Queer Security Advice in the U.S.

Christine Geeng
University of Washington

Mike Harris
University of Washington

Elissa Redmiles
Max Planck Institute for Software Systems

Franziska Roesner
University of Washington

Abstract

We propose a project focusing on the online vulnerabilities of LGBTQ+ individuals specifically and the online safety, security, and privacy advice they seek. To assess where individuals seek advice and the utility of existing LGBTQ+ online security advice, we will conduct semi-structured interviews. Interviews will have questions around where participants learn mechanisms for supporting their online safety, what advice does not work for participants, and what advice they have provided to others.

1 Introduction

With about 90% of Americans using the Internet [4], LGBTQ+ individuals have used social media and other platforms to date and connect with loved ones. But due to the potential stigma attached to a queer identity, particular for transgender and non-binary individuals, the Internet both becomes a safety net to combat alienation [29, 40, 22], as well as a place of harm [40, 19, 46].

Given the specific challenges queer individuals face online, there are many security advice pages online devoted to queer social media usage, dating, sexting, and protests. While there is a lot of security research on where people learn general security advice [36] and how actionable general security advice is [37], these questions remain unanswered for queer-specific security/safety advice.

Our research questions are:

1. What online safety, security, and privacy advice exists for queer individuals, and how does it differ from general security advice?
2. Where do queer individuals in the U.S. learn about mechanisms for supporting their online safety?
3. In what specific contexts does online security advice fail for queer individuals?

We will conduct qualitative interviews with a diverse group of queer individuals across age, race, gender, sexuality, and socioeconomic status. Interviews will consist of questions around where participants learn about online safety and their context for the actions they have or haven't taken in response to security concerns, as well as what kind of online safety, security, or privacy advice they have given to others.

While safety, security, and privacy have different definitions in the academic community, participants will have their own differing or overlapping definitions. Therefore, we will include all terms when interviewing participants to tease apart connections between these concepts and potentially discuss how they differ from academic norms.

This work-in-progress workshop paper will describe our methodology, as data is still in the process of being collected. As we will have finished data collection by the time of the workshop, our goals for attending include getting feedback on preliminary results and brainstorming around the potential for designing an advice tool.

2 Related Work

2.1 Queer Security/Privacy Online

Social Media Ecosystems. Prior work has noted tensions queer individuals face on social media when selectively presenting their queer identity to different audiences, some who they are out to and some they are not out to [8, 17, 12, 20, 40], an issue general known as context collapse [32]. This can be especially stressful for transgender individuals navigating transitioning and coming out on social media [24, 34]. To manage different audiences, individuals use affordances including multiple social media sites or accounts, private accounts, and granular post visibility [17, 12, 20].

Dating and Sexting. Online dating can provide queer individuals connection [45], as a well as space to explore

one's identity [17]. It is also a site of privacy tensions, as users often provide location data, use it to connect with people outside of their known social network, and include more sensitive information in profiles [15].

Sexting through dating apps or through other messaging apps has become a common practice in the U.S. [27], and researchers have highlighted its positive role in relationship satisfaction [11, 18, 43]. Sexting also comes with risks that have worse consequences for women and non-binary individuals [21, 30].

Intersectional Identities. Collins writes that power relations, and by extension harms, should be analyzed via intersections of identities [7], including but not limited to age, gender, race, class and sexuality [16]. Being a woman raises one's risk of being harassed online, and this risk is higher for for queer women and women of color [14]. Black and minoritized women were more likely to see an increase in online abuse during Covid-19 [2]. Bangladeshi Hijra "third gender") have also experienced harassment on social media platforms [33]; researchers note that rather than education on social media privacy affordances being needed, instead social media needs to create community/collective privacy controls due to the strong community values in Hijra culture. When dating apps don't actively design for de-stigmatizing HIV status, platforms reinforce negative stereotypes that stem from the history of criminalization and surveillance of HIV [31]. While these aren't the only identities that intersect with queerness which lead to other vulnerabilities (e.g. LGBTQ+ refugees [5], sex workers), this research provides important context to understanding risk and harm.

This project does not aim to cover every possible security or privacy risk that queer individuals face, given the infinitely different experiences people have. But we will put in effort to recruit diverse participants across at least age, gender, race, class, and sexuality, and we will explicitly state the limitations of our participant pool.

As previous work has focused on the specific concerns that queer individuals have online and their mitigative practices, this project builds on those findings to ask where people learn these behaviors and what sort of advice they have provided others. The goal is to understand the specific contexts where some behaviors are useful or useless and how this knowledge is transferred and communicated.

