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

Linda N. Lee
UC Berkeley
lnl@berkeley.edu

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

David Wagner
UC Berkeley
daw@cs.berkeley.edu

ABSTRACT
Hello world.

Categories and Subject Descriptors
look it up [**keyword1**]: keyword2keyword3

General Terms
term1 term2 term3

Keywords
Privacy, User Studies, Ubiquitous Computing,Internet of Things

1. INTRODUCTION
Basically a longer version of the abstract, plus some additional motivational things thrown in here.

2014 is year of wearables [1]. 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 (61%), followed by smart watches (45%) and mHealth (mobile health) devices (17%). It is estimated that 15% use it in daily life [2][3].

End this section with an explicit list of contributions made by this paper.

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 Privacy for Smartphones and Wearables
Mention Adrienne's work here, and other cool smartphone studies of any sort. 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 other privacy studies for wearables (like the ones you can find at Ubicomp, CHI, or SOUPS), and give them a nod. Also highlight how my study is different from previous studies.

2.2 Ubiquitous Computing
2.3 User Perception
Mention how people are generally really bad at estimating the likelihood of some threat or event occurring. And since

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 Threat Landscape Investigation
(REDO) To generate the list of possible scenarios which can happen with a wearable device, we did three things. Firstly, we looked at the most popular list of wearable technologies (including the Fitbit fitness tracker, Pebble smartwatch, and Glass wearable computing device) and their sensors and capabilities. Secondly, we looked at past research in mobile devices, vision videos for wearables, and the news for possible concerns.

Write about how I came up with the questions, what was considered (looking at many wearable devices and possible sensors, looking through previous works, just thinking of as many as possible), and the final list.

Talking about the focus group here. Does this even need to happen?

3.2 Calibrating with Existing Works
(REDO) We used the same format as Adrienne's paper so that we can compare our results to the ones that she got in her study for mobile devices. Mobile devices threats are well studied and the closest well-researched thing to wearable device threats.

We used a prompt similar to Fischoff's study so that we could compare our results to the ones that he got in his study, and to put more of the new technologies onto the risk/benefit map. This way, we can have a sense of the risk and benefit with respect to well-studied and more familiar technologies.

3.3 Validation

(REDO) We conducted a focus group to look over the list, brainstorm more scenarios, and clarify any scenarios which were unclear (we also used this time to time the survey and make sure the formatting was clear.

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 applier. 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 factious 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 <LINK HERE>.

4.1 Format

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. (Ugh this is bad, re-write later)

4.1.1 Threat Perceptions

Format of question explanation, list the edge case questions here. Show an example of the question.

4.1.2 Technology Perceptions

Format of the question explanation, list the technologies here (is this too many?). Show an example of the question.

4.1.3 User Concerns

This is an open-ended question. Show the question here. Say that the participants had as much space as they wanted, although they were shown a line.

4.1.4 Additional Questions

demographics and IUIPC, explain why I used IUIPC instead of the Westin, just one or two sentences will do.

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

blah blah here.

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%)

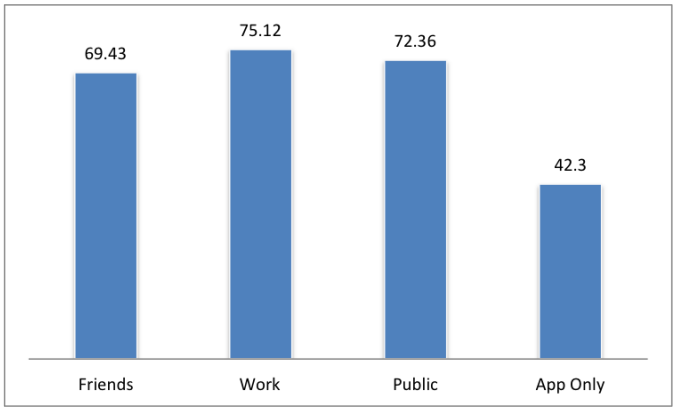

Figure 1: (This is a placeholder! TODO: generate a better plot for data recipient)

