Research Statement

Yixin Zou
yixinz@umich.edu
yixinzou.github.io

Most people care about their security and privacy, but they might not fully understand the respective risks; even if they do, they might not take action to protect themselves. Inaction after security incidents or privacy violations can further lead to harmful outcomes from financial loss to harassment and abuse. My research, which sits at the intersection of **human-computer interaction (HCI)**, **privacy**, and **cybersecurity**, makes the following contributions:

1. Identifying factors that prevent people from reacting to security and privacy risks when they emerge, such as after a data breach;
2. Understanding the unique threat models and safety needs of at-risk populations, such as survivors of intimate partner violence and older adults;
3. Using insights from #1 and #2 to develop human-centered solutions (e.g., technological innovations, policy changes, and education) that help people protect themselves from perceived risks.

As an interdisciplinary scholar, I draw inspiration from social psychology, behavioral economics, and public policy in addition to information science as my home discipline. I use a variety of methods in my work, including experiments [5, 7, 8], surveys [6, 13], interviews [9, 12], focus groups [11], content analyses [4, 14], and usability testing [3]. Over the course of my Ph.D., I have published 13 articles in top-tier peer-reviewed venues in HCI, cybersecurity, and privacy. My scholarship has been recognized with a SOUPS Distinguished Paper Award, two CHI Honorable Mentions, and a Honorable Mention in the Future of Privacy Forum's "Privacy Papers for Policymakers."

Impact on policy and industry practice. My research has directly impacted public policy and industry guidance. I have given multiple invited talks on my research [6, 10, 12, 14] at the US Federal Trade Commission's PrivacyCon, an annual symposium for regulators and policymakers showcasing outstanding privacy research. My work with Carnegie Mellon University collaborators [3, 4] has been cited in the rulemaking process for the California Consumer Privacy Act (CCPA), a landmark piece of privacy legislation impacting millions of US consumers. I also co-led the effort [5] that produced the Privacy Options icon now included in the official CCPA regulations.[1] My internship work at Mozilla has informed changes in Firefox Monitor's content strategy and interface design.[2] As a recipient of the highly competitive NortonLifeLock Graduate Fellowship (one of the three recipients worldwide in 2019), I have worked closely with the NortonLifeLock Research Group on research [11, 13] that provide insights for improving the company's antivirus software, identity theft monitoring service, and customer support in addition to broader research contributions.

Challenges in Reacting to Security and Privacy Risks

Creating effective security and privacy solutions requires knowledge of people's perceptions and behaviors. To this end, I combine qualitative and quantitative methods to study people's adoption of protective measures when facing security and privacy risks as well as reasons behind inaction.

One line of my research focuses on consumer reactions to data breaches, i.e., security incidents that put affected consumers at higher risk of cybercrimes as their sensitive personal information gets leaked. Even with improved threat detection techniques, data breaches will inevitably happen and affect consumers, and thus it is important to understand consumers' awareness and behaviors after these breaches. I started with an interview study with US consumers focusing on their risk perceptions and behaviors after the 2017 Equifax data breach [12]. We found that participants took limited protective measures despite concerns of identity theft and privacy invasion. Participants were unmotivated to take action due to optimism bias, a tendency to delay action until harm has occurred, and misconceptions about protective measures. The study received a Best Paper Award at SOUPS 2018 and wide press coverage including the New York Times and the Associated Press.

Building on this qualitative work on a specific breach, I co-led an online study (n=413) in which we presented participants with real-world breaches that have exposed their personal information using the Have I Been Pwned database [6]. We found that awareness of breaches was low: while participants were affected by 5.4 breaches on average, they were unaware of 74% of breaches we showed them. While some participants reported intentions to take action following the breach, most believed the breach would not impact them. Our findings suggest that existing mechanisms for notifying consumers of breaches fail at raising awareness and motivating consumers to take action.

Knowing consumers' low awareness and inaction after data breaches [6, 12], I led a content analysis of 161 breach notifications sent to consumers to identify potential readability and usability issues in these notifications [10]. We found that many notifications were vague about how consumers might be affected by a breach. Descriptions of recommended measures (e.g., credit freezes and fraud alerts) were often lengthy and complicated, which might pose barriers for consumers to follow through on the provided advice. Our findings indicate that regulation should prescribe

[1] `https://oag.ca.gov/privacy/ccpa/icons-download`
[2] `https://medium.com/firefox-ux/designing-a-content-first-experience-on-firefox-monitor-9b8875d44386`

user-tested breach notification templates to guide consumers in understanding risks and taking mitigations after a breach, since companies otherwise have little incentive to improve breach notifications for consumers [14].

