Gender & Digital Security

RESULTS FROM A SCOPING STUDY

By Maya Indira Ganesh,
on behalf of the Citizen Lab

Copyright

Document Version: 1.0

IDRC | CRDI
International Development Research Centre
Centre de recherches pour le développement international

gender at work

Contents

→ Scoping study on gender and digital security 4

→ Highlights 4

→ Citizen Lab's Work on Gender and Digital Security 5

DEFINITIONS 5

PRIOR RESEARCH 5

→ Mapping the Gender and Digital Security Landscape 8

FINDINGS FROM THE INTERVIEWS 8

Differing frames among the respondents 8

Digital security as infrastructure for human rights movements 9

"We are stuck in 2011" 10

Accountability of technology companies 11

→ Research and Knowledge Gaps in Gender and Digital Security 12

TARGETED THREATS 12

FREE EXPRESSION ONLINE 14

APP PRIVACY AND SECURITY 15

TRANSPARENCY AND ACCOUNTABILITY 15

→ Conclusion 17

→ Works Cited 18

Scoping study on gender and digital security

In Fall 2018, the Citizen Lab commissioned a scoping study in the context of its existing research streams—Targeted Threats, Freedom of Expression Online, App Privacy and Controls, and Transparency and Accountability.[1] The purpose of the scoping study was to identify gaps relevant to these research areas in the field of gender and digital security.[2] Findings from this scoping study aim to inform the Citizen Lab's objective of producing evidence-based research on gender and digital security that enhances understanding and builds capacity, especially of partners in the Global South, as part of efforts to ensure a more open, secure, and equitable Internet.

Conducted over seven months, the scoping study included 30 interviews with Citizen Lab staff, partners, donors, and relevant experts, a review of academic and non-academic research literature, and group discussions with members of the Citizen Lab. This report contains a summary of the scoping study's results and it proceeds as follows: first, it outlines the Lab's work on gender and digital security; second, it maps the landscape of research and advocacy in this field and discusses the interviews' findings; and finally, it highlights some of the research gaps that are relevant to the Citizen Lab's work.

Highlights

- ✦ Organisational, legal, psycho-social, and educational resources to sustain digital security practices in human rights defence do exist, but they are limited by a lack of infrastructure and funding to maintain up-to-date training for security trainers and educators.

- ✦ Interviewees cited a lack of platform and corporate accountability for gendered attacks on social media. However, some argued that by expecting technological "fixes" to such issues to come from the companies themselves, it would only strengthen the position of social media companies, and perpetuate power imbalance between tech companies and individuals.

[1] "Research Archives," The Citizen Lab, accessed August 6, 2020, https://citizenlab.ca/category/research/.

[2] Throughout this report, 'gender' is the variable we mention most often to qualify this study of digital security. However, this study was developed in accordance with the Lab's commitment to an intersectional approach that aims for equity among and between different communities. Thus, the study was interested in digital security in the context of women-identifying people and those who are of non-normative genders, sexualities, caste, race, religious and Indigenous backgrounds, and are from Majority World backgrounds.

- As new technologies emerge, their implications upon gender and digital security research and practice will require further study. Equally, the accountability mechanisms of the social media and technology companies who may enable online abuse and gendered digital attacks will require a multidisciplinary analysis.

Citizen Lab's Work on Gender and Digital Security

DEFINITIONS

The Citizen Lab adopts definitions of gendered digital security threats and privacy violations that name particular behaviours and acts that can be clearly identified and mapped, such as interpersonal and targeted surveillance, verbal abuse, blackmail, "doxxing," threats, and non-consensual image sharing, among others.[3] The Lab adopts this approach following the work of groups such as the Association for Progressive Communications (APC) Women's Rights Program, which have named 13 manifestations of "gender-based violence using technology," including acts that indicate controls on access to information or use of the Internet, such as "attacks on communication channels" and "omissions by regulatory actors."[4] This approach to digital security shifts focus away from the victimised individual and from the interpersonal dynamics of an attack to both the actors involved in co-ordinated and distributed attacks that force people offline, as well as to the inaction of legal or regulatory bodies to take attacks on women seriously.

PRIOR RESEARCH

The Citizen Lab, an interdisciplinary research lab on cybersecurity and human rights based at the University of Toronto's Munk School of Global Affairs & Public Policy has documented the gendered and sexualised dimensions of digital security. Prior research by the Lab's partners in the Cyber Stewards

[3] Doxxing is "a complex, gendered communicative process by which one or several person(s) (doxxer/doxxers) seek private or personal identifying information about another individual (subject/target) and widely distribute it through undesired online mass media channels without the consent of that person, who would be made vulnerable by mass media disclosure." Stine Eckert and Jade Metzger- Riftkin, "Doxxing," in *The International Encyclopedia of Gender, Media, and Communication* (American Cancer Society, 2020), 1–5, https://doi.org/10.1002/9781119429128.iegmc009.

[4] These 13 manifestations include: "unauthorised and controlling access [of devices], control and manipulation of information, impersonation and identity theft, surveillance and stalking, discriminatory speech, harassment, threats, non-consensual sharing of private information, extortion, disparagement, technology related sexual abuse and exploitation, attacks on communication channels, omissions by regulatory actors." See: "13 Manifestations of GBV Using Technology," Take Back the Tech (Association for Progressive Communications and Luchadoras and SocialTIC, August 17, 2018), https://www.takebackthetech.net/blog/13-manifestations-gbv-using-technology.

Network (CSN) illustrates the importance of addressing the intersectional impact of technology-facilitated abuse.[5] For example, research by CSN partners Sula Batsu in Costa Rica and Colnodo in Colombia illustrates how advancements in information and communication technologies (ICTs) have resulted in negative externalities for women civil society members, such as journalists and human rights defenders (HRDs).[6] The study found that these women, especially those living in rural areas, face multiple levels of risk.[7] They not only confront powerful actors with entrenched economic interests, but their public leadership roles are also seen as violating prevailing gender norms. In addition, their economic conditions (e.g., poverty) may limit their access to legal recourse and their regional or ethnic origin (e.g., as members of religious or ethnic minority groups) may heighten their vulnerability.

