Internet of Torment: The Governance of Smart Home Technologies against Technology-Facilitated Violence

by

Olivia Faria

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of

Master of Arts

in

Communication with specialization in Data Science

Carleton University
Ottawa, Ontario

Abstract

While smart home technologies (SHTs) such as smart speakers are often marketed as solutions to automate daily household activities and chores, such as managing calendars, ordering food, playing music or locking the doors, these same technologies can be used to cause harm. This thesis examines the emergence of smart home technology-facilitated violence (smart home TFV) in Canada to assess 1) how these Internet of Things (IoT) devices can be misused as technologies of torment and 2) how and why we may want to examine this phenomenon as part of a wider sociotechnical system of human and non-human actors. First, smart home technologies are situated in the history of home automation and gendered design, conceptually in the research of technology facilitated violence, within a Canadian policy and legal environment and as part of technical research on smart home technology safety by way of an interdisciplinary literature review. Secondly, a modified Walkthrough Method (Light, Burgess and Duguay, 2018) was applied to study the popular *Google Nest Mini* smart speaker to identify how this device may be misused, which features enable potential misuse and to better understand how the device is reflective of broader corporate values, visions and operating models. Thirdly, a hybrid theoretical framework combining assemblage theory (Kitchin, 2014), actor-network theory (Latour, 1988; Latour, 2005) and multi-scalar analysis (Edwards, 2003) was developed and applied to frame the study of this complex technological system and to structure the collection of observations and analyze results arranged into micro, meso and macro scales. This approach illuminates what may initially be misconstrued as an isolated, one-on-one dispute as a practice that is enabled, mitigated, and ultimately shaped by a variety of contexts and interactions with other components within a complex and heterogeneous sociotechnical assemblage (Kitchin, 2014). This thesis argues that conceptualizing the issue in this way is effective as an interdisciplinary approach, foregrounds the mutually shaping relationship between technology and society and how these issues are reproduced across different scales, which informs and facilitates remedial actions. The thesis concludes with recommendations and reflections on the strengths and limitations of this research.

Acknowledgements

Para minha querida família, sou grato por seus sacrifícios e amor incondicional. Nenhuma outra alegria se compara a ver todos vocês orgulhosos de mim.

Thank you to Dr. Tracey Lauriault, my mentor and thesis supervisor, who has guided and supported me through my academic journey over the past four years. She has provided me several academic opportunities, encouraged me to pursue a master's degree, taught me so many things about becoming a scholar and I will always cherish my time working with her. I will miss sitting in her comfy visitor's chair and seeing the stack of books from the *Lauriault Library* pile up on the ottoman as we brainstormed ideas.

Thank you to my committee of Dr. Rena Bivens and Dr. Stephen Fai for your insightful feedback and diverse perspectives that ultimately enhanced this work.

I would also like to thank the Department of Communication and Media Studies as a whole. As an undergrad from a different department, I always felt so welcomed by the wonderful faculty and staff of this department. It has been an honour and privilege to do my master's degree there. I would like to extend an extra thank you to Dr. Liam Young and Dr. Dwayne Winseck who saw potential in me during my undergrad and encouraged me to pursue graduate studies, something I never thought possible at the time.

To my friends, near and far, thank you for always putting a smile on my face and getting me through this gruelling yet rewarding process. Special thanks to Maya (for always being the supportive voice of reason), Magda (for always making me laugh even at the lowest points) and Kalila (for letting me vent and ramble whenever and always cheering me on from across the pond).

Last but certainly not least, I am grateful for the financial support from the Social Science and Humanities Research Council (SSHRC) and the Federation of Portuguese-Canadian Business & Professionals (FPCBP) Antonio Sousa Community Pioneer Award.

Table of Contents

Abstract ii
Acknowledgements iii
Table of Contents iv
List of Tables vi
List of Figures vi
List of Appendices viii
Chapter 1: Introduction and Thesis Question 9
1.1 Introduction 9
1.2 Thesis Questions and Roadmap 13
Chapter 2: Literature Review 15
2.1 History of Home Automation and Gendered Design 16
2.2 The State of Technology Facilitated Violence (TFV) Research 23
2.3 Canadian Policy and Legal Environment 31
2.4 Technical Research on Smart Home Technology Safety 44
2.5 Summary 56
Chapter 3: Theoretical Framework 58
3.1 Assemblage Theory 59
3.2 Actor-Network Theory (ANT) 63
3.3 Multi-Scalar Approach to Sociotechnical Systems (Edwards) 65
3.4 Hybrid Theoretical Framework 67
Chapter 4: Methodology 68
Chapter 5: Observations from the Walkthrough Method 75
5.1 Environment of Expected Use 75
5.1.1 Vision 76
5.1.2 Operating Model 86
5.1.3 Governance 90

5.1.4 Technical Walkthrough 92
5.2 Modifications to the Walkthrough Method 98
5.2.1 Unintended Uses 98
5.2.2 Data 102
5.3 Summary 109

Chapter 6: Discussion 110
6.1 Micro Scale Analysis 111
6.2 Meso Scale Analysis 117
6.3 Macro Scale Analysis 129
6.4 Summary 136

Chapter 7: Conclusion 138
7.1 Limitations, Future Work and Final Thoughts 143

Appendices 146
Appendix A : Charlevoix Commitment (G7 Nations, 2018) 146
Appendix B : Funded Initiatives under the Strategy to Prevent Gender-Based Violence (derived from Department of Women and Gender Equality, n.d.). 147
Appendix C : Theories of Technology and Society (derived from Feenberg, 1999 as adapted by Quan-Haase, 2015) 148

Works Cited 149

List of Tables

Table 1: Summary of Literature Review Documents 16

Table 2: Literature Review Summary 57

Table 3: Smart Home Context Elements of Kitchin's Sociotechnical Data Assemblage (Kitchin, 2014) 62

Table 4: Edwards' Multi-Scalar Approach (Edwards, 2003) 66

Table 5: Summary of documents collected for the Environment of Expected Use 76

Table 6: Comparison Chart of Google Home Devices (derived from Google Support, n.d.) 78

Table 7: Information collected by Google Services (derived from Google Safety, n.d. and Google Policies, 2020a) 103

Table 8: Data collected by Google connected home products (Google Support, 2020c) 106

Table 9: Summary Table of Micro Scale Actors 117

Table 10: Summary Table of Meso Scale Actors 128

Table 11: Summary of Macro Scale Actors 136

List of Figures

Figure 1: Selection of Home Technology Advertisements from MacLean's Magazines, 1921-1962 (Maclean's, 1921-62) 18

Figure 2: Screenshots from Westinghouse's All Electric House Video, around mid-1950s (Westinghouse, n.d.) 21

Figure 3: Tech Abuse Diagram extracted from a policy brief (Tanczer, 2018) 24

Figure 4: Visions of IoT Venn Diagram (Atzori, Iera and Morabito, 2010, p.3) 45

Figure 5: Open Research Issues in IoT (Atzori, Iera and Morabito, 2010, p.11) 46

Figure 6: Six Classes of Smart Home Threat Agents Compared by Motive and Capability (Bugeja et al., 2017, p.4).....49
Figure 7: Types of Data collected by Device Type (Bugeja et al., 2018) 51
Figure 8: Examples of Dual-Use Apps (derived from IPV Tech Research - *App Classification Guide*, n.d.) 53
Figure 9: Header of Google Nest Mini landing page in English and Portuguese and back of the Google Nest Mini Box (Google Store, 2020a; Google Store, 2020b).....77
Figure 10: A screenshot of a Google Home/Home Mini advertisement from Google Spain stating 'A Big help in different sizes' (Google España, 2018) 79
Figure 11: A Collage of Google Nest Mini's Placements (Google Nest, 2019a; Google Nest, 2019b) 80
Figure 12: Google Branded Products and Services (Google, 'Products', 2020).....84
Figure 13: Google Partner Notice + Learn More Page in Google Home App during Nest Mini Setup.....88
Figure 14: Contents of the Google Nest Mini Box 92
Figure 15: Swim Lane Diagram of Google Nest Mini Setup 93
Figure 16: Device Statistics and Crash Report Consent Screen in Google Home app 95
Figure 17: Swim Lane Diagram of Creating a Home in Google Home App 95
Figure 18: Flowchart of Google Assistant Setup in Google Home app 97
Figure 19: Comparison between phone on same Wi-Fi network (left) and cellular network (right). Differences highlighted in blue, green and yellow.....101
Figure 20: Swim Lane Diagram of My Activity Review 105
Figure 21: Three Examples of Detailed Activity 105

List of Appendices

Appendix A : Charlevoix Commitment (G7 Nations, 2018) 146

Appendix B : Funded Initiatives under the Strategy to Prevent Gender-Based Violence (derived from Department of Women and Gender Equality, n.d.) 147

Appendix C : Theories of Technology and Society (derived from Feenberg, 1999 as adapted by Quan-Haase, 2015) 148

Chapter 1: Introduction and Thesis Question

1.1 Introduction

In 2018, Ross Cairns was jailed for 11 months for harassing and stalking his ex-wife through their Manchester smart home (Spillett, 2018; Hammersley, 2018). Cairns used the home's ELAN system[1] to remotely eavesdrop and spy on his ex-wife through the administrative access he had to the ELAN system via an iPhone app, culminating with Cairns threatening his ex-wife in person after hearing her say she didn't love him anymore (Hammersley, 2018). In an interview with *The Sunday Telegraph*, another woman described the harrowing methods her estranged husband used to terrorize her and her daughters, including the "heating game" where he would remotely set the home's central heating to its maximum in the summer and repeatedly switch it off during an autumn cold snap (Sigee, 2019). These two stories are examples of how Internet of Things (IoT)[2] smart home technologies can become tools of domestic abuse (Bowles, 2018). In general, a smart home differs from a 'regular' home through the addition of smart home technologies (SHTs), which refer to various hardware and software components "networked together to enable automation as well as localized and remote control of the

[1] ELAN is a brand of smart home systems (ELAN, n.d.).
[2] Many definitions of IoT exist across various disciplines and is heavily debated. The International Standards Organization (ISO) defines IoT as "An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react"(ISO, 2018). Smart home technologies such as internet connected lights, security cameras and speakers are considered part of the IoT as they are internet connected devices with sensing capabilities and can communicate with other devices. Definitions of IoT will be further explored in the literature review.

domestic environment" (Hargreaves and Wilson, 2017).[3] The 'smart' component of the smart home derives from SHTs' ability to collect data via sensors (e.g. temperature or motion), analyze them and relay the information back to the user, thus "enhancing the potential for managing different domestic systems" (p.2). Control over smart homes and individual SHTs is typically through a software (e.g. a mobile app) and/or hardware (e.g. wall mounted display) interface (p.2) and are also increasingly voice activated.

As seen in the previous examples, seemingly innocuous features of the smart home such as the ability to control heating and lights via internet enabled mobile applications can now also be turned into tools of torment in the hands of an ex-partner, abusive spouse or even an employer in the case of house cleaners or home-care assistants (Hall, 2018). This phenomenon is an emerging form of technology facilitated violence (TFV). While there is no solid consensus on the terms to define violence and abuse against intimate partners (Dragiewicz et al., 2018), the prefix of 'technology facilitated' is often used to separate actions facilitated by digital media such as social media harassment, stalking via the internet or GPS data and monitoring of data from other forms of violence (p.3). This distinction between 'traditional' and technological abuse is often made because technologies can "enable domestic violence perpetrators to expand the reach of control and abuse, disrupting women's[4] efforts to protect themselves" (p.617) as a result of the various affordances[5] these technologies can provide in comparison to non-technological violence.

---

[3] The definition created by Hargreaves and Wilson was chosen for this thesis as it acknowledges smart homes have many configurations and can range from a few devices to a fully automated home as well as address the data component of smart homes.

[4] While the author focused on women, this thesis is cognizant that TFV can happen to anyone, regardless of gender, but that women are currently disproportionately affected by domestic violence according to existing reports and studies.

[5] Affordances refer to the characteristics of technology that "make behaviours possible, shaping users' options and actions" (boyd, 2015 in Dragiewicz et al., 2018, p.510)

For example, Dragiewicz et al. (2018), a legal studies professor working with a team of psychologists and digital media scholars, use the term Technology Facilitated Coercive Control (TFCC) to "encompass the technological and relational aspects of abuse in the specific context of coercive and controlling intimate relationships" in reference to violence facilitated by digital media (p.3). Legal studies scholars Anastasia Powell and Nicola Henry use the term Technology Facilitated Sexual Violence (TFSV) to describe "criminal, civil and otherwise harmful sexually aggressive behaviors perpetrated against women with the aid or use of new technologies" in five main forms: 1) unauthorized distribution and appropriation of sexual images 2) distribution of sexual assault imagines 3) online sexual harassment 4) gender-based hate speech and 5) virtual rape (Henry and Powell, 2015, p.4). Furthermore, legal studies professor Jane Bailey states that the prefix of technology facilitated in lieu of "cyber" (e.g. cyberviolence) is preferred as "cyber" tends to be more easily dismissed or downplayed (Bailey and Mathen, 2017). For the purposes of this thesis, violence in the form of harassment and torment, facilitated by smart home technologies will be referred to as smart home technology-facilitated violence (Smart Home TFV). This definition was created for two main purposes: 1) to distinguish this form of TFV from others such as online sexual harassment which are studied more extensively and 2) to focus on the various sociotechnical implications of smart homes.

Beyond the site of an individual's home, smart home TFV should also be a consideration in the deployment of large IoT projects such as smart cities[6] (Infrastructure Canada, 2018) and

[6] The Smart Cities Challenge was a competition launched by Infrastructure Canada, the department responsible for the oversight of urbanization and infrastructure deployment. The challenge sought to "empower communities to adopt a smart cities approach to improve the lives of their residents through innovation, data and connected technology" (Infrastructure Canada, 2018).

large urban development projects such as Google's Sidewalk Toronto[7] as smart homes and SHTs constitute part of the IoT. In addition to these developments, various business, technology, and consulting firms estimate that anywhere between 18 to 500 billion IoT devices will be deployed globally over the next five to ten years (2025-2030)[8] across industries. The Canadian Internet Registration Authority (CIRA)'s 2020 Internet Factbook also found that 41% of their Trends in Internet Use and Attitudes survey respondents had a Bluetooth speaker in their home and 26% had a smart speaker such as Amazon Alexa or Google Home (CIRA, 2020). Other popular SHTs in Canada identified by CIRA's survey included smart thermostats (17%), home security systems (15%) and smart plugs (12%) (p.1). CBC's Media Technology Monitor also reported a significant uptake with smart speaker ownership in Canada tripling since 2018 (MTM, 2020). In terms of industry, the smart home technology industry is growing in Canada, with the Boston Consulting Group (BCG) that identified about 57 smart home start-ups in Canada in 2018 (Ali & Yusuf, 2018).

Despite this, there is still no national, provincial or local action plan to govern the mass adoption of IoT devices across industries in Canada despite numerous government departments and citizens being impacted by this impending 'IoT boom' (Gilchrist, 2016). As IoT proliferates throughout the country, the risk of smart home TFV perpetrated by a variety of actors has the potential to rise. For example, technologies such as smart locks are becoming increasingly popular with landlords, meaning many people are subject to SHTs without their explicit consent

[7] Sidewalk Toronto was an urban development project in Toronto's eastern waterfront (beginning with Quayside) by Sidewalk Labs, a subsidiary of Google's parent company, Alphabet Inc. Launched in 2017, Sidewalk Toronto sought to reimagine the formerly industrial waterfront area into a 77-hectare 'IDEA' district (Sidewalk Toronto, 2019). In 2020, the Sidewalk Toronto project was cancelled because of public outcry (Carter and Rieti, 2020).
[8] Estimates derived from Cisco (2016), McKinsey (Dahlqvist et al., 2019) and IDC (2019)

(Doctorow, 2019a; Doctorow 2019b). There is therefore a sense of urgency to govern SHTs now and alert industry and government to pre-empt smart home TFV and to govern IoT.

1.2 Thesis Questions and Roadmap

Because smart home TFV is a relatively new phenomena, there is not much literature about this emerging issue, especially in Canada. Inspired by Dr. Leonie Tanczer's ongoing research on the *Implications of IoT on Victims of Gender-Based Domestic Violence* at the University College London (Tanczer et al., 2018; Tanczer et al., 2019), this thesis seeks to answer the following questions: 1) how are smart home technologies being misused for TFV and 2) how can smart home TFV be conceptualized as part of a large sociotechnical system and what are the benefits of this approach? To answer these research questions, I adopt an interdisciplinary and mixed methods approach as follows. In chapter two I provide an interdisciplinary literature review divided into four main sections: 1) the historical underpinnings and gendered design of smart homes, 2) current research on smart home TFV, 3) technical research on smart home security 4) the Canadian policy environment as relevant to smart home TFV. In chapter three describes a hybrid theoretical framework I developed to study this sociotechnical smart home and smart home TFV system. The theoretical framework includes elements of assemblage theory (Kitchin, 2014), actor-network theory (ANT) (Latour, 1987; Latour, 2005) and a multi-scalar analysis (Edwards, 2003). In chapter 4 I describe the Walkthrough Method developed by digital media scholars Ben Light, Jean Burgess and Stefanie Duguay (2018) which I adopted and modified to study a *Google Nest Mini* installation. In Chapter 5 I provide the observations resulting from having conducted the modified Walkthrough Method. The Google Nest Mini was specifically selected because of its low price point and ease of use and because smart home speakers are the most popular SHT in Canada (CIRA, 2020) and as of 2020, Google is the

number one choice in Canada (MTM, 2020). It is important to note that the focus of this thesis is smart home TFV, and not hacking in general, as these issues are already well-known and sufficiently addressed in technical literature and that distinction will be made clearer in section 2.4. In chapter 6, I arrange the analysis into three interrelated scales. The micro scale analysis which focuses on the technical components of the smart home and its immediate impacts on the dwellers of the home. The meso scale analysis discusses the impacts of smart home TFV on various organizations and institutions that act on a 'local' level such as policing or social work. Lastly, the macro scale analysis encompasses the micro and meso but considers large scale actors such as governments and smart city applications of IoT. Furthermore, the discussion chapter seeks to demonstrate how smart home TFV is a far reaching and important issue that goes beyond a single home or one-on-one dispute and is part of a wider assemblage of actors. Finally, the last chapter will summarize the findings of the thesis, include some recommendations, and discuss limitations and highlight areas for future work and research.

