GLOBAL IDEAS INSTITUTE (GII)
munk school OF GLOBAL AFFAIRS & PUBLIC POLICY
UNIVERSITY OF TORONTO

Global Ideas Institute 2020-2021

Bolstering the Digital Safety of Marginalized Communities

Challenge Statement

As our lives increasingly take place online, our ability to engage meaningfully and safely with digital technology is crucial to our well-being, especially as risks associated with digital technology disproportionately impact marginalized individuals. **How can we bolster the digital safety of marginalized communities?**

Expanding Considerations:

While the Internet can be a source of endless information, opportunity, and connection, it can also exacerbate existing inequities and threaten the safety and well-being of individuals, especially those in marginalized communities. While digital technologies have enabled innovative responses to COVID-19 and helped to contain the virus through methods like contact tracing, this brief will discuss how some of these responses have also entailed human rights violations and have highlighted the digital vulnerabilities of the marginalized groups they disproportionately impact. Examples include contact tracing's threat to data privacy and the increased use of surveillance technologies. Through analyzing digital responses to COVID-19, what can we learn about the digital safety of marginalized communities? What are the contexts, challenges, and barriers which must be considered to begin to meaningfully understand the digital experiences of marginalized individuals? How can we begin to address their digital vulnerabilities?[1] As the purpose of this year's challenge is to address the digital vulnerabilities faced by marginalized communities, a diverse range of marginalized voices will be amplified throughout the program.

This year, GII challenges students to develop innovative approaches, be they technical, educational, policy-oriented, or other, to bolster digital safety amongst marginalized communities.[2]

[1] While numerous marginalized groups have been impacted by digital technology responses to COVID-19 and warrant analysis, Global Ideas Institute (GII) teams will focus on one marginalized community highlighted in this brief. Narrowing the scope of this brief to the highlighted groups will allow teams to conduct focused analysis to address the unique needs and challenges faced by one marginalized group. The communities highlighted in this brief are by no means exhaustive, and the brief is not intended to discount the experiences of groups not highlighted, such as Indigenous communities, migrants and refugees, and many more.

[2] As a team, you will look at how digital responses to COVID-19 have impacted your chosen marginalized group and what lessons can be learned from these responses about their general state of digital safety. For example, if you choose to focus on the LGBTQ+ community, many COVID-19 contact tracing efforts risk the exposure of sensitive personal data which could be used to fuel stigma and discrimination against LGTBQ+ communities and individuals. From this, we observe that data privacy is key to the safety of LGBTQ+ individuals, and that more should be done to bolster data privacy. Later in the program, you will move forward in brainstorming how to address the specific vulnerability you identify.

UTS UNIVERSITY OF TORONTO SCHOOLS
UNIVERSITY OF TORONTO OISE | ONTARIO INSTITUTE FOR STUDIES IN EDUCATION
Rotman I·Think
World Vision

Challenge Overview

"The fate of the Internet and the fate of humanity are deeply intertwined."[3]

The Current State of Data Regulations

Digital safety entails the ability to participate and engage meaningfully with digital platforms and technologies free from threat to one's privacy, security, and overall well-being. Much of our digital presence depends upon the accumulation of our personal data, yet our control over and knowledge of its' collection, protection, and regulation is weak and obscure.[4] The quality and extent of data regulations also vary greatly across and within countries. The European Union's General Data Protection Regulation presents a high standard in data protection.[5] It streamlines data regulation across the EU, bolsters user ownership over personal data, and increases transparency over data collection. Yet elsewhere, such as in the U.S., existing legislation is fragmented and does not go far enough.[6] Furthermore, 10% of countries currently have only draft legislation on data protection, while 19% have none at all.[7] Even more pressing, methods of data collection and use are characterized by constant change and innovation, rendering regulation efforts stuck playing catch up and compounding difficulties in understanding where and how our data is used.[8]

Privacy as a Human Right

The Internet can provide a sense of community and a crucial source of information, especially for marginalized communities unable to find similar spaces off-line—provided that privacy is safeguarded. Privacy is enshrined as a human right in Article 12 of the Universal Declaration of Human Rights,[9] as well as Article 17 of the International Covenant on Civil and Political Rights,[10] both foundational international human rights documents. Sustainable Development Goal (SDG) 16 seeks to "promote peaceful and inclusive societies" and institutions for all, with increased accountability and access to justice, while SDG 9 promotes building resilient infrastructure, inclusive industrialization, and fostering innovation.[11] The aims of each of these goals cannot be achieved without respect for the digital safety of marginalized communities, which largely depends upon the right to privacy and adequate data protections.

