Allison McDonald | Research Statement

Privacy & Security at the Margins

Despite advances in security and privacy research and practice, access to safe, trustworthy technical tools and platforms is not a reality for many people, such as those who face challenges like a targeted adversary, government censorship, discrimination, or harassment. My research focuses on understanding the complex sociotechnical factors contributing to this disparity in safety and access, and designing technical and policy mitigations to address that disparity.

My research goals are to: (1) investigate the privacy and security challenges of high-risk populations; (2) advance holistic digital safety for these populations and the general population through designing and evaluating technical solutions; and (3) conduct scholarship that supports policy improvements for companies and governments. Working at the intersection of computer security and privacy and human-computer interaction (HCI), I am a computer scientist who leverages a diverse set of methods to investigate causes of and solutions to privacy and security harms, including interviews [Sec21a, CHI21b, CHI18], surveys [CHI21a, Sec21a], focus groups [Sec21b], large-scale network measurement [IMC18, Sec18, FOCI17], and lab experiments [SP20]. My work has received multiple best paper awards at both top-tier security and HCI venues.

Understanding Barriers to Safety

The first thread of my work focuses on understanding barriers to digital safety for high-risk populations at multiple focal points and with varying methods: qualitatively investigating individual risk management, surveying public documents and individual experiences at scale to identify regulatory failures, and measuring global barriers to information access.

How do individual safety strategies fall short? High-risk populations face greater risks and consequences of privacy invasions and security failures. By studying how people with a heightened need for digital safety manage privacy and security, my research has provided both insights into how to better protect particularly vulnerable people online, as well as insights into which individual safety strategies are most and least easy to implement and effective for everyone.

In a study that won a Best Paper Award at CHI 2018, the premier peer-reviewed publication venue for HCI research, my collaborators and I conducted interviews to investigate how undocumented immigrants, who face harassment, detention, and deportation, were conceptualizing and managing risk [CHI18]. We found that our participants had complex threat models for offline risks (e.g., deciding when and whether to drive, opting out of benefits for their citizen children), but that this risk awareness did not translate to equivalent online behaviors (e.g., strategic avoidance of immigration-related pages, opting out of social media). The concrete benefits of participating online, like keeping in touch with families in their countries of origin and coordinating immigration resources in their communities, outweighed the uncertain risks of visibility online. Participants also indicated a resignation to surveillance: if the US Immigration and Customs Enforcement (ICE) knew everything about them anyway, they perceived their online behavior as making no difference to their risk level.

To investigate whether more tangible digital risks lead to increased digital security practices, I considered the safety needs and practices of another high-risk population—sex workers [Sec21a, CHI21b]. In a study that won a Distinguished Paper Award at the 2021 USENIX Security Symposium, a top-tier venue in security, we conducted interviews with sex workers in European countries where sex work is legal. Sex work nevertheless continues to be highly stigmatized, and sex workers may manage aggressive clients, police violence, exclusion from on- and offline spaces, doxxing, and online harassment. In contrast to our findings in the undocumented immigrants study, our participants were aware of concrete online risks, and most had sophisticated strategies for managing safety online. We also found, however, that privacy and security were not always the highest priority: some participants made exceptions to their careful protocols if it meant making more money or more effective ads. Furthermore, participants' safety practices were not just a balancing of effort and efficacy; maintaining reliable *access* to resources that keep them safe required significant effort. For example, many participants had social media and financial accounts banned because of their identities as a sex workers, despite the fact that their work was legal. Our research highlights how company policies and data practices can severely impact the safety of high-risk communities.

Research on privacy and security behavior often focuses on maximizing adherence to best practices through education and usability improvements. However, other goals that lead someone to *not* comply are often ignored. In all of these studies [CHI18, Sec21a, CHI21b], we found that participants reasoned about their privacy and security practices alongside other needs: keeping in touch with family, joining support forums, getting paid even if it violated their pseudonymity. My

research reframes these trade-offs as optimizations toward holistic safety: behaviors like seeking financial security or physical safety *are* safety decisions even if the behavior is counter to security or privacy best practices. Going forward, my research will focus on holistic safety—finding the ways technology creates barriers to safety across multiple dimensions and developing solutions that address the fundamental reasons security and privacy break down.

Where do company policies and government regulations fall short? Individual protective behaviors are only one piece of the puzzle: how technical tools and core Internet infrastructures are run and regulated also fundamentally impacts people's access to safe participation online. My research investigates this problem in both technical and legal contexts.