Chapter 2: Literature Review

As the smart home and smart home TFV are considered to be a part of a large and social and technological system (Hughes, 2012), I purposely selected scholarly and grey literature from multiple disciples ranging from science and technology studies (STS), law and legal studies, communication and media studies, sociology and systems and computer engineering, among others and resources from multiple sectors such as reports, pamphlets and guides pertaining to TFV and cybersecurity tips from non-profit organizations and consultancies and government policy documents as listed in Table 1 (below). The analysis of the literature reviewed in this chapter is structured as follows: 2.1) provides an overview of the history of home automation and gendered design, 2.2) examines the state of research on TFV, 2.3) discusses technical research on smart home security, 2.4) is an overview of the Canadian policy environment of smart technologies and TFV and 2.5) summarizes key concepts and issues derived from the literature.

Section	Source type and authors
2.1 - History of Home Automation and Gendered Design	**12 academic articles** (Davis, 1993; Aldrich, 2003; Barber, 1985; Vanek, 1974; Bell and Dourish, 2007; Berg, 1999; Cockburn, 1993; Cockburn, 1997; Crowley and Coutaz, 2015; Livingstone, 1993; Rode et al., 2004; Blackwell, 2006), **1 commercial** (Westinghouse n.d.) and **11 magazine clippings from Macleans** (1921-62)
2.2- The State of TFV Research	**8 academic articles** (Henry and Powell, 2014; Henry and Powell, 2015; Powell and Henry, 2018; Finn and Atkinson, 2008; Dimond, Fiesler and Bruckman, 2011; Dragiewicz, Harris and Douglas, 2019; Woodlock, 2017; Maalsen and Sadowski, 2019), **1 policy brief derived from an academic research project** (Tanczer, 2018), **2 reports derived from an academic research project** (Tanczer et al., 2018; Tanczer et al., 2018b)
2.3- Canadian Policy and Legal Environment	**2 academic articles** (Dekeseredy and Dragiewicz, 2014; Bailey and Mathen, 2019), **1 presentation on academic research** (Bailey and Mathen, 2017), **3 academic reports** (Khoo, Robertson and Deibert, 2019; Parsons et al., 2019; Hou, Tops and Ou, 2019), **18 government documents** [reports, webpages] (G7 Nations, 2018, Global Affairs Canada, 2017; Finestone, 1995; Office of the Auditor General of Canada, 2009; United Nations, 1995; Status of Women Canada [GBA], n.d.; Status of Women Canada, 2017; Teasury Board Secretariat, n.d.; Impact Canada, n.d.; Status of Women Canada, 2018; Department of Women and Gender Equality, 2017; Department of Women and Gender Equality, 2018; Department of Women and Gender Equality, 2019; Public Safety Canada, 2020; Public Safety Canada, 2018; Canadian Centre for Cyber Security. n.d.; Canadian Centre for Cyber Security, 2019; City of Cote Saint-Luc, 2019) **3 reports/guides from frontline organizations** (Fairbairn and Black, 2015; Wong, 2019; National Network to End Domestic Violence, 2018)
2.4- Technical Research on Smart Home Tech Safety and Security	**14 academic articles** (Atzori, Iera and Morabito, 2010; Atzori, Iera and Morabito, 2017; Alaa et al., 2017; Geneiatakis et al., 2017; Bugeja et al., 2017; Freed et al., 2018; Bugeja et al., 2018; Zheng et al., 2018; Apthorpe et al., 2017; Birchley et al., 2017; Freed et al., 2017; Freed et al., 2018; Havron et al., 2019), 1 government document (Cyber Centre, 2019b), **1 corporate report** (Kaspersky et al., 2017) and **3 guides/webpages from a research project's website** (IPV Tech Research, n.d.; IPV Tech Research, n.d(b); IPV Tech Research, n.d.(c))

Table 1: Summary of Literature Review Documents

2.1 History of Home Automation and Gendered Design

The following is a review of scholarly research articles, mainly from science and technology studies (STS) and history. This situates the smart home in its historical roots, describes its evolution and links gender and smart home technology. In addition, I examined several archived Maclean's magazine (ranging from 1921-1962) and a commercial of the Westinghouse Home of the Future which are illustrative of the evolution of smart homes in Canada. As will be seen, this is useful, as the literature counters the contemporary and dominant 'innovative' and 'disruptive' technology narrative of smart home technology and situates these as part of a discourse of gendered technologies in the home while also affirming that these are

not as neutral as they are made out to be, as they embed a form of gender politics (Winner, 1980).

For centuries, mechanical innovations have been introduced into the home to reduce the burden of women's work. It is however beyond the scope of this thesis to examine all of these and I have chosen to start with the electrification of the home, as this is an enabler of home automation and smart home technologies. In Canada, electricity distribution varied between rural and urban households, thus home automation arrived in different places at different times. For example, Canadian historian Angela Davis highlights that despite various electric devices for the home being available at trade shows as early as 1910, electricity was not commonplace for people in rural areas in the Prairies in part due to the high cost of electrical generation plants and because the government and private companies neglected to extend power sources to these areas (Davis, 1993). The Second World War and the economic depression were also mitigating factors which further tampered efforts to extend electrical power to these communities (p.1).

Electrification is associated with the talk of 'labour-saving' electric appliances primarily in the United Kingdom, the United States of America and Canada which begins in the 1920s for urban areas (Aldrich, 2003; Barber, 1985). Appliances such as electric sewing machines and vacuum cleaners are introduced primarily to reduce the burden of household labour on women. However, access to these technologies remained relatively scarce due to their high cost and the uneven geographical distribution of electrical power. Shortly after the Second World War, the autonomy and technical competence demonstrated by women's contributions to the war effort were overshadowed by patriarchal ideals of women resuming their traditional roles as housewives, and this is further reinforced by post-war propaganda (Aldrich, 2003, p.19). During the 1950s, many appliance companies highlighted how electric devices could take away the

monotony of tedious domestic tasks such as laundry, cooking, and cleaning to grant housewives more time for leisure or other responsibilities. To illustrate how domestic technologies were marketed and framed, I selected several advertisements from multiple issues of Maclean's Magazine, ranging from the 1921 Sovereign Electric Iron to the 1962 Bell telephone, and others mostly published in the mid to late 1950s as seen in Figure 1 below.

Figure 1: Selection of Home Technology Advertisements from MacLean's Magazines, 1921-1962 (Maclean's, 1921-62)

This era was the precursor to today's smart homes, and the discourse of gendered spaces and practices in the home. As seen in the advertisements, many household appliances were target marketed at women and reinforced ideas that some spaces in the home such as the kitchen were largely 'feminine' domains. Moreover, almost all the advertisements contain photos of white, presumably middle to upper class women (due to the prices of these technologies). During this time, domestic technology advertising and women's magazines idealized the "white, middle-class family" and were not representative of other minority groups and classes (Walker, 2000). Furthermore, the appliances ads claimed that these technological innovations would save time, although as it turned out, it was discovered that this was not always the case (Vanek, 1974). Instead of saving time, some scholars have argued that these appliances merely changed how work was done and expectations by increasing volume of work, how often tasks should be performed, ultimately causing housewives to spend more time on housework before their introduction (Vanek, 1974; Bell and Dourish, 2007). These perceptions persist about labour saving technologies persist. For example, sociologist Anne-Jorunn Berg, after conducting interviews with three smart home prototype creators, concluded that assumptions that 'labour' saving devices make housework less tedious are often related to a lack of understanding of housework and women as a relevant social group who should be included in the design of these technologies (Berg, 1999). Like Berg, feminist sociologist Cynthia Cockburn (1997) noted the societal undervaluing of feminine and private spheres in terms of domestic technology and their designers as they still failed to meet user needs. More broadly, Cockburn argued that modern science and technology have been "deployed symbolically by men, the active sex in this project, as masculine" (Cockburn, 1993). As a result, she states that "contemporary western femininity has involved the construction of identities organized around technological incompetence" (p.37).

This mischaracterization of women consumers, negating to include women design choices and fundamental misunderstanding of household labour by the technology designers are likely some of the reasons that 'labour saving' devices did not really save any time at all. Furthermore, this discrepancy draws attention to the importance of the subjectivities of designers and how individual ideologies and social norms can become embedded into the final product, which unfortunately once they gain technological momentum and are hard to change and take back (Hughes, 1993).

So-called 'time-saving' technologies are often contrasted with 'time-using' technologies, which aim to make leisure time more enjoyable, and the television is an example of this. Some descriptions of time-using technology also claim that these technologies improve quality of life through improving leisure time (Crowley and Coutaz, 2015). Uses and descriptions of time-using technologies also often reinforce ideas of gendered spaces and practices in the home and depending on the price-points, perhaps class divides (who could afford time-using technologies and who had the 'downtime' to use them). For example, Davis (1993) argued that the telephone and radio which are typically classified as time-using devices had a greater positive impact on rural women's quality of life than time-saving electric appliances as these connected them to the outside world and provided entertainment during housework. A similar argument was made by Livingstone (1993), where women emphasized white goods[9] (i.e. time-saving) as necessities and entertainment objects (i.e. time-using) as luxuries even though these 'luxuries' were often used to make housework more bearable, such as the telephone to 'combat isolation' and a cassette player to 'return one's sense of self'. These views starkly contrast perceptions of the home and its technologies held by men, who see the home primarily as a site of leisure and technology such

[9] White goods refer to large household appliances such as refrigerators or ovens.

as the telephone as a means to facilitate business affairs (Livingstone, 1993). These discrepancies echo informatics scholar Paul Dourish and cultural anthropologist Genevieve Bell's (2007) statement about the history of domestic technology also serving as 'history of gender relations in the home' (p.7).

Inching closer to today's 'smart home', the mid 1950s and 1960s introduced visions of the all-electric home (Westinghouse, n.d.; Berg, 1999) and the beginning of 'wiring' homes with technologies such as electric heating and cooling (Aldrich, 2003). A video from the mid-1950s by the Westinghouse Electric Corporation enthusiastically depicted a home full of electric appliances while also perpetuating previous gendered divisions between home, work, and leisure. For example, women are shown cheerily using electric washing and drying machines, men are in awe of their ability control the heating and cooling of their homes and the entire family gathers around the television in the home entertainment centre (Westinghouse, n.d.; Figure 2).

Figure 2: Screenshots from Westinghouse's All Electric House Video, around mid-1950s (Westinghouse, n.d.)

The relationship between men and programming domestic technology is a normalized and dominant discourse. For example, the Westinghouse video links the ability of men to program the heating and cooling of their homes as an exercise of control. Livingstone (1993) found that women often viewed control as "keeping potential domestic chaos at bay" while control for men

signaled an “expression of expertise, permitting the exercise of control or power”. This later became associated to functionality, where men tended to use the terms ‘utilitarian’ and ‘functional’ to describe technology and emphasized the properties of an object rather than its role in their lives (Livingstone, 1993). In Bell and Dourish’s (2007) analysis of the shed as a hypermasculine space of the home, the authors drew upon a study by Rode et. al (2004) that identified gender division in terms of when, why, and what people program. Broadly, their study revealed that men were more likely to find programming entertainment devices such as VCRs and personal computers easier while devices of domestic control such as ovens were easier to use by the women surveyed. However, it is important not to misconstrue this as a lack of technical competency, as Cockburn (1993) previously noted. Blackwell (2006) conducted a study on domestic programming where men and women were asked to program a VCR. The research found that women were less likely to feel confident in their initial ability to program the VCR, citing a lack of expertise. However, it also found that despite this lack of confidence and purported lack of expertise women were equally capable of doing so and had high success rates when they attempted to do so. The results of these studies on programming align with Berg’s argument that despite the absence of women in the development of these technologies and the gendering of consumer technologies to be largely for the ‘technically-interested man’, technology is a process that is “open to flexible interpretation by its various user groups” (Berg, 1999, p.312). Therefore, even if technologies are designed without women in mind, it does not exclude women as a user group from using these technologies as they see fit.

Conversely, it is this very flexibility that enables smart home technology to be used for malice as just discussed, a brief review of the electrification of household appliances demonstrates how ideologies and social norms about gender become embedded within devices

and later, with broad use and some help with the marketing department, society. Thus, to understand the complexities of the contemporary, highly gendered issue of smart home TFV, it is helpful to examine the past gendered history of domestic technology, and to acknowledge that the discourse of innovation and disruption discourse when it comes to 'domestic technologies' are not new even though smart home technology enthusiasts frame it that way.

2.2 The State of Technology Facilitated Violence (TFV) Research

The concept of 'smart home tech abuse' also known as smart home TFV was developed by Dr. Leonie Tanczer, an international security and technology researcher (Tanczer et al., 2018). Tanczer and her team at the University College London analyzed the "evolving privacy and security risks of IoT systems in the context of domestic violence and abuse" and mobilized this knowledge into public facing material such as information pamphlets for local women's charities/shelters, police forces and IoT developers as seen in Figure 3 below (p.4).

Figure 3: Tech Abuse Diagram extracted from a policy brief (Tanczer, 2018)

Tanczer's research team in the United Kingdom (UK) conducted in-depth interviews, two workshops and several focus groups with 45 individuals (Tanczer et al., 2018, p.2; Tanczer et al., 2018b, p.4). They identified the need for 'tech abuse' to be recognized as a new category of abuse requiring resources such as skill development, the training of staff to handle these incidents and funding. Furthermore, the study found a general lack of awareness and data about smart home 'tech abuse' (Tanczer et al., 2018, p.5).

There are many forms of related TFV, cyberbullying or cyberstalking are two examples. Here I examine the history and evolution of TFV in general and how these different forms specifically relate to smart home TFV. Two prominent scholars on TFV are Anastasia Powell and Nicola Henry, Australian criminology and legal scholars and authors of multiple works on

TFV and technology-facilitated sexual violence (TFSV). In a 2014 article, they stress the importance of avoiding a false dichotomy between 'online and offline words' as 'corporeal bodies' maintain a presence in techno-social contexts especially since there is increasing dependency in terms of 'social and sexual relationships with others' on techno-social platforms (Henry and Powell, 2014, p.92). This false dichotomy is often seen in the case of smart home TFV, where there is the ability for technology to facilitate violence from the 'online' world into the 'offline world', effectively blurring the lines between these distinctions. Thus, they argue that TFSV (their focus) uses 'new' technology to perpetrate 'old' behaviours (p.9), echoing Dragiewicz et al. (2018)'s rationale for distinguishing TFV from other forms of violence. While these "old behaviours" may be understood by its experts (criminologists, legal scholars, etc.), new technologies create new risks, environments, and methods for violence deserving of attention. In a 2015 article, Henry and Powell called for empirical research to be done on the nature, scope and impact of TFSV to support policy and legislative action on prevention, punishment and remedy, arguing that a lag of research in this area is partly attributed by the false dichotomy between body and online and to the rapid pace of technological change (Henry and Powell, 2015, p.25). These issues are also likely at play for smart home TFV, as the rapid pace of smart home technology deployments and its increasing affordability may make it difficult for regulators and policy makers to keep pace.

Lastly, in 2018 their research brought attention to the insufficient means to prevent, punish and remedy TSFV in Australia via 30 stakeholder interviews with police, legal services and domestic and sexual violence service sector providers (Powell and Henry, 2018, p.2). They found a significant gap in empirical research on policing responses to adult victims of TFSV and an 'overwhelming' focus on children and young victims of TFSV, such as child sexual

exploitation (p.3). This focus on children often stems from society's perceptions of children as innocent, vulnerable, and needing of protection as well as "erroneous assumptions that only young people are victims of online predatory behaviour" (p.202), perhaps from their naivety. In a broader context, it is generally understood that violence against children of any kind can have "serious and lasting impacts on children's physical and mental health" and negatively impact social and economic well-being (Public Health Agency of Canada, 2019)[10]. To better understand the experiences of various stakeholders, Powell and Henry interviewed 12 members of the police force of various ranks and units, including sexual offences and computer crime units, 8 interviews with legal services stakeholders and 10 interviews with domestic violence and sexual assault services stakeholders (p.4). A few common concerns were identified as follows:

1. Most of the stakeholders identified the potential for law enforcement and courts to minimize the harms of TFSV because it only exists in the 'online' world, reminiscent of the false dichotomy Powell & Henry identified earlier (p.12).
2. Another common thread between stakeholders was their frustration with telecommunications service providers (telcos), resulting in cost and lost time because of a lack of cooperation, with one police interviewee stating that "in Canada, they can access information within two hours. We have to wait four to six weeks sometimes, from the bigger telcos in Australia" (p.13).
3. Lastly, stakeholders expressed an urgent need for more police training and resources on TFSV as well as legal reform.

Powell and Henry's interviews with stakeholders across policing are important as they affirm the need and desire for more training and resources in this sector and they provide insight into how TFV impacts organizations and institutions beyond an individual's household. Drawing upon the work on the continuum of sexualized violence by Liz Kelly, Powell and Henry poignantly state

[10] It is also generative to consider the concept of paternalism, which refers to "interference of a state or an individual with another person, against their will, and defended or motivated by a claim that the person interfered with will be better off or protected from harm" (Dworkin, 2020). While this may be helpful for protecting children, it can become tricky when paternalist rationales are used for protection of women as they may strip agency away from them through benevolent sexism, which refers to "prejudice expressed with a positive tone, with the assumption that women must be cherished and protected by men" (Estevan-Reina, de Lemus and Megías, 2020)

that “TFSV is not exclusively violence of a sexual nature, but rather it is much broader, encompassing gendered violence against deliberately constructed ‘sexed’ subjects the ‘myriad forms of sexism women encounter everyday through to the all too frequent murder of women and girls by men” (Powell and Henry, 2018, p.9).

