Catchy Part: Surveying Users' Perceptions of Threats for Wearable Devices

Linda N. Lee
UC Berkeley
lnl@cs.berkeley.edu

Serge Egelman
UC Berkeley
ICSI
serge@cs.berkeley.edu

David Wagner
UC Berkeley
daw@cs.berkeley.edu

ABSTRACT

(Okay, kind of intimidated with writing the abstract. My plan is to write intro/conclusion first and then condense it into here, while nodding off to the contributions that we made.) At the very least, I can say that we studied user perceptions for threats in wearable devices, along with user perceptions of risk and benefit for emerging technologies and what they thought was the biggest risk for using wearable devices. Data type, data recipient, and device type all matter different amounts. All new technologies were perceived to be low risk low benefit but we think this is because people are unfamiliar with these technologies. Privacy was the number one concern, followed by security, then health, money, social norms changing and social stigma. Fantastic ending sentence here.

Categories and Subject Descriptors

look it up [**keyword1**]: keyword2keyword3

General Terms

term1 term2 term3

Keywords

Privacy, Security, User Studies, Risk Perception, Ubiquitous Computing, Wearables

1. INTRODUCTION

Wearable technology has many potential benefits, ranging from a more natural, human-centered interface for computing to healthier living through fitness tracking. Wearable devices, or wearables, are the new front of ubiquitous computing and big data, constantly capturing data and interpreting information to deliver insights to the user. Wearbles are gaining lots of attention: Forbes has named 2014 the "Year of Wearable Technology, [**?**]," and market research companies estimate that 52% are aware of wearables and among those, 33% said they were likely to buy one [**?**].

More formally, a survey consisting of 3,956 respondents who are either current users or non-users with high interest in wearables says that most popular devices are fitness bands (61%), followed by smart watches (45%) and mobile health devices (17%)[**?**]. It is estimated that 20% the general population owns at least one wearable and 10% uses at least one wearable in their daily lives [**?**]. The demographics of wearables consumers are young and rich–48% of owners are between 18 and 34 years old, and 29% make over $100,000 per year. However, it is expected that this $700 million industry will reach other demographics soon as the prices of wearable devices drop [**?**].

Even in early adoption, security and privacy concerns regarding wearable devices are becoming heightened as companies make headlines for incidents resulting in users' sexual activities exposed to the public. This occured when Fitbit's fitness profiles were public by default and allowed users to track sex as an exercise[**?**]. In other instances, public discomfort prevented certain capabilities from being enabled. Google's Glass had to disable facial recognition for Glass [**?**] upon release. To avoid both scandalous breaches of privacy and public opposition for new capabilities, it is critical that we understand the threat landscape for wearable devices and which issues users most care about–before wearbles get increasingly more ubiquitous and powerful [**?**]. In this work, we contribute the following:

- We show users' perceptions of a wide range of wearables threats. We contribute a topmost and bottommost concerns , along with an evaluation of which factors contribute to the severity of a threat. We find that data type, data recipient, and device type matter A%, B%, C%, respectively. See section <todo> for details.
- We investigate how people's privacy preferences differ when data is perceived to be shared with people or a server.
- We show risk and benefit assessments of new technologies and capabilities; most are seen as low risk low benefit, but we hypothesize this is the result of limited exposure.
- We report people's self-reported top concerns for wearable devices. Privacy, by far, is the top concern. Other notable risks include information security, long-term health risks from use, finances, and change in social norms.

2. RELATED WORK

In this paper, we explore user perceptions of security threats for wearable devices. In this section, we discuss related works which explore threats for smartphones and wearable devices, discuss emerging challenges related to ubiquitous computing, and study user perceptions of threats and technologies.

2.1 Concerns for Smartphones and Wearables

(REDO) Mention Adrienne's work here, and other relevant smartphone studies of any sort. I will talk about how I model Adrienne's work in the next section, Survey, just give a nod to it here and go into it later. Since my results were that people care about privacy, security, health, and social change/social stigma, any phone studies which hint at any of those things will be good to put here. Be sure to go cite a fair number of them. Related work section is the part where it looks like I know stuff.

