

# 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. Wearables 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 occurred 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 wearables 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 bottom-most 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 a 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 Fischhoff 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. SURVEY

The survey design process consisted of synthesizing a relevant and comprehensive set of questions, validating the relevance, clarity, and completeness of the questions, and concluded with finalizing distribution logistics. Details on the synthesis, validation, methodology, and data are below.

### 3.1 Asking the Right Questions

We asked participants how they would feel if a device shared a particular piece of data with a target recipient. We purposefully asked specific questions limited to the participant, as these situations are easier to judge. The purpose of the bank of 300 questions was not necessarily to get an absolute ranking of what upsets people and what does not, since the list isn't comprehensive of all possible threats (although top 10 and bottom 10 concerns can be seen in section <linkhere>). The real purpose behind asking an array of questions was to determine how much the device, data type, and data recipient played a role in determining if a person was upset by an event, while also exploring the new threat landscape for wearable devices.

To synthesize the questions, we surveyed popular wearable devices' sensors, studied existing smartphone and wearables literature, and looked at vision videos for wearable devices. In the end, we especially chose to investigate questions which focused on continuous audio recording, discrete image capture, continuous video capture, and biometrics, due to the prevalence of devices which take voice inputs as commands [?], concern for image capture [?], and popularity of fitness tracking [?]. Exploratory questions, including but not limited to threats regarding information security, pattern recognition, and emotion detection are also studied.

Questions which addressed situations applicable for both smart phone and wearables were deemphasized because these situations had been investigated. However, we did include these questions, primarily to calibrate our results for the other scenarios. We used a seven-point likert scale and used similar wording as Felt in her smartphone study [?] so that we could determine both how changing the device in question caused a change in threat perception and how threatening new wearables threats were with respect to existing threats.

### 3.2 Looking at the Bigger Picture

To complement our bank of targeted questions, we also asked participants to assess the comprehensive risks and benefits of a particular technology, over a long period of time, for all parties affected by the technology. The purpose of these questions were not necessarily to get an absolute ranking of technologies by risk or benefit, as perceptions may change (although you can see the rankings in appendix <linkhere>). However, the purpose of these questions was to gain insight into how participants perceived new technologies.

We used a prompt similar to a seminal study in risk perception [?] and also asked our participants to rate some of the technologies in the study. We used technologies such as lawnmowers (considered to be low risk and low benefit) and electricity (considered to be low risk and high benefit) as comparison points for other technologies we ask our participants to assess. As a result, we have a mapping of risks and benefits of new technologies with respect to the well-studied technologies.

### 3.3 Validation

We conducted a focus group to validate our survey scope. 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. This time was used to discuss benefits and risks associated with wearables, talk through common concerns, and brainstorm additional scenarios for the survey. The focus group was also used to gauge survey comprehension, user fatigue, and other logistics.

### 3.4 Methodology

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. QUESTIONS

The survey consisted of questions regarding concerns with respect to a fictitious wearable device called the Cubetastic3000 (this was done to prevent any biases in answers from participants with respect to specific 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>.

### 4.1 Format

(REDO) In total, the survey consisted of 367 unique questions, with each participant answering 27 questions. Out of the 27 seen by the participant, 10 of the questions are randomly selected from a particular set of questions (see below).

- 2 comprehension questions
- 6/305 questions about various 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, we randomized the order in which users saw groups of questions. That is; the participant has an equal chance of seeing questions related to threat perceptions or questions related to risk and benefit assessment of technologies. Additionally, each question in the sections

about various scenarios, questions about smartphone scenarios, and IUIPC questions were randomly selected. A participant was also equally likely to see the risk or benefit questions first when they got to the section pertaining to risk and benefit assessment of technologies.

#### 4.1.1 Threat Perceptions

(REDO) Before they get to the wearable device question, they must answer these two questions about the Cubetastic3000. people who did not answer these two comprehension questions were filtered out (this was about 4% of our participants). These questions both filtered out people who were not paying attention, people who were rushing through it for money, etc.

