FUTURE CITIES CANADA

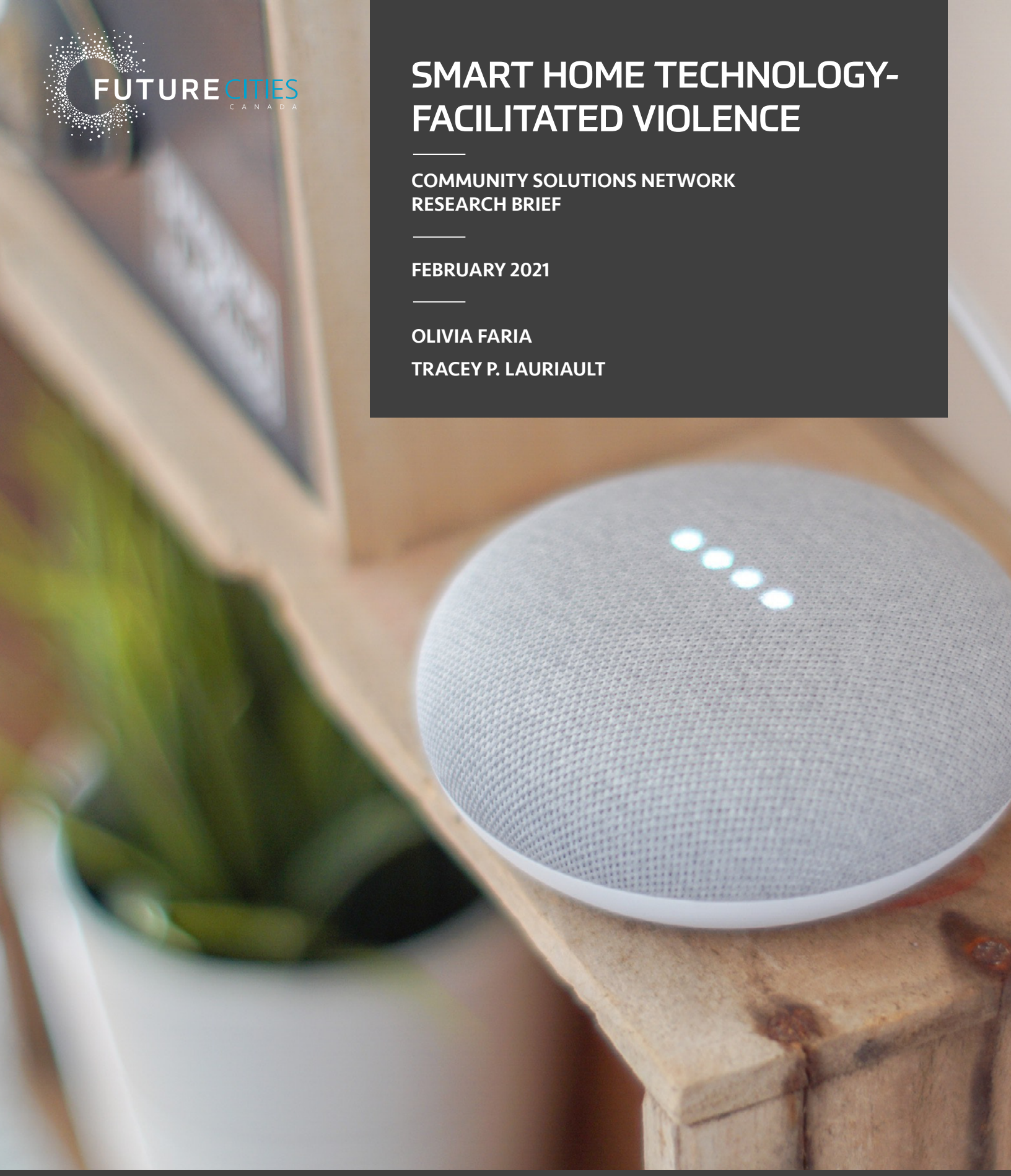
SMART HOME TECHNOLOGY-FACILITATED VIOLENCE

COMMUNITY SOLUTIONS NETWORK
RESEARCH BRIEF

FEBRUARY 2021

OLIVIA FARIA

TRACEY P. LAURIAULT



Led by: EVERGREEN

Lead technical partner: OpenNorth

With funding provided by: Infrastructure Canada, Canada

Table of Contents

Executive Summary

From smart door locks to smart speakers, smart home devices promise to make our day-to-day lives safer, easier and more efficient. However, these same technologies are also being misused with harmful repercussions. This policy brief will introduce the emerging problem of smart home technology-facilitated violence (SH-TFV), where Internet of Things (IoT) devices can quickly turn into the *Internet of Torment* in the hands of an ex-partner, abusive spouse, an employer or a landlord. The same functionalities that make our homes "smart" can and have been used for harm, by remotely controlling lights, heating and door locks for intimidation, harassment or stalking via activity logs or security systems with cameras. Currently, there is little research or policy action on SH-TFV, especially within the Canadian context, despite the growing adoption of both smart home technologies and IoT more broadly.

This brief will focus on SH-TFV policy considerations and risks and mitigation opportunities from a sociotechnical perspective. This brief will not provide extensive, in-depth explanations of legal remedies, technical insecurities or domestic violence in Canada. The goal is rather to illuminate how SH-TFV is a complex issue that requires a multi-stakeholder approach to the governance of smart home technologies and to mitigate this form of abuse and violence. This brief will highlight current and future challenges regarding the mitigation of SH-TFV, including:

- How Canadian multi-jurisdictional governance complicates issues such as SH-TFV;
- Concerns about data collection and management practices at various scales of IoT deployment (smart homes, smart buildings, and smart cities), including the emerging practice of smart home data as evidence in criminal justice;
- The need for inclusive design in technology and national policy;
- How emerging industries such as property technology (smart home technology for landlords) have the potential to introduce new forms of SH-TFV; and
- The blurring of online and offline harm in the smart city.

As our homes and communities continue to embrace data-driven technologies, emerging issues such as SH-TFV should be at the forefront of our conversations as they present serious implications for the future of cybersecurity, technological design and policymaking. The governance of SH-TFV requires a multi-stakeholder approach as its impact is embedded within a vast network of public and private institutions and is not an issue to be dealt with solely by social workers, police officers or technology designers.

Foreword

by Open North

First defined in 2018 by Lauriault, Bloom and Landry, an Open Smart City is one where all actors, including residents, collaborate in mobilizing data and technologies to develop their community through fair, ethical, and transparent governance that balances economic development, social progress, and environmental responsibility.