Mention any studies for wearables (like the ones you can find at Ubicomp, CHI, or SOUPS), and give them a nod. Especially mention ones on privacy and perceptions, since I know those exist. I doubt there will be ones for social norm shifts/social stigma, or health concerns, but maybe I can at least include some security ones here too. Throughout mentioning all of these works, highlight how my study is different from previous studies.

2.2 Ubiquitous Computing

(REDO) As technology becomes more and more ubiquitous, more sensors will record more things about more people more of the time. There are an endless amount of unique situations which can negatively impact a person's privacy or security. There is a clear need to better communicate these risks to people (cite webcam paper and other papers here?), but there are too many things to warn people about. Therefore, we need to know what are the most threatening and also most relevant situations to inform the users about, since we can't bug them all the time about everything.

We need to investigate the threat landscape and people's privacy concerns now, before wearables are widely adopted, or designed without these considerations in mind. So although our research is at at time when things are rapidly changing and most people don't have wearables, it is crucial to do the research now so we can prevent badness later.

2.3 User Perception

(REDO) In this paper, we investigate one of the two important questions–what are the most relevant situations to people. We do this firstly because people are really bad at knowing the likelihood of something, especially a threat with respect to security or privacy, is going to happen (sources here). And while the most damaging situations should also be addressed, this is not yet possible since these technologies haven't been adopted and the damage hasn't happened, so we don't know yet. Additionally, since the number one concern that people had with these devices was privacy (can I say result here? I guess I already did in abstract), we need to know what people consider private, which is more nuanced and requires a user study like this survey.

We also study risk. Mention Fischoff here. This is a very seminal paper in risk perception and it also studies how safe enough something has to be before people can accept something. I will talk about how I model my work in the next section, Survey, just give it a nod here and go into it later. Also mention at least a couple more works related to risk perception here to round it off.

3. METHODOLOGY

The survey consisted of questions regarding concerns with respect to a factious wearable device called the Cubetastic3000 (done to prevent biases in answers from participants with respect to specific artifacts or companies), smartphone concerns, risk and benefit assessment of technologies, and exit questions. Details on the question ordering, question formatting, and sample questions are below. The full survey can be found at http://www.surveygizmo.com/s3/1657924/Wearables-Threats-User-Survey.

In total, the survey consisted of 367 unique questions, with each participant answering 27 questions. Out of the 27 seen by each participant, 17 of the questions were constant, whereas 10 of the questions were selected at random from larger sets of questions. During the course of the survey, each participant answered:

- 2 comprehension questions
- 6/304 questions about various wearables scenarios
- 2/5 questions about smartphone scenarios
- 1/20 benefit questions
- 1/20 risk questions (same technology)
- 4 demographics
- 1 open-ended question
- 10 questions of IUIPC

To mitigate any biases, the order in which question groups appeared to the user was randomized. Specifically, a participant had an equal chance of seeing questions related to the Cubetastic3000 or questions related to risk and benefit assessment. When a participant saw the risk and benefit assessment questions, risk or benefit questions were equally likely to be shown first. Whenever applicable, questions were randomly selected. For risk and benefit assessment, a technology was randomly selected for each participant, then risk and benefit questions for the same technology were selected for the participant.

3.1 Comprehension Questions

Because we were asking questions about a fictitious device, participants were presented with two comprehension questions before the start of the wearable device scenarios questions. These questions served to ensure that participants would be informed of the device which we were going to be referring to, but also served as a filter for people who were inattentive or chose not to answer questions correctly. Filtering incomplete and incorrect responses to either of these comprehension questions filtered out 16% (n = 366) of our participants, which were 79% of all incomplete or bad responses (n = 465).