Colnodo and Sula Batsu's study also underscores that online and offline threats should not be viewed as separate phenomena, but rather as overlapping and mutually reinforcing. With regard to digital surveillance of rights activists, this research found that surveillance has led to the collection of personal or professional information and the use of intimidation tactics, such as physical violence, harassment, intimidation, and even murder.[8] Given persistent challenges, evidence-based research is necessary to continue to uncover the unintended impacts of ICTs, and to examine the ways that various interests or communities (e.g., lesbian, gay, bisexual, transgender, intersex, and queer (LGBTIQ) and rural or Indigenous communities) are systematically excluded from discussions and policymaking around the security of the Internet.

The Citizen Lab has published reports that illustrate the gendered impact of digital security. Its reports on the use of the NSO Group's Pegasus spyware in Mexico—produced in collaboration with Mexican digital rights organizations Red en Defensa de los Derechos Digitales (R3D), SocialTic, and ARTICLE 19—found that targets included a well-known female journalist and her minor child, a prominent female lawyer representing the families of three slain women, and the wife of a murdered journalist, who was a reporter herself.[9]

[5] The Cyber Stewards Network is a global network of researchers and advocates working on various cybersecurity issues, funded by Canada's International Development Research Centre (IDRC). See: "Global Research Network Archives," The Citizen Lab, accessed August 18, 2020, https://citizenlab.ca/category/research/global-research-network/.

[6] Irene Poetranto, *Threats Facing Women Activists in Colombia and Costa Rica* (The Citizen Lab, August 26, 2020), https://citizenlab.ca/2020/08/threats-facing-women-activists-in-colombia-and-costa-rica/.

[7] Ibid.

[8] Ibid.

[9] John Scott-Railton et al., *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware* (The Citizen Lab, June 19, 2017), https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/; John Scott-Railton et al., *Reckless IV: Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware* (The Citizen Lab, August 2, 2017), https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/; John Scott-Railton et al., *Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware* (The Citizen Lab, March 20, 2019), https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/.

The Citizen Lab has also published reports on 'stalkerware' or 'spousalware,' which are tools with powerful surveillance capabilities that are used to facilitate intimate partner violence, abuse, or harassment.[10] The study focused on eight companies that appeared to be the most popular in the Canadian, American, and Australian commercial markets: FlexiSPY, Highster Mobile, Hoverwatch, Mobistealth, mSpy, TeenSafe, TheTruthSpy, and Cerberus. The report concludes that anyone who uses stalkerware is potentially breaking a number of laws, but thus far, the authorities in these jurisdictions have failed to curb its use and spread.[11]

In taking a gendered and intersectional approach to digital rights research, the Citizen Lab also accounts for the related but unique circumstances for LGBTIQ populations. Digital spaces are integral to providing access to potentially life-saving information, particularly around HIV/AIDS, as well as to connect, share resources, and form strong social bonds with one another as part of a wider community.[12] However, Citizen Lab's past research has shown that LGBTIQ news, lifestyle, and health websites are often targets of censorship.[13] Such censorship not only infringes on fundamental human rights, but also further isolates LGBTIQ community members living in societies that might criminalize their very existence.

Recognizing that women and girls are not only disproportionately targeted for online harassment in general, but also face unique gender-specific threats, the Citizen Lab made a submission to the United Nations Special Rapporteur on violence against women, its causes and consequences, Dr. Dubravka Šimonović, in preparation for her report to the Human Rights Council in June 2018.[14] Their submission makes a series of recommendations so that the Special Rapporteur is fully informed about the particular threats to women and girls online and can best advise states and various UN bodies to act appropriately. The Lab's submission highlights that further research is required to examine the consequences of censorship and other forms of information controls experienced by different genders, sexualities, and minority groups.

[10] Christopher Parsons et al., *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry* (The Citizen Lab, June 12, 2019), https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/.

[11] Anita Elash, "It's Time to Start Charging People for Using Stalkerware to Harass Their Partners, Watchdog Group Says," *CBC*, June 12, 2019, https://www.cbc.ca/news/technology/stalkerware-cell-phone-abuse-women-citizen-lab-1.5171458.

[12] Ronald Deibert, Adam Senft, and Miles Kenyon, *Identities in the Crosshairs—Censoring LGBTQ Internet Content around the World*, OpenGlobalRights, accessed August 6, 2020, https://www.openglobalrights.org/identities-in-the-crosshairs-censoring-LGBTQ-internet-content-around-the-world/.

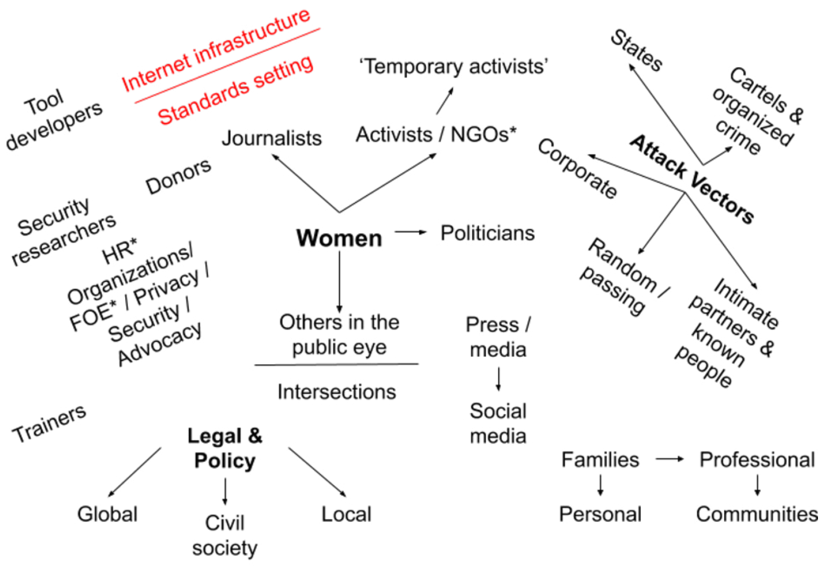
[13] Jakub Dalek et al., "Planet Netsweeper: Executive Summary" (The Citizen Lab, April 25, 2018), https://citizenlab.ca/2018/04/planet-netsweeper/.

