Design Implications of Lived Surveillance in New York

Ame Elliott
Simply Secure
2973 16th St. Suite 300
San Francisco, CA 94103
ame@simplysecure.org

Sara "Scout" Sinclair Brody
Simply Secure
609 Elm Ave.
Swarthmore, PA 19081
scout@simplysecure.org

Abstract

We share initial findings on the lived experience of surveillance of African-American New Yorkers. Their biggest concerns were employer surveillance and peer-surveillance by a "small adversary" such as an estranged partner, particularly in terms of physical device security. Their concerns have implications for both the design of improved user experiences for secure communication applications and for describing the overall value proposition of surveillance circumvention technology to a diverse, non-technical audience.

Author Keywords

Fieldwork, Design, User Experience, Security, Privacy, Mobile Messaging

ACM Classification Keywords

H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous. See: http://www.acm.org/about/class/1998/ Optional section to be included in your final version, but strongly encouraged.

Introduction

This workshop position paper on "Everyday Surveillance" shares emerging findings from a qualitative field study of New Yorkers' attitudes towards privacy, security, and surveillance and concludes with implications for design of secure communications systems.

Methodology

In December 2015, our team conducted field research with 12 African-Americans from Harlem and Brownsville to understand attitudes about mobile messaging and identify design directions for anti-surveillance tools. Our activities were 1) in-context, semi-structured interviews in homes, restaurants, and libraries with dyads of mothers and daughters or cousins and 2) a group interview of four young men at the office of a nonprofit social entrepreneurship incubator in Brooklyn.

Figure 1. Fieldwork discussing privacy in New York.

Everyone was an adult with a mobile phone (10 Android, 2 iPhone), and was an enthusiastic user of multiple messaging apps, but participants were not screened on the basis of privacy attitudes. Both 90-minute in-context dyads and 120-minute group interviews discussed current messaging practices, motivations for using a particular app, and thoughts of privacy and surveillance (including both physical and digital).

Emerging Findings

We briefly report participants' attitudes about different kinds of surveillance. Contrary to our expectations, governmental surveillance was seen as inevitable and reluctantly accepted.

Employer Surveillance

Participants may understandably be wary of criticizing the government in front of strangers and concerned about the consequences, but they were very vocal about the negative consequences of workplace surveillance. Much like being presumed guilty until a search proved them innocent, the participants knew they were working under suspicion of stealing, and numerous cameras in their workplace were seen as a possible recourse against false accusation.

Physical security for mobile phones and other devices were also concerns at work. Participants talked about retail jobs at Foot Locker, Chipotle, Best Buy, and other places, and employees are not allowed to have their phones on them while working in some places. Additionally, not every workplace has safe storage such as a private locker for personal belongings. The result is vulnerable workers may need to compromise control of their phones to do their jobs.

Peer Surveillance

Protecting themselves from peer surveillance was both the biggest concern and area where participants' felt the most agency. By opting into multiple messaging platforms, including the phones' native texting clients, WhatsApp, Facebook, SnapChat, Kik, Instagram, and Twitter, participants felt their peers were always watching where they were and what they were doing. For example, WhatsApps' check marks for read receipts made it "impossible to dodge" by removing plausible deniability for reading a message.

iPhone users talked about FaceTime video calling taking away their ability to lie about their whereabouts via text message because the recipient (parent, jealous partner, manager) could insist they FaceTime to prove they were where they said. One of the Android users was pleased to no longer have to dodge FaceTime requests when he gave up his iPhone.

The “Find My iPhone” feature was also used to track participants by their families or estranged partners. Economics drive people into family plans and forms of account sharing with people they didn’t wholly trust, so others being able to track you was seen as a consequence of saving money on cell phone plans.

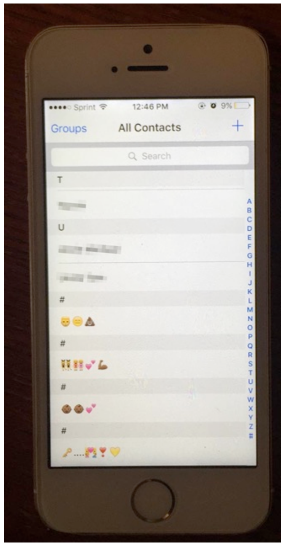

Figure 2. Contact names as emoji to preserve privacy from someone shoulder surfing.

Coping Strategies

Although many aspects of peer surveillance were accepted, this was the one type of surveillance participants felt they could protect themselves from. The participants’ dominant threat model was a known person getting access to your device. Shoulder-surfing, or someone nearby watching your screen, or someone you know going through your phone were the most pressing privacy concerns for all participants.

Using a screen-lock was the most common privacy-preserving strategy and viewed as a best practice, except by self-proclaimed social media addict.

A more unusual strategy was replacing contact names with emoji, making it difficult to determine at a glance who you were messaging. The 18-year old owner of the phone in Figure 2 considered giving an emoji contact name as a badge of intimacy reserved for important people she messaged frequently.

Design Implications

Our study identified a contradiction between the participants’ concerns and the priorities of the open-source security community. The participants believed that governmental surveillance is inevitable/inescapable, and that the physical security of their mobile devices is a pressing concern. The security app developers tend to be highly motivated by governmental surveillance and consider physical security a solved problem.

The emphasis on physical security make the privacy claims of SnapChat, which are generally considered without technical merit by the academic security community, make sense from a user perspective. Open-source secure communication applications can be technically robust anti-surveillance tools, but their user-facing language and value propositions are not effective at meeting the privacy concerns of users like the participants in this study who consider peer surveillance and physical security the most pressing threats.

References

[1] Americans’ Attitudes About Privacy, Security, and Surveillance. http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

[2] Secret, Mosi. “On the Brink in Brownsville,” *New York Times Magazine*, May 1, 2014. http://www.nytimes.com/2014/05/04/magazine/on-the-brink-in-brownsville.html?_r=0