Privacy-Protective Behaviors in the Face of Vulnerabilities

Shruti Sannon

Cornell University
Ithaca, NY
USA
ss3464@cornell.edu

1. INTRODUCTION

The goal of my research is to understand the factors that influence people's decisions to engage in (or abstain from) privacy-protective behaviors in multiple technological contexts, with a particular focus on vulnerable populations. People from marginalized groups can face unique privacy considerations and be disproportionately impacted by privacy violations; they may also face constraints on the extent to which they can protect their privacy. Investigating their perspectives and experiences can help identify new aspects of privacy decision-making that can contribute to existing theories of privacy, as well as raise creative implications for privacy-protective design. Thus far, I have examined two populations that face unique vulnerabilities online. Below, I outline some of the main findings and design implications that have emerged from my work in both contexts.

2. CHRONIC ILLNESS

First, I have explored the complex trade-offs that people with invisible chronic illnesses (ICIs) make when deciding whether to disclose sensitive health information on social media [2] .

People with invisible chronic illnesses can post sensitive content about their health conditions (including details about symptoms, doctors, and medication) publicly on social media sites, such as Twitter. My interviews with this population suggest that these individuals are not unaware of the privacy risks of such communicative practices; rather, they choose to make these disclosures based on a nuanced cost/benefit analysis. Individuals with invisible chronic illnesses can face invalidation from broader society, since their symptoms are not well-known or visible. This can motivate them to turn to social media to gain social support and raise awareness of their conditions publicly, despite the many risks that such communication can entail.

At the same time, my research finds that these individuals also desire to compartmentalize their health communication, separating it from their offline identities. For example, my interviewees often reported using multiple Instagram or Twitter accounts to separate the audiences for their content: for example, they would hold one account for their offline contacts and networks, and another for sharing their health information.

This population has particularly unique needs and constraints around sharing their information online, which calls for specific design implications. The need for granular control over one's online content is particularly important for this population. Since specific posts on Twitter or Instagram cannot be marked as private or restricted to a specific audience, individuals have to manage multiple accounts in order to manage their privacy while using these platforms. For people with ICI who can face significant cognitive burdens as part of their conditions, this strategy can be additionally burdensome in terms of time and energy. Thus, they may choose to eschew such strategies, which may make them more vulnerable to risk online. In such contexts, privacy-sensitive design needs to aid people in making sensitive disclosures in a way that minimizes the risk associated with such disclosures.

3. DIGITAL WORK

I am also currently investigating the privacy issues that emerge in digital labor markets. On Amazon Mechanical Turk (MTurk), a popular crowdsourced labor site, workers (or "MTurkers") report a range of privacy concerns and violations that arise during their work on the platform, such as concerns about data collection and profile, being stalked, and scams [5]. Although these issues are not unique to MTurk, they may be magnified in this context due to the stark information and power asymmetries on the platform, as outlined by [1].

While recent work finds that there are many privacy issues on MTurk [5], less is known about how MTurkers navigate these issues and make decisions about disclosing their personal data during tasks. To address this gap, my current research project seeks to answer the following research questions: How do MTurkers navigate issues of privacy during their work? When, why, and how do they decide whether to provide or conceal their personal information?

My preliminary research indicates that MTurkers often comply with privacy-invasive requests for information despite their privacy concerns about the request. They discount these legitimate privacy concerns for a range of reasons, such as to avoid negative consequences on the platform, like being blacklisted or receiving a poor rating [4]. However, MTurkers also often engage in privacy-protective behaviors, such as looking up reviews to find safe tasks to complete, lying about their personal data, or quitting tasks that ask them for too much information. Importantly, these privacy-protective behaviors come at a cost: reading reviews takes time and energy, lying about one's data can risk being rejected, and quitting tasks midway entails a lot of wasted time and effort.

My research on how MTurkers make decisions about revealing or concealing their personal data during tasks raises several implications for design. First, because MTurkers often lied when they perceived a requested data point to be irrelevant for the HIT, a straightforward design implication for requesters is to clarify why any specific data point is being requested to increase user trust and compliance. MTurkers also voiced a preference for consent forms, so that they could assess a task before beginning work. Non-academic requesters could also be mandated through design or policy to include fair and transparent data practices.

4. REFERENCES

[1] Martin, D., Hanrahan, B. V., O'Neill, J., & Gupta, N. (2014). Being a turker. In *Proceedings CSCW* (pp. 224-235).

[2] Sannon, S. (2017). When Privacy is Painful: Designing for Multiple Needs and Trade-offs. *CSCW 2017 Workshop on Networked Privacy*. Portland, OR.

[3] Sannon, S., Murnane, E., Bazarova, N., & Gay, G. (2018). Managing Privacy While Managing Pain: A Mixed Methods Study of Health Disclosures on Social Media. Presented at the *American Psychological Association's Conference on Technology, Mind & Society*. Washington, DC.

[4] Sannon, S. and Cosley, D. (2018). "It was a shady HIT": Navigating Work-Related Privacy Concerns on MTurk. In *Extended Abstracts on Human Factors in Computing Systems (CHI '18)*.

[5] Xia, H., Wang, Y., Huang, Y., & Shah, A. (2017). "Our Privacy Needs to be Protected at All Costs": Crowd Workers' Privacy Experiences on Amazon Mechanical Turk. In *Proceedings of the ACM Human-Computer Interaction*, 1, Article 113.