[14] Ronald Deibert et al., *Submission to the UN Special Rapporteur on Violence Against Women* (The Citizen Lab, November 3, 2017), https://citizenlab.ca/2017/11/submission-un-special-rapporteur-violence-women-causes-consequences/.

Mapping the Gender and Digital Security Landscape

The scoping study included a 'landscape mapping' exercise with the interviewees. The purpose was to identify the actors working on or influencing the field of 'gender and digital security,' and the interrelationships between these actors. In total, 22 civil society technologists, including digital security experts and trainers, feminist activists, human rights defenders, policy experts, and donors were interviewed using this landscape mapping technique.

Instead of using a typical interview guide as the basis for the interviews, the landscape mapping approach centred the discussion around a hand-drawn sketch of what the researcher perceived as the 'field' of gender and digital security. Working as a provocation and a prompt, the sketch invited interviewees to place themselves on it, comment on the boundaries of this field itself, and how it might be changing and shaped by relationships between different actors. A summary of the themes that emerged from these interviews follows.



* HR = Human Rights; FOE = Freedom of Expression; NGOs = Non-Governmental Organizations

A digitized version of the researcher's hand-drawn sketch of her perception of the 'landscape'.

FINDINGS FROM THE INTERVIEWS

Differing frames among the respondents

A frame determines how an individual or a project or organisation will privilege a particular topic, the other domains and communities it will influence, and how it will be funded and sustained in the long term. The frames mentioned by the interviewees included "Internet freedom and democracy," "justice and rights," and "ethics." Respondents presented different, shifting frames around the fields of technology and human rights, as well as Internet activism and digital rights, within which the relatively new sub-domain of gender and digital security is thought to be situated.

Each frame implies a different kind of approach to how security is perceived, implemented, or funded, and whether it is considered as a priority or not for a particular community. The relatively new frame of "public interest tech" emerging in the United States, for example, brings together law, policy, and technology to "promote the public good."[15] However, this framing does not explicitly centre human rights, whereas some of the others listed in this document do. Addressing gendered digital attacks as a human rights issue entails applying specific approaches to research, mitigation, and advocacy with particular actors, which is in contrast to the public interest approach.

Digital security as infrastructure for human rights movements

There are limited organisational, legal, psycho-social, and educational resources to sustain digital security practices in human rights defence. In their short survey, the technology non-profit Aspiration also found that there is no infrastructure in place to effectively sustain a culture and practice of security that is grounded in the realities of human rights defence.[16] The approach to digital security education for human rights activists has been interventionist (i.e., implemented only after attacks have happened) rather than organically built to proactively generate critical technical literacy in networks and movements. The latter approach requires longer-term accompaniment and support to communities that have been difficult to fund and sustain. Furthermore, because security threats continue to change shape, security trainers and educators themselves—many of whom work in HRD communities—find it difficult to maintain skills development and training in order to best serve their communities. Finally, security work in this field can be relatively dangerous for experts themselves.[17]

Feminist approaches to infrastructure and security

One strand of feminist engagement with digital security investigates how Internet infrastructure is implicated in digital attacks. Mallory Knodel and Juliana Guerra examined documents and processes at the Internet Engineering Task Force (IETF) to ask: "How might security engineering change if the realities of digital insecurity as experienced by the most vulnerable in society informed technical specifications?"[18]

[15] Bruce Schneier compiles a variety of definitions and resources. See: Bruce Schneier, "Public-Interest Technology Resources," July 4, 2020, https://public-interest-tech.com/.

[16] Beatrice, *Forging Careers in Human Rights Information Security Today: A Network Survey of Sustainability Challenges and Opportunities for Information Security Practitioners in the Human Rights Sector* (Aspiration Tech, January 8, 2019), https://aspirationtech.org/humanrights/reports/practitionersustainabilitysurvey.

[17] In 2018-19, the Citizen Lab's own researchers have been targets of social engineering. See: Ronald Deibert, "*Statement from Citizen Lab Director on Attempted Operations Against Researchers*," *The Citizen Lab* (blog), January 25, 2019, https://citizenlab.ca/2019/01/statement-from-citizen-lab-director-on-attempted-operations-against-researchers/; The Citizen Lab's colleagues from Amnesty International Turkey, among others, were detained and arrested by Turkish authorities in a crackdown on activists in the country. See: "Turkey: Year in Detention for Amnesty Chair a '*Gross Injustice*,'" *Amnesty International* (blog), June 6, 2018, https://www.amnesty.org.uk/press-releases/turkey-year-detention-amnesty-chair-gross-injustice.

[18] J Guerra and M Knodel, *Feminism and Protocols (Internet Engineering Task Force*, March 11, 2019), https://tools.ietf.org/id/draft-guerra-feminism-00.html.

For example, how would the protocols guiding the development of email or text messages change if women could redesign them from the perspective of the technology-mediated harassment they face? Knodel and Guerra argue that responding to online abuse is not only a matter of teaching and learning digital security practices, but also about eventually imagining an entirely different Internet, which is built from (or at least meaningfully include) the perspective of people who are more vulnerable to online attacks.[19]

Stuck in the Past

“We are stuck in the 2011 mindset” is how one interview respondent characterised the shaping of digital security between 2010-2014. At the time, security was framed in terms of protecting highly visible activists and journalists who were being digitally targeted by authoritarian states.[20] The respondent went on to assert that Western media narratives positioned social media platforms as enabling and shaping the voice of civil society against corrupt, authoritarian regimes, a narrative that has since been critiqued.[21] In this process, freedom of expression became atomised into activism both on and organized through social media platforms. Thus, the freedom of expression of those working on securing the right to freedom of expression has shaped a unique movement of its own.

Restrictions on the freedom of expression of rights defenders who work entirely offline, on the other hand, are often not addressed until they are victimised, such as the cases of Sabeen Mahmud and Berta Caceres.[22] Multiple interviewees argued that the scale of violent attacks on land rights and environmental activists implies an urgent need to scale up digital security and other security measures for these communities.[23] Interviewees encouraged more synergies between ‘Internet freedom’ and other human rights activist movements.

[19] “Feminist Principles of the Internet,” August 26, 2016. https://feministinternet.org/en.