The previous studies reveal some ways phone numbers can be a risk vector: they reveal people's physical location, expose social networks through group chats, and offer access to one's accounts. I conducted a qualitative elicitation survey (n=195) to catalog the privacy, security, and safety problems people have as companies use phone numbers as persistent, unique identifiers [CHI21a]. I made two important observations. First, phone numbers as persistent identifiers can enable serious risk, such as harassment across multiple platforms because one's number is searchable. Such experiences are even more dangerous for high-risk communities. Second, even minor problems can be persistently aggravating. For example, getting phone calls and text messages for a phone number's previous owner was surprisingly common, and could sometimes last for years. Phone number reuse exposed sensitive information about former owners, including text messages from banks, doctors, and accidental access to accounts. While these consequences are minimal in isolation, in aggregate they create real inconvenience and risk. Based on our findings, we identify several steps regulators could take to minimize the effects of phone number recycling, such as increasing the time a phone number stays out of circulation between owners. Our work also provided further evidence that companies should move away from SMS-based multi-factor authentication and offer alternate authentication mechanisms in addition to phone numbers.

As a result of my work on the digital risks of undocumented immigrants, I began an ongoing collaboration with the Center on Privacy and Technology at Georgetown Law on a technical report. Through freedom of information requests, mass processing of procurement transactions, and a synthesis of academic literature on the chilling effects of ICE surveillance, we paint a broad picture of ICE's surveillance capabilities and the consequences of mass surveillance on communities as a whole. In particular, we identified multiple ways the law currently fails to protect US residents' data—e.g., despite specific regulation to prevent ICE from accessing immigrants' data (e.g., driver's license photo, home address), ICE exploits legal and technical loopholes to gain access anyway, often through third-party data brokers. In some cases, the same loopholes also give them access to the majority of US residents' data. Our upcoming report outlines actions that federal and state governments can take to close these loopholes and increase transparency in ICE's surveillance capabilities.

How is digital participation threatened at scale? My work has looked at how digital inequities happen at scale. A core part of safe participation online is having fundamental access to information and online spaces. A major source of inequity comes from State censorship: a government may disallow their country's residents from accessing content online, e.g. by severing TCP connections to particular IPs or manipulating DNS records. A significant amount of research, including some of my own, has focused on measuring the scope of censorship [Sec18] and building circumvention tools [FOCI18].

However, governments are not the only source of access disparities between countries. Websites themselves may decide to geoblock particular regions from accessing their content. Geoblocking had not been systematically studied despite being a well-known phenomenon in heavily-blocked countries like Iran and impacting millions of people worldwide. I led a global measurement study to learn *which countries* are most blocked and from *what content* [IMC18]. The primary challenges were twofold: (1) identifying signals of geoblocking, and (2) building a measurement infrastructure that enabled us to visit thousands of websites from residential vantage points worldwide. To identify geoblock pages, I leveraged our discovery that many sites hosted by content delivery networks (CDNs) use built-in features that serve recognizable block pages. To gain a global view of the Internet, I built a large-scale measurement infrastructure using a service called BrightData,[1] which compensates a global network of participants for sharing access to their local bandwidth. This enabled us to conduct the first global analysis of geoblocking, testing several thousand of the most popular websites in 177 countries.

[1] Formerly known as Luminati; https://brightdata.com/

Among other findings, our measurements allowed us to observe the global impact of an American law: countries under US export restrictions—Syria, Sudan, Iran, and Cuba—were by far the countries with the most limited access, followed closely by China and Russia. Alarmingly, websites themselves were increasing access disparity by denying access to residents in countries already experiencing significant State censorship. Through a collaboration with a large CDN provider, Cloudflare, we confirmed our observations and observed that geoblocking has been growing significantly in the last few years. After our study, Cloudflare restricted access to its geoblocking features to only enterprise customers, removing access to the tools for many customers. Our findings also made an important methodological contribution: we confirmed that ongoing censorship measurement efforts were impacted by geoblocking by matching our known geoblock pages to an open-access corpus of censorship data collected by the Open Observatory of Network Interference. This study demonstrates one of the numerous ways that American laws and companies are shaping access across the globe, and the potential for Internet measurement to throw the consequences of national decisions on a global network into sharp relief.

Developing Holistic Safety Solutions

My research has focused not only on understanding safety challenges, but also on seeking and testing interventions that promote security and privacy while accommodating other safety and accessibility needs.