[3] "Mozilla Foundation Strategy Brief (Draft)." Mozilla Foundation. 2018.
[4] Kerry, Cameron F. "Why protecting privacy is a losing game today-and how to change the game." Brookings Institute. 2018.
[5] "Data protection in the EU." European Commission. 2020.
[6] Kerry, "Why protecting privacy is a losing game today-and how to change the game."
[7] "Data Protection and Privacy Legislation Worldwide." UN Conference on Trade and Development. 2020.
[8] Kerry, "Why protecting privacy is a losing game today-and how to change the game."
[9] "Universal Declaration of Human Rights." United Nations. 1948.
[10] "International Covenant on Civil and Political Rights." UN Human Rights Office of the High Commissioner. 1976.
[11] "About the Sustainable Development Goals." United Nations.

Yet tensions between privacy and corporate interest as well as privacy and public health can undermine the right to privacy. One of the biggest reasons that individuals' data is so extensively collected, with or without user consent, is to serve corporate interests. Be it in pursuit of building profiles of user interests to support targeted marketing, data on user activities to optimize business decisions, or merely profiting from the sale of user data to third parties, there is money in our data.[12] If inadequately designed to protect privacy, measures intended to bolster public health, such as responses to COVID-19, can also undermine or fail to protect the right to privacy.

Digital Disparities

The rapid development of the digital economy made the Internet integral to personal and professional success.[13] This has deepened the "digital divide," as those with access to the Internet, devices, and digital skills are enabled to succeed in the digital economy, while those without access lag behind. The digital divide runs along economic, racial, and ethnic lines and exacerbates existing inequities faced by marginalized groups, leaving them disproportionately disadvantaged in the digital sphere.[14] Furthermore, across the globe, users face limited experiences of the Internet with varying levels of personal risk. From heavy censorship of online content in countries such as China,[15] to global disparities in Internet access and quality,[16] the Internet is not experienced uniformly or equitably.

Furthermore, the digital transition has in many instances created a dynamic of false choice, such as the entrance fee of cookie acceptance for full use of most websites.[17] While copious disclaimers and user agreements are presented when engaging with digital platforms, there is little to no recourse for those who disagree with the terms and conditions (or have time to read them; reading Amazon's terms out load takes nine hours),[18] aside from abstaining from using that platform. However, given the prevalence of the digital economy in our daily lives, we rarely have a choice in which platforms we interact with. While alternatives exist, Google, despite its infringements upon user privacy in tracking browsing and location,[19] informs us; social media platforms such as Facebook, have been known to mismanage the personal data they collect,[20] connect us; and we consent to sharing our personal data in accessing health care and financial services which are vulnerable to breaches.[21] [22] Thus, power imbalances between users and providers are cemented.

[12] Freedman, Max. "How Businesses Are Collecting Data (And What They're Doing With It)." Business News Daily. 2020.

[13] Mühleisen, Martin. "The Long and Short of the Digital Revolution." International Monetary Fund, *Finance & Development*. 55(2). 2018.

[14] "Digital Divide." Stanford University.

[15] "Freedom on the Net 2019: China." Freedom House. 2019.

[16] "In Myanmar, Facebook is the Internet and the Internet is Facebook." Yale University. 2018.

[17] "Cookies: What you need to know and how they work." kaspersky. 2020.

[18] New York Times Editorial Board. "How Silicon Valley Puts the 'Con' in Consent." The New York Times. 2019.

[19] Murgia, Madhumita. "Google accused by rival of fundamental GDPR breaches." Financial Times. 2020.

[20] Nield, David. "All the Ways Facebook Tracks You—and How to Limit It." Wired. 2020.

[21] "Premera Blue Cross Hacked: 11 Million Customers Could be Affected." NBC News. 2015.

[22] Lieber, Ron. "How to Protect Yourself After the Equifax Breach." The New York Times. 2017.

Further concerning trends are observed in AI and big data technologies adapted by governments for a wide range of security-framed purposes, which share data with law enforcement. The algorithms behind AI are not bias free, and have great potential to further exacerbate discrimination against marginalized communities.[23] A worrying example is the work of Clearview AI, which scrapes images from the Internet (including social media profiles) and compiles them into an extensive national database. Their facial recognition services are used by approximately 600 law enforcement agencies.[24] While such technology can enhance the security of some, it has the potential to threaten privacy for all. It disproportionately impacts marginalized communities, especially as people of color are more likely to be overrepresented in systems and misidentified as potential suspects.

