)	45% (63)	28% (51)
eating patterns	42% (60)	41% (62)	45% (62)	75% (45)	12% (67)
name	42% (61)	50% (57)	68% (47)	26% (71)	32% (46)
sleeping patterns	40% (62)	43% (61)	41% (63)	62% (59)	21% (59)
eye patterns % (for eye tracking)	40% (63)	48% (60)	50% (61)	61% (60)	6% (71)
exercise patterns	38% (64)	33% (67)	34% (66)	66% (52)	16% (63)
when you are happy or having fun	34% (65)	40% (64)	32% (69)	43% (65)	24% (57)
television shows watched	30% (66)	38% (66)	33% (67)	36% (68)	11% (68)
when you are busy or interruptible	29% (67)	40% (63)	28% (70)	36% (68)	17% (62)
music on device	28% (68)	4% (72)	37% (64)	42% (66)	20% (60)
heart rate	27% (69)	21% (68)	36% (65)	44% (64)	9% (70)
age	24% (70)	17% (69)	33% (67)	36% (67)	14% (65)
language spoken	15% (71)	17% (70)	18% (72)	28% (70)	27% (53)
gender	15% (72)	15% (71)	19% (71)	15% (72)	9% (69)

Table 12: The VUR of all questions for all recipients.

D. FULL REGRESSION MODEL FROM DATA TYPES

Parameter Estimates

			95% Wald Confidence Interval		Hypothesis Test		
Parameter	B	Std. Error	Lower	Upper	Wald Chi-Square	df	Sig.
(Intercept)	2.747	.5302	1.708	3.787	26.850	1	0.0000
Data Type							
a photo of you intoxicated	-.077	.3027	-.670	.516	.065	1	0.7995
a photo of you off-guard	.340	.2783	-.206	.885	1.488	1	0.2226
a photo of you unclothed	-1.387	.4045	-2.180	-.594	11.760	1	0.0006
a picture of your signature	.474	.3242	-.161	1.109	2.138	1	0.1437
a video of you entering in a digital passcode to a locked door	-.747	.3317	-1.398	-.097	5.078	1	0.0242
a video of you entering in your PIN at an ATM	-1.704	.3908	-2.470	-.938	19.019	1	0.0005
a video of you intoxicated	-.542	.3372	-1.203	.119	2.585	1	0.1079
a video of you off-guard	-.018	.3019	-.609	.574	.003	1	0.9535
a video of you unclothed	-2.142	.4898	-3.102	-1.181	19.115	1	0.0005
an incriminating photo of you doing something embarrassing	-1.344	.3772	-2.084	-.605	12.696	1	0.0005
an incriminating video of you doing something embarrassing	-.998	.3558	-1.695	-.300	7.859	1	0.0051
copied and uploaded audio recordings you made on your device	.360	.2979	-.224	.944	1.460	1	0.2269
copied and uploaded music from your device	2.616	.2956	2.036	3.195	78.295	1	0.0000
copied and uploaded sounds saved on your device (notification noises, etc.)	1.258	.3031	.663	1.852	17.213	1	0.0005
how close you are to other people you interact with	1.718	.2899	1.149	2.286	35.111	1	0.0000
how much debt you have	-.267	.3156	-.886	.351	.716	1	0.3973
how much money you have	-.729	.3419	-1.399	-.059	4.549	1	0.0329
how much you use your computer	1.719	.2809	1.168	2.269	37.434	1	0.0000
how much you use your phone	1.456	.2789	.909	2.002	27.251	1	0.0000
how you were feeling based on heart rate, breathing, and/or temperature	1.627	.2809	1.076	2.177	33.521	1	0.0000
photos at work (with an outward-facing camera)	-.107	.3155	-.725	.511	.115	1	0.7346
photos of people (with an outward-facing camera) at random	.778	.2902	.210	1.347	7.197	1	0.0073
photos of you (with an inward-facing camera) at home	-.650	.3494	-1.335	.035	3.462	1	0.0628