2.2 Security Advice

Providing security education to users has often been a takeaway from user studies on people's security concerns and practices, especially for marginalized groups [41, 13]. Yet, many researchers note how inactionable general security advice online can be, whether due to the cost-benefit trade-off not being worth it [28], too much advice existing with no prioritization [38], or that "the right advice might change over time with the attack landscape, new technology, and experience" [39]. In an evaluation of security advice specifically for journalists, Berdan echoes this issue of lack of prioritized, contextualized, and actionable advice [6]. Rader discusses how non-expert users may change their behaviors from stories they learn from people, which raises the question of how the source of security advice may affect whether people act on it [36].

The safety priorities and contexts of queer individuals may be different from the general population, and therefore warrant different advice, as "people from different under-served groups may have profoundly different needs and challenges for security and privacy" [48]. Even amongst queer individuals, people's life experiences and concerns are very different [44]. Security advice exists specifically for women [9], gay online dating [1], and queer individuals using Instagram [35], to name a few examples. The Reconfigure Network organized feminist action research and found that contrary to popular cybersecurity narratives that users are uninterested in security, their participants demonstrated care and thoughtfulness in their own and community privacy practices, and their practices are shaped by privilege and oppression [3]. We detail our methodology for studying queer security advice below.

3 Proposed Methodology

To answer our research questions, we will conduct semi-structured qualitative interviews with queer individuals who use social media, dating apps, or apps for sexting. We will aim to have a range of ages, as well as making sure to have BIPOC participants. Participants will be recruited through flyers around the city of Seattle, Washington, as well as through postings in queer listservs and other online communities. Participant payment will be a $30 gift card.

Interview questions will cover:

1. What concerns have participants had about online safety / security / privacy related to queerness? Related to other aspects of their identity? Why do they have these concerns?

2. Have participants ever changed their behaviors to deal with these concerns? How or where did they learn to change their behaviors? Have behavior changes ever failed to solve the problem?

3. Have participants given online safety / security / privacy advice to others?

4. What online advice have participants seen but decided was not for them?

5. If people are unconcerned about online safety / security / privacy, what are they resigned to?

We will intentionally be vague about the terms safety, security, and privacy in order to ask participants to describe it themselves. Due to the potentially harmful memories these interview questions may bring up, we will take steps to mitigate harms from this line of questioning. Participants will be free to skip any question or drop the study, no questions asked, and still receive compensation. We will follow heuristics to ethically conduct research with marginalized populations [47]. Our study was approved by the University of Washington IRB board.

Our epistemological framework is feminist standpoint theory, which calls for an understanding that social knowledge and experiences are situated in a specific context, rather than being objective and generalizable [25, 42]. Rather, our results will be transferable, rather than generalizable [26]. We will respect each participant's responses and knowledge of their concerns and requirements, and will not prioritize our own knowledge as researchers over their own. Interviews will be transcribed by the researchers to avoid third-party access, and names in the data will be anonymized during the transcription process.

We will do inductive thematic analysis [10] to code the data with at least one other coder. We may find that participants do not care about many aspects of their online safety (which is not an uncommon finding in security literature [49]). Or participants may be resigned to the belief that certain institutions already having access to their data [23]. One sexting security study did find that survey participants had concerns around sending and receiving sexts [21]; it may be interested to hear why people may be more concerned over sexting versus managing multiple social media audiences, or over "general" security concerns (like malware). Our pilot interviewees did have much to say about dating and sexting security.

4 Conclusion and Future Work

Our next step will be to conduct this qualitative study. Depending on the data collected, we may either conduct an evaluation of queer online safety advice documents, or conduct participatory workshops with queer individuals to design a contextual online advice tool. This work contribute an understanding of how safety, security, and privacy advice is successfully passed on to more people, particularly for queer individuals who may face specific vulnerabilities from interpersonal relationships and institutions due to stigma around their identities.

By the time of the workshop, we will have preliminary results. We hope attending the workshop will provide valuable feedback on the implications of our results and will generate discussion on an inclusive, contextual understanding of security advice.

5 Author Positionality

Some authors identify as queer and others identify as straight. The authors are either East Asian or white. From an intersectional framework, we recognize that some of us are marginalized across some axes of identity and not others.

References

[1] GRINDR HOLISTIC SECURITY GUIDE. (Accessed on 02/07/2021).

[2] The ripple effect: Covid-19 and the epidemic of online abuse. https://fixtheglitch.org/wp-content/uploads/2020/09/Glitch-COVID-19-Report-final-1.pdf, Sep 2020. (Accessed on 02/07/2021).

[3] Reconfigure: Feminist action research in cybersecurity. https://www.oii.ox.ac.uk/wp-content/uploads/2021/01/Reconfigure-Report-v6-pages.pdf, Feb 2021. (Accessed on 02/17/2021).