Procedural interventions for technical problems. The most effective solution to a problem is not always a new system or tool. Changing company procedures, educational resources, or the priorities of existing solutions can also make an impact.

For example, survivors of intimate partner violence (IPV) face tech attacks from their abusers, such as spyware, account hijacking, or digital impersonation. However, IPV support organizations are often unequipped to give technical support. In collaboration with Cornell Tech and NortonLifeLock, I investigated the potential for customer support at computer security companies to assist survivors experiencing tech abuse [Sec21b]. Our team conducted focus groups with IPV support professionals to design educational and procedural interventions for customer support. Following this, we spoke with customer support agents at multiple large computer security companies to evaluate the effectiveness and feasibility of our proposals. Taking the suggestions and needs of both groups into account, we designed recommendations and customer support training materials that overviewed opportunities for agents to better support customers experiencing abuse. We presented these materials at one company and received positive feedback, and are developing a version to share publicly.

As another example, ballot-marking devices (BMDs) enable voters with visual impairments and other disabilities to vote privately and independently. However, any machine that creates or tallies ballots is an alluring target for hackers, so BMDs create an additional attack vector for modifying votes. My collaborators and I conducted a mock election using BMDs that allowed us to empirically establish the proportion of voters who manually verify their printed ballot—and detect the deliberate error we inserted [SP20]. We found that only 40% of voters looked at their ballots at all, and fewer than 10% reported the error to a pollworker. To increase this number, we designed several interventions and found that with verbal instruction to review their ballots, voters reported errors at much higher rates. Our findings suggest that, while current practices at polling locations are unlikely to lead to rapid detection of misbehaving BMDs, changes to polling location design and procedure may increase the reliability and safety of these important accessibility tools.

Towards trauma-informed computing. My research has also considered opportunities for the use of trauma-informed principles in computing research and development. In studying safety needs for high-risk communities, we inevitably hear stories of safety failures, technology contributing to harm, and the resulting trauma. To account for this trauma, I co-led the development of a framework for *trauma-informed computing* [UR21]. We demonstrate how understanding trauma will help researchers and practitioners understand tech-enabled harm and how people, in response, may interact differently with systems. Our framework adapts the six principles of trauma-informed care[2] for the design, development, evaluation, and operation of computing systems. We illustrate how to apply the principles in multiple areas of computing research and practice, including security, AI, and UX design. Along with applying these principles in my own work, I plan to study the impact of these principles in the redesign and development of technical artifacts that have previously been harmful.

[2] Substance Abuse and Mental Health Services Administration. 2014. SAMHSA's Concept of Trauma and Guidance for a Trauma-Informed Approach. https://ncsacw.samhsa.gov/userfiles/files/SAMHSA_Trauma.pdf

Future Directions

My past work has highlighted that privacy and security needs do not exist in a vacuum. Many other competing needs, from physical safety to the need for participation in a community, are a part of the privacy and security decisions people make. My future research will seek to promote digital safety more broadly—considering not only traditional security goals (e.g., secrecy and integrity of communications), but also physical safety and digital equity as critical parts of safety. My research will continue to center the needs and experiences of high-risk populations to inform better design for both these communities and the general population. In particular, my research agenda focuses on understanding the limitations of existing technology and tech policy for high-risk populations and envisioning, creating, and evaluating safer alternatives. In addition to continuing and expanding my ongoing research lines, I will expand my work into two additional domains.

Understanding collective negotiation of digital safety priorities. Research on understanding safety and protective practices usually focuses on the individual. However, individuals do not operate in isolation; what we know about safety is also based on the experiences and needs of the people we are most connected with. I will build on my work investigating safety management for high-risk individuals to explore how grassroots organizations that face external risks construct a shared threat model, navigate digital security while achieving other goals, and manage security failures. Specifically, I intend to work with immigrant rights organizations to leverage my expertise on immigration-related surveillance risks.

I intend to start this investigation by looking to partner with local immigrant rights organizations. I have previously worked with similar organizations in Ann Arbor and will lean on my experience studying ICE surveillance at the federal level to offer useful support in return. I will conduct interviews and collect observational data to (1) understand the organization's perceived threat model, and (2) establish what strategies are happening in practice. In addition to research contributions, this work will lead to tangible outcomes for the organizations in the form of security trainings and technical interventions or resource improvements to keep all group members and their constituents safer.