[20] One example is the Citizen Lab’s investigation into the use of Finfisher software against activists, journalists and bloggers as detailed in their 2013 report. See: Morgan Marquis-Boire et al., You Only Click Twice: FinFisher’s Global Proliferation - Citizen Lab (The Citizen Lab, March 13, 2013), https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

[21] Maeve Shearlaw, “Egypt Five Years on: Was It Ever a ‘Social Media Revolution’?,” The Guardian, January 25, 2016, sec. World news, https://www.theguardian.com/world/2016/jan/25/egypt-5-years-on-was-it-ever-a-social-media-revolution.

[22] Sabeen Mahmud was an outspoken human rights activist and social worker in Karachi, Pakistan. She was shot point-blank in the head on her way home from hosting a debate on the Balochistan conflict. See: “Karachi’s Wild Child; Sabeen Mahmud,” *The Economist*, May 2, 2015, https://www.economist.com/obituary/2015/05/02/karachis-wild-child; Berta Caceres was a Lenca indigenous rights activist in Honduras who defended Lenca land rights for over two decades; her organization COPINH successfully prevented the construction of a dam on the Gualcarque River. In March of 2016, unidentified assailants broke into her house and murdered her in her bedroom. See: “Case History: Berta Cáceres,” Front Line Defenders, December 5, 2018, https://www.frontlinedefenders.org/en/case/case-history-berta-c%C3%A1ceres.

[23] *Front Line Defenders’ New Global Analysis Shows 77% of Attacks Connected to Defense of Land, Environment & Indigenous Rights* (Business & Human Rights Resource Centre, December 7, 2018), https://www.business-humanrights.org/en/front-line-defenders-new-global-analysis-shows-77-of-attacks-connected-to-defense-of-land-environment-indigenous-rights.

Accountability of technology companies

The Citizen Lab's recent assessment of the legal landscape in Canada as it relates to the stalkerware apps industry found that "many of the companies studied were actively promoting their software for the purposes of facilitating stalking and, by extension, intimate partner violence, abuse, and harassment."[24] In Canada, even though laws that "criminalize domestic abuse, harassment, and serious invasions of privacy" and "prohibit many forms of technology-facilitated abuses, including the use, sale, and/or distribution of spyware" already exist, there remains a measurable gap between what the law dictates about stalkerware use and whether legal remedies are readily available to victims in practice.[25] At the time of the report's publication, there were no reported criminal prosecutions in Canada for cases involving mobile phone spyware apps used for intimate partner surveillance.[26]

With regard to attacks perpetrated on social media platforms, attackers are often shielded by the anonymity offered by the platform.[27] Questions of platform and corporate accountability for gendered attacks came up repeatedly across interviews. Interviewees maintained that expecting companies to mitigate attacks contributes to their power accrual by encouraging the development of technological 'fixes' to social problems. Some of these interviewees suggested that the social, cultural, and political dimensions of online abuse had to be addressed through a combination of public education, law, and policy, rather than fixed computationally by platforms. However, interviewees do acknowledge that some specific kinds of attacks could be mitigated by platforms, such as "dogpiling" and the generation of sock puppet accounts.[28]

[24] Parsons et al., *The Predator in Your Pocket.*

[25] Cynthia Khoo, Kate Robertson, and Ronald Deibert, *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications* (The Citizen Lab, June 12, 2019), https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/.

[26] Ibid.

[27] Emily Van der Nagel and Jordan Frith, "Anonymity, Pseudonymity, and the Agency of Online Identity: Examining the Social Practices of r/Gonewild," *First Monday* 20, no. 3 (February 22, 2015), https://doi.org/10.5210/fm.v20i3.5615.

[28] In their article titled "Online Harassment and Content Moderation: The Case of Blocklists," Jhaver et al. define the term "dogpiling" as: " Many users posting messages addressed to a single individual. The intent of any sender may not be to perpetrate harassment, but it results in the targeted individual feeling vulnerable." See: Shagun Jhaver et al., "Online Harassment and Content Moderation: The Case of Blocklists," ACM Transactions on Computer-Human Interaction 25, no. 2 (March 22, 2018): 12:1–12:33, https://doi.org/10.1145/3185593; Jhaver et al. define "sockpuppeting" as: " Using an alternate account to post anonymously on social media. This is often done to feign a wider support of one's own postings." See: Jhaver et al., "Online Harassment and Content Moderation."

Research and Knowledge Gaps in Gender and Digital Security

The landscape mapping, reviews of academic and non-academic research literature, and interviews with the Lab's partners and staff revealed the following gaps thought to exist in research.[29]

TARGETED THREATS

New questions for future research on targeted digital threats that emerged from the interviews (see "Future research questions" below) can be categorised in two streams, broadly.

1. The first stream refers to work that would seek to actively respond to existing gaps in the law, society, and technology that introduce gendered vulnerabilities. For instance, research efforts that complement and support work to mitigate attacks, as well as advocacy, legal, or policy efforts to directly address the impact of digital attacks on human rights defenders, journalists, democratically elected leaders, and activists.

2. The second stream examines the conditions of law, policy, and technology that enable or prevent digital attacks, and the implications they exert upon civil society. For example, legal, theoretical, and empirical social science research about surveillance, privacy, freedom of speech and expression, platform accountability, and security.

These two streams of research are not necessarily mutually exclusive, but require prioritisation and collaborative partnerships, for instance, between civil society and technical communities. Citron and Penney's paper is an example of one which combines legal research with empirical work to challenge the claim that online harassment laws would stifle online expression. On the contrary, they find that the law's expressive function could be harnessed to actively support victims of online harassment to speak about the attacks they face, and infuse caution and thoughtfulness in the speech of others online who do not consider themselves to be the victims of gendered digital attacks.[30] More such creative methodological approaches could address the intersections of gender and digital security.

[29] Some of these questions were directly framed by the Lab's partners and landscape-mapping respondents' thus the names of those comfortable with being publicly credited are included at the end of this document.

[30] Danielle Keats Citron, Jon Penney, and Danielle Keats Citron, "When Law Frees Us to Speak," Fordham Law Review, U of Maryland Legal Studies Research Paper, 87 (January 2, 2019): 2317.