As Canadian communities across the country explore smart city initiatives, there is a pressing need to better understand the opportunities and risks presented by data and emerging technologies and put open smart city principles into practice.

Open North has commissioned a series of research briefs for policymakers and practitioners to provide insight into how data and technology intersect with challenges local communities are grappling with, such as food security and shared transportation. The research briefs identify complex policy issues from an open smart city lens, describe their importance and provide key considerations for policymakers.

This research brief describes the challenges that arise when smart home technologies are used for abuse and violence, which is known as smart home technology-facilitated violence (SH-TFV). As the adoption of IoT devices such as smart cameras, smart speakers and smart doorbells grows, this issue becomes increasingly urgent for multiple levels of government. This brief identifies the policy issues associated with SH-TFV and identifies potential opportunities to take early action to mitigate vulnerabilities.

Acknowledgements

This brief is an extract of Olivia Faria's unpublished Master's thesis entitled Internet of Torment: The Governance of Smart Home Technologies against Technology-Facilitated Violence. The thesis was supervised by Dr. Tracey Lauriault, Associate Professor of Critical Media and Big Data at Carleton University and financially supported by a Social Science and Humanities Research Council (SSHRC) Canada Graduate Scholarship. The full thesis is available as an open access document via the Carleton University Research Virtual Environment.

The research builds on the Open Smart Cities Guide, which provided the first ever definition of an Open Smart City. It was published in 2018 as a part of a year long collaborative research project led by Open North and funded by Natural Resources Canada's GeoConnections program in 2018. The authors are Dr. Tracey P. Lauriault (Carleton University), Rachel Bloom (Open North) and Jean-Noé Landry (Open North).

These research briefs are produced for the Community Solutions Network, a community-centric platform for communities to connect and build a national centre of excellence in open smart cities. As the project lead, Evergreen is working with lead technical partner Open North and other partners to provide valuable information, learning opportunities, advisory and capacity building services to Canadian communities in key areas of data and technology, helping to improve the lives of residents.

We offer—at no cost to communities—a comprehensive Advisory Service for Canadian communities interested in developing and implementing open smart cities projects. To learn more about the Advisory Service, please visit communitysolutionsnetwork.ca.

A program of Future Cities Canada, the Network receives funding from the Government of Canada. The views expressed in this publication do not necessarily reflect those of the Government of Canada.

Series editor: Nabeel Ahmed
Graphic design: Tatev Yesayan

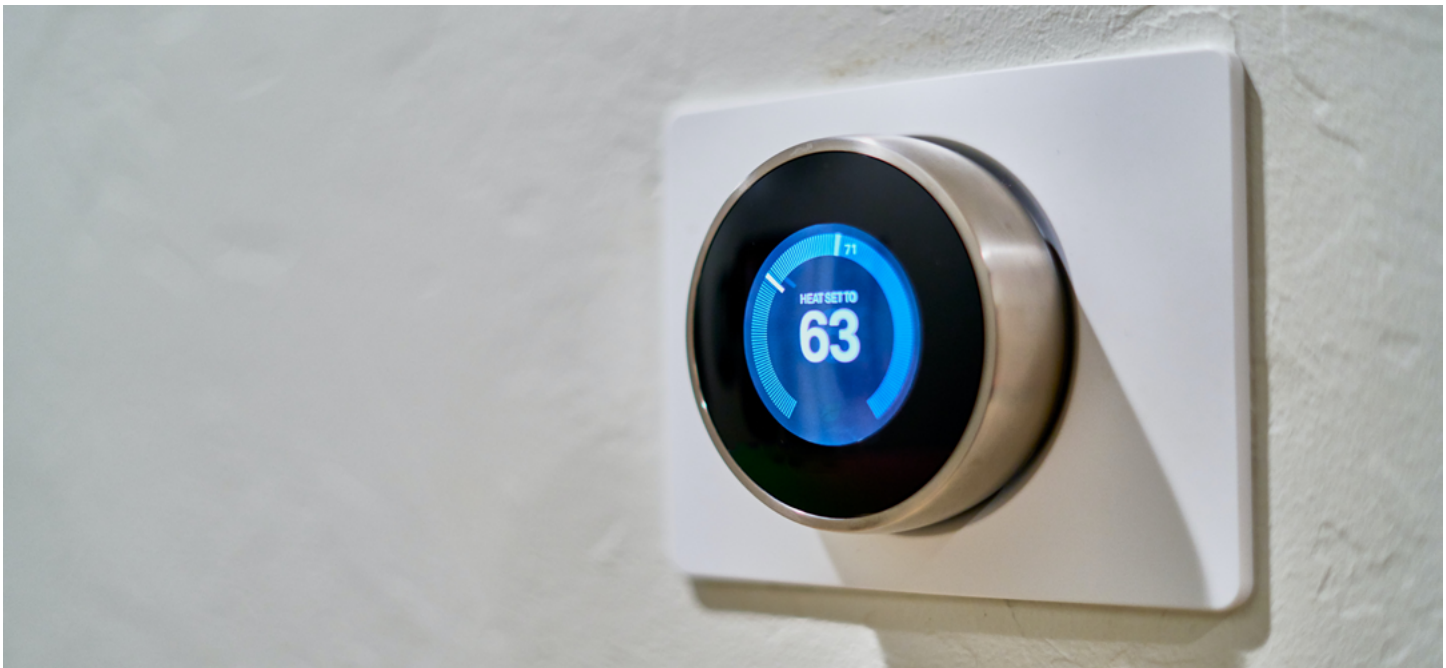
Introduction

What is Smart Home Technology-Facilitated Violence?

It is estimated that anywhere between 18 to 500 billion Internet of Things (IoT) devices, such as internet connected devices with analytics capabilities, will be deployed globally over the next five to ten years (2025-2030) across industries (IDC, 2019). While the IoT spans many sectors, one specific subsection experiencing growth in Canada is smart home technology, with surveys from the Canadian Internet Registration Authority and the Media Technology Monitor noting increased usage and ownership of devices such as smart speakers, thermostats, security systems and smart plugs (CIRA, 2020; MTM, 2020). These devices promise to make our day-to-day lives more efficient by automating daily household activities and chores, such as managing calendars, ordering food, playing music, or locking the doors. One of the common criticisms or concerns of the burgeoning IoT sphere is that these devices are generally technically insecure (e.g. prone to cyberattacks via the use of default usernames and passwords), causing a litany of privacy and security concerns. As a result, there is extensive research and investment in making these devices more secure from technically sophisticated "bad" actors such as malicious hackers or nation states (Bugeja et al., 2017; Geneitakis et al., 2018; Canadian Centre for Cyber Security, 2019). Concerns with the safety of IoT devices do not end with technical insecurity.

