Respecting Participants in Privacy-Related User Studies

Case Study of Mobile Messaging by Low-Income New Yorkers

Ame Elliott
Simply Secure
ame@simplysecure.org

1. INTRODUCTION

This presentation makes two contributions to emerging topics in Privacy Enhancing Technologies. First, it shares results from a mobile messaging user study describe how social, economic, and technical systems shape priorities for secure communication by low-income people of color in New York City. Second, it discusses how the human-centered design methods used in this study can be extended to help other software development teams ethically conduct user research.

2. CASE STUDY: SURVEILLANCE IN NYC

There is a long history of surveillance of African-Americans dating back to the earliest days of the USA [1], while recent reports show people of color being disproportionately targeted by surveillance from law enforcement [2]. While other efforts in the internet freedom space have explored the needs of populations at risk around the globe, there has been comparatively little attention paid to marginalized people in the United States context. Moreover, people of color are underrepresented in many current conversations around data privacy, encryption, and government surveillance [3] .

2.1. Methodology

In December 2015, in partnership with Blue Ridge Labs, wSimply Secure conducted fieldwork on mobile messaging with twelve participants in Brownsville and Harlem, New York City. Participants were recruited through Blue Ridges Labs, a social incubator focused on economic inclusion in New York.

All participants were African-American adults with mobile phones (10 Androids, 2 iPhones), and were enthusiastic users of messaging apps, sending at least 30 a week and some sending more than 100. Participants were not screened on the basis of privacy attitudes or tech savvy. Although Brownsville and Harlem have robust activist communities with technical security skills in circumventing surveillance, for example Harlem CryptoParty, our participants did not self-identify as concerned about surveillance.

2.2. Activities

The research activities were 1) four 60-minute, in-context interviews in homes, restaurants, and libraries with pairs of mothers and daughters or cousins, and 2) one 90-minute group interview with four young men at the office of a non-profit in Brooklyn. The sessions started with an ice-breaker/rapport builder, continued with discussion of their current messaging practices, apps used, and motivations for using particular apps (including looking at examples where the participants were willing). Next we discussed the participants' thoughts on privacy, and finally they gave feedback on app store descriptions of secure messaging apps.

2.3. Results

Against a backdrop of inevitable surveillance, participants shared their 1) concerns about physical device security, particularly shoulder surfing, 2) negative consequences of family plan group billing arrangements giving unwanted access, and 3) renter's mindset that the handset is controlled by an adversarial carrier.

Participants shared how the social, economic, and technical systems surrounding them shape their priorities for secure communication. Time and again, participants expressed that they find no safe harbor from surveillance at home, at work, or in public. Participants' lived experience of surveillance spanned physical environments, social relationships, cellphone carriers, device hardware , and application use.

The overarching message we took from this study is that if you're poor and Black, surveillance in your daily life is the norm. Everything you do is suspect, and you're always on camera, and always at risk of being accused of some crime. Many of the participants work in retail and are on camera the entire time they are on the job, presumably as a deterrent against theft. If you work at a fast-food restaurant like Chipotle, electronics store like Best Buy, or shoe store like Foot Locker, as some of our participants did, you are assumed to be stealing, and constantly under a supposition of guilt. Appealing to the video was viewed as a possible tool for proving innocence.

3. ETHICAL RESEARCH

At Simply Secure, as we strive to strike a balance between sharing photos and stories about our participants to build empathy and protecting participants' privacy. There is an urgent need to develop best practices for informing the design of privacy-enhancing technologies with user research, where the act of gathering research must also respect participants' privacy.

3.1. Don't Gather What You Don't Need

Our partner, Blue Ridge Labs, handled the recruiting and led us to meet participants. We did not know their addresses, names, or contact information, an important step to protecting their privacy. We were not connected to participants via email, mobile phone number, or calendar invitation. As part of our consent process, participants understood that they could give us an assumed name, disappear back into New York, and we would have no way to find them.