Data breaches are not the only problem that affect consumers. Over the years, experts have recommended many best practices for mitigating security, privacy, and identity theft risks. To understand whether end-users follow through expert advice and why (not), I led an online survey (n=902) on the adoption and abandonment of 30 expert-recommended practices [13]. Participants reported abandoning practices that were impractical (e.g., keeping track of unique passwords), burdensome (e.g., two-factor authentication requiring intermittent actions) or when they no longer felt the risk. Age, gender, income, and education were significantly correlated with a practice's adoption, showing structural inequities in people's security and privacy behaviors. Our research, recognized by a Honorable Mention at ACM CHI, highlights the importance of making protection tools less burdensome to use, providing more practical advice, and tailoring advice in ways that mitigate structural inequities.

Digital Safety for At-Risk Populations

Building on my work that showed a "digital divide" in people's security and privacy behaviors [13], my recent research examines how certain populations are disproportionately affected by digital risks. For instance, I have contributed to research on child safety risks in smart homes [9] and privacy experiences of Muslim-American women. Below I discuss two projects I led that involve survivors of intimate partner violence (IPV) [11] and older adults (ongoing work).

IPV survivors face unique challenges in protecting themselves: survivors may still live with their abuser or share social circles, and even routine protective behaviors like turning off location tracking could escalate the violence. Working with Cornell Tech and NortonLifeLock researchers, I led a study that explored how customer support at computer security companies can better serve IPV survivors who experience technology-enabled stalking and abuse [11]. We uncovered issues in real-world support cases, such as overpromising security software's protection without acknowledging the customer's traumatic experience. We further elicited practical recommendations from IPV advocates and customer support professionals and incorporated these suggestions in creating training materials for customer support agents. We are working with the Coalition Against Stalkerware[3] to disseminate our materials so that member companies can use our materials to provision better customer support with trauma-informed language and referrals to broader resources for survivors.

Older adults are at risk in their online activities due to declining health and memory loss associated with aging. In ongoing work, I have interviewed 43 older adults on their risk perceptions and mitigation strategies around security, privacy, and holistic safety. Our findings show differences between contexts: participants were more aware of risks around cybercrimes and social media than emerging technologies such as wearable devices and Zoom. Additionally, tech-savvy participants were well-versed in protecting themselves and helping others, whereas less tech-savvy participants shared more encounters with scams, harassment, or struggles with navigating the online world safely. By highlighting the diverse experiences within older adults, our research suggests the importance of identifying and addressing factors beyond age—such as digital literacy—that cause or amplify some older adults' vulnerability. Such findings are crucial to future efforts of designing technical protections or providing educational resources for older adults in ways that honor their heterogeneous needs and preferences.

Develop Solutions Across Technology, Policy, and Education

Knowing people's struggles in protecting themselves and the substantial harm of information leakage on certain populations, I employ a holistic approach in developing solutions that help people better manage their security and privacy. I strive for, and have been successful in generating not only technological innovations [7, 8], but also effective proposals for policymaking [5] and meaningful public outreach.

In developing technical solutions, I draw on behavioral economics and social science research to align technology design with human risk perception and decision-making models. In my ongoing work, I leverage Protection Motivation Theory to craft and validate data breach notifications that motivate people to change exposed passwords by highlighting the breach's threats and coping options. In another work on improving email phishing warnings [8], we designed and tested a "forced attention" feature that deactivated the suspicious link in the email body while forcing the user to click an unmasked URL if they want to proceed. Regarding privacy controls for smart speakers [7], we developed and evaluated a novel prototype that leverages interpersonal communication cues: changing the microphone's status based on the user's voice volume or gaze to seamlessly integrate privacy controls into one's user experience. I further evaluate these prototypes through large-scale behavioral experiments with high ecological validity. For example, in my ongoing work I measure participants' responses to notifications of real-world breaches that exposed their provided email addresses, rather than asking participants to imagine possible reactions in hypothetical scenarios.

I seek to make my research findings and recommendations relevant to policymakers. An example is the collaborative

[3] `https://stopstalkerware.org/`

research effort I co-led that informed the CCPA rulemaking process [5]. Upon noticing the CCPA's mandate of a "Do Not Sell My Personal Information" opt-out, we developed icon designs for this need, evaluated them in experiments with crowd workers, and submitted our recommendations to the California Office of the Attorney General (OAG). Upon the OAG's request, we redesigned our experimental protocol and performed more evaluations on their proposed icons [2]. Our research led to the removal of a confusing icon from draft regulation and the adoption of our user-tested Privacy Options icon in the final CCPA regulations. Our collaboration with the OAG also demonstrates the importance and feasibility of including rigorous user research and providing evidence-based recommendations to inform policy and rulemaking activities.

