Perceptions of Information Disclosure Risks for Wearable Devices

Linda Lee, JoongHwa Lee, Serge Egelman, David Wagner
University of California, Berkeley
{lnl@,dlwndghk94,egelman,daw}@cs.berkeley.edu

***Abstract*—Wearable devices, or "wearables," bring great benefits but also potential information disclosure risks that could expose users' activities without their awareness or consent. We surveyed 1,782 Internet users about various data associated with the capabilities of popular wearable devices on the market to identify which users find most concerning if disclosed. Our study relatively ranks a range of potential data capture scenarios enabled by wearable devices, investigates the impact of the recipient of the data on the perceived risk of data disclosure, and concludes with a survey of users' risks perceptions associated with wearable devices. Users perceive associate risks of owning a wearable with compromised privacy and security, but also consider factors such as safety risk, changes in social behaviors, and how wearable devices are unfashionable. To our knowledge, this is the largest user-based experiment concerning information disclosure regarding wearables. We hope that this work will aid in the design of future user notification, permission management, and access control schemes for wearables.**

I. Introduction

Wearables are a $700 million, growing industry [2]. With 20% of the general population owning at least one wearable and 10% using it daily [10], wearables are bringing ubiquitous computing to everyday life. This trend will likely continue, as 52% of technology consumers are aware of wearables and 33% are likely to buy one [6].

Wearable devices enable benefits ranging from a fitness-data inspired lifestyle to a virtual-object filled augmented reality. However, wearable devices also bring new potential privacy and security risks that could expose users' activities without their awareness or consent. Although wearable devices are still in their infancy, we have already seen manifestations of these risks. Fitbit's default privacy settings inadvertently exposed information about some of their users' sexual activity [18]. Public discomfort toward facial recognition caused Google to prohibit Google Glass applications from using facial recognition [27], but still resulted in tech hate crimes against its users [34], [13].

USEC '16, 21 February 2016, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2016.23006

Wearables' sensor capabilities, continuous access, and ubiquitous presence will result in a firehose of familiar and unfamiliar types of data, at a rate which will likely dwarf the amount of data currently captured by smartphones. Bystanders of wearable devices have already expressed interest in such communication, desiring notification before data about them is captured [12]. However, subjecting people to increased notifications is not a sound option, as it has shown to lead to negative effects, such as frustration and habituation [7]. An understanding of user concerns may allow for targeted and effective communication with the user, inform design of future permission systems, or provide insight for access control mechanisms.

The goal of this work is to motivate research on the still-malleable future of wearable interaction models to preserve privacy and security, which we found are the top user perceived risks associated with wearable devices. Our survey of 1,782 Internet users contributes the following:

- We give a relative ranking of 72 potential capture scenarios, which were inspired from the capabilities from the most popular wearable devices on the market at the time of the study.
- We study 4 possible data recipients to find that the recipient of the data contributes to the magnitude of overall perceived risk, but do not find statistically significant correlated factors of risk between data and recipient.
- We sketch a landscape of users' self-reported concerns regarding wearable devices and analyze responses using logistic regression models.

II. Methodology

We designed a survey for our IRB-approved study to capture the general public's perception of wearables risks. To determine which of the current data capture scenarios were most concerning to users, we asked them to rate their level of concern for a handful of scenarios from a list of possible scenarios. 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 [14]. To get a qualitative, unbounded measurement of what people thought the most common risk associated with wearables are, we asked our participants an open-ended question.

To obtain a representative list of scenarios, 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; the Pebble smartwatch, which can take pictures, send texts, show notifications from online, and push notifications to services; and Google Glass, which can take pictures, record video, and perform a subset Internet-based tasks such as search, reading emails, etc. These devices' capabilities and requested permissions were the basis for the list of possible data capture scenario questions used in this study, which we feel will be representative of what users are likely to encounter today.

A. Survey Questions

We report on participants' responses to 23 questions across 4 survey sections:

- 2 reading comprehension questions
- 6 questions regarding possible wearables scenarios
- 1 open-ended wearables risk question
- 14 demographic questions

To reduce fatigue, we gave our participants a randomly selected subset of wearables scenarios. The average survey completion time was 11.5 minutes, which includes four questions that we omitted from this paper due to lack of participants' familiarity with specific devices and a misguided attempt to directly compare smartphones and wearables. See Appendix A for details.