3.2 Wearables Scenarios

After participants had answered the two comprehension questions, participants were presented with 6 randomly selected questions from a set of 304 questions on various scenarios

which can occur when wearing the Cubetastic3000 fictitious wearable device. Out of these 304 questions, 292 (73 data * 4 recipients) were questions of the format: *"How would you feel if an app on your Cubetastic3000 learned <data> and shared it with <recipient>, without asking you first?"*. Additionally, there were 13 questions which did not follow the above format, lacking data to be shared and/or a recipient of any data. Of these questions, 5 questions were to calibrate with Felt's study on smartphones and the other 7 were exploratory questions. An example of a regular question, a calibration question, and exploratory question, respectively, are below:

How would you feel if an app on your Cubetastic3000 learned how you were feeling based on your heart rate and shared that with the public, without asking you first?

How would you feel if an app on your Cubetastic3000 connected to a Bluetooth device (like a headset) without asking you first?

How would you feel if an app on your Cubetastic3000 turned your device off, without asking you first?

The main purposes of these questions were to, firstly, determine how much the device, data type, and data recipient played a role in determining if a person was upset by an event or not and, secondly, to investigate what information would most upset users when shared and which recipient of the shared data would most upset users. The calibration questions were modeled after Felt's mobile user study, where we ask the same questions but with respect to wearables rather than smart phones, to see if a change in device changes users' risk perception. The remaining exploratory questions were additional scenarios which did not fit the standard question format but were relevant to ask our participants.

3.3 Smartphone Scenarios

Following the wearables scenario questions were 2 randomly selected questions from a set of 5 questions on various scenarios which can occur when using a smartphone. These five scenarios, ranging from the most upsetting scenario to the least upsetting scenario, were purposefully selected from Felt's mobile user study for eliciting varying reactions from users. These questions were the basis for the five calibration wearables scenarios from the above section. Because we asked users questions differing only by the device in question, we are able to see how the change in device changes users' risk perception. Additionally, we compare our participants' perceptions of wearable device scenarios with existing perceptions of mobile device scenarios.

3.4 Risk and Benefit Assessment

In addition to investigating personal reactions to particular scenarios, we also wanted to study broad perceptions of various new technologies. Each participant saw 1 risk assessment question and 1 benefit assessment question regarding the same four previously studied technologies from the the seminal risk perception study by Fischhoff (handguns, motorcycles, lawnmowers, electricity), and 1 of the 20 new technologies. Participants were asked to rate the same randomized new technology for both risk and benefit assessment. The format of the questions were as follows:

Fill in your risk (benefit) numbers for the following technologies:

Handguns: _____
Motorcycles: _____
Lawnmowers: _____
<Randomized>: _____
Electricity: _____

To parallel the risk perception study, we gave our participants a similar prompt which instructed the participants to numerically express the conceived gross risk (gross benefit) for a long period of time for all parties involved. The prompt can be seen at appendix A. Specifically, we asked participants to evaluate the of following 20 new technologies: 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.

3.5 Additional Questions

The exit portion of the survey consisted of demographics questions to better understand the answers. We included standard demographics questions such as age, gender, and education status, but also asked participants if they owned a wearable device to survey the population's exposure to these devices, prompted them with an open-ended question on what would be the most likely risks associated with wearable devices, and finished with questions from a privacy index to gauge their privacy preferences. We used the Internet Users' Information Privacy Concerns (IUIPC) index [**?**], rather than the Westin Index, which was found to be very coarse [**?**].

3.6 Focus Group

We conducted a one-hour focus group to validate our design, gauge survey comprehension, and measure user fatigue. The focus group began with participants taking the survey. Afterward, the participants were asked to give feedback on the format and the content of the survey, noting any instructions or questions which were unclear and stating any suggestions for the content of the survey. The focus group concluded with a discussion of possible benefits and risks of wearable devices, to brainstorm any additional scenarios which may occur. Afterward, participants were debriefed and given $30 in cash. Of the 13 participants 54% female, 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.

