

Risk Perceptions for Wearable Devices

Anonymous

Some Place

ABSTRACT

Along with great benefits, wearable devices, or “wearables,” bring new potential privacy and security risks which expose users’ activities without their awareness or consent. With the additional capabilities of wearable devices and their increasing popularity, people have expressed interest in being notified before data capture, but human attention is a finite resource. Therefore, user concerns should be investigated to warn users only about situations they are likely to care about. Informed, select notifications make for a better user experience and prevents habituation to such notifications while avoiding scandalous breaches of privacy. To this end, we conducted the first large-scale study to investigate user security and privacy concerns for wearable devices. We surveyed 1,784 Internet users for their perceptions of wearable devices and contribute: relevant perceived risks for wearables, effects of data type and data recipient on perceived risk, users’ self reported concerns, and an assessment of how wearable device capabilities compare to familiar technologies. We conclude with a discussion on future research directions for wearable devices.

Categories and Subject Descriptors

K.6.5. [Management of Computing and Information Systems]: Security and protection—*Unauthorized access*

Keywords

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

1. INTRODUCTION

Wearable technologies, or “wearables,” are a \$700 million industry [?] of electronically enhanced clothing items and accessories that interweaves technological interaction with everyday life. A top 25 market research company estimates that 52% of technology consumers are aware of wearables and 33% said they were likely to buy one [?]. With 20% of the general population owning at least one wearable and

10% using it daily [?], wearables are transforming ubiquitous computing into a part of every day life. Forbes has named 2014 the “Year of Wearable Technology [?].”

The constantly captured data from these devices has many benefits, ranging from a more natural, human-centered interface experience to a healthier, fitness-data inspired lifestyle. There will likely be many more applications in the future which take advantage of such data. It is clear why wearable devices are becoming even more popular, especially as they have more capabilities and benefits over traditional devices.

Along with these benefits, wearable devices bring new potential privacy and security risks which expose users’ activities without their awareness or consent. Fitbit allowed sex to be tracked as exercise while fitness profiles were public by default [?], resulting in the inadvertent disclosure of sensitive information. Public discomfort toward facial recognition prevented the capability from being deployed to Google Glass [?]. Google Glass, the iconic wearable of its time, has since disappeared [?]. Most suspect that the reason for its disappearance was because it was not a shift in interest, but public concern over privacy issues [?]. Some Glass wearers faced assault [?, ?, ?] from uncomfortable bystanders.

We have seen similar privacy [?, ?, ?] and security issues [?, ?] related to data capture with respect to smartphones. Mobile platforms have tried to address this by communicating data capture to users as the data is captured. However, many users are habituated to these notifications, because they see them all the time, often for things that they don’t care about [?].

With the additional capabilities of wearable devices and their increasing popularity, people have expressed interest in being notified before data capture [?], but human attention is a finite resource [?]. Therefore, user concerns should be investigated to warn users only about situations they are likely to care about. Informed, select notifications make for a better user experience and prevents habituation to such notifications while avoiding scandalous breaches of privacy.

The goal of this paper is to gain a better sense of user concerns for wearables. To our knowledge, this is the first large-scale study to investigate user security and privacy concerns for wearable devices. We surveyed 1,784 Internet users for their perceptions of wearable devices and contribute the following:

- Comparisons of users’ perceptions of a range of privacy and security risks of wearables. We found that users care much more about the type of data than the recipient of the data.
- Insight into 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, comparatively to sharing with an application’s servers.
- A report and categorization of users’ self-reported top concerns for wearable devices. We give an sense of what broad concerns users have, which can be used to guide research in unexplored use cases.
- Rankings of how data-collection capabilities of wearable devices compared to more familiar technologies. Most saw new capabilities as benign, but we suspect that this may be due to a lack of exposure to these newer technologies.

2. RELATED WORK

We discuss related work that has examined users’ perceptions surrounding security and privacy risks.

2.1 Wearables Concerns

A small-scale interview of how bystanders feel about wearable devices [?] found that bystanders were predominantly split between having indifferent and negative reactions to the device. A variety of factors that make recording more or less acceptable, including what they are doing when the recording is being taken. Additionally, bystanders are expressed interest in being able to give permissions for the data being captured. We also investigate how the type and mechanism of data capture affects privacy concerns, but we examine the privacy concerns of wearables owners at a large-scale while their research examined the privacy concerns of wearables bystanders at a small-scale.