In 2009, Finn and Atkinson highlighted the need for increased consumer education about the risks associated with information technology, especially to vulnerable populations such as domestic violence victims (Finn and Atkinson, 2009, p.7). The outcome of their research project was that training was useful and empowering for the participants. Also, suggestions to improve the training was largely positive, for instance to disseminated training materials more widely via a variety of formats such as in downloadable brochures, books, video and television public education and through broader community education as to schools and parents, social services, etc.) (p.6). This led to suggestion for a wider rollout of the Technology Safety Project[11] created by the Washington State Coalition Against Domestic Violence as a potential approach. It is suggested that the ‘newness’ of smart home TFV, will also likely require the means to better educate institutions and the public much like the knowledge mobilization material produced by Tanczer and her team (2018).

In a separate study of female survivors living in domestic violence shelters, Dimond, Fiesler and Bruckman found that many of the research participants were harassed by their abuser with the use of information communication technologies (ICTs) such as social media, texting and threats of GPS tracking (2011, p.1). As feminist human computer interaction (HCI) scholars,

[11] This project provided computer and Internet resources to domestic violence service providers in order to “(1) increase safe computer and Internet access for domestic violence survivors in Washington; (2) reduce the risk posed by abusers by educating survivors about technology safety and privacy; and (3) increase the ability of survivors to help themselves and their children through information technology” (Finn and Atkinson, 2009, p.1).

they drew attention to the ways that ICT enabled abuse changed the way survivors interacted with technologies such as mobile phones and social media. They also unfortunately observed that many of the women interviewed began to limit their participation on social media and the internet in general, which had a snowball effect when the time came to apply for jobs, as women stated they were scared to apply to any online job postings in fear that their abusers could gain access to information such as addresses (p.6). This fear also prevented many women from keeping in contact with their families, as some women reported their family members getting harassed and threatened by their abusers for information on the survivor (p.6). Dimond, Fiesler and Bruckman's research effectively drew attention to the potential safety issues related to survivors' usage of ICTs and the potential for these tools to further marginalize vulnerable people.

To prevent any disengagement with technology related to fear, Dragiewicz, Harris and Douglas recommend that future scholarship should "continue to investigate the helpful uses of technology, including apps and online support groups to better understand how survivors and advocates can increase safety and well-being" and potentially prevent domestic violence (2019, p.17). On the other hand, they also suggest further research be conducted about abuser behaviour and how to better understand their tactics to harm others (p.17). This is important because a significant portion of the research in this area involves studying the survivors rather than the abusers themselves, likely due to the difficulty of finding abusers willing to identify themselves and the safety risks posed to researchers. However, it is important to note that academic research is only one aspect of preventing further instances of domestic violence. There are many other key actors and industries that must be involved to enact meaningful change, socially and technologically, and unfortunately understanding the use patterns of abusers, is part of that

process. Thus, research and action using both victim-centered approaches and abuser behaviour centered approaches are integral to truly understanding the intricacies of smart home TFV. In this thesis, I will not examine the abuser's behaviour and how they manipulate their victims, but I examine, in Chapter 5, how smart home devices are re-purposed for abuse and what kind of features enable this behaviour.

Sociologist Delanie Woodlock in their article *SmartSafe* identified a demographic gap in terms of technology abuse victims in their study with the Domestic Violence Resource Centre Victoria (DVRCV) (Woodlock, 2017, p.1). The purpose of the *SmartSafe* study was to "examine how mobile technologies provide additional opportunities for the perpetration of stalking and domestic violence against women", with an emphasis on smartphones (p.5). While study results did indeed identify mobile technologies as a tool of domestic violence, Woodlock raised an important point on the limitation of surveying victims of tech abuse. That is, most survey respondents in the *SmartSafe* study were Anglo-Australian, which was an overrepresentation of one group (p.15). Domestic violence refuge workers confirmed Woodlock's concern, namely that "women from non-English speaking backgrounds are particularly vulnerable to technology-facilitated stalking" despite not participating in the survey (p.15). Clearly, an approach to the study of TFV that is cognizant of factors such as binary sex classifications, race, sexual orientation, ability, class and certain forms of labour is important in order to be fully representative of the broad range of potential victims. For example, victims of smart home TFV are not limited to intimate partners but could also be homecare/elderly care providers, housekeepers, or tenants, among others. In this thesis I will primarily focus on smart home TFV committed in a general familial environment (spouses, family members, ex-partners) as this is

the most commonly reported and documented form and when relevant, I will reference other potential scenarios.

Another good example of intersectional thinking about smart homes is Sophia Maalsen and Jathan Sadowski's article on domestic surveillance via smart home technologies and the implications of its evolving entanglement with the 'FIRE' sectors (finance, insurance, and real estate). In their article, the authors argue that it is critical to pose "political economic questions about whose interest and what logics are materialized by the smart home" and to move beyond the standard, basic technical questions such as encryption and data anonymization to evaluate the safety of these technologies (Maalsen & Sadowski, 2019, p.2). Theirs is an important intervention in the context of smart home TFV as a common misconception of smart home devices and IoT in general is that technical measures such as encryption make a device inherently safe to use[12]. By focusing on the FIRE sectors, the authors outline the potential risks of smart home data collection by third parties and the possibility of punitive corporate surveillance by companies in these sectors. For example, the dataveillance[13] conducted by insurance companies through access to smart home devices can directly impact someone's insurance policy and premiums if the insurance company deems their behaviour as 'bad' or 'high-risk', mirroring current credit scoring practices (p.4; Roderick, 2014; CIPPIC, 2006). This type of dataveillance is also appearing in the real estate sector, where the profiling, rating and management of tenants is becoming increasingly common (p.5). These practices are compared to predatory inclusion, "wherein financial actors like lenders offer needed products and services to members of marginalized groups but on exploitative terms that limit or eliminate their long-term

[12] See Apthorpe et al. and research conducted by IPV Research group at Cornell Tech in section 2.4.
[13] Dataveillance refers to the monitoring of online data through the continuous tracking of (meta)data for unstated, preset purposes with implications across the social fabric (Van Dijck, 2014, p.9).

benefits" (p.5). Furthermore, this predatory inclusion has the potential to become mandatory inclusion in the context of landlords or social housing, where tenants must accept that certain 'smart tech' will be installed in the home if they want to live there. Overall, this article is helpful in identifying other actors that have vested interest in the deployment of smart homes (in addition to smart home technology vendors) and the political economy of smart home tech data by exposing the broader surveillance apparatus. For the purposes of this thesis, this paper was helpful in outlining some of the broader power dynamics at play in the smart home in addition to the abuser versus victim/survivor. Furthermore, the role of the FIRE sectors in smart home data collection could be a consideration for consumer protection policy or legislation to limit the power of corporate surveillance, enhance privacy legislation, to provide clearer user agreements, in addition to provoking important legal questions when these sectors come to be implicated in smart home TFV and collect behavioural data about an incident.

There is extensive literature on the topic of TFV more broadly, but research about smart home TFV is only beginning to emerge. As smart home technology becomes ubiquitous and affordable, it will be imperative to pre-empt the potential harmful that smart home TFV may cause, not unlike the ongoing work related to other forms of TFV such as cyberbullying and cyberstalking.

2.3 Canadian Policy and Legal Environment

In this section I review relevant Canadian policy and legal actions related and applicable to smart home TFV. Here I also highlight some of the relevant government and non-government initiatives in Canada. This will provide a snapshot of the current policy and legal environment in in addition to relevant academic works.

Sociologists DeKeseredy and Dragiewicz (2014) have studied the history of 'Woman abuse' in Canada by examining sociological research conducted here since the 1980s (p.1). One of the most significant achievements highlighted by the researchers was the *Statistics Canada's Violence Against Women Survey* (VAWS), considered to be a world first in terms of a "national survey specifically designed to investigate multiple types of male-to-female violence" (p.1). Furthermore, the *Canadian National Survey (CNS) of Woman Abuse in University/College Dating* was "also the first countrywide study of its kind" (p.2). DeKeseredy and Dragiewicz explore how sociologists studied domestic violence in Canada, the creation of subcategories such as "intimate femicide" and how changes in governments and the political economy changed perceptions and actions (p.4). In terms of smart home TFV, the concept of "patriarchal discourses and practices" is important, as it encapsulates the issue of how information technologies such as websites "featuring women being degraded and abused in horrible ways" including pornography propagate this form of thinking (p.7). While it does not mention smart home TFV explicitly, their work to situate domestic violence research in Canada in its historical context is important , especially when considering the role of state actors such as Statistics Canada's to foreground these issues and how research such as this is funded, revealing the political economy of state funded research and government departments and their priorities at the time.

More recently, Canada signed onto the G7 *Charlevoix Commitment to End Sexual and Gender-Based Violence, Abuse and Harassment in Digital Contexts* (G7 Nations, 2018). This commitment includes an acknowledgement of the positive role technology can have to advance and empower women while also recognizing that the "benefits offered may be undermined by the perpetuation of new forms of violence, abuse and harassment" (p.2). G7 Nations committed

to a variety of actions (Appendix A), such as the promotion of "legal regimes, national anti-violence strategies and educational approaches", aimed to improve responses to data privacy breaches and to support the removal of "gender biases in the development of digital platforms and connected technologies from design to end-use" (p.3; Appendix A).

An interim compliance report by researchers from the Munk School of Global Affairs at the University of Toronto gave Canada a "+1" score (the highest possible) for compliance to this commitment. The researchers highlighted that the country's leadership on this issue within the Human Rights Council, the creation of the *Playbook for Gender Equality in the Digital Age* and announcing up to "$50 million CAD in funding for programs to support survivors of gender-based violence, including those addressing violence in the digital context" as proof of compliance to the Charlevoix Commitment (Hou, Tops & Ou, 2019). The *Playbook* was created in response to the United Nations' Special Rapporteur on Violence Against Women's call for documents on online violence against women (Global Affairs Canada, 2017). The Playbook's four areas of engagement such as: Access, Culture, Education, and International Frameworks were created based on a global survey conducted by Global Affairs Canada's Digital Inclusion Lab in November 2017. This survey included 50 stakeholders from civil society, public and private sector in addition to discussions at the following events: An event on Online Hate in Ottawa (February 2017), a workshop at the Internet Governance Forum (December 2017) and two rounds of online consultations (April and May 2017) (Global Affairs Canada, 2017). Each area for engagement included ten priority actions, with many relevant actions to smart home TFV such as:

- acknowledging systemic barriers for women, girls, and gender non-conforming individuals (literacy, education, location, mobility and social class) that could prevent effective use of information from digital technologies,
- the effects of technology on intersecting factors (age, ethnicity, race, religion, disability),
- personal ownership and control of devices,
- identification of existing power dynamics,
- teaching digital literacy and security basics in primary school and
- better training for law enforcement and prosecutors to better understand TFV among others (p.1).

Despite not explicitly acknowledging smart home TFV, the recognition of intersectional identities such as race, gender, class, etc. these are important and a government acknowledgement of the complexities related to these issues is promising (Woodlock, 2017).

The Government of Canada is also committed to addressing gender inequality with the implementation of Gender-Based Analysis + (GBA+) when it comes to government departments and procurement. Cabinet originally committed to Gender-Based Analysis (GBA) in 1995 following the ratification of the *Beijing Declaration*[14] by the United Nations at the Fourth World Conference on Women. At this conference, Canada's statement by the Honourable Sheila Finestone, the Secretary of State, Multiculturalism and Status of Women at the time, mentioned Canada's leading role in eliminating gender-based violence, including "strengthened laws, public education campaigns, building shelters, conducting the world's first national survey on violence

[14] The Beijing Declaration was created following the United Nations' Fourth World Conference on Women. The declaration affirmed the participating government's commitment to "advance the goals of equality, development and peace for all women everywhere in the interest of all humanity" (United Nations, 1995)

against women" and initiating the UN General Assembly's "Declaration on the Elimination of Violence Against Women" (Finestone, 1995). From 1995-2011, GBA was defined as "an analytical tool whose objective is to examine the differential impacts on both women and men of government policies, programs, and legislation" (Office of the Auditor General of Canada, 2009). However, no policy action was made on the implementation of GBA following the commitment in 1995. In 2009, the Auditor General created a report on the implementation of GBA and found that a lack of government-wide policy enforcing its use meant GBA was inconsistently implemented across the seven departments audited[15] and their respective programs, policy initiatives and acts of legislation, ranging from complete GBA frameworks in some departments (Indian and Northern Affairs) and no framework at all in others (Transport, Veterans Affairs) (p.1).

In 2011, GBA was rebranded to GBA+ by the department for the Status of Women[16] to incorporate intersectional identity such as race, ethnicity, religion, age, mental and physical disabilities, and non-binary people (Status of Women Canada, n.d.). As of 2016, all Memoranda to Cabinet and Treasury Board submissions require the addition of GBA+ (Status of Women Canada, 2017; Treasury Board Secretariat, n.d.). For other government processes, it is largely left to the discretion of the individual department to determine the extent to which GBA+ is integrated into their work (Status of Women Canada, 2016). However, the Privy Council Office

[15] The audited departments were: 1) Department of Finance, 2) Health Canada, 3) Human Resources and Skills Development Canada, 4) Indian and Northern Affairs Canada, 5) the Department of Justice Canada, 6) Transport Canada and 7) Veterans Affairs Canada (Office of the Auditor General of Canada, 2009).
[16] Status of Women Canada became the Department of Women and Gender Equality Canada (WAGE) as of December 13th, 2018 (Status of Women Canada, 2018). Most citations will use its former name for documents published before the rebranding and undated documents as the website retains the former name.

and Status of Women Canada are responsible for identifying departments who may need further support and training on GBA+ (p.1).

One relevant example of GBA+ use outside of Memoranda to Cabinet and Treasury Board submissions is the *Smart Cities Challenge* initiative by Infrastructure Canada. The *Finalist Guide* for submissions indicated that final proposals should detail "efforts made to be inclusive and consider the diversity of residents" in their engagement plans and suggest that GBA+ is an effective tool to accomplish this as it incorporates many of the considerations and intersections relevant to inclusivity and equity in cities (Impact Canada, n.d.). By integrating these considerations into urban planning and smart cities, this, in theory, is a step in the right direction to creating equitable and inclusive cities at large as these principles are 'baked in' rather than retrofitted afterwards.

In June 2017, the Department of Women and Gender Equality Canada launched *Canada's Strategy to Prevent and Address Gender-Based Violence,* which broadly sought to 'build on current federal initiatives, coordinate existing programs and lay the foundation for greater action on gender-based violence' under three pillars: 1) prevention, 2) support for survivors and their families and 3) promotion of responsive legal and justice systems (Status of Women Canada, 2017; Appendix B). The strategy includes six funded partners:

1) the Department of Women and Gender Equality Canada,
2) the Public Health Agency of Canada,
3) Public Safety Canada,
4) the Department of National Defence,
5) the Royal Canadian Mounted Police and
6) Immigration, Refugees and Citizenship Canada (Department of Women and Gender Equality, 2017).[17]

[17] The strategy also notes that other initiatives and agencies are important to this issue, such as Northern Affairs Canada, the Department of Justice, Statistics Canada and the Canadian Mortgage and Housing Corporation (Status of Women Canada, 2017)

Each of these departments has received funding for specific initiatives related to the three pillars outlined in the strategy (Appendix B).

The Department of Women and Gender Equality provides an Annual Progress document on the strategy, two of which have been published (2017-18 and 2018-19). In 2017-18, there was very little mention of any sort of TFV besides mentioning the *Charlevoix Commitment* and stating that 'work must be done in this area' (Status of Women Canada, 2018). This report also described an initiative with the Canadian Mortgage and Housing Corporation (CMHC) to integrate housing for women and children fleeing family violence as a priority housing category in the Canadian National Housing Strategy, but there is no mention of smart home TFV (Employment and Social Development Canada, 2018, p.1). One year later, in 2019, the Annual Report included *Addressing technology's role in gender-based violence* as a subheading of Pillar I: Preventing gender-based violence. While this is a step in the right direction, the focus is still mainly on forms of TFV such as cyberstalking, cyberbullying, and online child exploitation, with no mention of smart home technology (Department of Women and Gender Equality Canada, 2019). Many of the steps taken to address these forms of TFV are applicable to smart home TFV, such as identifying the need for national awareness. However, the exclusion of smart home TFV is quite unfortunate, especially as smart homes (and usage of individual smart home technologies) begin to proliferate, thus warranting attention.

In terms of cybersecurity, there have been no publications by departments such as the Communications Security Establishment and Public Safety Canada about smart home safety and cybersecurity. In their 2020-21 Departmental Plan, Public Safety Canada does not mention any action related specifically to smart homes, but some of the goals in the "Implementation of the National Cyber Security Strategy" section remain relevant. One relevant goal includes its

leadership in the government's 5G wireless network policy coordination efforts (Public Safety Canada, 2020, p.12), as 5G is considered a key enabler for IoT deployments such as smart cities (Dobby, 2018) and by extension smart homes. Other goals such as supporting the development of the Canadian Centre for Cyber Security[18] and coordinating a "cross-cutting government-wide data strategy for cyber security" including "measuring the impact of cybercrime on Canadian businesses" could be helpful for issues such as smart home TFV in the future should they be expanded upon.