3.2. Empowering Consent with a Bill of Rights

Participants were also given a Participants' Bill of Rights (see the Resources section for a link to download) outlining consent procedures, including ability to refuse any questions or quit and still be compensated. Informed consent is a standard part of research protocols at many organizations such as universities. However, the explicitly empowering language, such as titling it

"Bill of Rights" rather than a medically-oriented description like "Human Subjects Protocol" made the consent process a tool for dialogue about the research and data-collection generally.

3.3. Opt-In Only

To be selected to participate, candidates filled out a minimal screener that only included necessary information. No need to ask for exact income or birthdate, or many common other attributes requested in social science research. During the interviews, the researchers only took notes on paper, without using audio or video recording. There's an inherent paradox in recording a conversation about surveillance, and for this project, handwritten notes sufficed to clearly illustrate attitudes towards surveillance and privacy-preservation strategies. We showed participants images from the Humans of New York (HONY) Instagram feed [4] – which they were all familiar with – as an example how we might share their stories and personally identifiable photos on the public web with their permission.

Participants then had the option of 3 levels of photographic participation: no photography, photographed in non-identifiable ways (such as their shoes or purses), and photographed in an identifiable way that required a signed a model release allowing their images to be shared publicly. Participants got copies of photos they wanted and approved images for public use.

Figure 1: (Top) Non-identifiable photo. (Bottom) Opt-in photo with a model release for use on the public web.

4. RESEARCH IN OTHER CONTEXTS

The fieldwork described in this research was done in partnership with an incubator with deep ties to the participant community. Blue Ridge Labs trains interviewers on how to behave respectfully in participants' homes. Many censorship circumvention tools are in urgent need of user feedback, but lack the infrastructure for such labor-intensive research.

A key challenge facing the PETS community is how to ethically capture data from participants in qualitative and quantitative research at scale. Starting with qualitative research, Simply Secure is building a set of resources for user studies, including screeners, consent forms, and interview guides. These are available on GitHub, and we welcome discussion and examples adapting these materials to different contexts. Responding to different threat models with appropriate responses to safeguarding participant privacy is an important evolution in privacy-oriented research.

On the quantitative side, there is a dearth of tools for understanding online behavior that treat participant data respectfully. Many tools for logging online behavior are developed as part of an advertising-driven revenue model, and there are few frameworks for appropriate metrics for privacy-preserving projects. The Participants' Bill of Rights could be extended to quantitative studies, but it is more challenging to identify clearly understood analogies to a non-personally identifiable photo in the online world. HotPETS would be an exciting place to have discuss appropriate metrics for user research.

5. CONCLUSION

A Human-Centered Design approach to technology development is grounded in empathy for the lived experiences of people. Capturing user research in a compelling away can help a broad team of stakeholders make more appropriate technology that meets the needs of real people. This presentation shared a case study of mobile messaging practices by low-income New Yorkers to illustrate opportunities for respectful and ethical data collection. Methods for ethical research, such as a Participants' Bill of Rights, should be extended to reach a broader audience – for example quantitative research and metrics for online behavior.

6. RESOURCES

See Simply Secure's GitHub Repository for examples of consent forms, model releases, participant Bill of Rights, screener, and interview guide. We welcome adaptations to other contexts and conversations about how to improve them. https://github.com/simplysecure/resources/tree/master/Research/2015_NYC_Mobile_Messaging

7. ACKNOWLEDGMENTS

Thank you Gillian "Gus" Andrews, Sara "Scout" Brody, and Blue Ridge Labs for contributions to this research.

8. REFERENCES

1. Browne , Simone, Dark Matters: On the Surveillance of Blackness. Duke University Press, 2015.
2. George , Joseph, "Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson" The Intercept, July, 24, 2014.
3. McLaughlin, Jenna, "The FBI vs Apple Debate Just Got Less White." *The Intercept*, March 8, 2016.
4. Stanton, Brandon, Humans of New York . h ttps:// www.instagram.com/humansofny, Accessed April 21, 2016.