Increasingly, smart home devices such as smart door locks, smart speakers and cameras are being misused for abuse. While this practice does not have a standardized definition, this research brief uses the term ***smart home technology-facilitated violence*** (SH-TFV). Technology-facilitated violence is an umbrella term that typically captures actions such as cyberbullying, cyberstalking, revenge porn and online child exploitation. It is often distinguished from non-technological violence because technologies may provide new methods of abuse and/or expand the reach and control of abusers (Dragiewicz et al, 2018). This term is also commonly used in academic research (primarily disciplines such as legal studies and sociology), by non-profit organizations as well as by the Canadian federal government in their progress report regarding the country's Strategy to End Gender-Based Violence (Department of Women and Gender Equality Canada, 2019). Also, "technology-facilitated violence" is used in lieu of terms such as "intimate partner violence" to account for instances of abuse that may happen outside of an intimate relationship, such as between an employee and an employer or a landlord and a tenant.

As work on abuse facilitated by smart home technologies is still relatively new and emerging, the "smart home" prefix is added to focus on and draw attention to the unique affordances these technologies provide to abusers. Generally speaking, smart home devices provide two potential avenues



of abuse. First, these technologies enable remote control of home appliances, usually via mobile app (such as the Google Home app for Google/Google compatible products). Second, this increased control can also facilitate remote monitoring and stalking of dwellers in the home via checking respective activity logs.

Despite these risks, there is still relatively little research and policy action on this practice both globally and in the Canadian context. Globally, the most prominent research on this topic comes from Dr. Leonie Tanczer, a lecturer of international security and her team at the Gender and IoT Lab's research at the University College London. In Canada, there is a dearth of research specifically about smart home technology-facilitated violence, but there is research about adjacent technologies such as stalkerware[1] (which refers to monitoring software that is used to facilitate abuse) and a newly published overview of technology-facilitated violence in Canada[2] (Dunn, 2020). Finally, there is mention of the threat of technology-facilitated violence in the Strategy to End Gender-Based Violence and the signing of the G7 Charlevoix Commitment[3] (Faria, 2020).

1 The Citizen Lab is an interdisciplinary research lab based at the Munk School of Global Affairs and Public Policy, University of Toronto that developed two comprehensive guides (legal and holistic) on stalkerware in Canada (Khoo, Robertson and Deibert, 2019; Parsons et al., 2019).

2 This brief published by the Centre for International Governance Innovation (CIGI) provides an overview of TFV in Canada with a focus on various forms of online harassment and exploitation (e.g. revenge porn). It does not include SH-TFV.

3 Canada signed onto the G7 Charlevoix Commitment to End Sexual and Gender-Based Violence, Abuse and Harassment in Digital Contexts in 2018, which sealed its commitment to various actions (e.g. national anti-violence strategies and education, supporting removal of gender biases in technology development) (G7 Nations, 2018).

Examples: Harassment and Stalking Through Smart Home Tech

In their research at the University College London, Dr. Leonie Tanczer and her team at the Gender and IoT lab highlighted how nine common smart home technologies could be misused, including remote controlled lighting and heating being used to coerce and intimidate or smart security systems facilitating monitoring and stalking (Tanczer et al., 2018). There have also been various news stories of SH-TFV, including a man in the UK who stalked his ex-wife through a smart home to which he had administrative access to via an iPhone app and subsequently threatened her in person after over-hearing her say in the privacy of her own home that she no longer loved him (Hammersley, 2018). There is also the story of a woman whose estranged husband terrorized her and her daughters by remotely manipulating their home's heating and cooling system to its maximum in the summer and repeatedly switched it off during an autumn cold snap (Sigee, 2019). A final example of SH-TFV comes from the CBC's interview with Ferial Nijem, a survivor of this type of abuse. Ferial was living alone in a smart home that her ex had installed. However, her ex retained control of this technology after moving away and would use it to harass and intimidate her from afar. While sleeping, her ex would turn the lights on and off, blare music and remotely turn on all the TVs in the house, disrupting both Ferial and her pets. Even if she tried to manually turn them off, he could always turn them back on, making her feel as though she was "going crazy" in a "gilded cage" or living in a haunted house (Ghebreslassie, 2018). Smart home devices can and do currently provide new ways for abusers to cause emotional, psychological, and sometimes even physical harm. This must be addressed.

Key Considerations from a Policy Perspective

As adoption of smart home technologies and other IoT technology grow, it is important to discuss the threat of smart home technology-facilitated violence as it can reproduce harm at larger scales (such as a smart apartment/building or smart city) if not mitigated at the outset (Faria, 2020). In a way, it is helpful to view a smart home as an analogous micro smart city in terms of policy considerations relevant to SH-TFV.