2.2 Ubiquitous Sensing Concerns

Many authors have emphasized that we are rapidly moving towards a world of ubiquitous sensing and data capture, with ensuing privacy challenges [?, ?, ?]. Many researchers have worked to study how privacy can be preserved in such a future. Examples of such efforts include frameworks to design for privacy [?, ?, ?] or evaluate privacy [?] in ubiquitous computing applications. Others have suggested various models for understanding privacy in ubiquitous computing systems [?, ?]. However, none of these works attempted to quantify or rank user concern over different privacy risks.

2.3 Smartphones Concerns

Many researchers have attempted to study end-user concerns about security or privacy issues associated with their smartphones [?, ?, ?].

2.4 User Perceptions and Behaviors

In this paper we focus on measuring people’s perceptions of security and privacy risks. One limitation of user perceptions is that people don’t always have enough information to make privacy-sensitive decisions; even if they do, they often trade off long-term privacy for short-term benefits [?]. Also, actual behavior may deviate from self-reported behaviors [?] and privacy preferences [?].

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. At the time of this study, August 2014, the most popular wearable devices included the fitbit fitness tracker which performs continuously monitors heartbeat, steps taken, and sleep patterns [?, ?], the pebble smartwatch which can take pictures, send texts, show notifications from online, and push notifications to services [?, ?, ?], and google glass [?, ?]. These wearable devices, along with other comparable wearable devices on the market, were researched as inspiration for the survey questions.

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. In the other section, we asked participants to compare the risks and benefits of wearable technologies to better understood technologies, following the same methodology as a seminal study in risk perception by Fischhoff *et al.* [?]. Our survey design is based on two prior perception studies, as we describe next.

3.1 Motivation

3.1.1 Smartphone Risk Scenarios

Felt *et al.* previously studied the security concerns of smartphone users by conducting a large-scale online survey [?]. Their survey asked 3,115 smartphone users about 99 risk scenarios. Participants were asked how upset they would be if a certain action had occurred without 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 different scenarios chosen to shed light on security and privacy risks of wearable devices.

3.1.2 Technology Risk Perception

Fischhoff *et al.* performed a seminal study of perceived risks with 30 widely used technologies [?]. In their study, participants were asked to separately rate the risks and benefits for those technologies. They were told to think about all people affected by the technology, and to think about long-term vs. 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 risk rating 20 is considered twice as risky compared to a technology with a risk rating of 10). We apply their methodology to evaluate perceived risks and benefits of several technologies related to wearable computing.

3.2 Survey Questions

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

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

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.

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. To ensure that participants had read and understood this device’s capabilities, we ask them two multiple-choice comprehension questions.

3.2.2 Wearables Scenarios

We presented scenarios involving data capture using the Cubetastic3000 and asked them to rate how upset they would be if a particular data type (e.g., video, audio, gestures, etc.) were shared with a particular data recipient without asking first (see Figure 1). Responses were collected on a 5-point Likert scale (from “indifferent” to “very upset”), which was modeled after Felt et al.’s study of smartphone users’ risk perceptions [?]. Our questions were of the format:

“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>). The 4 possible data recipients were:

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

The purpose of these questions was to determine the extent data types and data recipients play a role in upsetting participants when data is inappropriately shared. There were a total of 288 questions in this set, from which we randomly 6 questions for each participant.

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 of the scenarios that Felt et al. found

least and most concerning to their participants [?]. We randomly presented each participant with 2 of these 5 questions:

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?

So that we could perform controlled comparisons based on device type, we also included a version of each of these questions in the wearable scenarios section that substituted “Cubetastic3000” for “smartphone.” Thus, there were a total of 293 Cubetastic3000 scenarios, from which each participant was randomly assigned 6.

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. [?], 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, which 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 firstly consisted of questions asking for age, gender, and education. Then, we 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 end with the 10-question Internet Users' Information Privacy Concerns (IUIPC) index [?], 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 August 7th-13th 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. 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 ($\sigma = 10.37$). 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 were upset, at least a little, in all scenarios when a device takes 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.

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 con-

cerns), 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

We present our survey results and provide analyses of the data. We first discuss participants' responses to the various data-sharing scenarios, and how data type, data recipient, and device contributed to how threatening a situation was perceived. 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 factors, including demographic traits.

4.1.1 Data Type

Based on our data, we observed that the largest effect stemmed from the data being shared. We present various statistical models in section C to support this conclusion. The 10 top and bottom concerning data can be seen in Table 9, and the full list of data can be seen in Appendix [?].