Comprehension Questions The beginning of the survey introduced participants to the "Cubetastic3000," which was the basis for all questions on wearables risks. Because participants might be biased to specific companies (e.g., visceral reactions to Google Glass based on popular media stories), we framed our scenarios on a fictitious wearable. 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 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, you can install third-party applications from an app store, and these applications can use the information from the Cubetastic3000.*
>
> *With a wide range of applications, 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*
> *—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 things*
> *...and much more!*

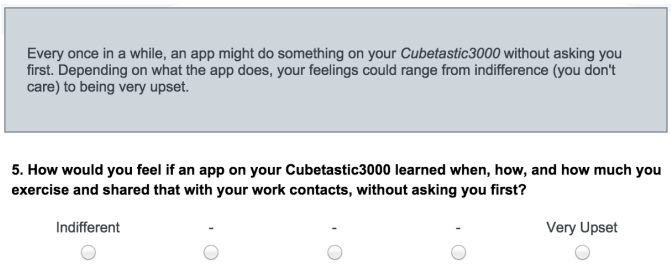

Fig. 1. An example of a wearable scenario question participants saw while taking the survey.

To guarantee that participants had understood its capabilities, we asked two multiple-choice comprehension questions and filtered out responses from participants who did not answer both questions correctly.

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., how much you exercise) was shared without permission with a particular recipient (e.g., work contacts). 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. Responses were reported on a 5-point Likert scale (from "indifferent" to "very upset"). Figure 1 shows an example. Specifically, 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 combined 72 data types, (*data*), with 4 data recipients, (*recipient*), to form a pool of 288 scenarios (Table VII). Each participant answered 6 questions that were randomly drawn from this pool, displayed in random order. We clarified for our participants that "app" meant the app's server, and that the data was not shared with anyone else.

1) Additional Questions: The exit portion of the survey contained demographic questions (age, gender, and education), and then asked about wearable device ownership so we could control for prior exposure. An open-ended question on what would be the most likely risks associated with wearable devices was included to capture user concerns more broadly. To avoid biasing the open-ended question, we asked before concluding with the 10-question Internet Users' Information Privacy Concerns (IUIPC) index [25], which was included so

we could control for participants' general privacy attitudes. However, we do realize that we asked this open-ended question after we had exposed our participants to a variety of wearables scenarios, which may have heightened their awareness of the possible risks. We talk about this more in Section 4.

B. 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 then giving 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.

C. 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 for being 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 [14]. 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 distinguishing factor is whether a participant was maximally upset. A 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.

III. Results

In this section, we present participants' responses to the various data-sharing scenarios, and discuss how and which various factors contributed to their risk perceptions. We had at least 141 responses per data type, 2,779 per recipient, and 35 responses per each unique data type/recipient combination. We conclude the section with participants' self-reported wearables concerns.

Data Type Based on our statistical models (later reported in Section III), we observe that the largest effect on participants' VURs stemmed from the data being shared, rather than with whom the data is shared. The most and least concerning data types are listed in Table I.

Participants were most concerned about photos and videos, especially if they contained embarrassing content, nudity, or financial information. As seen in Table I, 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 I, 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 Table VII.

Data Recipient A statistically significant difference in VUR exists between data shared with an application versus 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 II). A chi-square test indicated that these differences were statistically significant (Table III). 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 ($\phi = 0.004$).

The statistical significance arises for two distinct reasons. Firstly, sharing data only with an application's server carries

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 I
THE 10 MOST AND LEAST UPSETTING DATA TYPES, ACROSS ALL RECIPIENTS.

less social impact. And for our participants, it may seem that it is shared with fewer people. Additionally, there is a class of data which may be considered odd for a human to know, but completely normal for a wearable device to know (e.g., it's okay if your Fitbit knows when you sleep, but maybe less so for your friends).

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. Our results motivate mechanisms for data taint tracking and accidental data sharing prevention.

However, 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 recipients. For instance, participants were significantly more uncomfortable sharing if they were lying, nervous, or stressed to work contacts compared to the rest of the data recipients. Table VII shows the complete VURs and rankings of all data types by recipient.