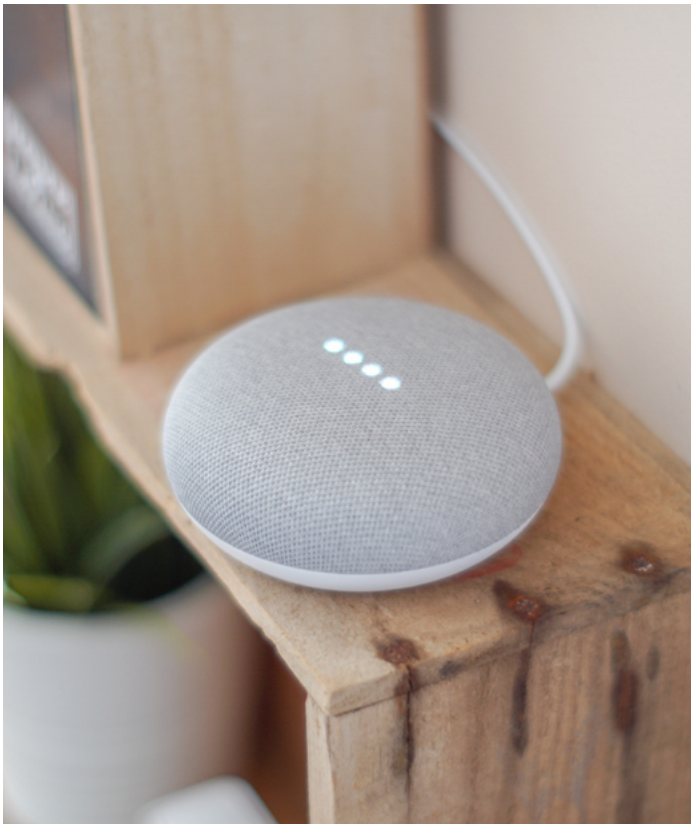
Collaborative Governance

Like a smart city, the governance of SH-TFV must be collaborative and responsive and include people with lived experience in design and governance (Lauriault, Bloom & Landry, 2018) as this issue is intricately interrelated with decisions made at various levels of government (federal, provincial, municipal, Indigenous communities) as well as in the private sector and in non-government organizations. What makes the governance of SH-TFV so complex is that different *components* of the problem fall within different jurisdictions. For example, an individual device may be subject to private sector terms of service (TOS) and privacy policies. In a scenario with multiple devices (especially with multiple vendors) terms of service and privacy policies have the potential to differ or conflict. An instance of SH-TFV might fall under municipal, provincial, or federal law enforcement, but municipalities have no jurisdiction over smart home technologies.

Beyond IoT devices, SH-TFV is impacted, among other things, by factors such as the federal allocation of funding to provincial and municipal community support services and the availability of these support services (e.g. counselling, shelters, legal clinics, multilingual crisis hotlines, cultural services) by region. The availability of support for victims of SH-TFV (and other forms of abuse) are complicated by the provinces' respective autonomy to write their own legislation, which experts have stated leads to the balkanization of policy such as discrepancies on issues related to domestic violence leave and territorial tenancy acts (Martin & Stewart, 2018) and this includes knowledge gaps between provinces on certain kinds of abuse such as emotional and financial abuse (Nicholson, 2020). As our homes and communities become increasingly *smart*, collaboration and knowledge mobilization between multiple levels of government, frontline organizations, technology experts, academic researchers and many others are crucial to the mitigation of SH-TFV.

Data Management and Data as Evidence

Not surprisingly, data management is a key concern with SH-TFV. It is well known that smart devices collect vast amounts of data, ranging from technical data like IP and MAC addresses to personal activity logs. In the increasingly connected home and city, concerns about data linkage, triangulation and subsequent exploitation are warranted. Seemingly harmless data such as device information, when combined with other data, provide a clear and scarily complete picture of someone's activities, preferences, locations, etc. (Zheng et al., 2018, p.4). Furthermore, some of these data may be collected without the participant necessarily knowing or consenting, as



a by-product of their activities (Zheng et al., 2018; Bugeja et al., 2018). On a macro scale, the main concern with these practices is the ability for multinational companies to monetize this information for their own gain.

However, a new concern with IoT data collection is emerging that is especially pertinent to SH-TFV: the use of smart home devices data as evidence. For example, activity logs can reveal the occupancy of a home at a certain time and can be used to establish an alibi, especially if certain settings are enabled such as saving recorded audio snippets (Fussell, 2020). This type of evidence can be weakened by certain privacy settings (such as not enabling the saving of audio snippets or deleting certain records), opening up the possibility of gaslighting by an abuser. Despite this unreliability, companies like Google and Amazon are receiving more requests for user information from government agencies, including law enforcement (Google Transparency Report, n.d.; Fussell, 2020). In the case of Google, requests for user information are processed on a case-by-case basis by Google's legal team, but it is worth questioning whether the current system may change into a more automated solution (or even direct collaboration as seen with Amazon Ring and police departments in the United States [Kelley & Guariglia, 2020][4]) should requests for information increase substantially in the future. The implications for individual privacy and criminal justice become nebulous.

It is these and other issues that amplify the need to include these types of technologies in a national data strategy so as to build in protection, as called for by scholars and experts. Legal scholar Dr. Teresa Scassa pointed out that relevant considerations for a national data strategy include addressing issues of cross-border data flows, data ownership, data protection and privacy considerations, data security, data sovereignty and data justice, requiring consensus at federal and provincial levels to maintain consistency in enforcement across the country (Scassa, 2019). The newly tabled consumer privacy and data protection act Bill C-11 may prove to be very helpful, although it is too soon to tell. As Scassa (2020) notes, potential gaps left by Bill C-11 include formulating *valid consent* in a manner that may leave vulnerable populations such as children unprotected[5] and its inability to "tread" on provincial jurisdiction, making data protection governance across the country inconsistent.