3.7 Recruitment

We recruited 2,250 participants August 7th-13th 2014 via Amazon's Mechanical Turk. We restricted participants to those over 18 years old. No other restrictions on participation were applied. We asked questions regarding participants' perceptions of various situations which might occur when wearing a wearable device, and about the risks and benefits of new technologies.

4. RESULTS

After removing 465 incomplete responses, our sample consisted of 1,785 participants. Of these X, A% were male, with a median age of B. Two researchers independently coded 1,785 open-ended responses, discussed any disagreements, and resolved them so that the final codings reflect unanimous agreement.

Generally, any photos, videos, audio recordings, or financial information is considered to be highly sensitive, whereas publicly deductible traits, such as the language being spoken, gender, and age, is considered the least sensitive. Additionally, data shared in any way, whether the recipient be friends, work contacts, or the public, is much more upsetting than the data is only shared with an app's server; there is no statistically significant difference between how upset a person would be if data was shared between the various recipients. Interestingly, people had another set of prioritized concerns when data was perceived to be shared with an app rather than a human recipient (for instance, people were okay with people knowing if they were busy or not, but not their device). Although whether the device in the scenario being a wearable or smart phone did elicit unique reactions of the situation from participants, no statistically significant conclusion can be made about whether one device was seen as more threatening than another device.

Participants assessed many of the new technologies similarly as low risk and low benefit, which we suspect is due to the fact that most are not consciously aware of the way these technologies are being used. Through our open-ended question, we find that the number one self-reported concern when owning and interacting with wearable devices is the loss of privacy.

4.1 Data Type

To determine the most concerning and least concerning data types, we consider the very upset rate (VUR) of various scenarios. To calculate these rates, we take the rate of responses where participants had indicated that they would be "very upset" (the maximum rating) with respect to the total number of responses for the question. Since people considered different things more or less sensitive with respect to the data recipient, we present the most and least concerning shared data along with the most and least concerning "not shared" data:

For shared data (friends, work, public)

1. social security number (98.04%)
2. a video of you unclothed (97.44%)
3. bank account information (97.10%)
4. recordings of your work conversations (96.97%)
5. a photo of you that is incriminating/embarrassing (96.36%)
6. a photo of you unclothed (96.30%)
7. credit card information (95.92%)
8. username and password for websites (95.41%)
9. a video of you entering in your PIN (93.91%)
10. recordings of your phone conversations (93.88%)

64. your name (47.25%)
65. when and how much you exercise (46.07%)
66. when you were happy or having fun (38.10%)
67. what television shows you watch (35.96%)
68. when you are busy or interruptible (34.34%)
69. your heart rate (32.28%)
70. music from your device (31.87%)
71. your age (29.67%)
72. the language you speak (20.95%)
73. your gender (16.81%)

For not shared data (appserver only)

1. bank account information (90.91%)
2. a video of you unclothed (90.62%)
3. social security number (88.68%)
4. video of you entering your PIN (88.57%)
5. a photo of you that is incriminating/embarrassing (78.05%)
6. a photo of you unclothed (77.78%)
7. a video of you entering a passcode to a door (75.00%)
8. when and how much you have sex (73.08%)
9. a video of you that is incriminating/embarrassing (71.88%)
10. a photo of you at home taken randomly by an inward-facing camera (66.67%)

64. when and how much you exercise (16.67%)
65. how much you use your phone (15.79%)
66. your age (14.29%)
67. how much you like the people you interact with (13.79%)
68. when, what, and how much you ate (12.50%)
69. which television shows you watch (11.43%)
70. your gender (9.52%)
71. your heart rate (9.09%)
72. eye movement patterns (for eye tracking) (6.98%)
73. the language you speak (2.50%)

Commonly, bank info, SSN, PIN, embarrassing photo, naked photo, naked video were considered to be highly sensitive. When people perceived that the data would be shared with the app only, the other top five concerns included the passcode to a door, how frequently one has sex, embarrassing videos, and photos at home. When people perceived that the data would be shared with a human audience, their other top concerns were work conversations, credit card information, username and password combinations for websites, and phone conversations. When data is perceived to be shared by an app, people are more concerned with issues of being spied on or tracked, whereas when data is perceived to be shared with an individual, people are concerned more with theft or reputation.