[4] ANDERSON, M., PERRIN, A., JIANG, J., AND KUMAR, M. 10% of americans don't use the internet — pew research center. https://www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they/, April 2019. (Accessed on 02/09/2021).

[5] ANDREASSEN, R. Social media surveillance, lgbtq refugees and asylum. *First Monday* (2021).

[6] BERDAN, K. An evaluation of online security guides for journalists. https://cltc.berkeley.edu/wp-content/uploads/2021/01/Online_Security_Guides_for_Journalists.pdf.

[7] BILGE, S., AND COLLINS, P. H. Intersectionality. *Cambridge, UK: Polity* (2016).

[8] BLACKWELL, L., HARDY, J., AMMARI, T., VEINOT, T., LAMPE, C., AND SCHOENEBECK, S. Lgbt parents and social media: Advocacy, privacy, and disclosure during shifting social movements. In *Proceedings of the 2016 CHI conference on human factors in computing systems* (2016), pp. 610–622.

[9] BLUE, V. *The Smart Girl's Guide to Privacy: Practical Tips for Staying Safe Online*. No Starch Press.

[10] BRAUN, V., AND CLARKE, V. Using thematic analysis in psychology. *Qualitative research in psychology 3*, 2 (2006), 77–101.

[11] BURKETT, M. Sex (t) talk: A qualitative analysis of young adults' negotiations of the pleasures and perils of sexting. *Sexuality & Culture 19*, 4 (2015), 835–863.

[12] CARRASCO, M., AND KERNE, A. Queer visibility: Supporting lgbt+ selective visibility on social media. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018), pp. 1–12.

[13] CHEN, C., DELL, N., AND ROESNER, F. Computer security and privacy in the interactions between victim service providers and human trafficking survivors. In *28th {USENIX} Security Symposium ({USENIX} Security 19)* (2019), pp. 89–104.

[14] CITRON, D. K. *Hate crimes in cyberspace*. Harvard University Press, 2014.

[15] COBB, C., AND KOHNO, T. How public is my private life? privacy in online dating. In *Proceedings of the 26th International Conference on World Wide Web* (2017), pp. 1231–1240.

[16] CRENSHAW, K. Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *u. Chi. Legal f.* (1989), 139.

[17] DEVITO, M. A., WALKER, A. M., AND BIRNHOLTZ, J. 'too gay for facebook' presenting lgbtq+ identity throughout the personal social media ecosystem. *Proceedings of the ACM on Human-Computer Interaction 2*, CSCW (2018), 1–23.

[18] DROUIN, M., COUPE, M., AND TEMPLE, J. R. Is sexting good for your relationship? It depends.... *Computers in Human Behavior 75* (2017), 749–756.

[19] GAY, L., NETWORK, S. E., ET AL. Out online: The experiences of lesbian, gay, bisexual and transgender youth on the internet. *New York, NY* (2013).

[20] GEENG, C. LGBTQ privacy concerns on social media. In *Proceedings of the 2018 CHI Conference Workshops and Symposia on Human Factors in Computing Systems*, ACM Press.

[21] GEENG, C., HUTSON, J., AND ROESNER, F. Usable sexurity: Studying people's concerns and strategies when sexting. In *Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020)* (2020), pp. 127–144.

[22] GRAY, M. L. Negotiating identities/queering desires: Coming out online and the remediation of the coming-out story. *Journal of Computer-Mediated Communication 14*, 4 (2009), 1162–1189.

[23] GUBEREK, T., MCDONALD, A., SIMIONI, S., MHAIDLI, A. H., TOYAMA, K., AND SCHAUB, F. 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*, ACM Press, pp. 1–15.

[24] HAIMSON, O. L., BRUBAKER, J. R., DOMBROWSKI, L., AND HAYES, G. R. Disclosure, Stress, and Support During Gender Transition on Facebook. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, ACM, pp. 1176–1190.

[25] HARAWAY, D. Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist studies 14*, 3 (1988), 575–599.

[26] HATCH, J. A. *Doing qualitative research in education settings*. Suny Press, 2002.

[27] HERBENICK, D., BOWLING, J., FU, T.-C., DODGE, B., GUERRA-REYES, L., AND SANDERS, S. Sexual diversity in the united states: Results from a nationally representative probability sample of adult women and men. *PloS one 12*, 7 (2017), e0181198.

[28] HERLEY, C. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop* (New York, NY, USA, 2009), NSPW '09, Association for Computing Machinery, p. 133–144.

[29] HILLIER, L., MITCHELL, K. J., AND YBARRA, M. L. The internet as a safety net: Findings from a series of online focus groups with lgb and non-lgb young people in the united states. *Journal of LGBT Youth 9*, 3 (2012), 225–246.