photos of you (with an inward-facing camera) at random	-.033	.3412	-.702	.636	.009	1	0.9231
recorded the sound around you	.856	.3101	.248	1.464	7.621	1	0.0058
recorded you talking to yourself (making voice notes)	.296	.2794	-.252	.843	1.121	1	0.2897
recorded your passing conversations	-.111	.3246	-.747	.525	.117	1	0.7324
recorded your phone conversations	-.713	.3551	-1.409	-.018	4.038	1	0.0445
recorded your work conversations	-.901	.3303	-1.548	-.254	7.440	1	0.0064
scanned your eye to learn your eye patterns (for eye tracking)	1.892	.2766	1.350	2.434	46.796	1	0.0000
shared photos others sent to you saved on your device	.330	.3054	-.269	.928	1.164	1	0.2806
shared photos you downloaded from the internet saved on your device	.419	.2862	-.142	.980	2.147	1	0.1429
shared photos you which are already on your device	.696	.2900	.128	1.265	5.762	1	0.0164
shared videos others sent you saved on your device	.304	.3018	-.287	.896	1.017	1	0.3133
shared videos you downloaded on the internet saved on your device	.722	.2860	.162	1.283	6.382	1	0.0115
shared videos you which are already on your device	.483	.3083	-.121	1.087	2.455	1	0.1171
the language you were speaking	3.470	.3279	2.827	4.113	111.953	1	0.0000
videos at work (with an outward-facing camera)	.487	.3013	-.104	1.077	2.610	1	0.1062
videos of people (with an outward-facing camera) at random	1.017	.2884	.452	1.582	12.437	1	0.0005
videos of you (with an inward-facing camera) at home	-.336	.3061	-.936	.264	1.206	1	0.2721
videos of you (with an inward-facing camera) at random	.153	.2940	-.423	.730	.273	1	0.6016
what medical conditions you have	.114	.2955	-.465	.693	.149	1	0.6997
what medication you take	.501	.2976	-.082	1.084	2.832	1	0.0924
what products you buy	1.494	.2871	.931	2.056	27.071	1	0.0000
what television shows you watch	2.467	.2850	1.908	3.026	74.910	1	0.0000
what websites you go to	.610	.2862	.049	1.171	4.542	1	0.0331
when and how much you have sex	-.341	.3302	-.988	.306	1.067	1	0.3016
when and how much you spend time alone	.966	.2803	.416	1.515	11.871	1	0.0006
when and how well you are sleeping	1.842	.3005	1.253	2.431	37.576	1	0.0000
when you are busy or interruptible	2.497	.3028	1.904	3.090	68.012	1	0.0000
when you are sick or healthy	1.557	.2657	1.037	2.078	34.364	1	0.0000

when you were happy or having fun	2.325	.2995	1.738	2.912	60.277	1	0.0000
when you were lying, nervous, or stressed	.428	.2847	-.130	.987	2.264	1	0.1324
when, how much, and what you are eating	1.767	.2751	1.228	2.306	41.249	1	0.0000
when, how, and how much you exercise	2.003	.2985	1.418	2.588	45.037	1	0.0000
where you are (like a GPS)	.888	.2829	.334	1.443	9.855	1	0.0017
where you are currently going (by observing maps, etc.)	1.044	.2942	.468	1.621	12.598	1	0.0005
where you are very accurately (more than GPS, like where you are in a room)	.697	.2828	.143	1.252	6.082	1	0.0137
where you live somehow (looking at your map settings or history or observing documents and commutes)	.770	.2953	.191	1.348	6.793	1	0.0091
where you work somehow (looking at your map settings or history or observing documents and commutes)	1.017	.2886	.451	1.583	12.417	1	0.0005
who you were spending time with	.913	.2989	.327	1.499	9.332	1	0.0023
your address	.283	.3011	-.307	.873	.881	1	0.3478
your age	2.872	.2926	2.299	3.446	96.396	1	0.0000
your bank account information	-2.173	.4635	-3.082	-1.265	21.988	1	0.0000
your credit card information	-1.121	.3495	-1.806	-.436	10.287	1	0.0013
your fingerprint somehow	.325	.3131	-.288	.939	1.079	1	0.2990
your gender	3.481	.3288	2.837	4.126	112.075	1	0.0000
your heart rate	2.681	.2917	2.109	3.252	84.432	1	0.0000
your name	1.922	.3031	1.328	2.516	40.221	1	0.0000
your social security number	-2.110	.4468	-2.986	-1.234	22.298	1	0.0000
your username and password for websites	-1.050	.3387	-1.713	-.386	9.600	1	0.0019
your username for websites							
Data Recipient							
appserver	1.879	.0858	1.710	2.047	479.614	1	0.0000
friends	.379	.0781	.226	.532	23.511	1	0.0000
public	.158	.0758	.009	.306	4.326	1	0.0375
work							
Male	1.985	.6361	.738	3.232	9.739	1	0.0018
IUIPC	-.809	.0787	-.963	-.655	105.729	1	0.0000
Male * IUIPC	-.301	.1044	-.506	-.097	8.330	1	0.0039

Dependent Variable: VUR
Model: (Intercept), Data Type, Data Recipient, Male, IUIPC, Male * IUIPC