In addition to technical solutions and policy changes, I pursue ways to make my research directly useful to broader audiences. In my ongoing work with older adults, almost all participants expressed the need for training and resources that teach them how to protect themselves, more than novel software or stronger regulations. In response, I offered a multi-week workshop series about online self-defense in November 2021 at three local senior centers. My efforts in running the workshops also represents my philosophy in research with vulnerable populations and human subjects in general: consider what information would be interesting and useful to participants and return such knowledge to them; engage participants as active stakeholders in the research process rather than sources for knowledge extraction.

Future Directions

Going forward, I will continue conducting research that addresses privacy and security challenges of societal importance, with an emphasis on developing solutions that enhance consumer protection and cater to the needs of at-risk populations. I envision three threads that align with my prior work while expanding into new contexts, user groups, and methodologies: (1) understanding the longitudinal harms of data breaches; (2) making security and privacy solutions more trauma-informed; and (3) addressing privacy challenges in cross-cultural contexts.

Quantifying longitudinal harms of data breaches on affected consumers. My prior work has examined consumer reactions to data breaches [6, 12], which put them at greater risk of identity theft, targeted scams, and phishing attempts. This raises the question: for affected individuals, how do potential risks manifest into actual financial and emotional harms over time? Quantifying privacy risks and harms is notoriously difficult. Yet, such quantification is critical as it helps inform necessary interventions (e.g., automatically enrolling affected consumers in identity theft protection services rather than using an opt-in model) and optimize advice to consumers about protective measures (e.g., prioritizing actions that mitigate the most common and/or most severe harms).

Building on the topic and methodological expertise I accumulate in my prior work, I will investigate the likelihood of consumers experiencing actual harms as a result of data breaches and what can be done to address harms with a multipronged approach. This includes (1) longitudinal surveys with consumers to understand the harms they experience and how they change over time; (2) regression models that correlate survey responses with records of data breaches (e.g., from the Identity Theft Resource Center) and cybercrime cases (e.g., from the FTC[4]); (3) interviews with consumers that experience actual harms to identify potential changes that could be made (e.g., policies at credit bureaus and financial institutions) to smooth their recovery process.

Developing trauma-informed security and privacy solutions. Trauma is the aftermath of distressing events such as domestic violence, natural disasters, or severe illness. In recent work, I co-led the development of a framework for trauma-informed computing: drawing on social work and public health literature, we illustrate how trauma-informed principles could apply to technology design in areas such as security and privacy, artificial intelligence, and user interfaces [1]. In particular, security compromises and privacy violations could lead to traumatic experiences. People who experienced scam, sextortion, or identity theft report lasting emotional distress or even suicidal thoughts in extreme cases.[5] Even simple user interface elements in line with established design guidelines (e.g., using red or other warm colors, using words like "threat" or "compromise") could trigger panic in traumatized users with hypervigilance. This begs the question: how can we design security and privacy solutions that account for the possible effects of trauma on users while informing users of risks and needed actions?

Building on my recent work and leveraging my connections with Cornell Tech and NortonLifeLock, I will start with a research agenda on making antivirus notifications more trauma-informed: (1) conducting feature analyses of how existing notifications may violate trauma-informed principles; (2) running co-design workshops with IPV advocates and survivors who experience tech-enabled stalking to generate design ideas; (3) develop prototypes of new notifications and evaluate their usability and safety, such as by using the Trust and Abusability toolkit.[6] I expect to further apply this same approach to other contexts such as breach notifications and phishing warnings to generate relevant insights.

[4] https://www.ftc.gov/enforcement/data-visualizations/explore-data
[5] https://www.idtheftcenter.org/identity-theft-aftermath-study/
[6] https://nrl.northumbria.ac.uk/id/eprint/47508/1/TrustAndAbusabilityToolkit.pdf

Investigating privacy and surveillance in cross-cultural contexts. Most existing privacy research has relied on WEIRD (Western, Educated, Industrialized, Rich, and Democratic) samples. Yet, understanding the privacy needs and challenges of people with diverse social and cultural backgrounds—especially those underrepresented—is imperative for developing privacy solutions for all, not just for privileged groups. In ongoing work, my collaborators and I examine privacy concerns and behaviors of Muslim women in the US, who have to contend with government and social surveillance, Islamophobia, media stigmatization all while navigating their own individual privacy beliefs. Having a cross-cultural lens on privacy research also provides broader transnational implications, as more countries start to enact privacy laws and there is an emerging need for global standards on data protection principles.[7]