Targeted Threats Research Gap: *More contextualized and disaggregated data and qualitative studies about gendered digital security attacks are required. The shifting landscapes and systemic challenges of digital security education requires more critical discussion and research.*

Although studies on children or teenagers facing digital online attacks exist, there are generally fewer academic studies into the experiences of adults as targets of digital security attacks.[31] There is also a lack of academic research that disaggregates data about digital attacks by gender identity, age, race, class, caste, and Indigeneity. The focus of research in Western contexts (e.g., Australian, British, Irish, European, and North American) and across a variety of Social Science disciplines, from Psychology to Education to Urban Studies, has traditionally been that of children, youth, and young adults. Cyber-bullying, online victimisation by familiar and unknown people, and the romantic and sexual relationships of youth online also tend to be the thematic focus of this work.

In contrast, research by civil society and in the field of journalism focuses on attacks on women journalists, human rights defenders, and Indigenous and land rights activists. However, when these analyses do not specify the details of how attacks take place, where they originate from, and who the attackers are, it makes it difficult to hold attackers to account. As a result, contemporary civil society research and advocacy tend to emphasize on the impact of attacks and the importance of digital security and privacy training for people to protect themselves. Future qualitative and quantitative work could be disaggregated to reveal the specific dynamics of abuse through various technologies and platforms, potentially allowing for a more granular and contextualised approach to prevention, mitigation, and, most critically, accountability.

Future research questions

- ✦ How do state actors use online and offline tactics to engineer co-ordinated, large scale, systematic gendered and sexualized attacks on high profile journalists, writers, and activists? What are the similarities and differences in attacks that happen on men and women of similar public profiles? How might evidence of these attacks be compiled and presented so that they are accessible and easily understood?

- ✦ How does the frame of "digital security-as-infrastructure for human rights movements, journalism, and civil society" shape approaches to digital security and privacy practices and education? What kinds of ongoing 'accompaniment' might be possible through the development of new cadres of digital security 'maintainers'—like systems administrators—to support the digital security needs of HRDs and activist movements and organisations?

[31] Nicola Henry and Anastasia Powell, "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research:," *Trauma, Violence, & Abuse*, June 16, 2016, https://doi.org/10.1177/1524838016650189; See: Li et al. (2012); Kowalski et al. (2014); and Abreu and Kenny (2018) for research on the cyber-bullying faced by children and teenagers.

- How might critical assessments of different types of security training and education, from more traditional approaches to holistic, feminist, or intersectional approaches, contribute to the creation of more effective tools, strategies, and infrastructure for human rights?

- How effective are digital security education and technical literacy programs in supporting activists, journalists, human rights defenders and others in response to digital attacks? What are the local, contextual methods that specific communities develop in response to the attacks they face?

FREE EXPRESSION ONLINE

Future research questions

- Moving the focus away from attacks on individuals, how has women's, queer and trans* people's, feminist, and Black, Indigenous and people of color (BIPOC) speech online been restricted through various kinds of attacks on speech, attacks on movements or campaigns, disinformation, coordinated attacks on influential individuals, and network-level or algorithmic filtering of content? What methods can we use to measure this censorship? And how do particular communities push back against censorship? What kinds of tactics do they use? For example, the 'Free the Nipple' campaign has emerged as a response to nudity laws on social media platforms.[32]

- There is a body of culturally specific and theoretically rigorous civil society/ practitioner research and academic research about gender, sexuality, and surveillance. How might this work be expanded, as well as included into legal and other accountability measures around freedom of speech and expression online?

- What sort of updates are required to traditional legal notions of speech and expression online considering the global scale of the Internet and the diversity of gendered attacks taking place? How can law and policy address gendered digital attacks and online abuse from a variety of different positions such as standpoint theory, a feminist ethics of care, or intersectionality, and not just that of 'freedom of speech and expression'? [33]

[32] Sarah Myers West, "Raging Against the Machine: Network Gatekeeping and Collective Action on Social Media Platforms," *Media and Communication* 5, no. 3 (September 22, 2017): 28–36, https://doi.org/10.17645/mac.v5i3.989.

[33] Brenda Allen explains that standpoint theory "contends that humans produce knowledge through power relations that construct and divide social groups into dominant and nondominant categories. Experiences within those categories produce different, unequal opportunities that cultivate distinct ways of knowing and being." See: Brenda J. Allen, "Standpoint Theory," in *The International Encyclopedia of Intercultural Communication* (American Cancer Society, 2017), 1–9, https://doi.org/10.1002/9781118783665.ieicc0234.; Bogaert and Ogunbanjo explain the concept of the feminist ethics of care in their article: "care is a core femininist value [...] Instead of following general ethical rules (for example, respect for autonomy), one does what the "loving" thing is to do in the given circumstances." See: Knapp D. van Bogaert and G. A. Ogunbanjo, "Feminism and the Ethics of Care," South African Family Practice 51, no. 2 (March 1, 2009): 116–18, https://doi.org/10.1080/20786204.2009.10873822; Kimberle Crenshaw coined the term "intersectionality" in 1989 and offers a threefold

APP PRIVACY AND SECURITY

App Privacy and Security Research Gap: *The need to consider new emerging technologies and their implications for gender and digital security research and practice.*

A quantitative survey of over 5,000 Australian and British adults by Powell, Scott and Henry found that those who are marginalised because of their gender identity or sexual orientation face significant abuse online but that this phenomenon tends to be under-reported.[34] ARTICLE 19 documents the risks of using social media and dating apps for LGBTIQ communities in Egypt, Iran, and Lebanon. These risks include entrapment by the police in Egypt, state surveillance of Iranian LGBTIQ Telegram chat groups and arrests of the admins of these groups, as well as the stop-and-search policy against Syrian refugees in Lebanon (i.e., Lebanese authorities searched Syrian refugees' phones for apps or personal information that might serve as 'evidence' of their queerness).[35]

Future research questions

- How do "anti-rape" apps or violence/harassment alert apps, and the legal and policy frameworks they operate within, enable or limit women's safety?