Inclusive Design

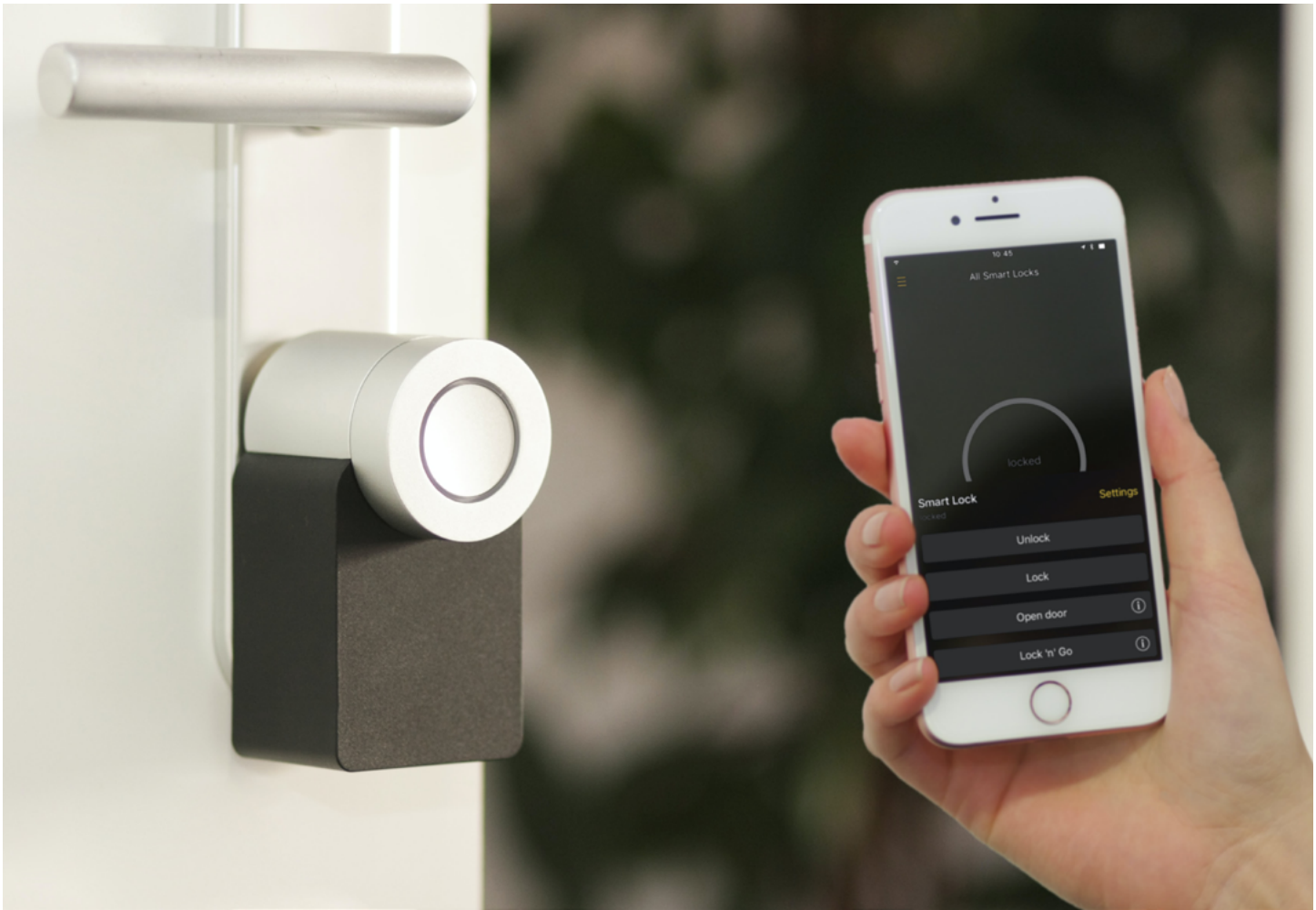
From individual technologies to national policy, inclusive design is an important step towards the mitigation of SH-TFV. Technologically, there is a delicate balance to strike between usability and security. To mitigate the possibility of SH-TFV in the future, it is important for these kinds of threats to be considered in the technology design process. For example, technologist Diana Freed suggested that there is perhaps a need for human-computer interaction (HCI) professionals to consider hampering usability for adversarial users such as TFV perpetrators, even though their role is typically to increase usability (Freed et al., 2018). One way inclusive design can manifest is through developing diverse design teams, including people with lived experience on these issues or consulting with other experts (ie. frontline support services). Furthermore, improvements in the technology design process have the potential to decrease the security burden on the user, as IoT security often falls on the user to take care of via the adoption of strong passwords and maintaining good cyber hygiene (Faria, 2020). While good cyber hygiene should be encouraged and more public-facing resources via institutions like the Canadian Centre for Cyber Security are crucial, there

4 Partnerships between Amazon Ring and police departments have been criticized by the Electronic Frontier Foundation (EFF) for privacy, security and civil liberties concerns around the ability for police to obtain video from the doorbells without a warrant, technical insecurities and general lack of transparency (including Amazon subsidizing/incentivizing police to distribute the devices within their community for free or discounted rates) (Kelley and Guariglia, 2020). Despite these risks, police departments across the United States (and now Canada via Windsor) are showing interest in this partnership, often citing operational benefits such as quicker identification of criminals (Daigle, 2020)

5 This is due to valid consent no longer being assessed by "the ability of those targeted for the product or service to understand the consequences of their consent" (Scassa, 2020). Scassa uses the example of children in her blog post, but this reformulation could also have implications for SH-TFV victims, especially those who may belong to other vulnerable populations (e.g. non English or French speakers, certain disabilities, eldercare)

are various reasons as to why someone may not be able to maintain good cyber hygiene habits (educational/technical literacy, income, control over devices, etc.) in addition to the technical vulnerabilities most IoT technologies inherently have.

On the policy side, inclusive design involves the broader enforcement of tools such as Gender Based Analysis (GBA+), an analytical tool which incorporates considerations for "intersectional identity such as race, ethnicity, religion, age, mental and physical disabilities, and non-binary people" (Status of Women Canada, n.d.). With the exception of Treasury Board Secretariat submissions and memoranda to cabinet (Status of Women Canada, 2017; Treasury Board Secretariat, n.d), the use of GBA+ in the federal government is largely left to the discretion of respective departments (Status of Women Canada, 2016). However, the effectiveness of GBA+ still relies on the public service's awareness of emerging issues. For example GBA+ was used as a process for those submitting to the Infrastructure Canada *Smart Cities Challenge*, yet even here, issues such as SH-TFV did not come up (Impact Canada, n.d.); further amplifying the need for knowledge mobilization between government, non-government organizations, private sector and academia. GBA+ could serve as an important tool to ensure that policy actions on SH-TFV consider intersectional issues like systemic racial and gender biases in criminal justice (Bailey & Mathen, 2017) that may complicate reporting and evidence, availability of support services beyond English and French for non-Anglo/non-Francophone victims and increased messaging about abuse in non-heteronormative and non-romantic relationships. Just as in the case of smart cities (Lauriault, Bloom & Landry, 2018), technological solutions cannot and will not out-engineer societal issues such as misogyny or abuse, but this does not mean we cannot improve these processes to mitigate risks.



Potential Risks and Opportunities

Exacerbating SH-TFV: Potential Sources of Risk

The greatest risk pertaining to SH-TFV is the potential for this problem to be left undiscussed and thus unmitigated. This would in turn increase the possibility for SH-TFV to be reproduced in larger scale deployments of IoT such as smart buildings and smart cities, especially as IoT adoption continues to grow. This section examines three potential sources of risk in larger scale IoT deployments.

COVID-19: An unintended consequence of COVID-19 orders such as quarantine and social distancing has been a significant uptick in domestic violence, including TFV (Koshan, 2020; United Nations, 2020; Marganski & Melander, 2020)[6]. Furthermore, lockdowns have also made it difficult for victims to seek help, including legal remedies as courts have been stalled (Koshan, 2020), reduced hours of support services or simply trying to leave the house undetected. Broader consequences of the pandemic include how the integration of various technologies meant to facilitate remote tasks (think working from home and online schooling software) or maintaining public health (poorly secured contract tracing apps, tenant surveillance for symptoms) are "reinforc[ing] and digitally recalibrat[ing] home" by heightening surveillance and control creep (Maalsen & Dowling, 2020).