E. FULL REGRESSION MODEL FROM DATA RISKS / DATA CATEGORIES

Parameter Estimates

			95% Wald Confidence Interval		Hypothesis Test		
Parameter	B	Std. Error	Lower	Upper	Wald Chi-Square	df	Sig.
(Intercept)	2.990	.4588	2.090	3.889	42.456	1	.000
Risk							
financial	-1.870	.4010	-2.656	-1.084	21.744	1	.000
image	-.942	.2031	-1.340	-.543	21.481	1	.000
medical	-.200	.3556	-.897	.497	.316	1	.574
physical	-1.212	.3357	-1.870	-.554	13.023	1	.000
relationships							
Data Category							
audio	-1.172	.1927	-1.549	-.794	36.979	1	.000
behavior	.697	.1889	.327	1.067	13.629	1	.000
biometric	.918	.2984	.333	1.503	9.468	1	.002
demographic	1.395	.2762	.854	1.937	25.519	1	.000
photo	-.269	.1695	-.601	.063	2.525	1	.112
video							
Recipient							
appserver	1.830	.1922	1.453	2.207	90.686	1	0.000
friends	.131	.1971	-.255	.518	.445	1	.505
public	-.084	.1948	-.466	.297	.188	1	.665
work							
Male	1.812	.5787	.677	2.946	9.798	1	.002
IUIPC	-.720	.0706	-.858	-.582	103.943	1	0.000
Male * IUIPC	-.272	.0950	-.459	-.086	8.211	1	.004
[risk=financial] * [medium=demographic]	-.171	.4364	-1.026	.684	.153	1	.695
[risk=financial] * [medium=photo]	2.354	.4272	1.517	3.191	30.377	1	.000
[risk=financial] * [medium=video]	0[a]						
[risk=image] * [medium=audio]	2.373	.2269	1.928	2.818	109.373	1	0.000
[risk=image] * [medium=behavior]	1.107	.2195	.677	1.538	25.446	1	.000
[risk=image] * [medium=demographic]	2.152	.3778	1.411	2.893	32.441	1	.000
[risk=image] * [medium=photo]	.308	.2017	-.087	.703	2.329	1	.127
[risk=image] * [medium=video]	0[a]						
[risk=medical] * [medium=behavior]	-.210	.3561	-.908	.488	.347	1	.556
[risk=medical] * [medium=biometric]	0[a]						
[risk=medical] * [medium=demographic]	0[a]						
[risk=physical] * [medium=behavior]	.906	.3239	.271	1.541	7.826	1	.005

[risk=physical] * [medium=demographic]	0[a]						
[risk=physical] * [medium=video]	0[a]						
[risk=relationships] * [medium=audio]	0[a]						
[risk=relationships] * [medium=behavior]	0[a]						
[risk=relationships] * [medium=photo]	0[a]						
[risk=relationships] * [medium=video]	0[a]						
[recipient= appserver] * [risk=financial]	-.663	.2801	-1.211	-.114	5.597	1	.018
[recipient= appserver] * [risk=image]	.027	.2196	-.404	.457	.015	1	.902
[recipient= appserver] * [risk=medical]	-.077	.2365	-.541	.386	.107	1	.743
[recipient= appserver] * [risk=physical]	-.353	.2576	-.858	.152	1.879	1	.170
[recipient= appserver] * [risk=relationships]	0[a]						
[recipient= friends] * [risk=financial]	-.422	.3088	-1.027	.184	1.864	1	.172
[recipient= friends] * [risk=image]	.244	.2317	-.210	.698	1.109	1	.292
[recipient= friends] * [risk=medical]	.570	.2295	.120	1.020	6.165	1	.013
[recipient= friends] * [risk=physical]	.191	.2743	-.346	.729	.486	1	.486
[recipient= friends] * [risk=relationships]	0[a]						
[recipient= public] * [risk=financial]	-.256	.3087	-.861	.349	.690	1	.406
[recipient= public] * [risk=image]	.394	.2244	-.046	.834	3.077	1	.079
[recipient= public] * [risk=medical]	.508	.2354	.047	.969	4.655	1	.031
[recipient= public] * [risk=physical]	-.364	.2830	-.919	.190	1.658	1	.198
[recipient= public] * [risk=relationships]	0[a]						
[recipient= work] * [risk=financial]	0[a]						
[recipient= work] * [risk=image]	0[a]						
[recipient= work] * [risk=medical]	0[a]						
[recipient= work] * [risk=physical]	0[a]						
[recipient= work] * [risk=relationships]	0[a]						

Dependent Variable: VUR

Model: (Intercept), risk, category, recipient, Male, IUIPC, Male * IUIPC, risk * category, recipient * risk

a. Set to zero because this parameter is redundant.