*Where and when would you wear the Cubetastic3000?*

*What can the Cubetastic3000 do?*

The purpose of the 6/305 questions were to 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. These are word for word modeled after the mobile user study. You can see that in the first example question, these three controls are highlighted. Other questions were used for calibration with the smartphone study, where we literally ask the same questions as the study, but toggling the device type, to see if this plays a role in risk perception.

*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 smartphone connected to a Bluetooth device (like a headset) without asking you first?*

Concluding blurb here about how we were actually able to tease those dimensions out and have a regression model in section <later section which doesn't exist yet>.

#### 4.1.2 Technology Perceptions

(REDO) The next set of questions are with respect to the Fischhoff study on users' perception of benefit and risk. We wanted to study personal but also broad perceptions of wearable risks. We prompted the users with the same prompt that the participants in the Fischhoff study was presented with, giving instructions to consider gross risk and gross benefits for a long period of time for all people, with specific instructions to numerical rankings. We did this so that we can calibrate the new technologies that we ask about with the existing seminal study. Prompt can be seen at appendix A.

After that prompt, users were given this question and asked to fill in the numbers according to the previous prompt's instructions. Each person got the same four calibration questions (handguns, motorcycles, lawnmowers, electricity), and 1/20 randomized new technology. People rated the same randomized new technology for both benefit and risk.

*Fill in your benefit numbers for the following technologies:  
Fill in your risk numbers for the following technologies:*

*Handguns:* \_\_\_\_\_  
*Motorcycles:* \_\_\_\_\_  
*Lawnmowers:* \_\_\_\_\_  
*<New Tech Here>:* \_\_\_\_\_  
*Electricity:* \_\_\_\_\_

The list of technologies included: 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.

Note that some of these technologies were general technologies (internet), other were devices (smartphones), but most of them were new capabilities (facial detection). We were more interested in the capabilities, but found those other points to be useful for understanding where the risk/benefit of those capabilities stand respectively.

#### 4.1.3 User Concerns

(REDO) Lastly, after investigating user perceptions of personal threats, general perceptions of risks and benefits, we thought we could just ask the users what they thought were the most likely risks.

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

Take this with a grain of salt since users are not the most accurate at determining which is the most likely, but we can really see what users care about. The participants had as much space as they wanted to write their reply. People were primed for this question because we asked it after the other two sets of questions, but this just means that people have been thinking about it for a while. We were not looking for hard results, but more of inspiration to direct future work and to just check if we were also asking the right questions which captured the people's concerns throughout the survey.

#### 4.1.4 Additional Questions

(REDO) During the exit portion of the survey, we asked for demographics (gender, age, education) along with if the person owns a wearable or not. We thought that would be important to know. Also, we imagined that privacy would be correlated to these results, which is why we made everyone take the IUPIC to see how much they cared about privacy. Explain why I used IUPIC instead of the Westin, just one or two sentences will do (cite the IUPIC paper, and the SOUPS paper on how the Westin is not so accurate).

## 5. RESULTS

After removing X incomplete responses, our sample consisted of Y 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.

### 5.1 Factors in Upsetting Users

We found that the data type and data recipient, respectively, are the most significant predictors of how upsetting or threatening a situation is perceived by a user. On the other hand, the device type does not significantly impact how users perceive a situation.

#### 5.1.1 Data Type

(REDO) Okay, I list all of the top 10/bottom 10 lists I generated: the one for all recipients, one only with respect to friends, work, and public, and another for the app only. I think the interesting thing to do is to show the shared vs app only lists, and to highlight what is different. If I could show the whole list of 70+ for both, that would be most insightful, but I don't have the place for it in this paper, so this will have to do. Maybe I can do a top/bottom 15 at the least, maybe that will be better?