Measuring impact and effectiveness of law and policy. Internet regulation and company policies, even when enacted to meet a particular need or prevent harm, can have cascading effects across the Internet. Research can help us shape policy decisions before they are made, but continued systematic study of the impacts of policies after implementation is a critical, and often missing, part of understanding their effectiveness and potentially unintended consequences. My work on geoblocking shows the potential of measurement as one method to expose the externalities of laws regulating the Internet and corporate attempts at compliance. I plan to build a research stream that focuses on empirically evaluating the impacts of technology regulation and corporate policy changes, especially as they relate to digital equity, access, and safety.

I plan to conduct studies with several focuses and methods; I will overview two here. First, I plan to assess changes in corporate content policies around the passage of the US Fight Online Sex Trafficking Act (FOSTA). There is significant evidence that FOSTA has made sex work more dangerous and sex trafficking harder to combat by pushing both consensual and noncensual sexual solicitation off of known platforms. To quantify and characterize changes in content policies, I will conduct a large-scale content analysis of community guidelines and terms of service relating to sexual content on major websites over the past decade. This will reveal trends in moderation and show the effects of FOSTA across platforms. Second, I will continue measuring the prevalence of geoblocking globally. As more regional privacy laws are enacted with differing scopes and requirements (e.g., in different US states, Brazil's General Law for the Protection of Personal Data), sites may increasingly choose to geoblock regions with effortful regulation rather than attempt to comply with increasingly varied regional laws, as was the case when the European General Data Protection Regulation (GDPR) went into effect. Longitudinal data on geoblocking will shed light on the state of our increasingly fractured Internet and equip advocacy organizations and policymakers to better fight for a globally accessible Internet.

Over the next decade, we are likely to see significant changes globally to privacy laws, corporate content policies (as misinformation and other harmful content are scrutinized), age verification mechanisms, and consumer protection regulations. By deploying a mix of methods to observe and evaluate the impacts of these changes, this line of research will enable policymakers and legislators to see the unintentional consequences of policies and laws, provide data that empowers civil rights groups to more effectively advocate for marginalized groups, and inform future regulation.

References

[FOCI17] Sergey Frolov, Fred Douglas, Will Scott, **Allison McDonald**, Benjamin VanderSloot, Rod Hynes, Adam Kruger, Michalis Kallitsis, David G. Robinson, Steve Schultze, Nikita Borisov, Alex Halderman and Eric Wustrow. 2017. An ISP-Scale Deployment of TapDance. In the *7th USENIX Workshop on Free and Open Communications on the Internet (FOCI'17)*.

[CHI18] Tamy Guberek, **Allison McDonald**, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*.

[IMC18] **Allison McDonald**, Matthew Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. Alex Halderman, and Roya Ensafi. 2018. 403 Forbidden: A Global View of CDN Geoblocking. In *Proceedings of the Internet Measurement Conference 2018 (IMC '18)*.

[Sec18] Benjamin VanderSloot, **Allison McDonald**, Will Scott, J. Alex Halderman and Roya Ensafi. 2018. Quack: Scalable Remote Measurement of Application-Layer Censorship. In *Proceedings of the 27th USENIX Security Symposium (Sec'18)*.

[SP20] Matt Bernhard, **Allison McDonald**, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang and J. Alex Halderman. 2020. Can Voters Detect Malicious Manipulation of Ballot Marking Devices? In *2020 IEEE Symposium on Security and Privacy (SP'20)*.

[CHI21a] **Allison McDonald**, Carlo Sugatan, Tamy Guberek and Florian Schaub. 2021. The Annoying, the Disturbing, and the Weird: Challenges with Phone Numbers as Identifiers and Phone Number Recycling. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI'21)*.

[CHI21b] Catherine Barwulor, **Allison McDonald**, Eszter Hargittai, and Elissa M. Redmiles. 2021. "Disadvantaged in the American-dominated Internet": Sex, Work, and Technology. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI'21).*

[Sec21a] **Allison McDonald**, Catherine Barwulor, Michelle L. Mazurek, Florian Schaub, Elissa M. Redmiles. 2021. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *Proceedings of the 30th USENIX Security Symposium (Sec'21).*

[Sec21b] Yixin Zou, **Allison McDonald**, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, Acar Tamersoy. 2021.The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence. In *Proceedings of the 30th USENIX Security Symposium (Sec'21).*

[UR21] Janet X. Chen*, **Allison McDonald***, Yixin Zou*, Emily Tseng, Kevin A. Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. Trauma-informed computing: Towards safer technology experiences for all. 2021. Under review. (* denotes equal authorship)