On the other hand, exercise details, age, tv shows, gender, heart rate, and language were commonly considered to be lease concerning. When people perceived that the data would be shared with the app only, the other indifferent data included phone use, how much one liked the people around, when and what you ate, and eye patterns. When people perceived that the data would be shared with a human audience, the least concerning data included one's name, if one was having fun, music on the device, and if one was busy or interruptible. When sharing with an application, information otherwise considered personal such as phone use, opinions of people, food eaten, or eye patterns were okay to share, since these seem like useful information to improve one's device experience. However, people are not likely to share the same with people, but are more comfortable with

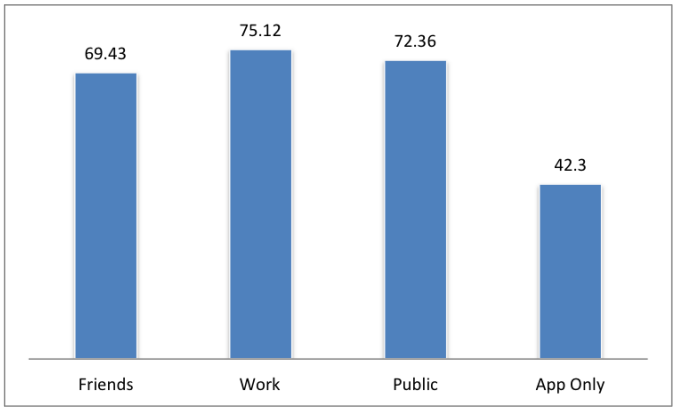

Figure 1: (This is a placeholder! TODO: generate a better plot for data recipient)

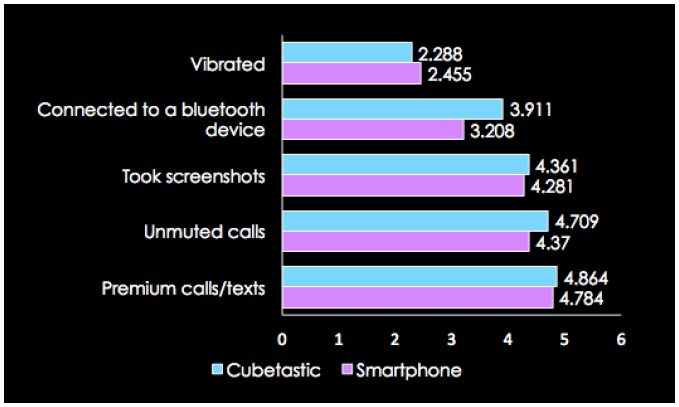

Figure 2: (This is a placeholder! TODO: generate a better version of this)

sharing data about topics which would come up in causal conversation.

SAY THIS: full on stats test on all 74 data types seems unreasonable. Look at the regression model below.

4.2 Data Recipient

People are upset when their data is shared without their permission, regardless of who the recipient is. Generally, there isn't a statistically significant difference between how upset people would be if data were to be shared with friends, work, and public, although when considering each scenario, there are certain scenarios which are considered to be more sensitive with one recipient than another.

Out of all the recipients, friends are considered to be the least upsetting audience, but not too significantly (do statsy thing here). There might have been a perception of sharing which resulted in sharing with the public being less upsetting than sharing with work contacts–people assumed that sharing it with work was a push and sharing it to the public would require people to pull the available information which was shared.