The National Cyber Security Strategy briefly mentions the rapid growth of the IoT and its cybersecurity concerns, including IoT devices' vulnerability to hacking (Public Safety Canada, 2018) Besides this, the strategy notes that our current cybersecurity methods such as encryption will soon be challenged by the arrival of quantum computing[19] (p.15). The strategy also notes the government's commitment to making "smart investments in cyber security while also advocating for its partners in the private sector and other jurisdictions to do the same" in the context of smart cities (p.29). There is also no mention of TFV.

Finally, the Canadian Centre for Cyber Security (nicknamed the Cyber Centre) created in 2018, to consolidate "Public Safety Canada's Canadian Cyber Incident Response Centre and Get Cyber Safe public awareness campaign, Shared Services Canada's Security Operations Centre and the Communications Security Establishment's Information Technology Security branch" (Public Safety, 2018b). The Cyber Centre's main purpose is to provide a "single unified source

---

[18] Cyber Security is two words in this instance as it is the name of the centre, however it is generally one word and will continue to be throughout this thesis, unless referring to the Cyber Centre or publications that use this convention.

[19] The Canadian Centre for Cyber Security's Glossary notes that a quantum computer differs from a classic computer because of its ability to "process a vast number of calculations simultaneously". A quantum computer's ability to use "ones, zeroes and 'superpositions' of ones and zeroes" (instead of a classic computer's usage of ones and zeroes) facilitates tasks previously thought impossible, such as cracking encryption codes (Canadian Centre for Cyber Security, n.d.).

of expert advice, guidance, services and support on cyber security for government, critical infrastructure owners and operations, the private sector and the Canadian public" (Canadian Centre for Cyber Security – 'About Us', n.d.). An example of guidance provided by the Cyber Centre is their quick guide to IoT security for small and medium organizations, which clearly explains what IoT is, some risks for organizations and basic security hygiene such as installing patches and changing default passwords (Canadian Centre for Cyber Security, 2019). While it is excellent that these resources are being developed, it is important to note that this guidance does not necessarily explain how to do some of the tasks they are recommending, which may pose problems for less technically savvy people as these resources assume a baseline of technical knowledge, which can vary greatly in the smart home TFV context (e.g. different family members' experience or comfort with technology, a senior gifted a smart home device).

Shifting to the state of the Canadian legal environment, legal scholars Jane Bailey and Carissima Mathen conducted a review of over 400 TFV cases in Canada and discussed how current state of criminal law is responding to TFV, with their reviewed cases being filed under 27 different offences, but not without some issues (Bailey and Mathen, 2019). In a presentation of their work, Bailey pointed out that for a handful of the cases examined, court analysis of harm and violence was decontextual or acontextual from the cases, causing misinterpretations of harm (Bailey and Mathen, 2017). Bailey uses the example of a case where a man was acquitted from a criminal harassment charge as the court deemed his actions: moving to the same province as an ex-partner, posting pictures of places the ex-partner frequented and posting comments expressing longing for her on Facebook; as non-threatening and benign because they were posted publicly and not directly sent to the ex-partner (Bailey and Mathen, 2017). Clearly, this interpretation is problematic for cases of TFV where threats and harassment may be subtle or present in new

forms for which there may not have a developed precedent for. Furthermore, Bailey and Mathen (2019) also note the limitations of criminal law, including its disproportionate effect on racialized people, especially Black and Indigenous and the need for broader social transformation to truly eradicate all violence against women and girls (p.695). One relevant finding from Bailey and Mathen (2017) in a broader context is a noted lack of safeguards for women's expectation to privacy in public, which may be an important consideration for deployments such as smart cities where data collection becomes ubiquitous. Thus, it is interesting that despite the flaws Bailey and Mathen note, Canada still received a top score in commitment to gender equality as mentioned previously (Hou, Tops and Ou, 2019), meaning that top rankings do not necessarily mean no room for improvement.

In their legal review of spyware and stalkerware[20] in Canada, researchers at the Citizen Lab[21] made similar findings to Bailey and Mathen in terms of the reach of Canadian law whereby the creation, use and sale of spyware violates numerous civil, criminal, privacy and regulatory laws but its legality has not been closely considered by the Canadian legal system (Khoo, Robertson and Deibert, 2019, p.1-2). Furthermore, the report highlighted three potential loopholes in the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's consumer privacy and data protection law, that "may allow stalkerware vendors to circumvent accountability" (p.2). The end of their report included recommendations for actors in criminal and family justice systems, federal and provincial lawmakers, the Office of the Privacy

[20] As defined by the Citizen Lab, spyware refers to software that "possesses powerful surveillance capabilities", often marketed "intimate partner surveillance, parent-child monitoring, or monitoring of employees. When these powerful capabilities are used to facilitate intimate partner violence, abuse, or harassment, we refer to such spyware as stalkerware. (Parsons et al., 2019)

[21] The Citizen Lab is an interdisciplinary research lab based at the Munk School of Global Affairs and Public Policy, University of Toronto concerned with issues at the intersection of "information and communication technologies, human rights and global security" (Citizen Lab, n.d.).

Commissioner of Canada and to app developers, technology companies and app intermediaries (such as app stores) (p.170-74). Like Bailey and Mathen, the Citizen Lab's holistic review of spyware and stalkerware stated that while their recommendations are meant to help address TFV in Canada, they still cannot sufficiently address "the reason for which stalkerware is a problem in the first place: the broader context of patriarchal gender inequalities, misogyny, and corrosive societal norms around controlling, abusive, and violent behaviour directed at women, girls, non-binary persons, and children" (Parsons et al., 2019, p.145).

At a more grassroots level, a variety of coalitions, charities, and other non-government organizations (NGOs) committed to ending gender-based violence and/or domestic abuse have published guides for victims of tech abuse and the organizations that support them. In 2015, the Ottawa Coalition to End Violence Against Women (OCTEVAW) published their report on Cyber Violence against Women and Girls with the purpose to explore "what research and news media coverage tell us about cyberviolence, what sorts of social responses have taken place to date, and the relationship between social media structures and policies and cyberviolence" (Fairbairn and Black, 2015). Interestingly, the report categorizes cyberviolence into three subsections:

1) online harassment,
2) non-consensual distribution of intimate images and
3) cyberstalking/digital dating violence (p.9).

Furthermore, the report focuses on cyberviolence as a phenomenon that remains in the online realm, rather than technology facilitated 'real-world' or 'physical' abuse such as human trafficking via the Internet (p.14). The report also stresses the evolving nature of cyberviolence and emphasizes the importance of using sources within the last five years (p.9). As this report is

close to five years old, it is important to think about how much the landscape has changed since then, including the new phenomenon of smart home TFV and will continue to change. These rapid changes illustrate why it is so important to distinguish tech violence from others because it is constantly redefining how violence can occur and how new 'categories' emerge over time.

More recently, the British Columbia Society of Transition Houses (BCSTH) published a guide entitled *"A guide for Canadian women experiencing technology-facilitated violence: Strategies for Enhancing Safety"* in 2019. This guide includes general technology safety planning tips such as changing passwords and smartphone settings, keeping copies of evidence and strategies for safer technology use (Wong, 2019). While the report does not explicitly discuss smart home TFV, the report links to BCSTH's "Technology Safety and Privacy Toolkit for Canadian Women Experiencing Technology Facilitated Violence" page, which includes a brief 'explainer'-style paper on the privacy and safety concerns of IoT devices. This paper links to more in-depth papers written by the National Network to End Domestic Violence (NNEDV), an American non-for-profit organization. NNEDV's paper on home automation provides a brief explanation of home automation abuse survivor privacy risks and strategies, including a list of potential technologies that can be abused as well as how they may be used for safety (National Network to End Domestic Violence, 2018). However, due to its brevity, it does not discuss in detail what a victim should do if they are subject to this kind of abuse. In addition, since it is a brief explanatory paper, it does not discuss how this abuse could potentially be mitigated by industry and/or government intervention, connecting the topic to the wider smart city discussion.

In terms of the wider smart city discussion, a potential new site of smart home TFV is the integration of smart devices to care for the elderly. In their Smart Cities Challenge proposal, the city of Cote Saint-Luc, Quebec discussed their VillAGE initiative, which they describe as "the

future of aging in community, positioned to support the health sector while leveraging the trust and relationships that exist between people and their community (City of Cote Saint-Luc, 2019). Using a smart home solution developed at the University of Sherbrooke coupled with a mobile app, VillAGE seeks to achieve the following results for its senior residents

> (1) live more safely and independently in their homes; (2) be better connected to their communities and city services; (3) be more socially engaged, improving the overall well-being and quality of life for older adults and reducing stress on families and caregivers, the healthcare system, and long-term care facilities. (City of Cote Saint-Luc, 2019).

While the report discusses some privacy measures such as Privacy by Design[22] and the creation of data governance and privacy protection policies, it is not clear if the team considered the potential for abuse. Other considerations that are relevant to this smart city submission but not necessarily discussed are issues of repair and maintenance over time.

Overall, there has been important action in Canada to raise awareness and begin to create various preventative and reactive measures to counter gender-based violence, including some related to TFV. The actions taken in Canada seem to confirm some of what the academic research has found in terms of TFV globally, such as the fear of minimization by law enforcement, the need for more training on TFV and the importance of thinking inclusively about the impacts of technology. Also, as discussed, an important pattern in TFV research is that much of the responsibility for safety falls upon a user or victim/survivor, raising questions as to why more responsibility for safety is not put on other stakeholders such as the police, federal government or technology designers.

---

[22] Privacy by Design are a set of information management principles created by Dr. Ann Cavoukian, former Privacy Commissioner of Ontario, that can be applied to "specific technologies, business operations, physical architectures and networked infrastructure − entire information ecosystems" (Cavoukian, 2011).

2.4 Technical Research on Smart Home Technology Safety

Academic literature from disciplines such as systems and computer engineering and human-computer interaction are included in this chapter to explain how these technologies operate and to identify current and emerging technical issues (e.g. cybersecurity and data collection concerns). I begin by examining issues surrounding IoT in general and then narrow to issues specific to stalkerware and smart home TFV.

One of the most well-cited articles on IoT examines the origins and consequences of the very term 'Internet of Things', its architecture, use cases and potential challenges for IoT implementation (Atzori, Iera and Morabito, 2010). The authors, all electronic and computer engineers, view IoT as a paradigm with many 'visions' that contributes to the relatively vague and nebulous term 'Internet of Things' which are: 1) Internet Oriented, 2) Things Oriented and 3) Semantic Oriented visions (Atzori, Iera and Morabito, 2010, p.3; Figure 4).

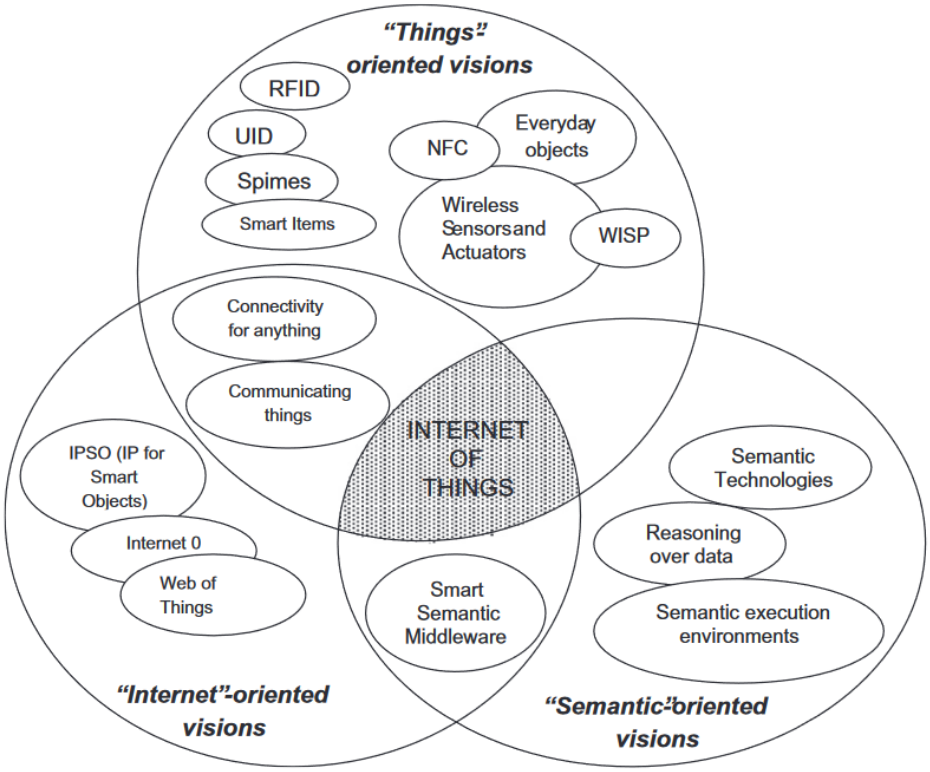


Figure 4: Visions of IoT Venn Diagram (Atzori, Iera and Morabito, 2010, p.3)

Figure 4 illustrates the internet-oriented visions focus on the networked portion of IoT such as internet access or IPSO, a communication protocol for smart objects. Things oriented visions, as the name suggests, are concerned with both the 'physical' parts of the IoT (devices, sensors) and enablers of individual devices (unique identifiers, near field communications). Semantic oriented visions emphasize what may be conceived as the 'smart' component of IoT in other disciplines, such as the ability for IoT devices to understand data. Ideally, all three visions are considered equally to form the best representation of what the IoT is. However, the authors argue that a consequence of the nebulous term is that these different visions have the potential to confuse or 'push' people towards a certain view over others, which can have major implications for institutions trying to define IoT, especially in a policy or governance context, as in the case of smart home as it is an IoT application (Atzori, Iera and Morabito, 2010, p.3; Figure 4). These

visions also represent the subjectivities of various stakeholders who may be drawn to one vision or component. For example, a data scientist may be pushed towards the semantic vision of IoT while an environmental scholar may be concerned with e-waste and be drawn to the 'Things' oriented vision.

Atzori, Iera and Morabito also listed many IoT use cases as seen in Figure 5 below, many of which are relevant to smart homes and smart cities such as healthcare (assisted/elderly living at home) and smart environments (authors include 'comfortable homes/offices) (p.8) and they identify several open issues that need to be addressed.

Open research issues.

Open issue	Brief description of the cause	Details in
Standards	There are several standardization efforts but they are not integrated in a comprehensive framework	Section 5.1
Mobility support	There are several proposals for object addressing but none for mobility support in the IoT scenario, where scalability and adaptability to heterogeneous technologies represent crucial problems	Section 5.2
Naming	Object Name Servers (ONS) are needed to map a reference to a description of a specific object and the related identifier, and *vice versa*	Section 5.2
Transport protocol	Existing transport protocols fail in the IoT scenarios since their connection setup and congestion control mechanisms may be useless; furthermore, they require excessive buffering to be implemented in *objects*	Section 5.2
Traffic characterization and QoS support	The IoT will generate data traffic with patterns that are expected to be significantly different from those observed in the current Internet. Accordingly, it will also be necessary to define new QoS requirements and support schemes	Section 5.2
Authentication	Authentication is difficult in the IoT as it requires appropriate authentication infrastructures that will not be available in IoT scenarios. Furthermore, things have scarce resources when compared to current communication and computing devices. Also man-in-the-middle attack is a serious problem	Section 5.3
Data integrity	This is usually ensured by protecting data with passwords. However, the password lengths supported by IoT technologies are in most cases too short to provide strong levels of protection	Section 5.3
Privacy	A lot of private information about a person can be collected without the person being aware. Control on the diffusion of all such information is impossible with current techniques	Section 5.3
Digital forgetting	All the information collected about a person by the IoT may be retained indefinitely as the cost of storage decreases. Also data mining techniques can be used to easily retrieve any information even after several years	Section 5.3

Figure 5: Open Research Issues in IoT (Atzori, Iera and Morabito, 2010, p.11)

Many of the issues initially highlighted by Atzori, Iera and Morabito in 2010 remain as issues today. Specifically, issues related to standards, authentication, data integrity, privacy and digital forgetting are related to smart home TFV. Furthermore, issues of privacy and standards

have become a priority in technology policy more broadly due to events such as the enactment of the General Data Protection Regulation in the European Union (EU GDPR)[23].

In 2017, the same authors explored the evolution of the IoT and its role in addressing various societal challenges (Atzori, Iera and Morabito, 2017) and divided these into three 'generations': RFIDs & Sensors (1st Generation), Web Services and Internetworking (2nd Generation) and Social, Cloud and Information Centric Networking (3rd Generation) (p.2). Some of challenges relevant here include secure societies, inclusive/innovative and reflective societies and health and wellbeing (p.4). Another interesting aspect of this article was the inclusion of the roles of both the public and private sectors in spurring innovation and adoption of the IoT (p.4-5). Lastly, the authors provide a new definition of IoT, defining it as:

> a conceptual framework that leverages on the availability of heterogeneous devices and interconnection solutions, as well as augmented physical objects providing a shared information base on a global scale, to support the design of applications involving at the same virtual level both people and representations of objects (p.16).

This is especially relevant here because it provides a more holistic view of the IoT (including human and non-human actors) and is flexible enough to accommodate for future developments and deployments.

Due to the vast nature and rapid growth of the IoT, it can be difficult to keep track of emerging trends, problems and even types of devices. In their article, Alaa et al. (2017) attempt to create a 'coherent taxonomy' of smart home app research by scanning three databases (Web of Science, IEEE Explore and ScienceDirect) for relevant literature. In their study of 229 articles, they developed a taxonomy of four classes:

---

[23] The GDPR is a European Union regulation on data protection. Enacted in 2018, the GDPR sought to improve data protection in the EU and grant its citizens more control over their personal data (European Commission, n.d.).

1) review and survey articles,

2) Studies on IoT app usage in smart homes,

3) System Design Proposals and Frameworks for Development and Operation of apps and

4) Reports of actual attempts to develop apps (Alaa et al., 2017).