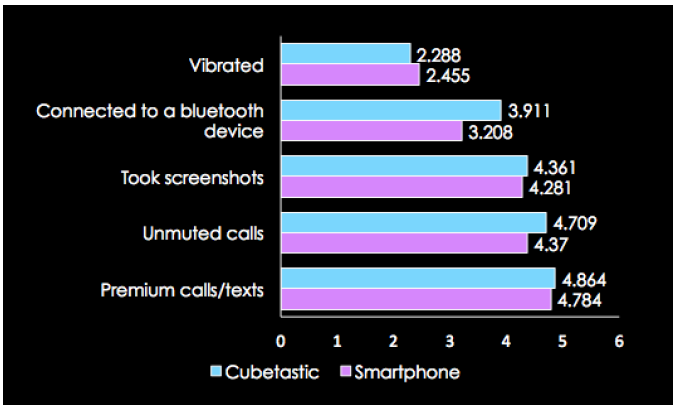

Figure 2: (This is a placeholder! TODO: generate a better version of this)

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/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%)

More text.

5.1.2 Data Recipient

5.1.3 Device Type

5.2 A Bigger Picture

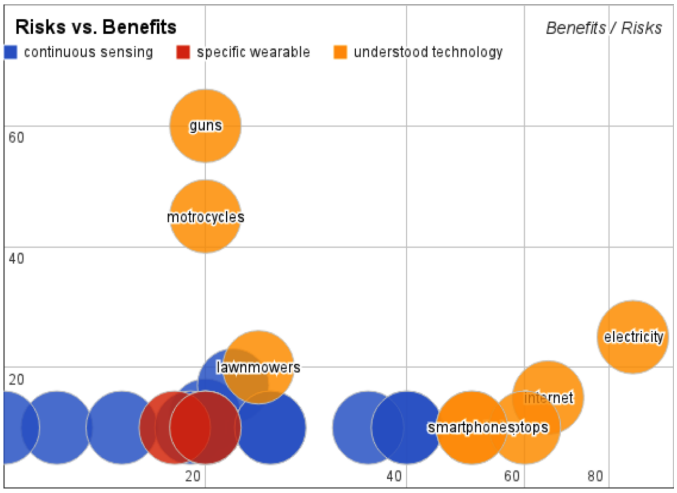

Figure 3: (This is a placeholder! TODO: generate a better plot; take out the specific wearables too.)

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

5.2.2 Lawnmower Ratios

5.3 Perceived Concerns for Wearable Devices

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*.

Talk about the results of the open-ended answers here.

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

<ask David's/Serge's input for this section>

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 [2][3], 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 [6]. 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 [7][5]. 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 [4].

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.

I messed up that motorcycle question.

7. CONCLUSION

END STRONG! Echo the conclusion a little, remind the people of the takeaways in a way that highlights the contribution of this paper.

8. ACKNOWLEDGMENTS

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

9. REFERENCES

[1] 2014 Will Be The Year of Wearable Technology. http://www.forbes.com/sites/ewanspence/2013/11/02/2014-will-be-the-year-of-wearable-technology/. Accessed: 2014-12-19.

[2] 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.

[3] 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.

[4] R. Kang, S. Brown, L. Dabbish, and S. Kiesler. Privacy attitudes of mechanical turk workers and the us public. In *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[5] P. G. Kelley. Conducting usable privacy & security studies with amazonâĂŹs mechanical turk. In *Symposium on Usable Privacy and Security (SOUPS)(Redmond, WA*. Citeseer, 2010.

[6] A. Kittur, E. H. Chi, and B. Suh. Crowdsourcing user studies with mechanical turk. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 453–456. ACM, 2008.

[7] J. Ross, L. Irani, M. Silberman, A. Zaldivar, and B. Tomlinson. Who are the crowdworkers?: Shifting demographics in mechanical turk. In *CHI'10 Extended Abstracts on Human Factors in Computing Systems*, pages 2863–2872. ACM, 2010.

APPENDIX

A. FULL SURVEY

B. DETAILED SITUATION RANKINGS

C. DETAILED TECH RANKINGS

D. FOCUS GROUP SCRIPT