Property Tech: As the property technology (smart home tech for landlords, also known as "proptech") sector grows, it is important to consider the TFV scenarios that can emerge from the relationship between a landlord and tenant or even employees and employers (e.g. eldercare, group residences for disabled people, housekeepers). These concerns are arising with landlords installing smart door locks before obtaining a tenant's consent (Doctorow, 2019) or the creation of a smart social housing complex in Peterborough, England (Stephens, 2019).

As the construction and building development industries continue to embrace (and perhaps eventually default to) building smart homes and apartments for efficiency, environmental reasons (e.g. energy saving) and possibly insurance, it is important not to lose sight of the privacy concerns, especially if smart homes become the default. For example, if a home developer requires smart home technologies to be installed in rentals or social housing as a condition for living in that form of public accommodation, individual agency of being able to choose whether to live with and be monitored by smart home technology may be taken away for some people, especially people who are already marginalized and may not be able to refuse such monitoring. Thinking further into the future, if smart homes become the default of home builders, it is important to consider what the options will be for those who want to opt out of smart homes and if there will be a premium on this modification. This would further limit the agency of anyone who may not be able to afford opting out or who have little to no choice in living in these environments, furthering the risk of privacy becoming a privilege rather than an inherent right.

In terms of the insurance sector, their presence in the smart home is emblematic of surveillance creep with the potential to unfairly discipline (Maalsen & Sadowski, 2019) as well as possibly encourage individual cyber hygiene by policies providing "incentives for implementing minimum security standards and safeguards against a range of IoT-specific threats" (Pothong, Brass & Carr, 2019, p.4). However, even "positive" incentives may punish those unable to implement said standards due to a variety of circumstances (education/technical literacy, income, control over devices among others), and fail to place accountability onto technology designers and manufacturers to create technologies up to these standards in the first place, which would lessen the security burden on individual users.

Moreover, the use of proptech can further complicate the jurisdiction and responsibility over smart home technology. For example, questions of interoperability between tenant-installed and landlord-installed devices, subsequent control of these devices and their settings naturally arise. In the case of full landlord control, or in social housing and an instance of SH-TFV within a tenant's home, there is an additional risk to a survivor whereby the landlord may deem them high friction and risk, possibly leading to eviction and further marginalization of

6 There have been no reports that specifically cite an increase in SH-TFV, but the increase in domestic violence and TFV more broadly are still relevant and important risks.

survivors. Lastly, there are valid questions as to who the final arbiter is and where a survivor might seek help.

Smart Cities: Living in the "always-on" smart city further blurs the lines between *online* and *offline* harms. In a smart city scenario, marginalized people (including victims of abuse) become increasingly entangled in surveillance and data dehumanization (Chuen, 2018; Murakami Wood & Mackinnon, 2019). The smart city also presents the potential for mass data collection and control exerted by a single—or coalition of—multinational corporations. This is especially concerning as many smart city developers are also smart home tech developers, leading to the potential for enhanced data triangulation should smart home and city data be combined.

Potential Opportunities of Taking Early Action on SH-TFV

There are nascent opportunities for the mitigation of SH-TFV. Early action on SH-TFV has the potential to slow its ability to manifest in larger scale deployments, where it becomes more difficult to mitigate the vulnerabilities as it becomes further ingrained in technology and society (e.g. considering SH-TFV as a risk in smart city development rather than retrofitting once a smart city has been deployed). This section will describe three opportunities for SH-TFV mitigation, at the outset.

Thinking sociotechnically about our future: In the *smart* world of ideas, it is becoming increasingly difficult and counterproductive to decouple social and technical phenomena from each other. As online and offline harms continue to converge, it is not sufficient to treat these issues symptomatically and it is more productive to view these issues more holistically.

For example, thinking about problems using multiple scales at once (micro, meso, macro; see Table 1 on page 12) can facilitate action by illuminating the interconnectedness of seemingly disparate human and non-human actors (e.g. devices, ideologies), and how they are interdependent (e.g. a single device being enabled by infrastructure, funding allocated to infrastructure deployment). Using multi scalar analysis not only traces the potential *journey* of a survivor from how the abuse occurs (micro) and where they might seek help (meso) but also creates an understanding of how this process is influenced by and intrinsically related to phenomena such as technological change and design, data collection and privacy policies, and corporate surveillance among others (micro, meso and macro).

Furthermore, through the use of scale, it becomes easier to see how issues are reproduced between them and how these issues become harder to mitigate as they are scaled up (e.g. the risks associated with one device in a home on a micro scale versus living in a macro scale smart city). Similarly, scale helps to demonstrate the impact of mitigation measures (e.g. macro scale actions such as federal policy or societal shifts in thinking are harder to implement but have significant impact). By doing so, the site of the smart home becomes an important part of broader networks such as smart cities and infrastructure deployments, even though it may not initially seem so.

Collaborative work and knowledge mobilization to shape law and policy: As this brief has shown, SH-TFV is not an issue that can be mitigated by one sole sector or dealt with on a purely individual basis. It is a complex sociotechnical issue that requires extensive collaboration between technology experts, policymakers, frontline service providers, academia and many more.

An excellent example of an effective multi-stakeholder approach to mitigating technology-facilitated violence more generally is the *Clinic to End Tech Abuse* (CETA), run by the Intimate Partner Violence (IPV) research group at Cornell Tech. Their clinic pairs survivors with technology experts (graduate students) in collaboration with the Mayor's Office to End Domestic and Gender-Based Violence in New York City to "uncover and end" technology-related abuses (CETA, n.d.). Furthermore, the research group's frequent collaboration with municipal governments and legal professionals who help survivors highlights the struggles that these stakeholders face, primarily a lack of best practices to turn to and the conflicting nature of survivor privacy needs and digital evidence collection process for prosecution purposes (Freed et al., 2017, p.2).