TRANSPARENCY AND ACCOUNTABILITY

Transparency and Accountability Research Gap: *The need to address the transparency and accountability of social media companies in enabling and regulating online abuse and gendered digital attacks.*

Future research questions

- Sam Gregory at Witness notes that one valuable direction for research might be for a detailed threat modeling around "deep fakes" and other forms of AI-generated "synthetic media" against key stakeholders (journalists, human rights defenders, and others)."[36] What is a gendered approach to legal, policy,

definition of the concept in her 1991 paper: "'Structural intersectionality' refers to the ways in which the location of women of color at the intersection of race and gender makes our actual experience of domestic violence, rape, and remedial reform qualitatively different than that of white women. 'Political intersectionality' describes the fact that historically, feminist and antiracist politics in the U.S. 'have functioned in tandem to marginalize issues facing Black women.[..] 'Representational intersectionality' concerns the production of images of women of color drawing on sexist and racist narratives tropes, as well as the ways that critiques of these representations marginalize or reproduce the objectification of women of color." See: Kimberle Crenshaw, "Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color," Stanford Law Review 43, no. 6 (1991): 1241–99, https://doi.org/10.2307/1229039.

[34] Anastasia Powell, Adrian J. Scott, and Nicola Henry, "Digital Harassment and Abuse: Experiences of Sexuality and Gender Minority Adults:," *European Journal of Criminology*, July 30, 2018, https://doi.org/10.1177/1477370818788006.

[35] *Apps, Arrests and Abuse in Egypt, Lebanon and Iran,* LGBTQ Online (Article 19, February 2018), https://www.article19.org/resources/apps-arrests-abuse-egypt-lebanon-iran/.

[36] Sam Gregory, "*Deepfakes and Synthetic Media: What Should We Fear? What Can We Do?*," WITNESS Blog (blog), July 30, 2018, https://blog.witness.org/2018/07/deepfakes/.

technical, and social initiatives to manage and limit the harmful effects of deepfake technologies?[37]

- From a cross-cultural perspective, how do corporate trust and safety practices work to limit gender-based digital attacks? What are users' experiences? How do these corporate commitments contradict, challenge, or converge with existing local laws and policies? What combination of legal and computational evidence will nudge greater corporate accountability for gender-based digital attacks?

- If platforms are to be held accountable for their inaction in the face of digital attacks facilitated by their technologies, then what constitutes a gendered perspective on corporate accountability for digital attacks?

- What can in-depth, cross-jurisdictional legal research tell us about effective strategies in local law enforcement responses to gendered attacks? What has worked in some areas, what kinds of pitfalls and gaps exist? And what is to be gained or lost through an approach that relies on local law enforcement to address the issue?

[37] In the months since the study was conducted, two valuable pieces of research about deep fakes have been published. These include Witness' series on preparing for the impact of deep fakes and synthetic media (See: Gregory, Sam. "*Deepfakes and Synthetic Media*"; and, Chesney, Robert, and Danielle Keats Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, July 14, 2018. https://papers.ssrn.com/abstract=3213954.

Conclusion

The large scale and varied nature in which digital insecurity is experienced requires interdisciplinary, rigorous, and civil society / practitioner-oriented scholarship to address it. Using a combination of technical, policy, socio-political and legal analyses is especially key given the diversity of terminologies and contextual factors involved in gendered digital attacks and privacy violations. Women's experiences, for instance, must remain central when we engage with them as researchers. Both 'studying ourselves' and 'studying up,' as well as validating women's subjectivity are essential in this process. This is research that might re-order how we know what it is that we know and it is work that "all of us can do, men and women, for all of us."[38] ●

Thanks to the following people who contributed their time to informing the ideas and questions presented here: Abir Ghattas, Human Rights Watch; Alexandra, Digital Defenders Partnership; Anja Kovacs, Internet Democracy Project; Betsy Bramon; Billie Goodman, Access Now; Danna Ingleton, Amnesty International; Data Justice Lab, Cardiff University; Centre for Applied Human Rights, York University, UK; Harlo Holmes, Freedom of the Press Foundation; Jenny Radloff, APC Women's Rights Program; Juliana Guerra, Derechos Digitales; Lindsay Beck; Mallory Knodel, Article 19; Maria Paz Canales, Derechos Digitales; Mariam Gagoshvili, Astraea Lesbian Foundation for Justice; Maya Richman, Mozilla Foundation Fellow at the Astraea Lesbian Foundation for Justice, 2018-19; Meerim Illyas, Frontline Defenders; Nighat Daad, Digital Rights Foundation; Olga Paz Martinez, Colnodo; Tara Tarakiyee; Vanina Serra, Mama Cash; Wilneida Negron, The Ford Foundation; and others who would prefer to remain anonymous. Thanks especially to the staff of the Citizen Lab for their time and participation in interviews and discussions. A special acknowledgement of inputs and revisions by Irene Poetranto; and comments by Caroline Wesley, Miles Kenyon and David Kelleher. Further questions may be addressed to irene at citzenlab dot ca

[38] Harding, Sandra G., ed. *Feminism and Methodology: Social Science Issues*. Bloomington : Milton Keynes [Buckinghamshire]: Indiana University Press ; Open University Press, (1987) 1-13.

Works Cited

"13 Manifestations of GBV Using Technology." Take Back the Tech. Association for Progressive Communications and Luchadoras and SocialTIC, August 17, 2018. https://www.takebackthetech.net/blog/13-manifestations-gbv-using-technology.

Abreu, Roberto L., and Maureen C. Kenny. "Cyberbullying and LGBTQ Youth: A Systematic Literature Review and Recommendations for Prevention and Intervention." *Journal of Child & Adolescent Trauma* 11, no. 1 (March 1, 2018): 81–97. https://doi.org/10.1007/s40653-017-0175-7.

Allen, Brenda J. "Standpoint Theory." In *The International Encyclopedia of Intercultural Communication*, 1–9. American Cancer Society, 2017. https://doi.org/10.1002/9781118783665.ieicc0234.

Amnesty International. "Amnesty International Staff Targeted with Malicious Spyware," August 1, 2018. https://www.amnesty.org/en/latest/news/2018/08/staff-targeted-with-malicious-spyware/.

"Apps, Arrests and Abuse in Egypt, Lebanon and Iran." LGBTQ Online. Article 19, February 2018. https://www.article19.org/resources/apps-arrests-abuse-egypt-lebanon-iran/.

Bayev and Others v. Russia, Pub. L. No. 67667/09, 44092/12, and 56717/12 (2017). https://hudoc.echr.coe.int/app/conversion/pdf?library=ECHR&id=003-5755355-7315126&filename=Judgment%20Bayev%20and%20Others%20v.%20Russia%20-%20legislation%20banning%20the%20promotion%20of%20homosexuality.pdf.