SAY THIS: we performed an exploratory analysis to examine the effect of data recipient using a chi square test; in order to do this, the assumption about independence of observations was violated.However, we do not believe that this impacted the outcome of the statistical test based on the randomization of treatments across all conditions, as well as the very large sample size. To examine whether the violation of this assumption impacted our results, we further created a mixed effects model, in order to isolate the subjects variable (i.e., to examine the extent to which random effects stemming from individual differences may be responsible for the effects that we observed) !!!report effect sizes

4.3 Device Type

(REDO) So, there is a difference between the device types, but I need to do more work to see if this is statistically significant or not. In either case, this matters the least, and device type and data recipient are more influencing factors. This is just the result of biases in people we can't quite quantify.

(cubetastic upset rate | smartphone upset rate)
Q1: (14.81% | 6.13%)
Q2: (44.11% | 19.85%)
Q3: (87.09% | 58.44%)
Q4: (52.77% | 55.79%)
Q5: (86.49% | 91.82%)

Exact question details here, and statistical stuff. Conclude with whatever conclusion I happen to come to after performing the statistical analysis.

4.4 Correlation with Demographics

We found that the very upset rate for participants was not correlated with (pick correct ones from IUIPC, age, gender, education, wearable ownership) (give correlation coefficients), positively correlated with (IUIPC, age, gender, education, wearable ownership) (give correlation coefficients), and negatively correlated with (IUIPC, age, gender, education, wearable ownership) (give correlation coefficients).

Because wearable devices have been adopted by a younger, rich, technology-savvy demographic [**?**], it is natural to see that younger or more educated participants have had a more favorable view of wearable devices. This may be due to cultural exposure through marketing or friends, or an attitude of openness to new technologies. Participants who had a higher IUIPC score, which infers a higher sensitivity to privacy, were more likely to be upset at the various scenarios which may occur when wearing a wearable device. Additionally, these people were more likely to be adverse to these technologies for the sake of preserving privacy, whether they had explicit concerns or a vague feeling of uneasiness. There was no correlation between a person's gender and their views of wearable devices, reaffirming that wearable devices are equally exposed to both genders.

4.5 Risk and Benefit Ranks

When assessing new technologies, participants generally had rated the technologies similarly, considering them low risk and low benefit (see figure 3). We suspect that these similar assessments are because most are not consciously aware of

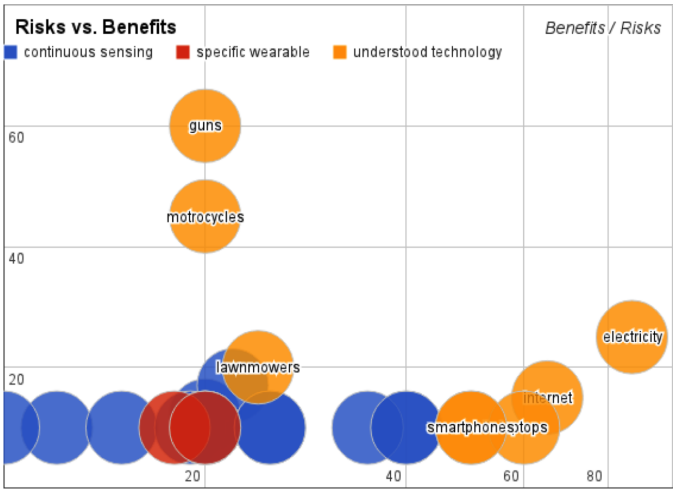

Figure 3: (This is a placeholder! TODO: generate a better plot; take out the specific wearables too.)

the possibilities of these technologies or how they are being used today. A list of the ranking of most risky and most beneficial technologies can be see in appendix B; the most risky and most beneficial technologies reveals the list of most familiar technologies for the average user (internet, laptops, email, smartphones, etc.).