Participants were most concerned about photos and videos, especially if they contained embarrassing content, nudity, or financial information. As seen in Table 9, photos and videos accounted for 5 of the top 10 concerns, and are almost unanimously considered to be concerning. Information that could be used to impersonate someone (e.g., usernames/passwords for websites) or invade privacy (photos of someone at home) were also among the most concerning data types.

Participants were least concerned about data that could be observed through observations of public behavior, such as demographic information (e.g., age, gender, language spoken) and information available to advertisers (e.g. TV shows watched, music on device). As seen in Table 9, participants had spread distributions in perceptions regarding such information. These may have appeared as uninteresting because of unfamiliarity in what applications would use this data for, or because there does not seem to be any immediate financial, social, or physical consequences from having this information shared.

For the complete ranked list of data considered in this study, see Appendix [?]. 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 any data which evoked strong disagreement on how upsetting it was. Generally, the rank of the data being shared is negatively correlated with the standard deviation of the answers.

4.1.2 Data Recipient

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 [?].

There was a statistically significant difference in VUR for an application’s servers comparatively to human data recipients. 42% of participants stated that they would be “very upset” if their data was shared with only the app’s servers, whereas the VURs for friends (70%), work contacts (75%), and the public (72%) were much higher (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. 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.

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. Appendix G shows the complete VUR and rankings of all data types by recipient.

4.1.3 Data Type and Data Recipient

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	5,198	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 compared the 10 most concerning scenarios when sharing with an app servers versus with a humans. We observed that there was a substantial overlap between these groups, in that 6 of the most concerning scenarios were the same:

1. Bank account information
2. A video of you unclothed
3. Social security number
4. Video of you entering your PIN
5. An incriminating/embarassing photo of you
6. A photo of you unclothed

While the concerning data types do not appreciably change based on the data recipient—even the non-overlapping scenarios all dealt with confidential data (e.g., passcode, credit card information, etc.)—only the level of concern changed. For instance, the 10th most concerning scenario for the non-human audience had a VUR of 66.67%, whereas the 10th most concerning scenario for a human audience has a VUR of 93.88%. This suggests that concern for different data types does not appear to vary relative to other data types based on recipient, but instead the recipient determines the overall magnitude of the concern.

4.1.4 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, 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.

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.

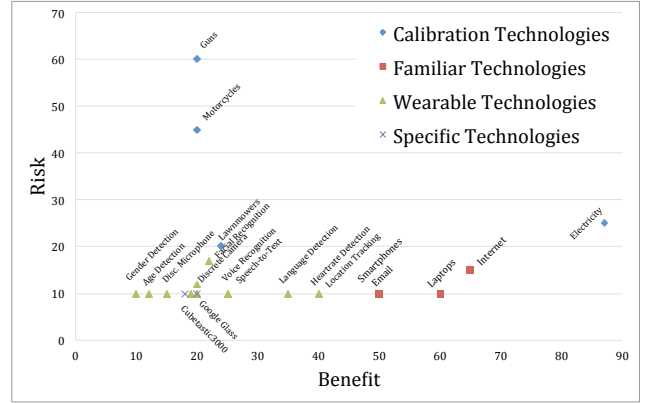


Figure 2: Participants’ median risk-benefit ratings of technologies examined by Fischhoff *et al.* [?], which we used for calibration, alongside familiar technologies (e.g., laptops, the Internet, etc.), wearable technologies, as well as two specific wearable devices (Google Glass and the Cubetastic3000).

To ensure independence of observations, we performed a Mann-Whitney U test by comparing participants’ average VURs for the Cubetastic3000 scenarios (i.e., 159 participants) to the remaining participants’ average VURs for the smartphone scenarios (i.e., 1,623 participants). We found this difference to be statistically significant (108,664.0, $p < 0.0005$), however, the effect size was incredibly 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. As a result, we can conclude that in general users are likely to be more wary of misbehaviors occurring on wearable devices than smartphones, the difference is likely negligible. Similarly, 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. [?]. We found that participants generally rated technologies related to wearables as being low-risk comparatively to other technologies (Figure 2). Appendix F 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 the more beneficial. We believe this is the result of exposure people have 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, privacy-invasive ones were perceived to be risky. Top risky technologies include 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”). The differences in risk that found between the different wearable-related technologies, are not tested for statistical significance, but given their minimal spread compared to the calibration options, the differences are negligible. Interestingly, privacy risks and are comparative to real physical risks; for instance, the capacity for facial detection on a wearable device is perceived to be almost as risky as interacting with a lawnmower.