This taxonomy is relevant here in the following two ways. First, the taxonomy is a demonstration of how siloed research in this area can be. While only three databases were chosen likely for brevity and proximity or 'relevance' to the author's technical fields, the addition of at least one social science-based database would have further enriched the results. For example, if a social science (or multidisciplinary including social science) database such as SAGE had been included, perhaps a category such as research on the social implications of IoT would have emerged. Furthermore, the article includes a 'challenges' section, where many of the challenges flagged by the authors are relevant to smart home TFV (security, privacy, data management and safety) but are never connected to smart home TFV by the authors themselves.

Geneiatakis et al. (2017) get a little closer to addressing smart home TFV through their creation of a smart home threat model using an architecture that would likely mirror a typical smart home set up of 'off the shelf' technologies that are interconnected (p.2). The authors found that the smart home was particularly vulnerable to attacks such as eavesdropping and software exploits but did not necessarily consider threats that occur when the adversary is someone in the home, such as an abusive spouse (p.3-6). The abusive spouse or ex-partner as a potential adversary is also not mentioned in Bugeja et al. (2017)'s six 'classes' of malicious threat agents for smart connected homes. Their six 'classes' include: 1) nation states, 2) terrorists, 3)

competitors 4) organized crime, 5) hacktivists and 6) thieves, which are then compared to one another by capability level and motivation as seen in Figure 6 below (p.3-4).

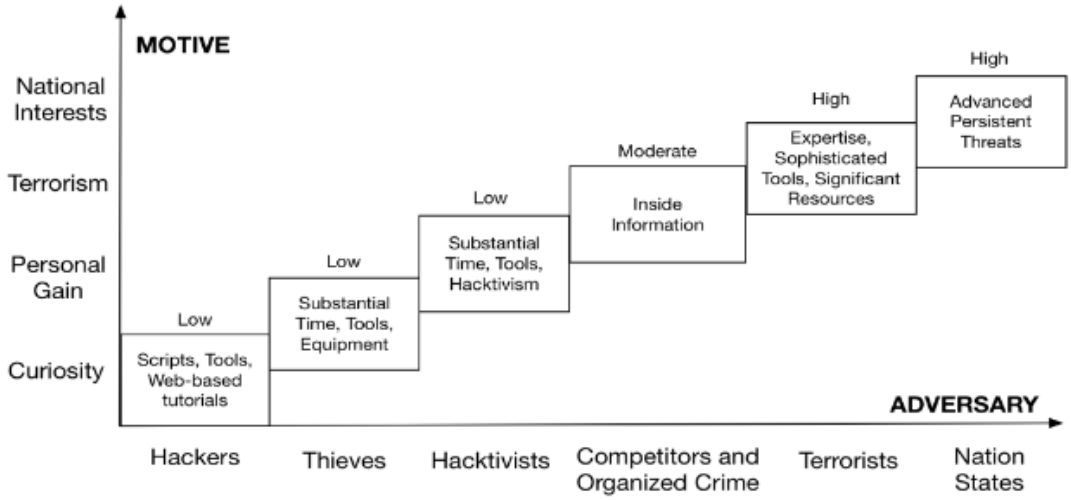


Figure 6: Six Classes of Smart Home Threat Agents Compared by Motive and Capability (Bugeja et al., 2017, p.4)

It is interesting to note that in their introduction to the Canadian Cyber Threat Environment, the Cyber Centre uses a nearly identical taxonomy: 1) nation states, 2) cybercriminals, 3) hacktivists, 4) terrorist groups, 5) thrill seekers and 6) insider threats (Cyber Centre, 2019b). While it is true that all of the threat agents could attack a smart home, the exclusion of in-home or remote adversaries such as ex-partners or abusive spouses that a home dweller may know personally is problematic because it contributes to the false narrative that smart home technology can only be weaponized by the technically literate (Freed et al., 2018) as even the least skilled of these threat agents, a hacker, is still more likely to be more sophisticated than an average smart home owner. However, it also could be argued that its exclusion is helpful in the sense that it highlights a gap in knowledge within the technical disciplines, as the authors used documents from 'scientific literature' as well as 'industry reports, news articles, penetration testing reports and hacking conferences' (Bugeja et al., 2017, p.1). In a different article, the same

authors conduct a study on the types of data captured by 39 smart home devices through an analysis of their privacy policies (Bugeja et al., 2018). While the authors do not connect the risks of this data collection with smart home TFV, it clearly demonstrates the sheer amount of sensitive data that these devices collect (p.11, Figure 7) and provoke questions about the consequences of their potential linkage or triangulation (Zheng et al., 2018) and exploitation which are cause for great concerns. Seemingly harmless data such as device information, when combined with other data, can provide a clear and scarily complete picture of someone's activity, preferences, location, etc. (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). Also as seen in the table, there are many simple technologies in a smart home, and it is one thing to control one device, but control of multiple SHTs can be become complicated in multivendor smart homes, where each device is subject to its own privacy policies and terms of use.

Device type	CI	DI	PAD	UAD	CS	LI	FI	ED	UGC	OD
Music player, gateway/hub	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Door bell, audio speaker, TV, irrigation controller	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
Scale, plug, light switch, light bulb, wireless signal extender	✓	✓	✓	✓	✓	✓	✓	–	✓	–
Switch, power outlet, oven, clothes dryer	✓	✓	✓	✓	✓	✓	–	✓	–	–
Vacuum cleaner, floor mopper, floor scrubber, gutter cleaner	✓	✓	✓	✓	✓	✓	✓	–	–	–
Tracker	✓	✓	✓	✓	✓	✓	–	✓	✓	–
Blood pressure monitor, temperature sensor	✓	✓	✓	✓	✓	✓	–	✓	–	–
Remote control, light strip, cooker	✓	✓	✓	✓	–	✓	✓	✓	✓	✓
Air quality sensor, rain sensor, CO2 sensor, wind speed sensor	✓	✓	✓	✓	–	✓	✓	–	✓	–
Siren	✓	✓	✓	✓	–	✓	✓	✓	✓	–
Cloud camera	✓	✓	✓	✓	–	–	✓	✓	✓	–
Shower head water meter	✓	✓	✓	–	✓	✓	✓	✓	✓	–
Bar code scanner	✓	✓	✓	✓	✓	✓	✓	✓	–	–
Thermostat, Smoke detector	✓	✓	✓	✓	✓	✓	–	✓	–	–
Cloud camera	✓	✓	✓	✓	–	–	✓	✓	✓	–
Door lock	✓	✓	✓	✓	–	✓	✓	–	–	–
Accelerometer sensor	–	–	✓	✓	–	✓	✓	✓	✓	–

"✓" = data type is captured; "—" = data type is not specified to be collected.

Legend

CI = Contact Information
DI = Device Information
PAD = Personal/Account Details
UAD = User Activity Data
CS = Configuration Settings
ED = Environmental Data
UGC = User-Generated Content
OD = Offline Data

Figure 7: Types of Data collected by Device Type (Bugeja et al., 2018)

Apthorpe et al. (2017)'s study on smart home devices demonstrates how technical measures such as encryption can still be circumvented. Even when data are encrypted, an actor such as an internet service provider (or a network observer) can still "infer privacy sensitive in-home activities by analyzing internet traffic" from smart home devises (p.1). The authors suggest potential mitigation measures such as traffic shaping, but also poignantly state that the reliance of smart home technology on internet infrastructure, the key to the 'smart' component of these devices is the root cause of their insecure nature. In fact, some smart home technologies do not have "minimum reliable product", meaning their products are rendered useless without an internet connection, incapable of functioning to the same level as their analog counterpart[24] (p.9).

[24] Another common occurrence is 'bricking' either via malware or software updates from the vendors themselves (usually to discontinue products) which refers to the "deliberate impairment or destruction of software with the intention of negatively affecting product functionality" (Tusikov, 2019).

While not necessarily related to smart home TFV, the issues identified by the paper are relevant to broader discussions of cybersecurity in the home.

Instead of focusing on only the IoT technology, Birchley et al. (2017) conducted a study on the people working on IoT and smart homes. The research team interviewed twenty early to mid-career smart home researchers about their concerns and priorities. Many of the interviewed researchers identified their primary concerns as being about the privacy and security of these devices, especially since they worked on medical devices, which often collect highly sensitive patient data. In addition, the interviewees discussed the notion of end-user choice and its relationship to user privacy at length (Birchley et al., 2017, p. 6-7). While a majority of interviewees felt that it was important for users to have a choice about what features are enabled or which kinds of data are collected, one specifically pointed out the complicated nature of 'choice' in the home, arguing that it is fine for a user to choose for themselves, however, they argued, this becomes ethically and perhaps legally complicated when the device is deployed in a household with children and/or non-consenting adults (p.7). While this article did not focus on smart home TFV, many of the core concerns associated with medical IoT devices are also present in smart home devices because of the intimate settings they are placed within and the potentially sensitive data they collect. Moreover, Birchley's approach to interviewing people involved in the research and development (R&D) of IoT technology serves as a helpful reminder that these technologies do not exist in a vacuum but have a multitude of actors associated with their conception, development, dissemination and end-use.

An interesting example of a multidisciplinary technical initiative is *The Intimate Partner Violence (IPV) Tech Research Group* at Cornell Tech. Founded in 2017, the research group combines expertise in computer security, social science, human-computer interaction and law

and policy to develop new tools, techniques and theory to combat TFV (IPV Tech Research – '*About*', n.d.). The research group includes a variety of partners ranging from other academic institutions, municipal government, and non-profit organizations focused on the eradication of domestic violence and top companies including Google[25], Facebook and Symantec (p.1). The group published a variety of academic articles in addition to public facing resources such as a privacy checkup guide, a Python software application that scans smart devices for spyware, and interview materials used in their computer security clinics with survivors of TFV (IPV Tech Research – *'Resources',* n.d.). One resource of interest is their app classification guide, which clearly demonstrates the 'dual-use' of various apps: intended and unintended uses (Figure 8; Khoo, Robertson and Deibert, 2019; Parsons et al., 2019).

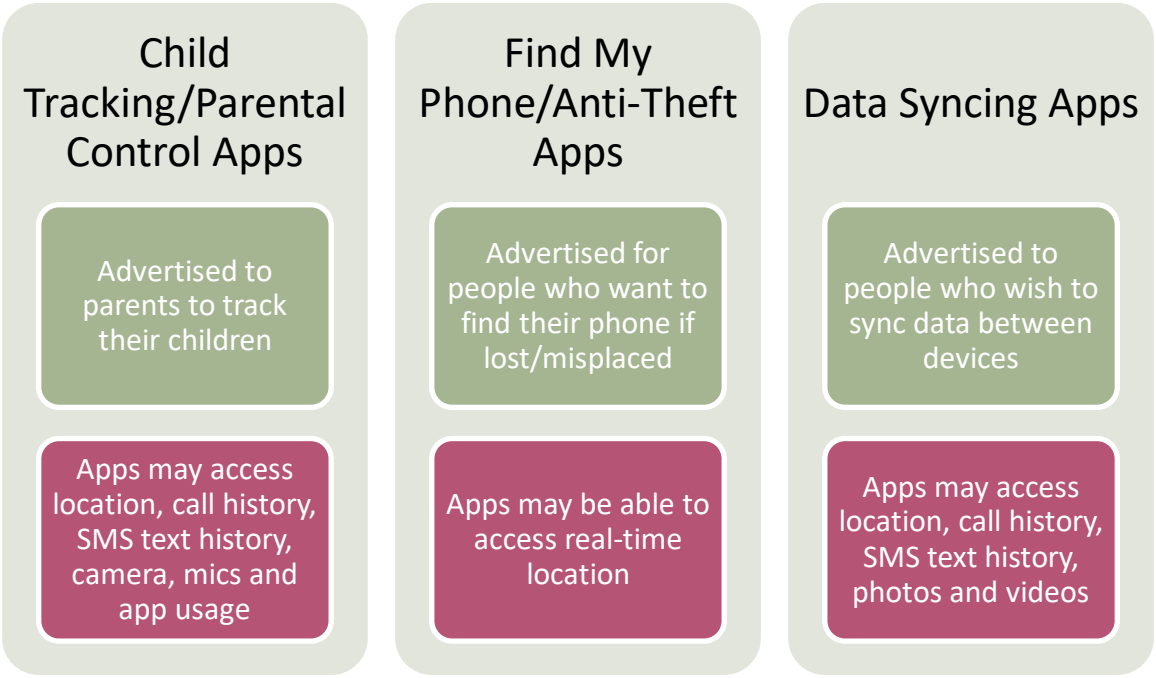


Figure 8: Examples of Dual-Use Apps (derived from IPV Tech Research - *App Classification Guide*, n.d.)

[25] Google is especially interesting as it is the maker of a variety of smart home technologies (including the Nest Mini examined in Chapter 5) and a major player in the discussion of smart cities via Sidewalk Labs.

Their education materials clearly emphasize the dangers of a variety of different smartphone and tablet applications and provide easy to use, tangible tools to combat them such as the spyware scanning app or the privacy checkup list, both with detailed instructions. The group's academic articles often involve qualitative interviews with survivors of TFV to ensure that their experiences are accounted for in any sort of recommendations or technical solutions the research group provides (Havron et al., 2019). By conducting these interviews, the researchers are able to discover different ways or 'channels' that survivors are being targeted, which is critically important as each case of TFV, smart home or not, is unique to the individual and there is likely not a 'one size fits all' solution. For example, an interviewee stated that an abusive ex uses the Facetime video chat app with their child to see where the family is at the time of the call and what they are doing, making the interviewee feel like the abusive ex never left (Freed et al., 2017, p.9). Furthermore, the group's frequent collaboration with municipal government (New York City) 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 (p.2). They too however have not specifically examined what the abuser does (see Dragiewicz, Harris and Douglas, 2019).

Lastly, the group's research provides salient points about the human-computer interaction aspects of TFV, which are relevant when discussing the social impacts of technology as interfaces and technology design play a direct and critical role in how technologies are used, as it is decisions on this level that determine the affordances that affect TFV methods. One of the benefits of interviews with survivors conducted by privacy researchers and computer security experts is that the team was able to identify that many of the attacks used against survivors in

cases of TFV were technically unsophisticated, meaning there is a higher risk of TFV occurring due to limited technical knowledge or savviness needed to harm someone (Freed et al., 2018; see Chapter 5). This is an important distinction to make as on the surface, TFV and smart home TFV may seem like they require deep technical knowledge to inflict harm, which is not the case. Furthermore, Freed et al. (2018) argue that despite HCI's purpose often to facilitate the use of technology, that there is perhaps a need for HCI professionals to consider hampering usability for adversarial users such as TFV perpetrators and for this to be a part of the design process (p.10).

Overall, the IPV Tech Research group publications are an excellent resource about TFV even though not explicitly about smart home TFV. Also the group included new actors with different subjectivities in their study, and demonstrated the importance of human computer interaction experts, and privacy and criminal justice specialists, and how their inclusion enriched their partnerships with a variety of stakeholder and provided assistance to survivors, important learnings when it comes to smart home TFV.

The research team also partnered with the *Coalition Against Stalkerware*, that included ten organizations ranging from cybersecurity, law and non-profit sectors who combined their expertise to "facilitate communication between the security community and those organizations working to combat domestic violence" in order to "help victims, facilitate knowledge transfer, develop best practices for software development" and increase public awareness (Kaspersky, 2019, p.2). A report published by the coalition includes new statistics on the prevalence of stalkerware worldwide, citing a 323% increase from 2018 in the proliferation of these technologies with 518,223 cases in 2019 in instances where their Kaspersky's software detected stalkerware already installed on a user's device or an attempt to install it (p.5). This is an

alarming, especially when considering this only accounts for stalkerware detected by one company's software and does not necessarily consider all the apps or devices that could be used for smart home TFV. The report goes on to detail the current threat landscape of stalkerware, including the top ten countries where stalkerware is installed, Canada is not one of them, and the rising popularity of stalkerware. The report concludes with recommendations such as: continuous collaboration between IT security companies and advocacy organizations (p.10) but overall, it is largely focused on improvements to Kaspersky's own detection software. In the context of smart home TFV, it would be interesting to see if such a coalition formed with stakeholders like the *Coalition Against Stalkerware* as most of these stakeholders are also impacted by smart home TFV. Furthermore, this report provided insight into the solutions created by industry and other private sector actors that are sometimes lacking in academic research despite their important role.

2.5 Summary

Here I examined literature in the social science and technical fields as well as grey literature from governments, civil society organizations and the private sector to identify any gaps in knowledge about smart home TFV. Table 2 (below) summarizes the findings of the literature review. Overall, there is a distinct lack of academic research and legislative action in Canada on smart home TFV. Currently, the most fruitful literature related to smart home TFV was concerned with other forms of TFV such as cyberstalking, cyberbullying, and online child exploitation. Furthermore, there is very little in the literature that connects any form of TFV with the current and future implementations of smart cities, and instead the focus is on how forms of TFV fit into current legal and policy regimes. Moreover, while this is rapidly changing, there is still a lack of acknowledgement of the dangers of smart home TFV and abusers as malicious actors or adversaries in some technical literature. However, the literature review did identify a

variety of stakeholders that may be affected by smart home TFV due to its proximity to other forms of TFV and that some issues and solutions although not specifically about smart home TFV are translatable to this context.

This thesis aims to mitigate this shortfall in the following ways: by conducting a study on smart home TFV in the Canadian context, connecting smart home TFV with the implementation of smart cities and mobilize knowledge from across disciplines to incorporate as many perspectives as possible.