For all recipients

1. a video of you unclothed
2. bank account information
3. social security number
4. video of you entering in your PIN
5. a photo of you unclothed
6. a photo of you that is incriminating or embarrassing
7. username and password for websites
8. credit card information
9. a video of you that is incriminating or embarrassing
10. a photo you at home taken randomly by an inward-facing camera
64. eye movement patterns (for eye tracking)
65. when and how much you exercise
66. when you are happy or having fun
67. which television shows you watch
68. when you are busy or interruptible
69. music from your device
70. your heart rate
71. your age
72. the language you speak
73. your gender

For shared only

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 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/embarassing (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/embarassing (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%)

Results were that in the top 10, both app only and shared had: bank info, SSN, PIN, embarassing photo, naked photo, naked video. Write a sentence on why I think that is here. The differences were that the app had: door pw, sex freq, embarassing videos, and photos at home, while the shared had the differing top 5 to be work conversations, credit card, username and password, and phone conversations. It's cool to see that it's like one is talking to a machine or a company and the other to a person, right?

In the low 10, the common 6 were exercise details, age, tv shows, gender, heart rate, and language. For the 4 different low 10, the app only had: phone use, how much you like people, when and what you ate, and eye patterns for tracking. For shared, these 4 were name, having fun or happy, music, and if a person was busy or interruptible. Also, this is interesting. People don't want to share phone use, opinions on people, food habits, or eye patterns, but would find it useful to have for apps, and well, people don't care about observable things or happy/music with people. But maybe not apps since it seems creepy or will give them ads.

### 5.1.2 Data Recipient

(REDO) Data recipient matters in how upset people get, or well, how much their privacy is invaded and even how secure their information is. What really matters is if it is shared to people or not. There isn't much difference between the friends, work, and public—they are all quite upsetting. Friends is a little lower, but not too significantly (do statsy thing here). The difference between public being lower than work is probably due to the fact that 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. Basically, what matters is that there are

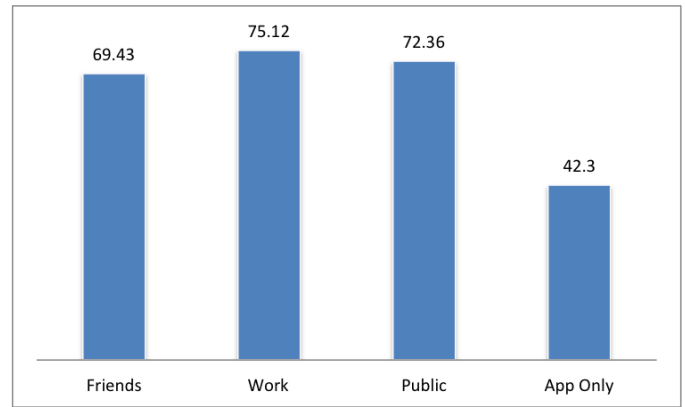


Figure 1: (This is a placeholder! TODO: generate a better plot for data recipient)

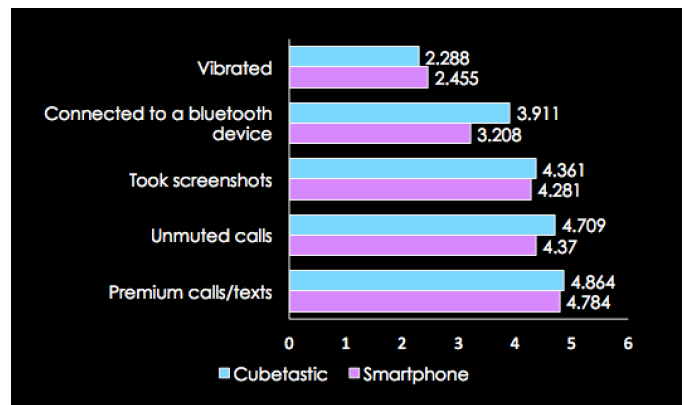


Figure 2: (This is a placeholder! TODO: generate a better version of this)

guarantees that the information is bounded and used in a way that people would assume it would be used.