Beatrice. "Forging Careers in Human Rights Information Security Today: A Network Survey of Sustainability Challenges and Opportunities for Information Security Practitioners in the Human Rights Sector." Aspiration Tech, January 8, 2019. https://aspirationtech.org/humanrights/reports/practitionersustainabilitysurvey.

Bogaert, Knapp D. van, and G. A. Ogunbanjo. "Feminism and the Ethics of Care." *South African Family Practice* 51, no. 2 (March 1, 2009): 116–18. https://doi.org/10.1080/20786204.2009.10873822.

Buyantueva, Radzhana. "LGBT Rights Activism and Homophobia in Russia." *Journal of Homosexuality* 65, no. 4 (March 21, 2018): 456–83. https://doi.org/10.1080/00918369.2017.1320167.

Front Line Defenders. "Case History: Berta Cáceres," December 5, 2018. https://www.frontlinedefenders.org/en/case/case-history-berta-c%C3%A1ceres.

Chen, Gina Masullo, Paromita Pain, Victoria Y. Chen, Madlin Mekelburg, Nina Springer, and Franziska Troger. "'You Really Have to Have a Thick Skin': A Cross-Cultural Perspective on How Online Harassment Influences Female Journalists:" *Journalism*, April 7, 2018. https://doi.org/10.1177/1464884918768500.

Chesney, Robert, and Danielle Keats Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, July 14, 2018. https://papers.ssrn.com/abstract=3213954.

Citron, Danielle Keats, Jon Penney, and Danielle Keats Citron. "When Law Frees Us to Speak." *Fordham Law Review*, U of Maryland Legal Studies Research Paper, 87 (January 2, 2019): 2317. https://papers.ssrn.com/abstract=3309227.

Crenshaw, Kimberle. "Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color." *Stanford Law Review* 43, no. 6 (1991): 1241–99. https://doi.org/10.2307/1229039.

Dalek, Jakub, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ronald Deibert. "Planet Netsweeper: Executive Summary." The Citizen Lab, April 25, 2018. https://citizenlab.ca/2018/04/planet-netsweeper/.

Deibert, Ronald. “Statement from Citizen Lab Director on Attempted Operations Against Researchers.” *The Citizen Lab* (blog), January 25, 2019. https://citizenlab.ca/2019/01/statement-from-citizen-lab-director-on-attempted-operations-against-researchers/.

Deibert, Ronald, Lex Gill, Tamir Israel, Chelsey Legge, Irene Poetranto, and Amitpal Singh. “Submission to the UN Special Rapporteur on Violence Against Women.” The Citizen Lab, November 3, 2017. https://citizenlab.ca/2017/11/submission-un-special-rapporteur-violence-women-causes-consequences/.

Deibert, Ronald, Adam Senft, and Miles Kenyon. “Identities in the Crosshairs—Censoring LGBTQ Internet Content around the World.” *OpenGlobalRights*. Accessed August 6, 2020. https://www.openglobalrights.org/identities-in-the-crosshairs-censoring-LGBTQ-internet-content-around-the-world/.

Duggan, Maeve. “Online Harassment.” Pew Research Center. *Internet, Science & Tech* (blog), October 22, 2014. https://www.pewresearch.org/internet/2014/10/22/online-harassment/.

Eckert, Stine, and Jade Metzger- Riftkin. “Doxxing.” In *The International Encyclopedia of Gender, Media, and Communication*, 1–5. American Cancer Society, 2020. https://doi.org/10.1002/9781119429128.iegmc009.

Elash, Anita. “It’s Time to Start Charging People for Using Stalkerware to Harass Their Partners, Watchdog Group Says | CBC News.” *CBC*, June 12, 2019. https://www.cbc.ca/news/technology/stalkerware-cellphone-abuse-women-citizen-lab-1.5171458.

Elder, Miriam. “St Petersburg Bans ‘Homosexual Propaganda.’” *The Guardian*, March 12, 2012. https://www.theguardian.com/world/2012/mar/12/st-petersburg-bans-homosexual-propaganda.

“Feminist Principles of the Internet,” August 26, 2016. https://feministinternet.org/en.

Ferrier, Michelle. “Attacks and Harassment: The Impact on Female Journalists and Their Reporting.” TrollBusters, International Women’s Media Foundation, September 2018. https://www.iwmf.org/wp-content/uploads/2018/09/Attacks-and-Harassment.pdf.

“Front Line Defenders’ New Global Analysis Shows 77% of Attacks Connected to Defense of Land, Environment & Indigenous Rights.” Business & Human Rights Resource Centre, December 7, 2018. https://www.business-humanrights.org/en/front-line-defenders-new-global-analysis-shows-77-of-attacks-connected-to-defense-of-land-environment-indigenous-rights.

The Citizen Lab. “Global Research Network Archives.” Accessed August 18, 2020. https://citizenlab.ca/category/research/global-research-network/.

Gregory, Sam. “Deepfakes and Synthetic Media: What Should We Fear? What Can We Do?” *WITNESS Blog* (blog), July 30, 2018. https://blog.witness.org/2018/07/deepfakes/.

Guerra, J, and M Knodel. “Feminism and Protocols.” Internet Engineering Task Force, March 11, 2019. https://tools.ietf.org/id/draft-guerra-feminism-00.html.

Hache, Alexandra, and Mayeli Sanchez. “Women’s Bodies on Digital Battlefields: Information Exchange and Networks of Support and Solidarity of pro-Choice Activists in Latin America.” Tactical Technology Collective and Accion Directa Autogestiva, 2017. https://donestech.net/files/womensbodies_0.pdf.

Harding, Sandra G., ed. *Feminism and Methodology: Social Science Issues*. Bloomington : Milton Keynes [Buckinghamshire]: Indiana University Press ; Open University Press, 1987.

Henry, Nicola, and Anastasia Powell. “Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research:” *Trauma, Violence, & Abuse*, June 16, 2016. https://doi.org/10.1177/1524838016650189.

United Nations Human Rights: Office of the High Commissioner for Human Rights. “Human Rights Documents.” Accessed August 6, 2020. https://ap.ohchr.org/documents/dpage_e.aspx?m=70&m=166.