Digital Technology Responses to COVID-19: Impact on Marginalized Communities

While COVID-19 has fundamentally changed many aspects of daily life for all, it has disproportionately impacted marginalized communities.[25] In addition to economic and health outcome disparities, digital solutions for the management of COVID-19 have the potential, if not designed equitably, to heighten pre-existing digital vulnerabilities and exacerbate historical discrimination. The following are examples of the disproportionate impact of digital technology responses to COVID-19 on marginalized communities:

Contact Tracing in South Korea: The LGBTQ+ Community

Contact tracing (CT) has been instrumental in identifying potential cases of COVID-19 and giving governments and publics a sense of control during a time of great uncertainty. However, CT depends upon the collection and use of vast amounts of personal data. While CT platforms claim this data is used anonymously, it contains unique characteristics from which identities can be inferred when adequate protections are not in place. The consequences of such identification are serious, as illustrated by South Korea's measures to trace a COVID-19 outbreak in Itaewon, a prominent LGBTQ+ district in Seoul.

The Korean government used CT efforts to locate those in Itaewon at the time of the outbreak and published anonymized information on infected individuals, such as their movements, for public access online. Fears that this data could be used to identify individuals and, from this, potentially infer their sexual orientation have been raised amongst LGBTQ+ Koreans. The increased attention on Itaewon has been followed by a rise in homophobia[26] and has caused individuals to change their

[23] Heilweil, Rebecca. "Why algorithms can be racist and sexist." Vox: recode. 2020.

[24] Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." The New York Times. 2020.

[25] Poetranto, Irene. Justin Lau. "[BigDataSur-COVID] COVID-19 and Its Impact on Marginalised Communities in Singapore, South Korea, Indonesia, and the Philippines." DATACTIVE. 2020.

[26] Borowiec, Steven. "How South Korea's Nightclub Outbreak is Shining an Unwelcome Spotlight on the LGBTQ Community." Time. 2020.

behavior, such as no longer frequenting bars prominently recognized as LGBTQ+ spaces.[27] It is easy to imagine the implications of such a system in countries which criminalize homosexuality or seek to persecute other minorities and may have less protections in place for the large amounts of data being collected in the name of CT. Furthermore, the New York Times exposed vulnerabilities in Korea's quarantine app which gave hackers access to personal information, including names, date of birth, real time location, and more.[28] According to Amnesty International, "if left unchecked and unchallenged, these measures have the potential to fundamentally alter the future of privacy and other human rights."[29]

Stalkerware and Stay Home Orders: Victims of Abuse and Gender-Based Violence

A major consequence of stay home orders imposed to curb the spread of COVID-19 is the heightened risk faced by victims of domestic abuse and gender-based violence. Stay home orders and societal pressure to self-isolate restrict the already limited mobility of domestic abuse victims and can keep them under the same roof as their abuser. This has led to an observation of at least 20-30% higher rates of gender-based and domestic violence in Canada.[30] While women and girls are disproportionately impacted by this, men and boys, as well as LGBTQ+ individuals, are also victims of domestic abuse. A crucial lifeline for individuals suffering from domestic abuse is their mobile phone; various online platforms exist to help victims find information and get help. Yet increasing instances of device surveillance have threatened this lifeline. Stalkerware can be used to "secretly follow a partner's online activities, block communications, monitor phone calls," track location, and more.[31] Thus, the digital sphere can be used both to bolster or threaten the safety of victims of abuse and gender-based violence. Furthermore, while Stalkerware requires physical access to a device to be installed, device surveillance holds critical implications for a myriad of groups regardless of whether or not direct access to a device is possible, such as protesters whose cell phone data can be surveilled and tracked by law enforcement and used to prosecute them. [32]

Amplifying Discrimination: Racial and Ethnic Minorities

The implementation of contact tracing (CT) measures can exacerbate historical discrimination, especially of racial and ethnic minorities. Despite the privacy and security issues previously mentioned, many "opt-in" tracing efforts can reinforce dynamics of false choice seen on the Internet more generally. While the tracing systems of companies and national governments claim to be based on user consent, the risks of declining are too great for some to bear. If law

[27] Min Joo Kim. Simon Denyer. "A 'travel log' of the times in South Korea: Mapping the movements of coronavirus carriers." The Washington Post. 2020.

[28] Choe Sang-Hun et al. "Major Security Flaws Found in South Korea Quarantine App." The New York Times. 2020.

[29] "COVID-19, surveillance and the threat to your rights." Amnesty International. 2020.

[30] Molnar, Adam. Christopher Parsons. "Stalkerware puts those living with abusers in even greater jeopardy during COVID-19 isolation." CBC News. 2020.

[31] Ibid.