Open-ended Concerns We captured participants' 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?*

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 II
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 III
RESULTS OF A CHI-SQUARE TEST TO EXAMINE VUR BASED ON DATA RECIPIENT, ACROSS ALL DATA POINTS.

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 IV
THE MOST COMMON OPEN-ENDED RISKS ASSOCIATED WITH OWNING A WEARABLE DEVICE.

The participants were presented with a blank box to write in, with no particular suggestion on what to talk about, and with no character limit to their open-ended responses. Table IV shows common user concerns related to wearable devices. Appendix A details the responses categorized in each coding label. Note that participants were especially concerned with privacy and security, however, we do realize that we asked this open-ended question after we had exposed our participants to a variety of privacy-related scenarios, which may have heightened their awareness of the possible privacy and security risks.

> *P246: "Privacy and security of your data, particularly for eg, [sic] stored financial/payment or medical information"*

> *P1256: "They can be hacked and then your security will be compromised."*

Other 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), and safety hazards from wearing the device, such as distractions that cause car accidents (Safety).

> *P1742: Capturing and sharing data and information that you are unaware of.*

> *P670: "Are there microwaves or some such type of waves that can pass through the brain and harm the brain? Wearing something all day can hurt that area of the body after a while."*

> *P1038: "Becoming distracted by the devices while doing other activities that require concentration such as driving."*

Interestingly, a modest amount of participants were also concerned with resulting changes in social behaviors, such as dependence on devices or spending less time with loved ones (Social Impact).

> *P1425: I think the biggest risk is how they may effect society as a whole... a wearable technology that's always on and available may push things even further to the point where people spend less time actually interacting with loved ones, and applying their own critical thinking in certain situations, instead always relying on their devices.*

The landscape of users' perceived risks associated with wearable devices is broad, encompassing concepts such as privacy and security, but also non-technical aspects such as health, safety, and change in social behaviors. We hope that this motivates researchers to investigate these aforementioned risks.

Demographics Factors We see that privacy is a main concern for wearables users. Additionally, we show that privacy preferences should also be a consideration when configuring a user's device. A participant's self-reported level of privacy concern—as determined by the IUIPC scale [25]—is the biggest demographic predictor of VURs. A Spearman correlation yielded a statistically significant effect between average IUIPC scores and average VUR ($\rho = 0.446$, $p<0.0005$), which suggests responses to questions were mostly based on privacy preferences. Additionally, we observed that age was another significant predictor of VUR ($\rho = 0.121$, $p<0.0005$), but we suspect that this effect 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

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 V
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 $p<0.005$.

protective [38].

While we initially observed an effect on VURs based on whether or not participants claimed to already own wearables (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.

Regression Models 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. This resulted in a total of 72 types of data shared with 4 possible recipients. Demographic factors used as covariates are: 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 participants' gender and IUIPC scores, which also exhibited an interaction effect with each other. Thus, we opted to remove the other covariates from our analysis. Table V 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 shown, the type of data being shared (data type) was found to be the strongest predictor of a high VUR.

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 these six 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 data types fell into these 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, 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 [16].

With regard to data types, the most concerning type of data is video (78.0%), which was ranked similarly to photos (76.2%). Next are 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 is

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 VI
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 $p<0.005$.

stolen and abused.

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 earlier, participants saw these as publicly observable and therefore 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.

IV. DISCUSSION

Limitations One of the limitations of our experiment is that our participants might not have knowledge or interest in wearables and their capabilities; 83% of our participants reported that they do not own a wearable. Because of this, our participants may be over or underestimating the risk, stemming from an unawareness of what can be inferred from the data, not having clear relations of new technology with respect to familiar ones, and a higher likelihood of being influenced by reports of recent events.[1] For instance, biometrics were generally not a concern for our participants, although there are many security and privacy implications [31]. Our participants also did not differentiate between the benefits and risks of various new capabilities.

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 [28], [10], 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 [29], [20]. 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).

Although we presented our participants with a prompt illustrating all the benefits of a wearable device, the questions we asked isolated the risk from the benefits of sharing data with a particular recipient. We sacrificed context due to the complexity of the question necessary for the participant to answer correctly. Users are willing to tolerate risks if there is enough benefit associated with that risk. We do believe that since all of our questions were out of context, our study does represent what data people ambiguously would like to be private and secure, and is accurate for measuring user perceptions of wearables.