Collaborative work and knowledge mobilization can also lead to enhanced law and policy action. With a better understanding of sociotechnical issues like data privacy, SH-TFV and

Table 1: Multi-scalar Thinking (adapted from Edwards, 2003)

Scale	Parameters	Risk Example	Mitigation Opportunity Example
Micro	Individuals and individual devices within a single home (inc. individuals outside of the home with access to the devices)	Abusive exes, spouses and family members, and/or employers in the case of domestic help.	Individual cyber hygiene practices (e.g. checking device permissions, strong passwords)
Meso	Apartments, condos, housing cooperatives and rented dwellings; institutions and organizations outside the home that individuals interact with on a *local* level (e.g. police, social workers) and provincial government	Abusive landlords via property technology, smart social housing, employers in smart buildings	Support and Community Services (e.g. distress centres, crisis lines) Province-Specific Actions (e.g. strategies, action plans, tenancy acts and family violence leave)
Macro	Federal government, multinational companies, smart cities, societal norms and ideologies	Concentration of corporate power and surveillance via smart cities, distinctions between on and offline harms become further blurred	Providing funding for meso scale initiatives Creating policies, standards and smart city designs with equity and inclusive principles in mind

cybersecurity, laws and policies can be amended to reflect this new understanding. Potential policy and legislative actions relevant to SH-TFV include modernization of existing legislation (such as PIPEDA) (Khoo, Robertson & Deibert, 2019), building codes on property technology with the Canada Housing and Mortgage Corporation (CMHC) increased training (and funding for training) of frontline organizations and law enforcement on TFV (Tanczer et al., 2018; Canada, 2017), recognition in the Strategy to End Gender-Based Violence, the broadening of definitions of domestic violence to fully encompass new and emerging methods such as smart home TFV and new ways of mitigating provincial discrepancies on consumer protection, data privacy (Scassa, 2020) and access to funding and training for frontline organizations.

Increased public awareness and dissemination of resources/educational materials: Highly contingent on collaborative work and knowledge mobilization between sectors, increased public awareness is crucial in mitigating SH-TFV. For example, the British Columbia Society of Transition Houses (BCSTH) developed guides and brief explainer-style papers on technology-facilitated violence topics, including how technology can be misused for abuse as well as utilized for safety. It is important to support frontline services with the ability to disseminate these resources and educational materials for victims (through funding, training and collaboration with technology experts among others), but there is also merit in publishing this information more broadly and to different audiences (e.g. academia, policymakers, technology designers) to truly raise awareness and public consciousness on this issue. For example, the Canadian Centre for Cybersecurity would be a good place to publish a plain-language, explainer-style infographic or brief on SH-TFV, as they have already done so for general cybersecurity practices for smart devices (Canadian Centre for Cyber Security, 2020) and also with the CMHC for housing developers and the real-estate and rental market sectors, who have not published any comprehensive guidance or briefs on this issue thus far.

References

Bailey, J., & Mathen, C. (2017, Nov. 22). *Criminal Law Response to Tech Facilitated Violence Against Women & Girls* [Video]. YouTube. https://www.youtube.com/watch?v=9RSp0DPZ9LA

Bugeja, J., Jacobsson, A., & Davidsson, P. (2017). An analysis of malicious threat agents for the smart connected home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 557–562. https://doi.org/10.1109/PERCOMW.2017.7917623

Bugeja, J., Jacobsson, A., & Davidsson, P. (2018). An empirical analysis of smart connected home data. *International Conference on Internet of Things*, 134–139.

Canada, Parliament, Senate. Standing Committee on the Status of Women. (2017). *Report of the Standing Committee on the Status of Women: Taking Action To End Violence Against Young Women and Girls in Canada.* 42nd Parl., 1nd sess. Rept. 7. Retrieved from the Parliament of Canada website: https://www.ourcommons.ca/DocumentViewer/en/42-1/FEWO/report-7/

Canadian Centre for Cyber Security. (2019). *An Introduction to the Cyber Threat Environment.* Government of Canada. https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf

Canadian Centre for Cyber Security. (2020, October). *How is Your Smart Device Listening to you?* https://cyber.gc.ca/en/guidance/how-your-smart-device-listening-you-itsap70013

Canadian Internet Registration Authority. (2020). *Canada's Internet Factbook—2020.* https://www.cira.ca/resources/factbook/canadas-internet-factbook-2020

Chuen, L. (2018). Watched and Not Seen: Tech, Power, and Dehumanization. *Guts Magazine, 10*. http://gutsmagazine.ca/watched-and-not-seen/

Clinic to End Tech Abuse. (n.d.). *Clinic to End Tech Abuse.* https://www.ceta.tech.cornell.edu/clinic

Daigle, T. (2020, Feb. 18). What Canada can learn from this Michigan city's use of doorbell cameras to catch criminals. *CBC News.* https://www.cbc.ca/news/technology/livonia-michigan-windsor-ontario-ring-doorbell-1.5464761

Department of Women and Gender Equality Canada. (2019). *A Year in Review (2018-2019): Canada's Strategy to Prevent and Address Gender-Based Violence (No. 2)*. Government of Canada. https://cfc-swc.gc.ca/violence/strategy-strategie/report-rapport2019-en.html

Doctorow, C. (2019, May). *After elderly tenant was locked in his apartment by his landlord's stupid "smart lock," tenants win right to use actual keys to enter their homes.* Boing Boing. https://boingboing.net/2019/05/10/latch-vs-keys.html

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies, 18*(4), 609–625. https://doi.org/10.1080/14680777.2018.1447341

Dunn, S. (2020). *Technology-Facilitated Gender-Based Violence: An Overview (No. 1; Supporting a Safer Internet, p. 38).* Centre for International Governance Innovation. https://www.cigionline.org/sites/default/files/documents/Safer-Internet_Paper%20no%201_Dec7_ABHI_1.pdf

Faria, O. (2020). *Internet of Torment: The Governance of Smart Home Technologies Against Technology-Facilitated Violence* [MA Thesis, Carleton University]. https://curve.carleton.ca/9ee3c754-614c-4710-a810-a7a34ae8e9dd

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proceedings of the ACM on Human-Computer Interaction, 1*(CSCW), 1–22. https://doi.org/10.1145/3134681

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3173574.3174241

Fussell, S. (2020). *Police Want Your Smart Speaker—Here's Why.* WIRED. https://www.wired.com/story/star-witness-your-smart-speaker/?utm_source=pocket-newtab

G7 Nations. (2018). *Charlevoix Commitment to End Sexual and Gender-Based Violence, Abuse and Harassment in Digital Contexts.* https://www.consilium.europa.eu/media/40514/charlevoix_commintment_sexual_gender-based_violence_digital_en.pdf

Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017). Security and privacy issues for an IoT based smart home. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1292–1297. https://doi.org/10.23919/MIPRO.2017.7973622