[32] Germain, Thomas. "How to Protect Phone Privacy and Security During a Protest." Consumer Reports. 2020.

enforcement is tasked with ensuring distancing and quarantining orders, implicit encouragement to use CT apps is fostered, as failure to do so may lead to unwanted police attention. Waterloo, Ontario's decision to grant police officers access to data on the COVID-19 status of individuals during Ontario's state of emergency presented numerous opportunities for discrimination against those without data on their status, or those who tested positive.[33] This decision was overturned in mid-August on the basis that such data sharing "violates individuals' constitutional rights to privacy and equality" following legal opposition by human rights groups.[34] As racial and ethnic minorities show disproportionately higher infection rates in countries like the U.S. and face less access to devices needed to use contact tracing apps,[35] such policies present a disproportionate risk for racial and ethnic minorities. This is especially concerning given their increased exposure to police surveillance and abuse.[36] Further, proof of COVID-19 status is required to enter certain government or public spaces and even stores, threatening individual's access to food and employment.[37] While the effectiveness of such measures is questioned, the surveillance structures they create may prove challenging to disassemble.[38] As previously mentioned, surveillance technology such as facial recognition mimics the biases of its creators and can serve to entrench and automate discrimination.

Conclusion

COVID-19 has fundamentally altered the way we live, worldwide. Amidst great uncertainty, digital responses to COVID-19 have innovatively addressed unprecedented challenges. However, these measures have not been free from error. As the world searches for ways to return to normal, many have called for a new, more inclusive, equitable normal. While crises are times of great upheaval, they are also full of opportunity to create a better tomorrow. Digital safety is an increasingly important element of our daily lives, and even more so given the prevalence of digital technology responses to COVID-19. Solutions to enhance digital safety are urgently needed, especially amongst marginalized communities. These solutions might be policy based, pushing for legislative or regulatory change, technical such as technological measures to enhance digital privacy and alert users to risks, or rooted in advocacy and raising awareness of the digital vulnerabilities faced by marginalized groups. Whatever their form, these solutions can play a crucial role in building a better, safer, and more equitable future. GII is excited to work with you over the course of the year to develop meaningful and impactful solutions to bolster digital safety among marginalized communities.

[33] "Waterloo regional police get access to COVID-19 status results." CBC News. 2020.

[34] The Canadian Press. "Ontario ends police access to COVID-19 database after legal challenge." CTV News. 2020.

[35] Cohen, Hannah. "The Disproportionate Effects of COVID-19 on Racial & Ethnic Minorities." RTI International. 2020.

[36] https://www.naacp.org/criminal-justice-fact-sheet/

[37] Parsons, Christopher. "Contact tracing must not compound historical discrimination." Policy Options. 2020.

[38] Madianou, Mirca. "A Second-Order Disaster? Digital Technologies During the COVID-19 Pandemic." *Social Media + Society*. 2020.

References

"About the Sustainable Development Goals." United Nations. https://www.un.org/sustainabledevelopment/sustainable-development-goals/

Aktas, Fatih. Kate Pitts. Jessica C. Richards. Iveta Silova. "Institutionalizing Global Citizenship: A Critical Analysis of Higher Education Programs and Curricula." Journal of Studies in International Education. Vol 21 (1). 2017.

Borowiec, Steven. "How South Korea's Nightclub Outbreak is Shining an Unwelcome Spotlight on the LGBTQ Community." Time. 2020. https://time.com/5836699/south-korea-coronavirus-lgbtq-itaewon/

"CNIL Publishes Guidance on Web Scraping and Re-Use of Publicly Available Online Data for Direct Marketing" in Privacy & Information Security Law Blog. Hunton Andrews Kurth LLP. 2020. https://www.huntonprivacyblog.com/2020/05/04/cnil-publishes-guidance-on-web-scraping-and-re-use-of-publicly-available-online-data-for-direct-marketing/

Cohen, Hannah. "The Disproportionate Effects of COVID-19 on Racial & Ethnic Minorities." RTI International. 2020. https://www.rti.org/insights/covid-19-effects-on-minorities

Confessore, Nicholas. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." The NY Times. 2018. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

"Cookies: What you need to know and how they work." kaspersky. 2020. https://www.kaspersky.com/resource-center/definitions/cookies

"COVID-19, surveillance and the threat to your rights." Amnesty International. 2020. https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/

"Data Protection and Privacy Legislation Worldwide." UN Conference on Trade and Development. 2020. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

"Data protection in the EU." European Commission. 2020. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

"Digital Divide." Stanford University. https://cs.stanford.edu/people/eroberts/cs181/projects/digital-divide/start.html

Freedman, Max. "How Businesses Are Collecting Data (And What They're Doing With It)." Business News Daily. 2020. https://www.businessnewsdaily.com/10625-businesses-collecting-data.html