Section	Source type and authors
2.1 - History of Home Automation and Gendered Design	•Establishes clear evidence of gendered space and practice in the home and how domestic technology predates smart home devices •Introduces concept of time-using versus time-saving devices, nuance between entertainment and instrument
2.2- The State of TFV Research	•Research specific to smart home TFV beginning to emerge but still relatively lacking when compared to other forms of TFV •TFV blurring distinctions between online and offline harm •Training needed for frontline organizations on new forms of TFV
2.3- Canadian Policy and Legal Environment	•Canada taking necessary steps to address GBV, including a broad mention of TFV in its latest Strategy to End GBV progress report •Government of Canada cyber security initiatives briefly mention IoT, but still not a major concern; issues of TFV (broadly) not addressed in the Cyber Security Strategy or in resources by the Cyber Centre •Canada's legal system have the tools to prosecute TFV and stalkerware but are hindered by patriarchal norms
2.4- Technical Research on Smart Home Tech Safety and Security	•Issues with IoT from 2010 are still largely relevant today •Most technical literature is focused on large-scale threats such as nation-states and does not mention internal threats with low technical sophistication •HCI's role in mitigating abuse via technology and interface designs •Introduces the concept of dual-use apps and technologies whereby tech is designed for a specific purpose but misused for a malicious purpose •How technology can still be insecure and misused even with technical protections such as encryption

Table 2: Literature Review Summary

Chapter 3: Theoretical Framework

Since this is a study of smart homes and their relationship to TFV, the smart home is conceptualized as being a large social and technological system (Hughes, 2012), and because smart home TFV this is a relatively new system to study, I developed a hybrid theoretical framework to guide how smart home TFV is conceptualized and to guide the collection and analysis of observations. First, I adopt assemblage theory as reformulated by Rob Kitchin as the overarching theoretical framework (Kitchin, 2014) but acknowledge and discuss previous iterations of assemblage theory by Deleuze and Guattari and Manuel Delanda in this section to provide history and context of the theory before introducing Kitchin's iteration. For the remainder of the paper, only Kitchin's reformulation will be used. Secondly, I include elements of actor network theory (ANT) (Latour, 1988; Callon and Law, 1997) and thirdly I adopt Paul Edwards' (Edwards, 2003) multi-scalar approach. The following describes each, provides the rationale for their use, and explains how they have been integrated.

3.1 Assemblage Theory

Early iterations of assemblage theory are attributed to philosopher Gilles Deleuze and psychoanalyst Félix Guattari in their book, *A Thousand Plateaus* (1987). Their concept of *agencement or* assemblage[26] as described by Deleuze is defined as a "multiplicity which is made up of many heterogeneous terms and [with] established liaisons, relations between them across ages, sexes and reigns – different natures" (Deleuze and Parnet, p.69). In conversation with journalist Claire Parnet, Deleuze uses the example of a man, horse and stirrup to demonstrate how "an animal is defined less by its genus, its species, its organs and its functions than by the assemblages into which it enters" in this context (p.69). Once a stirrup is placed on the horse, a lance benefits from a horse's speed as well as from the lateral stability a stirrup provides, creating a "new man-animal symbiosis, a new assemblage of war", with this symbiosis being another key component of assemblages (p.70). While seemingly technologically determinist at first, Deleuze was careful to note that "there is always a social machine which selects or assigns the technical elements used" (p.70). This logic offers an alternative to Hegelian totality (Delanda, 2011) or the logic of organic wholes and unities whereby objects are defined by their intrinsic relations and components cannot be emancipated from each other[27] (Nail, 2017). Instead, assemblages are thought of as wholes characterized by relations of exteriority and the ability for any of their heterogeneous components to be integrated with other assemblages (Delanda, 2006,

---

[26] It is worth noting the translation of *agencement* to assemblage in English is contentious to some scholars as *agencement* and *assemblage* have different meanings in French. Specifically, *agencement* is considered to be a more precise term referring to parts fitted or fixed together (Phillips, 2006) or a construction/arrangement (Nail, 2017) than assemblage, which refers to a 'looser' gathering, blending and joining objects (Phillips, 2006). However, assemblage remains the widely used and accepted term. The thesis uses the interpretation of assemblage as a 'looser gathering' because this is how Kitchin (2014) conceptualizes assemblage.

[27] Philosophy scholar Thomas Nail uses the example of the human body to illustrate this logic of wholes. Within the human body, each organ (component) has a specific function that contributes to the overall harmony of the body (the whole). If an organ is separated from the body (Nail uses the example of the heart), neither the heart nor body survives the separation (Nail, 2017, p.3-4).

p.10). For Kitchin, like Deleuze and Guattari, he refers to the assemblage as a constellation of loosely connected and heterogenous apparati and elements, which when combined or assembled, or seen as a totality, distinguish one object or system from another, even though each object or system is part of or comprises many other assemblages or sub-assemblage. Deleuze and Guattari's original conceptualization of assemblage is very useful since, in the case of smart home technologies and TFV there are many interconnected, heterogeneous parts and wholes with different roles, connections to other phenomena informed by exteriorities, or as Kitchin would say contexts (Delanda, 2006; Kitchin, 2014).

Manuel Delanda, in working with Deleuze and Guattari's original works, splits assemblages into two dimensions, in the first axis is from the purely material to the purely expressive, differentiated according to different sets of capacities (Delanda, 2006, p.10). The second axis differentiates the ability for processes to stabilize or maintain the assemblage or to destabilize it, or territorialization and deterritorialization (p.10). These dimensions attest to the dynamic interaction of assemblage components and the whole, and this interaction is ever-changing depending on various exteriorities, important to understand multi-scalar social reality (p.38). Examples of territorial boundaries given by Deleuze and Guattari include houses with rooms with assigned purposes, streets according to the order of the city and factories according to the nature of work and operations within (Deleuze and Guattari, 1987, p.208). Broadly, smart home technologies have the potential to further territorialize through unique identifiers such as IP or MAC addresses or deterritorialize where actions are no longer bound to one room, as data collected by devices may be sent to the cloud beyond the home. Smart home technologies also exemplify various material and expressive roles such as the hardware of devices, sounds and

indicator lights, the ways in which people configure or utilize these devices including for smart home TFV.

Geographer Rob Kitchin applies assemblage theory in his work on big data (Kitchin, 2014; Kitchin and Lauriault, 2014; Kitchin, Lauriault and McArdle, 2015) and smart systems (Kitchin, 2014; Kitchin and Coletta, 2017; Kitchin and Dodge, 2019) by articulating their assemblages into their most common components social and technical as seen in Table 3 below. This is especially useful in this thesis, as it is by looking at the heterogeneous and loosely coupled social and technical components of a smart home that it is possible to assess how the smart home as a whole and in its parts are related to TFV. When doing so, it becomes clear that the smart home is deterritorialized from its typical political neutral, helpful, efficient and innovative discourse; and instead is territorialized within the social discourse of control, power, torment, gaslighting and violence as discussed in Chapter 6. As will be seen in Chapter 5, assemblage thinking shows how seemingly 'neutral' tasks, processes and systems, like code, interfaces and infrastructure (elements) related to smart homes are informed and situated by different contexts such as the political economy of smart homes and systems of thought such as the neutrality thesis of technology (Kitchin, 2014; Table 3). Put another way, "data do not exist independently of ideas, techniques, technologies, systems, people and contexts, regardless of them often being presented in this manner" (Lauriault 2012; Ribes and Jackson 2013).

Apparatus	Elements	Example in a smart home/city context
Systems of thought	Modes of thinking, philosophies, theories, models, ideologies, rationalities, etc.	Futurism/Techno-Utopian visions of the smart home, innovation agendas
Forms of Knowledge	Research texts, manuals, magazines, websites, experience, word of mouth, chat forums, etc.	Device manuals, public facing resources on TFV including journalism, surveys, policy briefs, digital security guides, support and FAQ pages, tutorials, government webpages and resources related to GBV, reports on GBV/TFV, research articles
Finance	Business models, investment, venture capital, grants, philanthropy, profit, etc.	Smart Cities Challenge, constant markdowns on smart tech by vendors, venture capital, data monetization
Political Economy	Policy, tax regimes, incentive instruments, public and political opinion, etc.	Strategy to End Gender-Based Violence, Privacy and Security concerns of citizens and experts alike
Governmentalities and Legalities	Data standards, file formats, system requirements, protocols, regulations, laws, licensing, intellectual property regimes, ethical considerations, etc.	Various technical standards (data, encryption), standards for digital evidence and supporting victims of TFV, relevant privacy laws (PIPEDA, Privacy Act)
Materialities and Infrastructures	Paper/pens, computers, digital devices, sensors, scanners, databases, networks, servers, buildings, etc.	Sensors, smart home devices, internet infrastructure, homes; electric power; hardware; software; interfaces
Practices	Techniques, ways of doing, learned behaviours, scientific conventions, etc.	Dual Use of application/weaponization of smart home devices, trained responses of police to TFV survivors
Organizations and Institutions	Archives, corporations, manufacturers, retailers, government agencies, universities, conferences, clubs and societies, committees and boards, communities of practice, etc.	Non-profit organizations, cybersecurity companies, smart home technology vendors and manufacturers, government agencies
Subjectivities and Communities	Of data producers, experts, curators, managers, analysts, scientists, politicians, users, citizens, etc.	TFV survivors, abusers, women's shelter/NGO workers, device manufacturers, police analysts, policymakers, privacy researchers, home-care workers, biases in technological design, lack of acknowledgement by academic technical research of low-level threat actors, academic researchers, city planners
Places	Labs, offices, field sites, data centres, server farms, business parks, etc. and their agglomerations	Smart home itself, women's shelters, legal clinics
Marketplace	For data, its derivatives (e.g. text, tables, graphs, maps), analysts, analytic software, interpretations)	Smart home tech vendors, real estate developers

Table 3: Smart Home Context Elements of Kitchin's Sociotechnical Data Assemblage (Kitchin, 2014)

As seen in Table 3 above, Kitchin's sociotechnical assemblage is both a theoretical framework but also it is an inventory of the various context components of a smart home (e.g. the smart home, the smart city, the connections between smart home devices and the vendors, etc.). By doing so, Kitchin's framework draws attention to "the smart home's political, material, social and economic mechanisms and the way these produce and reshape the world" (Maalsen, 2019, p.13). In the context of TFV, this approach is helpful as it illuminates how a seemingly one-on-one dispute or single site of a home is intrinsically tied to and a part of broader systems.

3.2 Actor-Network Theory (ANT)

As discussed in the literature review and theoretical framework, smart home TFV is an issue that is relevant to a variety of stakeholders across different and often siloed disciplines and sectors. To situate the linkages between the heterogeneous components of a smart home and smart home TFV, elements of Actor-Network Theory (ANT) are used here to connect seemingly disparate concepts and to make obvious how they are related. ANT was developed by sociologists Bruno Latour (1987, 1988, 2005), Michel Callon (1986, 1989) and John Law (1986, 1991), to "explore collective sociotechnical processes" (Ritzer, 2007) and counter 'great man' accounts of history by identifying the various human and non-human actors or 'enablers' that contribute to the production of scientific and technical knowledge (Latour, 1988; Callon and Law, 1997). Stemming from science and technology studies (STS), ANT's approach is similar to other approaches such as Donna Haraway's work on feminist technoscience (1991) and other constructivist approaches that seek to understand large technical systems (Bijker, Hughes & Pinch, 2012). However, ANT differs from social constructivist approaches as it does not privilege natural or cultural accounts of scientific production and instead views its production as a network of heterogeneous elements that are 'puzzled together' and transformed (Ritzer, 2007,

p.1). The equal weighting of the social and technical and the agency assigned to both human and non-human actors in ANT is helpful for understanding issues of smart home TFV to not minimize how either may influence the issue. Furthermore, Latour (1999) notes that when a system (such as a machine) runs smoothly, its success renders its components invisible, a phenomena knows as 'blackboxing' (p.304), which is the case for smart home technologies, they are there but not seen. It can be argued that instances of smart home TFV constitute a disruption within the network of smart home technology, rendering all the actors involved visible. Through this point of view, it becomes easy to highlight how smart home TFV is much bigger than a 'one on one' dispute between partners and is deserving of wider attention. Lastly, while there may not necessarily be a 'great man' account of history to counter in smart home TFV, ANT's approach is helpful in critiquing innovation and efficiency agendas of vendors and/or governments (Table 3). Lastly, from a sociotechnical assemblage perspective (Kitchin, 2014), ANT provides the means to examine linkages between various human and non-human actors, which is key when examining the content or more technical aspects of the smart home assemblage.

While ANT was formulated to counter multi-scalar approaches (Latour, 2005; Latour, 1996), scale is important in the study or smart home TFV. For ANT scholars express, scale is thought to separate actors into unnecessary hierarchies and deter from its agnostic nature (Latour, 2005, p.184-6). In the context of this thesis, the multi-scalar approach is not meant to separate actors into hierarchy, but rather, scale provides a useful way to structure the web of actors involved in smart home TFV in their sphere of influence. Applying a micro, meso and macro heuristic of actors is a boundary making exercise to heuristically depict the actors and their sphere of influence and/or knowledge. This framing is particularly helpful when formulating recommendations as will be seen in Chapter 6. ANT principles such as agnosticism foreground

the linkages between the content and context components (Kitchin, 2014) of smart homes and smart home TFV as well as provide the theoretical framing for the methodological approach that will be applied here to identify and discuss these components (Light, Burgess and Duguay, 2018).

3.3 Multi-Scalar Approach to Sociotechnical Systems (Edwards)

Finally, informatics scholar Paul Edwards' multi-scalar approach to study sociotechnical systems (2003) also frame the study of smart home TFV in this thesis. Edwards' argues that the study of science and technology from the lens of modernity studies and social constructivism[28], focus too narrowly on one specific scale which he suggests is detrimental to their analysis (Edwards, 2003, p.26). Edwards builds on the scalar thinking of Misa (1988;1994) and Bowker and Starr (1999) in their ethnographic work on infrastructure, and he conceptually splits social and technical systems into three levels or 'scales' of analysis: micro-scale, meso-scale and macro-scale (Table 4). According to Edwards, "each scale tells us something about the condition of modernity" and using a multi-scalar approach enables for a better perspective and understanding of a sociotechnological system (p.10). To illustrate the benefit of this approach, Edwards applies a scaled approach to the history of ARPANET[29] as seen in Table 4 below.

[28] Social constructivism argues that technologies "can acquire different values and uses according to the social context in which [they] are placed" (Quan-Haase, 2016, p.52-3)
[29] "ARPANET was a testing ground for innovative concepts such as packet switching, distributed topology and routing, and the connection of heterogeneous computer systems" (Abbate, 1994, p.1)

Scale	Definition (Edwards, 2003 derived from Misa, 1994)	ARPANET Example (Edwards, 2003)
Micro	Individuals, small groups, generally short term	• ARPANET protocol builders as legendary figures[30] • Promotion of ARPANET by its small staff
Meso	Institutions, such as corporations and standard-setting bodies, generally enduring over decades or longer	• US Military institutions "seeking a survivable command-control system for nuclear war" as a driving force (p.24) • RAND Corporation study on military communications problems suggesting packet-switching
Macro	Large systems and structures such as political economies and some governments, enduring over many decades or centuries	• "One step in the continuous evolution of better, faster information infrastructures" (p.24) • Part of a series of computer networking experiments already underway • Military backing of ARPANET as reason for fast growth , not necessarily influential on its structure

Table 4: Edwards' Multi-Scalar Approach (Edwards, 2003)

In this thesis, Edwards' categories are modified in terms of scope. The 'micro' scale will be expanded to include individual smart home technologies, their components or 'materialities' (Table 3) such as hardware and software and their derivatives (such as data). The 'meso' scale will remain largely the same and be primarily concerned with various practices, infrastructures, institutions, and marketplaces (Table 3). Institutions listed in the meso scale differ from those in the macro scale as those in the meso scale such as police, real estate and social workers 'act' on a local level, whereas macro scale institutions such as governments are much larger systems that act on a broader scale. Lastly, the 'macro' scale will continue to focus on political economies, governmentalities and legalities as Edwards intended as well as examining how smart home TFV and the site of the smart home are connected to the larger sociotechnical assemblage of a smart city.

[30] It is interesting to note that despite Latour's resistance to use scale (Latour, 2005), Edwards use of scale is similarly capable of identifying and dismantling 'great man' narratives by exposing all of the elements that contribute to scientific and technical knowledge, a key principle of ANT.

3.4 Hybrid Theoretical Framework

As will be seen in Chapters 4 and 5, these three theoretical frameworks provide the means to conceptually frame large and complex social and technical systems such as a smart home and smart home TFV. Assemblage theory, ANT and the multi-scalar approach theoretical are mutually complementary, provide for the sociotechnical analysis of the smart home and smart home TFV, and inform the methodological approach used to understand smart home TFV in Canada as discussed in Chapter 4. With assemblage theory, the heterogeneous elements/content and apparatus/context components of the smart home and smart home TFV become visible, ANT allows for an examination of the linkages between assemblage components (actors), human and non-human alike while Edwards' multi-scalar approach allows for an analysis of linkages and the sphere of influence of these actors.

Chapter 4: Methodology

To identify where in the social and technological assemblage, the network and at what scale the smart home and TFV intersect, I chose to adopt, modify and apply the walkthrough method developed by digital media scholars Ben Light, Jean Burgess and Stefanie Duguay (Light, Burgess and Duguay, 2018). The main affordance of the Walkthrough Method is the equal consideration of the technical and social, like the theoretical framework outlined in Chapter 3.

The original intent of the walkthrough method was to guide the empirical study of the discursive regime of mobile applications or apps such as dating and hook up apps Tinder (Duguay, 2017) and Ashley Madison (Light, 2016)[31]. Namely, it posits that apps are a form of discourse and are reflective of broader social values as well as the specific values and biases of their developers[32]. The method is divided into two approaches, first it includes the 'step-by-step observation and documentation' of screens, features, and activity flows to the study of apps (p.2). This process affords the identification of seemingly mundane uses and actions related to an app

[31] Similar approaches are taken by Bivens (Bivens and Hasinoff, 2016; Bivens and Hoque, 2018) in her empirical research examining the relationship between gender, software, and technical design.
[32] This view of technology would be categorized as critical theory by philosopher Andrew Feenberg (1999; Quan-Haase, 2016, p.45; Appendix C) as it recognizes technology as value-laden (instead of neutral) and that its meanings and use are determined by human action (instead of autonomously determined by technology) (Quan-Haase, 2016, p.47).

in such a way that qualitative data can be collected for critical analysis (p.2). One of the key differentiators between this method and a typical step-by-step technical walkthrough are its groundings in both STS, specifically Actor-Network Theory and cultural studies, which when combined provide the 'analytical power to identify connections between these contextual elements and the app's technical interface' (p.2). In other words, the walkthrough method can aid the researcher to uncover the mutual shaping aspect of a technology, in this case an app and society (Bijker, Pinch and Hughes, 2012).