Going forward, I am excited to conduct research that brings more diverse perspectives into privacy scholarship and shapes the global privacy landscape. For example, China recently passed the Personal Information Protection Law (PIPL), which is similar to the European Union's General Data Protection Regulation (GDPR). As a key step toward understanding the impact of privacy legislation in non-Western contexts, I plan to conduct longitudinal measurement of the PIPL's impact on consent notices and privacy controls for Chinese consumers. Such research will provide insights on developing privacy mechanisms that are sensitive to local constraints as well as improving privacy legislation to account for potential dark patterns. I also envision ways to expand my ongoing work with at-risk populations with a cross-cultural lens, such as developing digital literacy trainings for older immigrants in different languages and with customized content. Such work will contribute to the design of privacy solutions with intersectional thinking that recognizes multiple identities and vulnerabilities for any individual.

References

*Note: * indicates co-first authorship.*

[1] J. X. Chen*, A. McDonald*, **Y. Zou***, E. Tseng, K. A. Roundy, A. Tamersoy, F. Schaub, T. Ristenpart, and N. Dell. Trauma-informed computing: Towards safer technology experiences for all. Under review.

[2] L. F. Cranor, H. Habib, Y. Yao, **Y. Zou**, A. Acquisti, J. Reidenberg, N. Sadeh, and F. Schaub. CCPA Opt-Out Icon Testing – Phase 2. Technical report, The California Office of the Attorney General, 2020. `https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/dns-icon-study-report-052822020.pdf`.

[3] H. Habib, S. Pearman, J. Wang, **Y. Zou**, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub. "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 384:1–384:12, 2020. doi: 10.1145/3313831.3376511.

[4] H. Habib, **Y. Zou**, A. Jannu, N. Sridhar, C. Swoopes, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub. An empirical analysis of data deletion and opt-out choices on 150 websites. In *Symposium on Usable Privacy and Security (SOUPS)*, 2019. `https://www.usenix.org/system/files/soups2019-habib.pdf`.

[5] H. Habib*, **Y. Zou***, Y. Yao, A. Acquisti, L. F. Cranor, J. Reidenberg, N. Sadeh, and F. Schaub. Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 63:1–63:25, 2021. doi: 10.1145/3411764.3445387.

[6] P. Mayer*, **Y. Zou***, F. Schaub, and A. Aviv. "Now I'm a bit angry:" User Awareness, Perception, and Responses to Data Breaches. In *USENIX Security Symposium*, pages 393–410, 2021. `https://www.usenix.org/system/files/sec21-mayer.pdf`.

[7] A. Mhaidli, M. K. Venkatesh, **Y. Zou**, and F. Schaub. Listen only when spoken to: Interpersonal communication cues as smart speaker privacy controls. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2020(2):251–270, 2020. doi: 10.2478/popets-2020-0026.

[8] J. Petelka, **Y. Zou**, and F. Schaub. Put your warning where your link is: Improving and evaluating email phishing warnings. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 518:1–518:15, 2019. doi: 10.1145/3290605.3300748.

[9] K. Sun, **Y. Zou**, J. Radesky, C. Brooks, and F. Schaub. Child safety in the smart home: Parents' perceptions, needs, and mitigation strategies. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):471:1–471:41, 2021. doi: 10.1145/3479858.

[10] **Y. Zou**, S. Danino, K. Sun, and F. Schaub. You 'might' be affected: An empirical analysis of readability and usability issues in data breach notifications. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 194:1–194:14, 2019. doi: 10.1145/3290605.3300424.

[11] **Y. Zou**, A. McDonald, J. Narakornpichit, N. Dell, T. Ristenpart, K. A. Roundy, F. Schaub, and A. Tamersoy. The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence. In *USENIX Security Symposium*, pages 429–446, 2021. `https://www.usenix.org/system/files/sec21-zou.pdf`.

[12] **Y. Zou**, A. H. Mhaidli, A. McCall, and F. Schaub. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 197–216, 2018. `https://www.usenix.org/system/files/conference/soups2018/soups2018-zou.pdf`.

[13] **Y. Zou**, K. A. Roundy, A. Tamersoy, S. Shintre, J. Roturier, and F. Schaub. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 443:1–443:15, 2020. doi: 10.1145/3313831.3376570.

[14] **Y. Zou** and F. Schaub. Beyond mandatory: Making data breach notifications useful for consumers. *IEEE Security & Privacy*, 17(2):67–72, 2019. doi: 10.1109/MSEC.2019.2897834.

[7] `https://techcrunch.com/2021/10/02/navigating-data-privacy-legislation-in-a-global-society/`