Notably, technologies perceived to be beneficial include location tracking and heart rate detection. Again, this is probably do to the exposure people have to these technologies–most people use GPS or other location-based applications on their smart phones and fitness trackers are the most popular type of wearable device. Technologies considered to be risky, such as a discrete camera and facial detection, seemed to be based on media exposure or general aversion to privacy invasion. However, people are becoming increasingly aware of such risks and are comparing these risks of privacy invasion 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 physical lawnmower. As a takeaway, these assessments of the most risky or beneficial technologies may not be the most accurate, but do reflect the exposure of various technologies to the general public and also prove that people do perceive risks in a real way related to these technologies.

4.6 Perceived Concerns for Wearable Devices

Near the end of the survey, we asked the participants an open-ended question regarding the most likely risks associated with owning and interacting with wearable devices. Without any doubt, the answers reaffirm that the most common concern for owning and interacting with wearable devices for the average user is the *possible loss of privacy*:

Privacy 464 (25.99%)
Security 94 (5.27%)
Hacking 38 (2.13%)
Spying 50 (2.80%)

Unaware Use 167 (9.36%)
Accidental Sharing 66 (3.70%)
Unaware Collection 64 (3.59%)
Unaware Access 44 (2.46%)
False Information 33 (1.85%)

Health Risk 252 (14.12%)
Safety 147 (8.24%)
Financial Cost 201 (11.26%)

Social Impact 135 (7.56%)
Social Stigma 39 (2.18%)
Aesthetics 19 (1.06%)

Miscellaneous 76 (4.26%)
None 51 (2.86%)
Don't know 30 (1.68%)
Don't care 6 (0.34%)

Other significant secondary concerns included information compromise (Security), financial cost of buying, replacing, or caring for the device (Financial), long-term health effects caused from wearing the device (Health), safety hazards from wearing the device, such as battery burns or distractions causing car accidents (Safety), and changes in social behaviors, such as dependencies on devices or spending less time with loved ones (Social Impact). Refer people to the appendix C for detailed information on coding labels.

5. DISCUSSION

We take this section to discuss complementary future research directions in fields of privacy, ubiquitous computing, and user studies, along with specific limitations of this survey.

5.1 A Regression Model

(REDO) Talk about the REGRESSION MODEL here. Say that the data type was x% responsible, the data recepient y% responsible, and the device type z% responsible for how upset people seemed to be when they answered the questions.

5.2 Future Research Directions

(REDO, ask David's/Serge's input for this section) Additional future work is encouraged in the area of studying privacy with respect to ubiquitous computing, since we proved it was the number one concern of the users of wearable devices. Clearly, this is a hard question which has been worked on for a long time but not yet fully addressed. Even this survey just barely touched on the various factors which can influence privacy perceptions and how upset people would be.

Also, maybe some work with respect to security threats, and how feasible they might be, and some defenses against stopping wearables devices from getting sensitive information (like blocking text, detecting sensitive situations like the bathroom, etc.). Research which defends against false information, false positive commands, and just more safeguards against the new system for wearables, whatever that is, is also something to really look into.

Work making sure that people are aware of what is going on, using indicators, not-too-transparent interfaces, and maybe being polite (recording rules follow social rules–think polite glass talk from Jaeyeon at MSR) are going to be valuable

as wearables get more sophisticated but also more adopted by people. Think about it–put people in control of the technology, not technology shifting the social norms (our survey says that one of the top concerns of people were about how wearables will change social norms).

5.3 Limitations

One of the main limitations of this work is that our participants might not have interest, or an accurate idea, of wearable devices and their capabilities. 83% of our participants reported that they do not own a wearable device, but at this time, about 15% of the general population own and use wearable devices [**?**][**?**], so our study is reflective of the status quo. We believed that getting a representative survey base was a useful endeavor, although we could have easily recruited only wearable device owners or people specifically interested in wearables. However, that will also have its own bias and limitations as well, since they would not reflect the general population. We expect user perceptions to change as rapidly as wearable technologies and the rate of adoption change.