The walkthrough method will help with the identification of assemblage content and context components, actors, networks, interconnections and the sphere and scale of influence these occupy, enabling a multi-scalar analysis of the smart home and its relationship with TFV. Observations derived from this analysis are listed in Chapter 5 Observations and will be discussed in Chapter 6.

There are many smart home technologies, and for the purpose of this thesis I chose to apply the walkthrough method to study a common, popular[33] and relatively affordable, easy to use and interoperable smart home technology as follows:

- The *Google Nest Mini* suite that includes:
    - The Nest Mini device itself
    - the Google Home mobile app (iOS version)
    - Google Assistant[34], the voicebot AI that processes user queries.

[33] The Canadian Internet Registration Authority (CIRA) and the Media Technology Monitor found that smart speakers were the most common smart home technology in Canada (CIRA, 2020; Media Technology Monitor, 2020).

[34] Google Assistant is available in various forms such as its own mobile app and the native voicebot AI of Google Pixel phones, but this thesis will be focusing on Google Assistant within the Nest Mini device and within the Google Home app.

The walkthrough method involves examining a technologies vision, operating and governance model to establish its 'environment of expected use' and this can be done in preparation for or in tandem with a step-by-step walkthrough (p.4). As the authors note, this work establishes how the app provider "anticipates it will be received, generate profit or other forms of benefit and regulate user activity" (Light, Burgess and Duguay, 2018). This process and these categories are helpful to identify and inventory the Google Nest Mini context and content components (see Table 3), actors, how they interconnect and to assess at what scale these operate. There are several similar smart home technologies, namely the Amazon Echo, Apple HomePod or Sonos One smart speakers. Each of these have their merit, but the Google brand of smart speaker was chosen since market research identified this as the top brand in Canada (Media Technology Monitor, 2020). In addition, the Google Nest Mini is useful to study as it is a relatively easy device to operate[35] and can stand alone (although its functionality increases with additional smart home technologies to control), meaning it is more likely to be in the homes of a variety of users rather than only appeal to technology enthusiasts, home automation hobbyists, and experts, which means it is a technological system that will continue to be used by many (Table 3). Its ease of use and lower barrier to entry (e.g. expertise, cost, installation and maintenance time) also made it preferable to study as the findings will be more generalizable than a custom built or fully integrated smart home or a smart building (such as an apartment). Furthermore, examining an off the shelf solution (like Tanczer, 2018 and Geneitakis et al., 2017) allowed me to use the device firsthand in my own home. As the Walkthrough Method was initially devised for the study of apps, I modified and adapted the walkthrough method for this

[35] It is also interesting to note that the Google Nest Mini and its predecessor the Home Mini have previously been given away for free in cross-promotions with Spotify (Ng, 2019) and Google Play Music (Bennett, 2019) respectively, further broadening the device's appeal.

thesis by adding two new sections: one on the environment of 'unexpected use' (to address smart home TFV) and one concerned with data.

For this study I purchased a Google Nest Mini from *Best Buy* a technology retailer, installed the device in my bedroom and downloaded the Google Home app on my personal iPhone. I chose this location for the Mini to ensure it would only capture my data and cause minimal disruption to other members of my household (family members). Before installing the device, I notified my family members that the device would be turned on during specific hours in the day and discussed how it would be used and how data are captured, should they enter my room during this time. There was no backlash from my family and their data were not captured by the device as they were not in my room during the time the device was on. I then documented the step by step process of installing the Google Nest Mini, the Google Home app, using functions such as broadcasting and reviewing the My Activity page. As I did so, I took notes at each step of the installation process, I kept the manuals, and I took photos of the physical installation process, where it is situated in my home, and took screen captures as I registered myself and the components within the Google Home app. I then explored various functions of the Google Nest Mini (such as broadcasting, changing settings, casting, adding other apps, reviewing activity logs) between April 2020 to July 2020. In Chapter 5, I will share the observations collected from this step by step technical and use part of the walkthrough. To keep the findings of this research as generalizable as possible, personal anecdotes have been mostly omitted. Reflecting on my own positionality as a white, middle class, tertiary educated, able-bodied, cis-gendered woman, and technically 'savvy', my personal experiences with this device are not reflective or representative of most people. Thus, I endeavoured to focus specifically on how this device may be used for TFV and which specific features enable this behaviour.

As part of the walkthrough method, I also collected information related to the *Google Nest Mini* vision. Here I collected a variety of promotional material and kept its packaging as seen in Figure 14 and Table 5. I then conducted a content analysis of these data including promotional materials such as commercials and blog posts by Google in English, French, Portuguese and Spanish (see full list in Table 5). For the operating model and governance sections I collected relevant policy and legal documents, FAQs or support pages and blog posts (see section 5.1.2 and 5.1.3.). Once the environment of expected use was established, the technical walkthrough involved the step-by-step documentation of processes as just discussed, from purchase, installation, registration and closing the system. Here I collected analysis artefacts such as screens, interfaces, buttons and drop-down menus, and forms (see section 5.1.4). Section 5.1.4. will focus on three activity flows: registration, linking a smart device to the Google Home app and basic commands for the *Google Nest Mini*. This section will be primarily derived from firsthand use and observation of the Google Nest Mini and Google Home app, user manuals and FAQs and support pages (see Table 5). This process is particularly helpful for identifying technical components and infrastructures as well as beginning to establish linkages between components (e.g. Nest Mini is reliant on electrical power and Wi-Fi, certain actions must be done through specific channels, etc.).

Two additional sections have been added to the original Walkthrough Method to sufficiently address smart home TFV. Section 5.2.1. is dedicated to the environment of 'unexpected' use[36] where I identify how the Nest Mini (and smart technologies more broadly) are capable of being misused for smart home TFV, answering one of the key research questions

[36] Light, Burgess and Duguay do mention unexpected or unintended uses of apps but do not include it as a major category of analysis in the Walkthrough Method.

of this thesis. It is important to note that this thesis will focus on methods of smart home TFV that require minimal technical literacy and expertise to demonstrate that smart home TFV can be easily executed by non-technical actors. I will not cover the thoroughly well documented smart home and IoT cybersecurity vulnerabilities and literature (Kitchin and Dodge, 2019; Zheng et al., 2018; Geneitakis et al, 2018; Bugeja et al., 2018) as that is not the purpose of this thesis. The objective here is to demonstrate that smart home TFV is not limited to highly technical actors and is easily reproducible. The final section of the modified walkthrough method I will focus on data collection, such as how they are collected, transmitted, and stored by this set of smart home devices. Although there is much data collected and transmitted by smart home devices, and here I will restrict the collection, observations and analysis to data related to TFV as it is beyond the scope of this thesis to follow all of the data flows. In addition to the study of data flows, I will also collect information about technical issues such as interoperability between smart home devices.

Overall, the Walkthrough Method will be integral to identifying assemblage components such as the materialities, infrastructures (including enablers), subjectivities and practices of the smart home (Table 3) and to situate the Google Nest Mini and the findings of the walkthrough method within the assemblage of smart home TFV, primarily on the micro scale, which is mainly focused on the smart home, its dwellers and abusers who may not live in the home but retain access to the smart home technologies of the home. These will be discussed further in section 5.3. The meso-scale analysis will include the potential impacts of smart home TFV on various organizations and institutions as derived from the observations of the walkthrough method, the literature review and additional research about related public facing institutions, which will include organizational documents such as pamphlets, brochures, presentations and reports as

described in Chapter 6.2. For example, landlord, real estate, insurance, social services, and policing organizations related to homes and TFV. For the purposes of this thesis, the meso scale analysis will focus on institutions in Ontario, Canada with some examples for Canada, the United States or Europe when relevant. Section 6.2 will highlight elements of the assemblage such as organizations and institutions, subjectivities and communities, practice, and forms of knowledge (Table 3) as well as introduce human actors to the assemblage such as realtors, landlords, social workers, etc. Lastly, the macro-scale will consider the consequences of smart home TFV on the smart city and the wider Canadian political economy. This section will involve a discussion of various policies, initiatives such as Sidewalk Toronto discussed in the literature review and the observations from the Walkthrough Method to examine how smart home TFV fits into this wider sociotechnical assemblage, how it is currently being addressed and examine potential future issues. Similar to the meso-scale analysis, the macro-scale analysis will be limited in scope to Canada but may consider the United States and Europe, especially because there has been some action on smart home TFV in the United Kingdom that is associated with Dr. Leonie Tanczer and her research team on the Gender and IoT project (Tanczer et al., 2018b). The macro-scale analysis will be the final 'piece' of the assemblage, adding and expanding upon components such as governmentalities and legalities, practices, systems of thought and political economies among others, thus demonstrating how smart home TFV can be understood within a large sociotechnological system and is a part of an extensive and heterogeneous assemblage of human and non-human actors (Table 11). The modified walkthrough method as applied here to the study of the *Google Nest Mini* smart home technology and its relationship to TFV, is informed by the hybrid theoretical framework discussed in Chapter 3, the observations collected from this provided in Chapter 5, and these will inform the discussion in chapter 5.3.

Chapter 5: Observations from the Walkthrough Method

This chapter includes the observations collected from the modified walkthrough method described in Chapter 4 of the Google Nest Mini smart speaker suite. I follow the approach developed by Light, Burgess and Duguay (2018) and arrange the data I collected according to their framework, and start with the environment of expected use, that includes a technology's vision, operating model and governance and a technical walkthrough. The observations collected from the technical walkthrough will include a step-by-step documentation of three main activity flows: registration, adding a device and describing some basic functions such as broadcasting and casting media. I conclude with the environment of 'unexpected' use, that of the smart home TFV and also discuss issues surrounding the data collection of the device, including a review of the activity flow to review the My Activity page, where the user's usage history is housed. The observations provided here will be discussed in section 5.3.

5.1 Environment of Expected Use

As described in the methodology chapter 4, this section will detail what Light, Burgess and Duguay (2018) refer to as the environment of expected use which is about how a technology developer intends or envisions the product to be used. Table 5 below is a list of the documents reviewed. I also will include observations collected during the use of the device and software suite.

Document Type	Count and Sources)
Google Commercials	**14** (Google, 2020; Google España, 2018; Google France, 2017; Google France, 2019; Google France, 2020; Google Mexico, 2018; Google Mexico, 2018b; Google Nest, 2019; Google Nest, 2019b; Google Nest, 2019c; Google UK, 2019; Google UK, 2019b; Made By Google, 2018; Made by Google, 2019)
Packaging and Documents included with device	**4** (Nest Mini Box, Quick Start Guide, Privacy Guide and Safety, Warranty and Regulatory Manual)
Google Promotional/Blog Pages	**4** (Tasca, 2019; Google Nest, n.d.; Google Products, n.d; Youtube Blog, 2019)
Google Support/FAQ Pages	**6** (Google Support, n.d.; Google Support, 2020; Google Safety, n.d.; Google Support, 2020b; Google Support, 2020c; Google Developers, n.d.)
Google Product Pages (Store)	**3** (Google Store, 2020; Google Store, 2020b; Google Assistant, n.d.)
Google Policies	**3** (Google Support, 2019; Google Policies, 2020; Google Policies, 2020b)

Table 5: Summary of documents collected for the Environment of Expected Use

5.1.1 Vision

I examined Google Nest Mini promotional material such as advertisements in English, French, Portuguese and Spanish and organizational material such the packaging (Figure 14) and the literature it contained (see Table 5) and the homepage on the Google store website (Figure 9). These visions can be organized into three 'central' visions: 1) The Google Nest Mini's small size and its 'large' technological benefits, 2) the Google Nest Mini as a friendly or familial 'helping hand' or personal assistant and 3) the trustworthiness and prestige of the Google brand. Some of the advertisements examined were about the Google Home Mini and the original Google Home, I included these as they remain relevant to the Google Nest Mini as they highlight features available across the devices.

Vision 1: Size and power

One of the central visions associated with the Google Nest Mini is the focus on the device's small size. Almost all the advertising material and its packaging I examined, including the smart speaker's very name – the Google Nest *Mini* revolves around this theme. For example,

one of the taglines associated with the device is ‘small and mighty’, found on the Nest Mini’s product page in the Google Store and the back of its packaging (Figure 9) as well as advertisements (Google France, 2017).

Figure 9: Header of Google Nest Mini landing page in English and Portuguese and back of the Google Nest Mini Box (Google Store, 2020a; Google Store, 2020b)

This tagline is meant to draw attention to the impressive ‘tech specs’ of the seemingly simplistic device and convince potential buyers that they are not sacrificing any important features for its smaller size. For example, in comparison to its predecessors, the Nest Mini includes an extra far-field microphone (3 instead of 2) for better voice recognition, the addition of a processor and machine learning chip to process some requests locally (instead of constantly pinging Google’s servers) and increase speed of response, improved audio components for ‘richer’ bass and better sound than the Home Mini and Bluetooth 5 compatibility, the latest version of Bluetooth (Table 6). According to a technical paper published by the Bluetooth Special Interests Group (SIG), Bluetooth 5 includes faster data transmission speed, wider range (4x) and improved frequency hopping[37] among its improvements from previous versions, all of which are important for smart home applications (Wooley, 2019).

[37] Frequency hopping refers to the periodic changing of the carrier frequency of a transmitted signal to mitigate interference (Torrieri, 2011, p.159)

	Google Home (2016-17) 	**Google Home Mini (2017)** 	**Google Nest Mini (2019)** 
Dimensions and Weight	3.79-inch diameter 5.62-inch height 70.8-inch power cable 1.05 lb (477g) device 4.58 oz (130g) power adapter	3.86-inch diameter 1.65-inch height 4.92 ft (1.5 m) power cable 6.1 oz (173g) device 2.65 oz (75g) power adapter/cable	3.85-inch diameter 1.65-inch height 1.5 m power cable 181g device
Price Range as of 2020 (CAD) [38]	$129.99	$39.99-79.99	$49-69.99
Wireless Network	Bluetooth 4.1: AVRCP controller and target A2DP sink and source GATT server GAP 801.211b/g/n/ac (2.4GHz/5Ghz) Wi-Fi for high-performance streaming (WPA2-Enterprise not supported)	Bluetooth 4.1 AVRCP controller and target A2DP sink and source GATT server GAP 801.211b/g/n/ac (2.4GHz/5Ghz) Wi-Fi	801.211b/g/n/ac (2.4GHz/5Ghz) Wi-Fi Bluetooth 5 Chromecast built-in
Processor	N/A*	N/A*	Quad-core 64-bit ARM CPU 1.4 GHz High performance ML hardware engine
Speakers and Microphones (audio)	High excursion speaker with 2-inch driver and dual 2-inch passive radiators (rich bass) 2 far-field mics with voice recognition	2 far-field mics with voice recognition 360-degree sound with 40mm driver Chromecast/Audio built-in	360-degree sound with 40mm driver 3 far-field mics Voice Match technology
Sensors	Ambient light sensor Capacitive touch controls	Capacitive touch controls	Capacitive touch controls Ultrasound sensing

Table 6: Comparison Chart of Google Home Devices (derived from Google Support, n.d.)

[38] Prices derived from Canada Computers, Best Buy, The Source, Costco, Walmart and Google.

In the advertisements for the Google Nest Mini, Google often pairs the physical positioning of the device in a home with a descriptive voiceover of its powerful features. This method began with the original Google Home Mini and can be seen in an advertisement from Google Spain highlighting how the original Home and Home Mini have comparable features, offering a 'big help in different sizes' (Figure 10; Google España, 2018).

Figure 10: A screenshot of a Google Home/Home Mini advertisement from Google Spain stating 'A Big help in different sizes' (Google España, 2018)

For example, in the *Introducing Nest Mini* advertisement, pictures of the Nest Mini in different rooms of the house with objects around it for scale bring attention to its miniature size in addition to a comical voiceover stating 'It's bigger than ever…well, okay, not in size…but in sound!' (Google Nest, 2019a). Another example is found in the *How to get big help from a little Mini* advertisement, where the voiceover initially has trouble finding the Nest Mini because it is so small and can be wall mounted. The video later shows the device seemingly hidden among wall art, houseplants and blended in with a similar coloured kitchen counter (Google Nest, 2019b). The placement of the Nest Mini in its advertising material is important as it demonstrates its purposeful design to be small, unobtrusive and in some scenarios, somewhat covert (Figure 11).

Figure 11: A Collage of Google Nest Mini's Placements (Google Nest, 2019a; Google Nest, 2019b)

In addition to its small size, it is important to note other design aspects of the device that add to its unobtrusive appearance: its fabric top, muted colours and lack of visible buttons all aid in making the Nest Mini a seemingly approachable and stylish piece of smart home technology that easily blends in with a user's home.

Lastly, the 'small but mighty' narrative is reflected in its price point. While it is not the most robust smart speaker on the market in terms of sound quality, the Nest Mini is significantly cheaper than the original Google Home and other higher end smart speakers. At $69 CAD (although often on sale for as low as $49 and as noted in Footnote 35, sometimes free with cross-promotions), the Nest Mini has the potential to appeal to a wider range of consumers than the more expensive options, including people who may be purchasing their first smart home device.