People prompted to rate with respect to all considerations (see A), including physical harm risk to bystanders, financial cost, distress, misuse, or impact on public, personal, and private life, people may have still evaluated the risks with an emphasis toward physical risk and without an emphasis on privacy risk. Among the 5 presented options, the wearable-related one is the only one without some physical risk scenario, and physical risk is a clear, tangible risk to the users.

These perceptions of the most risky or beneficial technologies may not be reflective of actual risks or benefits. However, they do 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 of these technologies or how they could be used. We suspect that performing this experiment longitudinally may yield more interesting results, as these technologies become more and more pervasive (and therefore more familiar to participants).

4.3 Self-Reported Concerns for Wearables

We also wanted to capture the participants’ general reactions to wearable devices as a whole. To do this, we asked the participants the following open-ended question:

What do you think are the most likely risks associated with

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: A table listing the self-reported most common risks associated with owning a wearable device.

wearable devices?

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

Table 5 shows the most common user concerns related to wearable devices. Appendix B details the responses categorized in each coding label. Most of these concerns are related to privacy and security, but this self-report 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 in a general sense, significant concerns included being unaware of what the device is collecting, doing, or which information it is using (Being Unaware), 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 which cause car accidents (Safety), resulting changes in social behaviors, such as dependencies on devices or spending less time with loved ones (Social Impact), the high financial cost of buying, replacing, or caring for the device (Financial), and information compromise (Security).

4.3.1 Demographic Factors

Participants’ responses were correlated with demographic factors. We observed that the biggest 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 [?]. A Spearman correlation yielded a statistically significant effect between average IUIPC scores with the VUR ($\rho = 0.446$, $p < 0.0005$), which suggests that people’s responses to questions were mostly based on their 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 protective of their privacy [?].

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 \times 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 recipient and data type. Because the device type independent variable (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 5 data types from our models, which resulted in a total of 72 data types shared between 4 possible recipients. We also used our 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 and observed that 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 (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 C.

While these models clearly illustrate the relative weight that users might place on various types of information when determining whether a given privacy violation is truly upsetting, one shortcoming of this approach is its generalizability: the data type predictor is categorical and obviously limited to the data types that we specifically chose for this study. That is, it is not entirely clear how these models might apply to data types not among the 72 that we directly examined. Therefore, in an attempt 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 data type (e.g., video, audio, etc.) and in terms of the type of risk it might present to the user. Two researchers agreed on a codebook and independently coded each of the 72 data types.¹

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* is defined as measurements of the user’s body; and *demographic information* is defined as non-biometric information about the user’s traits. The associated risks for each data type fell into the following five 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 all data types with respect to these categories, the researchers met to resolve any disagreements, such that the resulting codings reflected unanimity. Prior to this resolution, there was 83% agreement. Cohen’s κ was 0.81 for the data categories and 0.75 for the associated risks, both indicating “excellent” agreement [?]. Applying this taxonomy to our collected data, we observed that average VURs were highest for financial risks (82.0%) and lowest for medical data risks (47.4%). In the middle were relationships (69.2%), physical (66.4%), and self-image (65.8%) risks. One reason why medical risks were ranked relatively low is that this may be a misnomer: in addition to covering scenarios involving data about the user’s health, it also covered basic demographics, such as age, gender, and emotional

¹We excluded the data types that did not feature a data recipient, the five misbehaviors used to examine device types.

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 \times 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 \times Gender	8.21	1	
Risk \times Data Category	303.44	8	
Recipient \times Risk	39.14	12	

Table 7: Goodness-of-fit 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 $p < 0.005$.

state. Similar to what we observed in Section 4.1.1, participants likely understood that many of these data types are publicly observable, which is why they were less concerned.

With regard to the VURs of the broad categories of data that we coded, 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. In this case, we suspect that demographic data was more concerning than we expected because it included information that could be used to perpetuate fraud or identity theft, such as a Social Security Number, bank account information, and other financial information. We were very surprised that biometric information was seen as relatively benign (at least as compared to the other broad categories of data). One hypothesis is that since most home users do not use biometric authentication, they may have a poorer understanding of the types of systems that might be at risk if biometric data were to be stolen and then abused.

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 D.

5. DISCUSSION

Here, we discuss complementary future research directions in fields of privacy, ubiquitous computing, and user studies, along with specific limitations of this survey.