"Freedom on the Net 2019: China." Freedom House. 2019. https://freedomhouse.org/country/china/freedom-net/2019

Germain, Thomas. "How to Protect Phone Privacy and Security During a Protest." Consumer Reports. 2020. https://www.consumerreports.org/privacy/protect-phone-privacy-security-during-a-protest/

Grogan, Kirk. "The dark side of our personal marketing data." TEDxSeattle. https://tedxseattle.com/talks/the-dark-side-of-our-personal-marketing-data/

Heilweil, Rebecca. "Why algorithms can be racist and sexist." Vox: recode. 2020. https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency

Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." The New York Times. 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

"In Myanmar, Facebook is the Internet and the Internet is Facebook." Yale University. 2018. https://seasia.yale.edu/myanmar-facebook-internet-and-internet-facebook

"International Covenant on Civil and Political Rights." UN Human Rights Office of the High Commissioner. 1976. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Kerry, Cameron F. "Why protecting privacy is a losing game today-and how to change the game." Brookings Institute. 2018. https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/

"Key Social Media Privacy Issues for 2020." Tulane University. 2020. https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020

Lieber, Ron. "How to Protect Yourself After the Equifax Breach." The New York Times. 2017. https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html

Min Joo Kim. Simon Denyer. "A 'travel log' of the times in South Korea: Mapping the movements of coronavirus carriers." The Washington Post. 2020. https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html

Madianou, Mirca. "A Second-Order Disaster? Digital Technologies During the COVID-19 Pandemic." *Social Media + Society*. 2020.

Molnar, Adam. Christopher Parsons. "Stalkerware puts those living with abusers in even greater jeopardy during COVID-19 isolation." CBC News. 2020. https://www.cbc.ca/news/opinion/opinion-stalkerware-abuse-covid-isolation-phones-1.5556379

"Mozilla Foundation Strategy Brief (Draft)." Mozilla Foundation. 2018.

Mühleisen, Martin. "The Long and Short of the Digital Revolution." International Monetary Fund, *Finance & Development*. 55(2). 2018. https://www.imf.org/external/pubs/ft/fandd/2018/06/impact-of-digital-technology-on-economic-growth/muhleisen.htm

Murgia, Madhumita. "Google accused by rival of fundamental GDPR breaches." Financial Times. 2020. https://www.ft.com/content/66dbc3ba-848a-4206-8b97-27c0e384ff27

New York Times Editorial Board. "How Silicon Valley Puts the 'Con' in Consent." The New York Times. 2019. https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html

Nield, David. "All the Ways Facebook Tracks You—and How to Limit It." Wired. 2020. https://www.wired.com/story/ways-facebook-tracks-you-limit-it/

Parsons, Christopher. "Contact tracing must not compound historical discrimination." Policy Options. 2020. https://policyoptions.irpp.org/magazines/april-2020/contact-tracing-must-not-compound-historical-discrimination/

Poetranto, Irene. Justin Lau. "[BigDataSur-COVID] COVID-19 and Its Impact on Marginalised Communities in Singapore, South Korea, Indonesia, and the Philippines." DATACTIVE. 2020. https://data-activism.net/2020/07/bigdatasur-covid-covid-19-and-its-impact-on-marginalised-communities-in-singapore-south-korea-indonesia-and-the-philippines/

"Premera Blue Cross Hacked: 11 Million Customers Could be Affected." NBC News. 2015. https://www.nbcnews.com/tech/security/premera-blue-cross-hacked-11-million-customers-affected-n325231

Sanders, James. Dan Patterson. "Facebook data privacy scandal: A cheat sheet." TechRepublic. 2019. https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/

Stone, Margaret A et al. "Sharing patient data: competing demands of privacy, trust and research in primary care." British Journal of General Practice. 55(519). 2005. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1562354/

The Canadian Press. "Ontario ends police access to COVID-19 database after legal challenge." CTV News. 2020. https://toronto.ctvnews.ca/ontario-ends-police-access-to-covid-19-database-after-legal-challenge-1.5067933

"Universal Declaration of Human Rights." United Nations. 1948. https://www.un.org/en/universal-declaration-human-rights/

"Waterloo regional police get access to COVID-19 status results." CBC News. 2020. https://www.cbc.ca/news/canada/kitchener-waterloo/waterloo-regional-police-covid-19-status-information-1.5533611

Westby, Joe. "'The Great Hack': Cambridge Analytica is just the tip of the iceberg." Amnesty International. 2019. https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/

"What your data reveals about you." A playlist from TED. https://www.ted.com/playlists/374/what_your_data_reveals_about_y