[30] LENHART, A., YBARRA, M., AND PRICE-FEENEY, M. Nonconsensual image sharing: one in 25 americans has been a victim of" revenge porn".

[31] LIANG, C., HUTSON, J. A., AND KEYES, O. Surveillance, stigma & sociotechnical design for hiv. *First Monday* (2020).

[32] MARWICK, A. E., AND BOYD, D. Networked privacy: How teenagers negotiate context in social media. *New media & society 16*, 7 (2014), 1051–1067.

[33] NOVA, F. F., DEVITO, M. A., SAHA, P., RASHID, K. S., ROY TURZO, S., AFRIN, S., AND GUHA, S. " facebook promotes more harassment" social media ecosystem, skill and marginalized hijra identity in bangladesh. *Proceedings of the ACM on Human-Computer Interaction 5*, CSCW1 (2021), 1–35.

[34] PINTER, A. T., SCHEUERMAN, M. K., AND BRUBAKER, J. R. Entering doors, evading traps: Benefits and risks of visibility during transgender coming outs. *Proceedings of the ACM on Human-Computer Interaction 4*, CSCW3 (2021), 1–27.

[35] PROJECT, T. T. PROTECT YOUR SPACE AND WELL-BEING ON INSTAGRAM. `https://www.thetrevorproject.org/wp-content/uploads/2019/06/IG-x-Trevor-Project_LGBTQ-Safety-Guide.pdf`. (Accessed on 02/07/2021).

[36] RADER, E., WASH, R., AND BROOKS, B. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (New York, NY, USA, 2012), SOUPS '12, Association for Computing Machinery.

[37] REDMILES, E. M. "Should I Worry?" a cross-cultural examination of account security incident response. In *2019 IEEE Symposium on Security and Privacy (SP)* (2019), IEEE, pp. 920–934.

[38] REDMILES, E. M., WARFORD, N., JAYANTI, A., KONERU, A., KROSS, S., MORALES, M., STEVENS, R., AND MAZUREK, M. L. A comprehensive quality evaluation of security and privacy advice on the web. In *29th {USENIX} Security Symposium ({USENIX} Security 20)* (2020), pp. 89–108.

[39] REEDER, R. W., ION, I., AND CONSOLVO, S. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy 15*, 5 (2017), 55–64.

[40] SCHEUERMAN, M. K., BRANHAM, S. M., AND HAMIDI, F. Safe spaces and safe places: Unpacking technology-mediated experiences of safety and harm with transgender people. *Proceedings of the ACM on Human-Computer Interaction 2*, CSCW (2018), 1–27.

[41] SIMKO, L., LERNER, A., IBTASAM, S., ROESNER, F., AND KOHNO, T. Computer security and privacy for refugees in the united states. In *2018 IEEE Symposium on Security and Privacy (SP)* (2018), IEEE, pp. 409–423.

[42] SLUPSKA, J., DAWSON DUCKWORTH, S. D., MA, L., AND NEFF, G. Participatory threat modelling: Exploring paths to reconfigure cybersecurity. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–6.

[43] STASKO, E. C., AND GELLER, P. A. Reframing sexting as a positive relationship behavior. Drexel University, 2015. `https://www.apa.org/news/press/releases/2015/08/reframing-sexting.pdf`.

[44] SULLIVAN, N. *A critical introduction to queer theory*. NYU Press, 2003.

[45] TAYLOR, S. H., HUTSON, J. A., AND ALICEA, T. R. *Social Consequences of Grindr Use: Extending the Internet-Enhanced Self-Disclosure Hypothesis*. Association for Computing Machinery, New York, NY, USA, 2017, p. 6645–6657.

[46] THOMAS, K., AKHAWE, D., BAILEY, M., BONEH, D., BURSZTEIN, E., CONSOLVO, S., DELL, N., DURUMERIC, Z., KELLEY, P. G., KUMAR, D., MCCOY, D., MEIKLEJOHN, S., RISTENPART, T., AND STRINGHINI, G. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In *IEEE Symposium on Security and Privacy (SP)* (2021).

[47] WALKER, A. M., YAO, Y., GEENG, C., HOYLE, R., AND WISNIEWSKI, P. Moving beyond'one size fits all' research considerations for working with vulnerable populations. *Interactions 26*, 6 (2019), 34–39.

[48] WANG, Y. The third wave? inclusive privacy and security. In *Proceedings of the 2017 New Security Paradigms Workshop* (New York, NY, USA, 2017), NSPW 2017, Association for Computing Machinery, p. 122–130.

[49] ZENG, E., MARE, S., AND ROESNER, F. End user security and privacy concerns with smart homes. In *thirteenth symposium on usable privacy and security ({SOUPS} 2017)* (2017), pp. 65–80.