5.1 Interpreting the Survey Results

One of the main limitations of this work is that our participants might not have interest in or knowledge of wearables and their capabilities. 83% of our participants reported that they do not own a wearable device. These participants may have underestimated or overestimated the risk perceived in various scenarios. People may be overreacting to recent events for scenarios ². People may be underestimating the risk of sharing certain data due to unawareness of what can be inferred from the data, or not have an idea of how to rate a new technology with respect to familiar ones. Biometrics were generally not a concern for our participants, although there are many security and privacy implications [?].

We believed that getting a representative survey base was a useful endeavor. We could have easily recruited only wearables owners or people specifically interested in wearables. However, that will also have its own biases and limitations, since this does not reflect the general population. At the time of this writing, about 85% of the general population do not own wearable devices [?, ?], so our study reflective of the status quo. We expect user perceptions to change as rapidly as wearable technologies and the rate of adoption change.

Privacy concerns asked out of context differ from how users may react to these same concerns in real life [?, ?]. This is an unavoidable, yet important consideration of any study of this nature. This privacy paradox means that our findings may not be exactly representative of how upset users may be in real life, but do reflect their perceptions of wearable devices and various associated scenarios.

5.2 Future Research Directions

Further work can be done to expand various aspects of this study. Investigating more fine-grained data types (e.g. investigating if various types of location data, versus just location data in general) would be a useful endeavor to gain further insight into user perception. Adding more recipients, like “advertisers” or “acquaintances” may lead to more contrasting results.

While privacy and security concerns were expected, consider the following self-reported user concerns as 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 infancy. Perceptions of situations and capabilities will change rapidly with advancements and in-

²During our study, there were many stories covering injuries from exploding batteries (<http://www.bloomberg.com/news/articles/2014-08-11/exploding-lithium-batteries-riskier-to-planes-research>), which were explicitly and repeated mentioned when self-reporting concerns.

creased exposure. However, videos and textual information are considered to be significantly sensitive by our participants, along with past participants of smartphone user perception studies. 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. CONCLUSION

Our 1,784 Internet users for their perceptions of wearable devices was the first large-scale study to investigate user security and privacy concerns for wearable devices. We identify that participants are most concerned about protecting their financial information, photos, and videos and least concerned about demographic or biometric data. We find that participants have a significant difference in perception of risk when data is being shared with an application's server versus other human recipients, and also that certain data is more comfortably shared with certain recipients. Participants' self-reported concerns of categories and perceptions of new wearable device capabilities are also presented to give a sense of the relevant user concerns, which can be used to guide future research in privacy with respect to wearable devices, especially warnings, notifications, and permissions. We perform two regression model analyses with respect to the type of data and the associated risks.

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

Privacy: "privacy," revealing personal information, spying.

Security: "security," compromise, malware, hacking.

GPS tracking: "location," "GPS," being monitored.

Unaware use: using data without permission or in a different way than understood by user.

Unaware collection: collecting data without permission.

Unaware access: disclosure of data without permission.

False information: inaccurate or maliciously false data.

Health Risk: radiation, cancer, or long-term effects.

Safety: distractions causing car crashes or injuries, mugging or violence because of the device, injuries from device malfunctions (battery burns).

Discomfort: eye strain, headache, obscured vision, irritation.

Financial cost: getting ripped off by buying the device or device accessories, having to buy another device when broken or stolen, financial compromise caused by device.

Theft: the device getting stolen.

Social Impact: dependency, distance from friends and family, changes in decision making, social changes, etc.

Social Stigma: judgment, hate, or bystander discomfort.

Aesthetics: fashion, the device being ugly, mentions of not looking cool/dorky.

Miscellaneous: odd comments, uncommon concerns.

None: "None," no threat, perceiving no big concerns

Don't know: "do not know," hinting at confusion

Don't care: "do not care," nonchalant answers

C. FULL REGRESSION MODEL FROM DATA TYPES

Parameter Estimates							
Parameter	B	Std. Error	95% Wald Confidence Interval		Hypothesis Test		
			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