Future Research Directions We find that although people have opinions on applications which are familiar, users do not know the risk associated with new data or unfamiliar applications. We hope our work both informs the direction for future research to secure video, audio, and other currently considered sensitive sensor input channels, but also encourages work for contextual and user-input-independent permission models and access control schemes.

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 illuminate areas

[1]At the time of the survey, stories of exploding batteries were in the news [24], which were explicitly reported as a concern in our open-ended question.

of possible future research, such as the design of a distraction-free interface to prevent safety issues, and how to minimize negative social impact.

V. Related Work

User Perceptions While risk communication for the physical world has been examined for several decades (e.g., [36], [15], [26]), 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 [17], [5]. While this work is likely applicable to wearable computing risk communication, we believe that a better understanding of users' information risk acceptance in this domain is warranted prior to examining risk communication.

Our study is limited to owners of general consumer wearable devices. Denning *et al.* study the effect of wearables on bystanders, to find that bystanders have a range of indifferent to negative reactions which depend on the how acceptable users find the recording to be. Nasir *et al.* specifically explore medical wearables, to find that perceived risk determines physician and user acceptance of wearable health technologies.

One limitation of user perceptions is that people do not always have enough information to make privacy-sensitive decisions. Even if users did have this information, it has been shown that users often trade off long-term privacy for short-term benefits [3]. Furthermore, actual behavior may deviate from stated privacy preferences [37]. However, understanding user concerns is a necessary first step not only for risk communication, but preventative measures in general against breaches of privacy and security in a new threat landscape.

Ubiquitous Sensing We are rapidly moving towards a world of ubiquitous sensing and data capture, with ensuing privacy challenges [1], [30], [8]. Roesner *et al.* urge the community to address potential concerns for wearable devices before the technologies become widespread [33] and explore the unique problems present in terms for law and policy [32]. Privacy preservation research in this age of ubiquitous sensing include frameworks to design for privacy [4], [9], [23], protocols for anonymous communication [11], evaluation metrics for privacy [35], and privacy models [19], [21]. Our work aims to guide these efforts with an insight into user acceptance of common information risks.

Lessons from Smartphones Not long ago, smartphones revolutionized applications' access to data. While this tends to benefit users, they do not think of the privacy implications. 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 [22], [39], which are applicable to wearables.

Felt *et al.* previously studied the security concerns of smartphone users by conducting a large-scale online survey [14]. 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.

VI. Conclusion

Our survey of 1,784 Internet users is the first large-scale study to investigate user-centric security and privacy concerns for wearable devices. We contribute a comprehensive ranking of possible risks associated with wearable devices, across various recipients. Our open-ended responses show that privacy and security are at the top of user's overall concerns. While wearables are still in their infancy, perceptions of situations and capabilities are likely to change rapidly with advancements and increased exposure. However, there has not been much prior work done to determine which threats in the emerging threat landscape are pertinent to focus on. Our examination of possible data concerns agree with previous studies of smartphone users that found that video capture and financial data are the most sensitive data types. 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. We also found that users' self-reported privacy preferences are correlated with how they may react, even with respect to situations that they are unfamiliar with. Our results may be used by system designers to create permissions and access control mechanisms that do not directly depend on users' inputs. We hope that this work has given a comprehensive overview of user concerns and informs designs of future privacy and security work for wearable devices.

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] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

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

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

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

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

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

[25] 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.

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

[27] 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.

[28] 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.

[29] 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.

[30] 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.

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

[32] 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.

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

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

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

[36] P. E. Slovic. *The perception of risk*. Earthscan publications, 2000.

[37] 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.

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

[39] 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

Our participants answered four additional question which are not detailed in this paper. Two questions compared smartphones to wearable devices, to investigate if participants inherently saw wearables as threatening due to its unfamiliarity. The questions were not particularly well suited for this task, and our results showed no significant difference between smartphone and wearables perceptions. The other two questions asked our participants to numerically rate the risks and benefits of common, familiar technologies versus wearables (e.g., an airplane versus a wearable). In addition to the fact that these comparisons were unsound to make, our results largely highlighted our participants' unfamiliarity with wearables or other less common devices; participants rated more familiar technologies as more beneficial or risky.

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

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 VII