### 5.1.3 Device Type

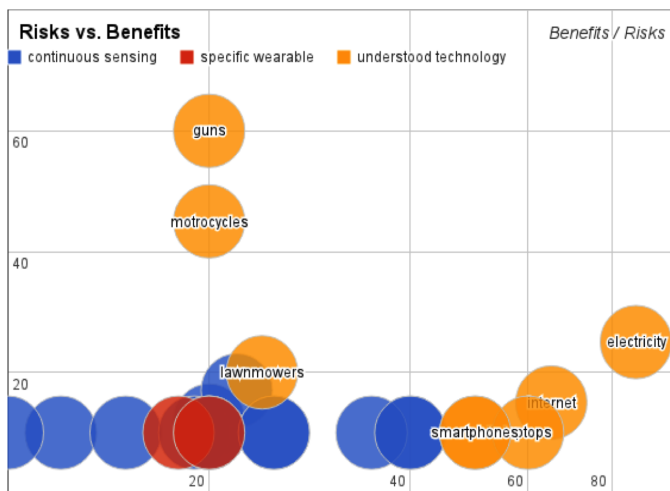
(REDO) So, there is a difference between the device types, but I need to do more work to see if this is statistically significant or not. In either case, this matters the least, and device type and data recipient are more influencing factors. This is just the result of biases in people we can't quite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

with upset rates (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.

### 5.1.4 What Matters in Upsetting People



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

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

Also go into any correlations that I found with respect to demographics and the IUIPC index (I should do all of these things ASAP as soon as this paper is in good shape). There should be some interesting stuff there, whether there are specific correlations, or whether there is not. Both are good things to report and should be put here.

## 5.2 A Bigger Picture

We asked users to rate how beneficial or risky a technology was, for all parties affected by the technology (including manufacturers, consumers, and bystanders), over a long period of time, with respect to other, well studied technologies. This gives us an interesting insight into how people perceive these new technologies. For instance, the capacity for facial detection on a wearable device is perceived to be as risky as interacting with a physical lawnmower.

### 5.2.1 Risk and Benefit Ranks

(REDO) Talk through the graph shown above. The basic takeaway is that all of the new technologies and capabilities are perceived to be low risk low benefit. We can see that for technologies that people are more familiar with, people rate it more beneficial and more risky (or is it because they are more relevant that they are more familiar to them? Can I make such a claim?). Interesting to note facial recognition versus detection, location tracking, and discrete camera. Refer to appendix B for the details (if I have space to include such a thing as the absolute benefit and risk ranking and quartiles in this paper..).

### 5.2.2 Lawnmower Ratios

(REDO) The basic idea for this is that I am going to compare all of the newly assessed technologies with respect to the well-studied technology generally considered to be low-risk and low-benefit, since all new technologies fit this mold. This

can give a more accurate idea into how each person thought something was risky or not (twice as risky as the closest tech they know, or about equal, etc.). Do some fancy graphing stuff here. Maybe another scatter plot, or an overlay of various distributions of ratio of perceived lawnmower risk to technology risk. Hmm.

## 5.3 Perceived Concerns for Wearable Devices

(REDO) Although we asked users about particular situations which might occur with a wearable device and asked them to assess technologies in a general sense, our open ended question asked the users to state the most likely risk(s) associated with owning and interacting with wearable devices. Without any doubt, the most common concern for owning and interacting with wearable devices for the every day user is the *loss of privacy*.

(I should probably make a table of the following. Ugh, but for now:)

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%)

Talk about the coding labels and what they mean, in a very vague and compact way. Refer people to the appendix C for what the coding means in detail.

Takeaway is that people care about privacy, then security, health, social impact. Other interesting things to note are aesthetics, social stigma, and false information, which could be cool things to look into.

## 6. 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.

### 6.1 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).

## 6.2 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.

Crowdsourcing 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 motor-cycle question. I wish I actually had a calibration point for high risk high benefit for the Fischhoff technology assessment questions. But well, none of the new technologies fit that description so we didn't really need it critically.

## 7. 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.

## 8. 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  
 motorcycles 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  
 motorcycles 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