D. FULL REGRESSION MODEL FROM DATA RISKS / DATA CATEGORIES

Parameter Estimates

Parameter	B	Std. Error	95% Wald Confidence Interval		Hypothesis Test		
			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] *	0 ^a						
[medium=demographic]							
[risk=physical] *	0 ^a						
[medium=video]							
[risk=relationships] *	0 ^a						
[medium=audio]							
[risk=relationships] *	0 ^a						
[medium=behavior]							
[risk=relationships] *	0 ^a						
[medium=photo]							
[risk=relationships] *	0 ^a						
[medium=video]							
[recipient= appserver] *	- .663	.2801	-1.211	-.114	5.597	1	.018
[risk=financial]							
[recipient= appserver] *	.027	.2196	-.404	.457	.015	1	.902
[risk=image]							
[recipient= appserver] *	-.077	.2365	-.541	.386	.107	1	.743
[risk=medical]							
[recipient= appserver] *	-.353	.2576	-.858	.152	1.879	1	.170
[risk=physical]							
[recipient= appserver] *	0 ^a						
[risk=relationships]							
[recipient= friends] *	-.422	.3088	-1.027	.184	1.864	1	.172
[risk=financial]							
[recipient= friends] *	.244	.2317	-.210	.698	1.109	1	.292
[risk=image]							
[recipient= friends] *	.570	.2295	.120	1.020	6.165	1	.013
[risk=medical]							
[recipient= friends] *	.191	.2743	-.346	.729	.486	1	.486
[risk=physical]							
[recipient= friends] *	0 ^a						
[risk=relationships]							
[recipient= public] *	-.256	.3087	-.861	.349	.690	1	.406
[risk=financial]							
[recipient= public] *	.394	.2244	-.046	.834	3.077	1	.079
[risk=image]							
[recipient= public] *	.508	.2354	.047	.969	4.655	1	.031
[risk=medical]							
[recipient= public] *	-.364	.2830	-.919	.190	1.658	1	.198
[risk=physical]							
[recipient= public] *	0 ^a						
[risk=relationships]							
[recipient= work] *	0 ^a						
[risk=financial]							
[recipient= work] *	0 ^a						
[risk=image]							
[recipient= work] *	0 ^a						
[risk=medical]							
[recipient= work] *	0 ^a						
[risk=physical]							
[recipient= work] *	0 ^a						
[risk=relationships]							

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.

- E. CONCERN FACTOR: DATA TYPE
- F. RISK BENEFIT ASSESSMENTS OF VARIOUS TECHNOLOGIES
- G. CONCERN FACTOR: RECIPIENT

























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 Video 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 in response to the Fischhoff-style prompt for various technologies and capabilities. Most technologies are capabilities with respect to wearable devices. Calibration technologies were electricity, guns, lawnmowers, and motorcycles. Wearable technologies included the Google Glass and the Cubetastic3000. Other specific technologies, such as internet, email, laptops, and smartphones, were also asked.

























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 Video 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 in response to the Fischhoff-style prompt for various technologies and capabilities. Most technologies are capabilities with respect to wearable devices. Calibration technologies were electricity, guns, lawnmowers, and motorcycles. Wearable technologies included the Google Glass and the Cubetastic3000. Other specific technologies, such as internet, email, laptops, and smartphones, were also asked.

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	video of you at home	81.05	0.60	
18	photo of you intoxicated	78.95	0.82	
19	photo of you at random	78.76	0.85	
20	audio recording of conversations	78.13	0.83	
21	medical conditions	77.7	0.86	
22	video of you at random	76.19	0.59	
23	video of you off-guard	76.0	0.62	
24	photo of your work or workplace	74.62	0.90	
25	username for websites	73.44	0.83	
26	address	72.61	0.86	
27	audio recording you captured	72.55	0.70	
28	photo of you off-guard	72.55	0.77	
29	photo downloaded from internet	71.81	0.90	
30	photo others sent you	71.63	1.03	
31	video others sent you	70.59	0.81	
32	video of your work or workplace	70.54	0.90	
33	fingerprint	70.12	0.86	
34	when you were lying nervous or stressed	69.74	0.91	
35	audio recording of you (voice notes)	69.59	0.91	
:	:			

Table 8: The 10 most and least upsetting data types, across all recipients. For the complete list of all data types across all recipients, see Appendix [?].




































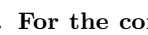
Rank	Question	VUR	σ	Distribution
	\vdots			
36	medication taken	69.49	1.01	
37	videos already on device	68.89	0.88	
38	photo of your signature	68.07	0.84	
39	web history	66.44	1.01	
40	photos taken on device	66.21	1.02	
41	home address	65.0	0.97	
42	fine-grained location tracking (+/- cm)	63.51	0.99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

Table 9: The 10 most and least upsetting data types, across all recipients. For the complete list of all data types across all recipients, see Appendix [?].

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

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