Crowdourcing user studies in Mechanical Turk has its challenges [**?**]. While the Amazon Mechanical Turk population is diverse across several significant demographic dimensions such as age, gender, and income, it is not a precise representation of the U.S. population [**?**][**?**]. Additionally, Amazon Mechanical Turk workers generally put a higher value on anonymity and hiding information, were more likely to do so, had more privacy concerns than the larger U.S. public [**?**].

The survey was constructed in a way to randomize the order of the particular sets of questions participants saw, except for the open-ended question, which was always near the end of the survey, asked along with the demographics. For this reason, people were heavily primed for the open-ended question. However, this question was always shown before the IUIPC questions, so our results on privacy being the top concern isn't because of the bias from the privacy index. The intent of the open-ended question was more to get a sense of what people were concerned of, and we believe the results do reflect their actual concerns, but with a bit more clarity, since the participants were already thinking about such risks related to wearables.

(REDO, Should I even say this?) I messed up that motorcycle question. I wish I actually had a calibration point for high risk high benefit for the Fischoff technology assessment questions. But well, none of the new technologies fit that description so we didn't really need it critically.

6. CONCLUSION

(REDO) END STRONG! Should I put this before the Discussion? Echo the introduction a little, remind the people of the takeaways in a way that highlights the contribution of this paper. Intro: "we studied user perceptions for threats in wearable devices, along with user perceptions of risk and benefit for emerging technologies and what they thought was the biggest risk for using wearable devices. Data type, data recipient, and device type all matter different amounts. All new technologies were perceived to be low risk low benefit but we think this is because people are unfamiliar with these technologies. Privacy was the number one concern, followed by security, then health, money, social norms changing and social stigma. Fantastic ending sentence here."

I can talk about the results a little bit more in depth because people have already supposedly read my whole paper now. Pull out the subtleties I couldn't have done in the introduction, and go into specific details, shooting out numbers and statistics. Then conclude the whole thing with an inspirational pitch on how there is much future work to be done in this area, how this area is exciting, and how I basically helped people see both of these things.

7. ACKNOWLEDGMENTS

NSF funding, SCRUB, BLUES. Also any people who helped.

APPENDIX

A. FISCHOFF PROMPTS

BENEFIT prompt:

"We would like to ask you to rate the benefits associated with each of the following technologies.

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 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 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)"

RISK prompt:

"We would like to ask you to rate the risks associated with each of the following technologies.

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 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 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.)"

B. RISK AND BENEFIT RANKINGS

BENEFIT:

technology median 25% 75%
electricity 87 50 100
internet 65 45 100
laptops 60 40 80
email 50 30 75
smartphones 50 32.5 75
location tracking 40 20 67.5
heart rate detection 40 28 62.5
language detection 35 15 60
voice recognition 25 15 40
speech to text 25 15 36.25
lawnmowers 24 15 40
facial recognition 22 13 40
guns 20 10 30
motrocycles 20 12 40
voice based emotion detection 20 10 30
facial detection 20 10 32
discrete camera 20 15 30
smartwatches 20 10 32.5
google glass 20 12 40
fitness trackers 19 10 30
cubetastic 18 10 30
discrete microphone 15 10 20
age detection 12 10 21
gender detection 10 10 15

RISK:

technology median 25% 75%
guns 60 40 80
motrocycles 45 27 70
electricity 25 15 40
lawnmowers 20 12 30
facial recognition 17 12.5 30
internet 15 10 30
discrete camera 12 10 30
location tracking 10 10 20
age detection 10 10 15
gender detection 10 10 12
language detection 10 10 10
voice based emotion detection 10 10 15
facial detection 10 10 25
voice recognition 10 10 15
heart rate detection 10 10 10
email 10 10 16
speech to text 10 10 10
discrete microphone 10 10 20
smartphones 10 10 19
laptops 10 10 15
fitness trackers 10 10 10
smartwatches 10 10 10
google glass 10 10 20
cubetastic 10 10 30

C. 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