Hylton, Emily, Andrea L. Wirtz, Carla E. Zelaya, Carl Latkin, Alena Peryshkina, Vladmir Mogilnyi, Petr Dzhigun, Irina Kostetskaya, Noya Galai, and Chris Beyrer. “Sexual Identity, Stigma, and Depression: The Role of the ‘Anti-Gay Propaganda Law’ in Mental Health among Men Who Have Sex with Men in Moscow, Russia.” *Journal of Urban Health* 94, no. 3 (June 1, 2017): 319–29. https://doi.org/10.1007/s11524-017-0133-6.

Jhaver, Shagun, Sucheta Ghoshal, Amy Bruckman, and Eric Gilbert. “Online Harassment and Content Moderation: The Case of Blocklists.” *ACM Transactions on Computer-Human Interaction* 25, no. 2 (March 22, 2018): 12:1–12:33. https://doi.org/10.1145/3185593.

“Karachi’s Wild Child; Sabeen Mahmud.” *The Economist*, May 2, 2015. https://www.economist.com/obituary/2015/05/02/karachis-wild-child.

Khoo, Cynthia, Kate Robertson, and Ronald Deibert. “Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications.” The Citizen Lab, June 12, 2019. https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/.

Kowalski, R.M., G.W. Giumetti, A.N. Schroeder, and M.R. Lattanner. “Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research among Youth.” *Psychological Bulletin* 140, no. 4 (2014): 1073–1137. https://doi-org.myaccess.library.utoronto.ca/10.1037/a0035618.

Li, Qing, Donna Cross, and Peter K. Smith. *Cyberbullying in the Global Playground*. Blackwell Publishing Ltd., 2012. https://onlinelibrary.wiley.com/doi/book/10.1002/9781119954484.

Marquis-Boire, Morgan, Bill Marczak, Claudio Guarnieri, and John Scott-Railton. “You Only Click Twice: FinFisher’s Global Proliferation - Citizen Lab.” The Citizen Lab, March 13, 2013. https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

Marrow, Alexander. “Russian Parliament Begins Legalising Ban on Same-Sex Marriage.” *Reuters*, July 15, 2020. https://www.reuters.com/article/us-russia-politics-gaymarriage-idUSKCN24G1CJ.

O’Flaherty, Michael, and John Fisher. “Sexual Orientation, Gender Identity and International Human Rights Law: Contextualising the Yogyakarta Principles.” *Human Rights Law Review* 8, no. 2 (January 1, 2008): 207–48. https://doi.org/10.1093/hrlr/ngn009.

Parsons, Christopher, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett` Haselton, Cynthia Khoo, and Ronald Deibert. “The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry.” The Citizen Lab, June 12, 2019. https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/.

Pichugin, Alexey, and Anastasia Shevchenko. “The Kremlin’s Political Prisoners: Advancing a Political Agenda by Crushing Dissent.” Justice and Accountability for Putin’s Political Prisoners. Raoul Wallenberg Centre for Human Rights, June 10, 2019. https://www.raoulwallenbergcentre.org/newsfeed/2019/6/10/the-kremlins-political-prisoners-advancing-a-political-agenda-by-crushing-dissent.

Poetranto, Irene. “Threats Facing Women Activists in Colombia and Costa Rica.” The Citizen Lab, August 26, 2020. https://citizenlab.ca/2020/08/threats-facing-women-activists-in-colombia-and-costa-rica/.

Powell, Anastasia, Adrian J. Scott, and Nicola Henry. “Digital Harassment and Abuse: Experiences of Sexuality and Gender Minority Adults:” *European Journal of Criminology*, July 30, 2018. https://doi.org/10.1177/1477370818788006.

The Citizen Lab. “Research Archives.” Accessed August 6, 2020. https://citizenlab.ca/category/research/.

Reventlow, Nani Jansen. “Online Harassment of Women Journalists and International Law: Not ‘Just’ a Gender Issue, but A….” *Medium*, November 16, 2017. https://medium.com/berkman-klein-center/online-harassment-of-women-journalists-and-international-law-not-just-a-gender-issue-but-a-b8c6a5c7e128.

Russian LGBT Activists Detained At St. Petersburg Protest. RadioFreeEurope RadioLiberty, 2019. https://www.rferl.org/a/russia-lgbt-rights-protest/29889686.html.

Schneier, Bruce. “Public-Interest Technology Resources,” July 4, 2020. https://public-interest-tech.com/.

Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ronald Deibert. “Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware.” The Citizen Lab, June 19, 2017. https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/.

Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ronald Deibert. “Reckless IV: Lawyers for Murdered Mexican Women’s Families Targeted with NSO Spyware.” The Citizen Lab, August 2, 2017. https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/.

Scott-Railton, John, Bill Marczak, Siena Anstis, Bahr Abdul-Razzak, Masashi Crete-Nishihata, and Ronald Deibert. “Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group’s Spyware.” The Citizen Lab, March 20, 2019. https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/.

Shearlaw, Maeve. “Egypt Five Years on: Was It Ever a ‘Social Media Revolution’?” *The Guardian*, January 25, 2016, sec. World news. https://www.theguardian.com/world/2016/jan/25/egypt-5-years-on-was-it-ever-a-social-media-revolution.

Amnesty International. “Turkey: Year in Detention for Amnesty Chair a ‘Gross Injustice,’” June 6, 2018. https://www.amnesty.org.uk/press-releases/turkey-year-detention-amnesty-chair-gross-injustice.

Van der Nagel, Emily, and Jordan Frith. “Anonymity, Pseudonymity, and the Agency of Online Identity: Examining the Social Practices of r/Gonewild.” *First Monday* 20, no. 3 (February 22, 2015). https://doi.org/10.5210/fm.v20i3.5615.

West, Sarah Myers. “Raging Against the Machine: Network Gatekeeping and Collective Action on Social Media Platforms.” *Media and Communication* 5, no. 3 (September 22, 2017): 28–36. https://doi.org/10.17645/mac.v5i3.989.

Rainbow Railroad. “What We Do: Chechnya,” 2019. https://www.rainbowrailroad.org/what-we-do/chechnya.

THECITIZENLAB

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF
TORONTO