Ghebreslassie, M. (2018). "Stalked within your own home": Woman says abusive ex used smart home technology against her. *CBC Marketplace.* https://www.cbc.ca/news/technology/tech-abuse-domestic-abuse-technology-marketplace-1.4864443

Google Transparency. (n.d.). *Google Transparency Report*. https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts,compliance;authority:CA;time:&lu=legal_process_breakdown&user_data_produced=authority:CA;series:compliance&dlr_requests=authority:CA;time:&legal_process_breakdown=expanded:

Hammersley, T. (2018, May 10). Jealous businessman spied on ex-partner using iPad mounted to kitchen wall. *Manchester Evening News.* https://www.manchestereveningnews.co.uk/news/greater-manchester-news/jealous-businessman-spied-ex-partner-14640719

Havron, S., Freed, D., Chatterjee, R., McCoy, D., Dell, N., & Ristenpart, T. (2019). Clinical Computer Security for Victims of Intimate Partner Violence. *28th USENIX Security Symposium (USENIX Security 19)*, 105–122. https://www.usenix.org/conference/usenixsecurity19/presentation/havron

IDC. (2019, June). *The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast.* IDC. https://www.idc.com/getdoc.jsp?containerId=prUS45213219

Impact Canada. (n.d.). *Smart Cities Finalist Guide.* https://impact.canada.ca/en/challenges/smart-cities/finalist-guide#toc5

Kelley, J., & Guariglia, M. (2020, June). *Amazon Ring Must End Its Dangerous Partnerships with Police.* Electronic Frontier Foundation. https://www.eff.org/deeplinks/2020/06/amazon-ring-must-end-its-dangerous-partnerships-police

Khoo, C., Roberston, K., & Deibert, R. (2019). *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications* (No. 120; Citizen Lab Research Report). University of Toronto.

Koshan, J., Mosher, J., & Wiegers, W. (2020, July). *COVID-19, Domestic Violence, and Technology-Facilitated Abuse.* ABlawg. https://ablawg.ca/2020/07/13/covid-19-domestic-violence-and-technology-facilitated-abuse/

Lauriault, T.P., Bloom, R., & Landry, J.N. (2018). *Open Smart Cities Guide v.1.0*. OpenNorth. https://opennorth.ca/publicationdetail?id=3Ptq7I6gVIfzBfl2ZAYoNs

Maalsen, S., & Dowling, R. (2020). Covid-19 and the accelerating smart home. *Big Data & Society, 7*(2). https://doi.org/10.1177/2053951720938073

Maalsen, S., & Sadowski, J. (2019). The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance. *Surveillance & Society, 17*(1/2), 118–124. https://doi.org/10.24908/ss.v17i1/2.12925

Marganski, A., & Melander, L. (2020, June). *Domestic abusers use tech that connects as a weapon during coronavirus lockdowns.* The Conversation. https://theconversation.com/domestic-abusers-use-tech-that-connects-as-a-weapon-during-coronavirus-lockdowns-139834

Martin, L., & Stewart, H. (2018). *Building a National Narrative.* Women's Shelters Canada.

Media Technology Monitor. (2020, June). *Smart speakers are growing, but not a staple.* Media in Canada. https://mtm-otm.ca/Download.ashx?file=Files/News/23-06-2020.pdf

Murakami Wood, D., & Mackinnon, D. (2019). Partial Platforms and Oligoptic Surveillance in the Smart City. *Surveillance & Society, 17*(1/2). https://doi.org/10.24908/ss.v17i1/2.13116

Nicholson, K. (2020, March). "Barriers" in Canada's legal system complicating fight to end domestic violence. *CBC News.* https://www.cbc.ca/news/barriers-in-canada-s-legal-system-complicating-fight-to-end-domestic-violence-1.5488510

Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry* (No. 119; Citizen Lab Research Report). University of Toronto.

Pothong, K., Brass, I., & Carr, M. (Eds.). (2019). *Cybersecurity of the Internet of Things: PETRAS Stream Report.* PETRAS IoT Research Hub.

Scassa, T. (2019). *Considerations for Canada's National Data Strategy.* CIGI. https://www.cigionline.org/articles/considerations-canadas-national-data-strategy

Scassa, T. (2020, November). *With a New Federal Bill Before Parliament, Is There Still a Case for Ontario to Enact its Own Private Sector Data Protection Law?* Teresa Scassa. http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=334:with-a-new-federal-bill-before-parliament-is-there-still-a-case-for-ontario-to-enact-its-own-private-sector-data-protection-law?&Itemid=80

Sigee, R. (2019, July 8). The rise of 'smart abuse': 'My ex was spying on me through my TV.' *The Sunday Telegraph.* https://www.telegraph.co.uk/women/life/rise-smart-abuse-ex-spying-tv/

Status of Women Canada. (2017). *Interim Progress Report on the Implementation of Gender-Based Analysis Plus (GBA+) Action Plan.* Government of Canada. https://cfc-swc.gc.ca/gba-acs/progress-etape-en.html

Status of Women Canada, Privy Council Office, & Treasury Board of Canada Secretariat. (2016). *Action Plan on Gender-Based Analysis (2016-2020).* Government of Canada. https://cfc-swc.gc.ca/gba-acs/plan-action-2016-en.html

Stephens, R. (2019, Nov. 18). *Delivering a sustainable future-what role can full fibre play?* Opportunity Peterborough. https://www.opportunitypeterborough.co.uk/delivering-a-sustainable-future-what-role-can-full-fibre-play/

Tanczer, L., Lopez-Neira, I., Parkin, S., Patel, T., & Danezis, G. (2018). *Gender and IoT Research Report: The Rise of Internet of Things and implications for technology-facilitated abuse* (pp. 1–9). Department of Science, Technology, Engineering and Public Policy.

Treasury Board of Canada Secretariat. (n.d.). *Gender-Based Analysis.* https://www.canada.ca/en/treasury-board-secretariat/services/treasury-board-submissions/gender-based-analysis-plus.html#gba2

United Nations. (2020). *Policy Brief: The Impact of COVID-19 on Women* (p. 21). https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/policy-brief-the-impact-of-covid-19-on-women-en.pdf?la=en&vs=1406

Zheng, X., Cai, Z., & Li, Y. (2018). Data Linkage in Smart Internet of Things Systems: A Consideration from a Privacy Perspective. *IEEE Communications Magazine, 56*(9), 55–61. https://doi.org/10.1109/MCOM.2018.1701245