Vision 2: A Part of the Family

Like domestic technologies of the early and mid-20th century (chapter 2.1); the Google Nest Mini is sometimes portrayed as a modern, 'smart' version of the past's kitchen 'helper'. In

fact, some scholars have argued that voice assistants have "reproduce[d] the gendered and racialized dimensions of domestic labour"[39] (Schiller and McMahon, 2019). A notable example of this vision is seen in an advertising campaign for the Google Home (and later rebranded for the Google Nest Mini) by Google UK. In one advertisement, a home baker with hands full of pie crust is attempting to finish their recipe, but their tablet went into sleep mode. To prevent them from having to clean their hands to turn on the tablet, the baker is rescued from this sticky situation by asking Google what the next step is, for which the device replies 'Now add eggs' (Google UK, 2019a). Another advertisement by Google UK depicts a father and son experiencing 'housework drudgery' (Barber, 1985) as they look at a huge pile of dirty dishes until they ask Google to play their 'washing up' playlist at full blast. Once the music is playing, the father and son pair enjoy their time together, dancing and washing dishes (Google UK, 2019b). Like domestic technology of the past, Google highlights how the Nest Mini's hands-free assistance can facilitate kitchen tasks or make them more enjoyable because it is "designed to help you" (Google France, 2019). It is interesting to note that while the Google UK advertisements did not exclusively use women in their advertisements (and frequently uses multiracial families), the Google Assistant's default voice as well as the narrators are usually female, drawing attention to how smart home assistants (and their predecessors, electric appliances as seen in section 2.1) are often positioned as gendered helpers (Humphry and Chesher, 2020). While this is slightly straying from the idealized white, middle-class family of

[39] One example Schiller and McMahon (2019) use to illustrate this point is how voice assistants (they focus on Amazon's Alexa) simultaneously possess "nurturant" (soothing, unthreatening voice) and "non-nurturant" (immediate responsiveness, only speaks when spoken to) qualities, which are often divided along racial lines, with the nurturing qualities being associated with white domestic workers and non-nurturant with women of color (p.12).They also note the history "relegation of 'dirty work' or unpleasant tasks to racialized women reproduced in voice assistants (p.18).

the 1950s (Walker, 2000), there are still remnants of this vision today, whether purposefully or subconsciously.

However, unlike electric mixers and ovens, Google's help also extends beyond the kitchen and offers assistance to multiple members of a household in various areas of the house, including children. In an advertisement by Google Mexico, a child is doing his homework and asks Google a question about space and gets distracted until his mother asks Google to turn up the volume of the music to get his attention again (Google Mexico, 2018). Besides helping children with homework (Google Mexico, 2018; Google France, 2020), the device can also assist by reading children bedtime stories. This feature began with the Google Home Mini, which allowed for sound effects to be played in sync with a child or parent reading select *Little Golden Books*. For example, one advertisement features a father and son reading the *Coco Little Golden Book*. When the son asks the father to skip to his favourite part, the guitar solo, the Google Home begins to play the sound of a strumming guitar, bringing the book to life (Made by Google, 2018). In 2019, the Nest Mini retained this capability while also adding the ability for the device to tell a series of exclusive stories based on the popular children's movie *Frozen 2,* with the stories being narrated by the cast of the film (Google Nest, 2019c). These features in particular highlight the "nurturant" qualities encoded within the Nest Mini (Schiller and McMahon, 2019; Footnote 38).

This is not surprising as the Google Nest Mini along with the other Google Connected Home products market themselves as family-oriented technologies, sometimes suggesting that these technologies are part of the family or a guest in the home. This role as 'part of the family' is reinforced by the device's ability to help with family routines (bedtime, calendar reminders) (Google France, 2020) and where it is located within the home. A survey conducted by market

research firm *Voicebot.Ai* identified the kitchen, living room and bedroom as the most common locations for smart speakers in the home, with the popularity of bedrooms steadily rising over the past three years (Kinsella, 2020). As these technologies continue to occupy increasingly intimate quarters within the home, questions surrounding the normalization of surveillance and monitoring, especially of children[40], capturing their voices, preferences, behaviour, including everything else in the household point to important privacy issues that will be discussed in the analysis. To mitigate some of these concerns, a company must prove themselves to be trustworthy to the consumer – the final vision associated with the Google Nest Mini.

Vision 3: Google as trustworthy

For the Google Nest Mini to be such a 'big' part of a user's life, part of the family, it is typically important for a user to have some sort of implicit trust at minimum in the device and/or its manufacturer. To gain this trust, Google Nest Mini and other Google products often leverage the company's reputation, ubiquity, and technological prowess in its advertising. As cultural historian Siva Vaidhyanathan explains in his book, *the Googlization of Everything (and why we should worry)*, Google began cultivating its reputation as reliable and trustworthy through its initial product Google Search in 1997, which provided an easy, streamlined way for users to explore the Internet (Vaidhyanathan, 2011). As Google expanded its scope to include products and services such as maps, satellite imagery, video via its acquisition of YouTube, e-mail and word processing software among many others, Vaidhyanathan argues that Google is "on the verge of becoming indistinguishable from the Web itself" (p.18). This becomes increasingly true

[40] It is important to acknowledge that Google has specific protocols and apps designed to promote children's safety (such as YouTube Kids to avoid explicit content and supervised Google account monitoring via Family Link for children under 13), but these are separate apps that may or may not be set up by families. Moreover, in the case of the Nest Mini, a child is free to ask the device anything even if they do not have a Google account associated with the device. Thus, this technology was not analyzed in the thesis.

as Google continues to add more products and services, ranging from classroom management software, telecommunications, payment systems (Figure 12) and even infrastructure for smart cities (Sidewalk Toronto, 2019).

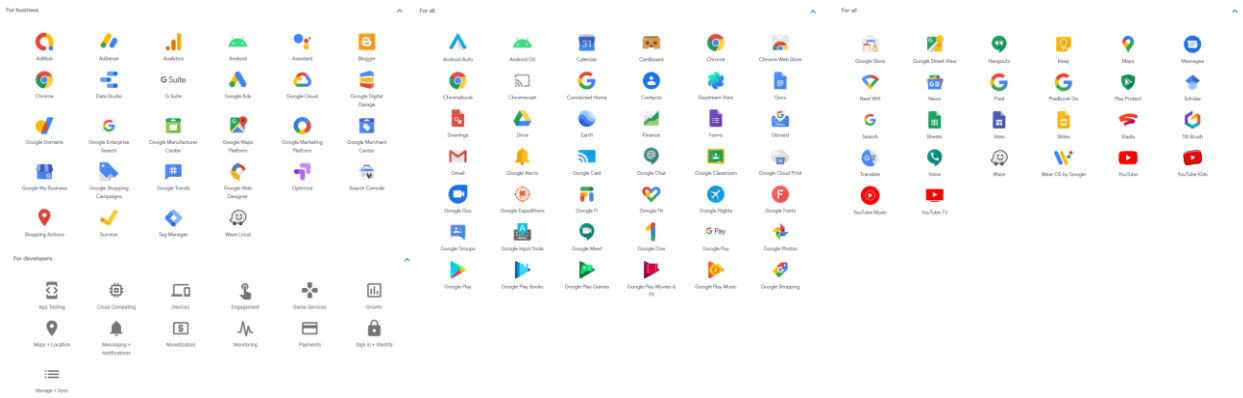


Figure 12: Google Branded Products and Services (Google, 'Products', 2020)[41]

Thus, Google's focus on fast and user-friendly services coupled with its sheer size, scope and success cultivates a public reputation for being reliable and trustworthy (as well as their former motto, "don't be evil"). Despite an increasing number of people problematizing its position of power, Google continues to be popular, powerful, and culturally significant due in part to its established reputation and history.

Two specific taglines used throughout its suite of products play on this vision. Notably, Google's mobile phone series, Pixel, often uses the tagline 'A phone made the Google way', implying the 'Google way' is smart, cute and trustworthy because it leverages services like Google Search (Made by Google, 2019). On the subject of Google Search, its trustworthiness has been called into question and problematized by scholars such as Latanya Sweeney (2013) and

[41] It is important to note that Figure 12 is not exhaustive as it does not include mergers and acquisitions by Alphabet, Google's parent company.

Safiya Umoja Noble (2018) who have discovered how the search engine can reinforce racism via its results by reproducing harmful stereotypes about racialized people, among others [42].

A similar tagline is used in a Google Home advertisement from Google Mexico, where the final shot is a close up of the device with the words '*Help at home, like only Google knows how*' (Google Mexico, 2018b). Both advertisements highlight the Google Assistant software, Google's voicebot AI, and demonstrate how it can answer virtually all a user's queries and requests through integration with other Google services like Maps and Search. Moreover, by showing a user interacting with the device and receiving a near instantaneous answer, Google is purposefully demonstrating the speed of its services. This is significant as speed has been an important metric for Google retaining its user base as it is a key component to "positive user experiences" (Vaidhyanathan, 2011, p.69).

Lastly, Google often combines this vision (Google as trustworthy) with its family-oriented vision to reinforce Google's role as 'part of the family' or a guest in the home. This combination is primarily found in advertising materials focused on privacy and security in the home. In the company's *Commitment to Privacy in the Home,* certain language is used to convey a personal connection between the company and the user, including writing directly to the reader (e.g. "Our commitment to you") and placing emphasis on the need for Google to establish trust with the user as they are "a guest in your home" (Google Nest, n.d.). This is an interesting approach as Google often brands itself as already trustworthy. To further contextualize this approach, it is important to consider that this commitment is public during a time where trust in technology companies is being questioned in the wake of events such as the Facebook and

[42] While for this thesis I am cognizant of the relationship between race and smart home TFV, research dedicated to fully exploring this relationship is a potential avenue for future work.

Cambridge Analytica scandal[43] and as seen in the 'techlash'[44] against the Toronto Sidewalk Labs Quayside Waterfront project (Marshall, 2020). Thus, it is in Google's interest to create a narrative around building trust with its users and being as transparent as possible about its privacy practices to differentiate its products from other company's offerings. The Google Nest Mini advertisements are an example of this.

5.1.2 Operating Model

There are two main operating models for the Google Nest Mini. In the short term, revenue is generated through the sale of the devices and the other main operating model is data monetization via the usage of the Google Nest Mini or other Google services at large. While Google's Privacy Policy states that they do not sell any information collected by their services, this does not necessarily mean information is not monetized by the company. Data monetization for these devices are contingent on the ways and the degree that the user participates in the Google 'ecosystem'.

Service Optimization

Some information is utilized by the company for service optimization (Google Policies, 2020a) including Google Assistant, the software that processes the requests, utilizing the user's Google search history associated with their Google account to provide answers that are more relevant to the user's interests or region if the *Web and App Activity* setting is enabled (Google Support, n.d.). While users have a choice to enable this option, users who do not enable it are

[43] Cambridge Analytica was a political consulting and data analytics firm involved in more than two hundred political campaigns around the world including Brexit and Donald Trump's electoral campaign (Srinivasan, 2019). The company ceased operations in 2018 after it was revealed they "harvested millions of Facebook profiles of US voters and used them to build a powerful software program to predict and influence choices at the ballot box" (Cadwalladr and Graham-Harrison, 2018).

[44] Techlash is a portmanteau of technology + backlash, referring to discontent and negative reactions to big technology companies such as Amazon, Google and Facebook (The Economist, 2018).

limited to certain features of Google Assistant and their smart home devices (see Figure 18). Moreover, if a user enables a setting that allows Google to retain their audio recordings, they are deleted by default[45], their audio recordings can be used to enhance Google's speech recognition technology, currently used for their Voice Match feature (Google, 2020). While not explicitly stated, a potential enhancement to their Voice Match feature via enabling audio data collection could be improved understanding of non-Anglo-American accents, a cultural bias that has plagued voice assistants from Amazon and Google alike, with Google acknowledging the utility of a larger sample size of diverse data to train their voice assistant (Fingas, 2018). The last way a user may contribute to service optimization is through opting in to sending device statistics and crash reports to Google (see Figure 16). Thus, users who have these settings enabled aid Google in creating better products and services, which in turn can provide the company with future revenue.

Google Assistant

As mentioned previously, users who enable the *Web and App Activity* setting in the Google Home app contribute to service optimization. Google Assistant provides plenty of opportunities for data monetization due to the degree of integration between Google Assistant and other services, Google or otherwise. When configuring a Nest Mini (as well as any other Google Home/Nest device), Google states that it is in a commercial relationship with many businesses via its Google Partner program. What this means for the user is that some businesses may pay Google to be featured or promoted over its competitors (Figure 13). While this is not necessarily a data monetization method, it is a core part of Google's broader business model. It is

[45] This feature was highlighted after public concern over human reviewers of Google Assistant queries (Tasca, 2019; Bohn, 2019)

the immense interoperability between Google services, the ease of use and frictionless experience between services that there is the potential to increase sales for the full Google Suite of technologies.

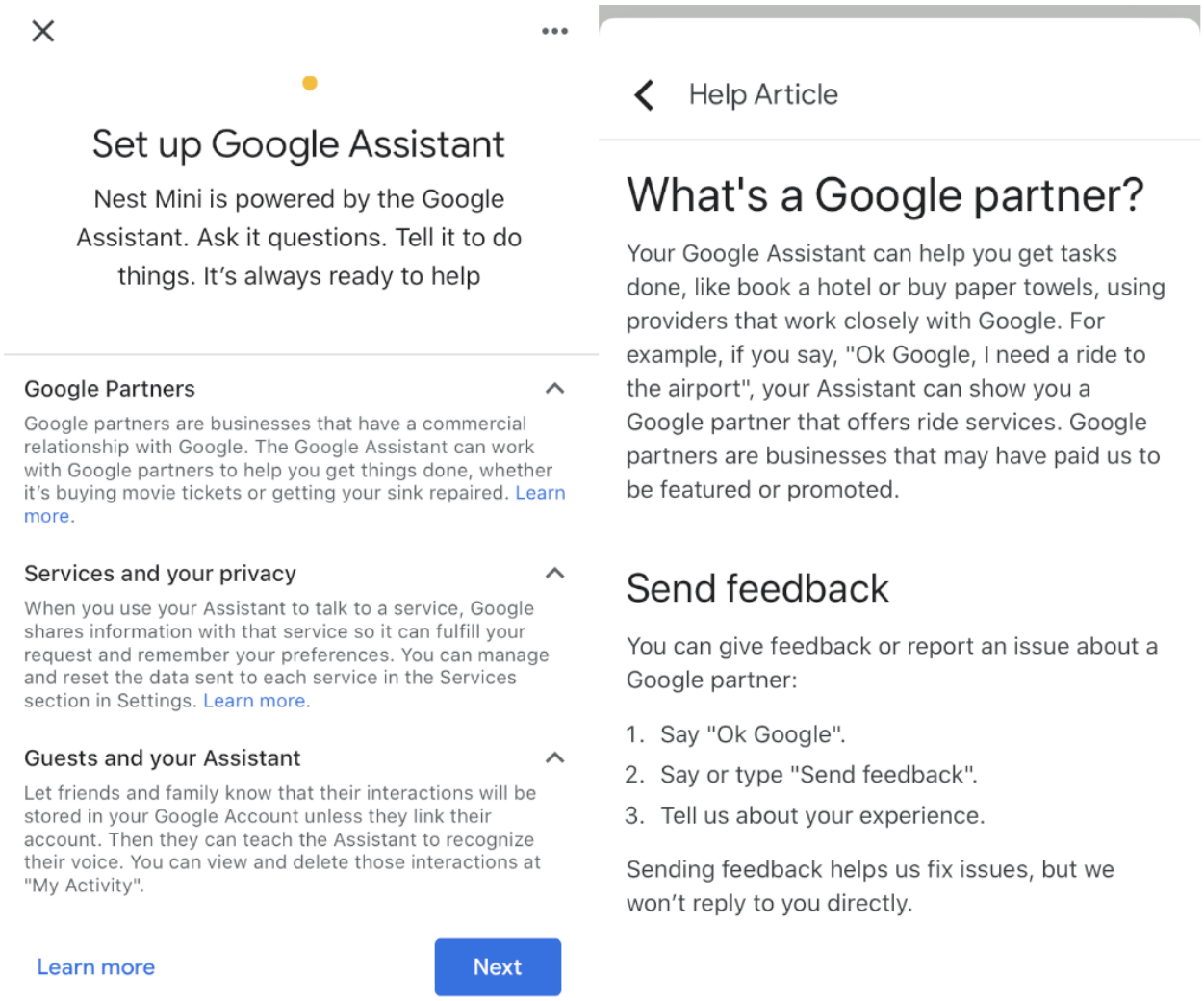


Figure 13: Google Partner Notice + Learn More Page in Google Home App during Nest Mini Setup

While its desktop and mobile interfaces[46] clearly label when a business is a Google Partner, this becomes murky when a user asks a query to a device like a smart speaker with no

[46] In 2019, Google has also modified its Google Assistant interfaces (app, phones) to look more like Google's search engine when giving an answer, including results marked as advertisements at the top (Buckley, 2019).

visual interface. Thus, when the Assistant responds, the user may not know if it is truly the most relevant result to their query or an advertisement. Other methods of monetization through Google Assistant include the ability to purchase digital goods and subscriptions from third parties via voice and Google Pay, including subscriptions to ad-free YouTube Music Premium, a music streaming service owned by Google, to which Google Home users automatically receive access to the free, ad-supported version (Google Developers, 2018; Condon, 2018; YouTube Blog, 2019). Overall, it is likely that Google will continue to find new monetization opportunities in its connected home products as they proliferate, especially as more connected home products have screens, meaning there is more visual advertising 'real estate' available (Townsend, 2017).

Real-Time Bidding

Another method Google uses to monetize data from its services and the web at large is through a process called real-time bidding (RTB). As described in a blog post by the Electronic Frontier Foundation (EFF), RTB is the "process by which publishers auction off ad space in their apps or on their websites. In doing so, they share sensitive user data—including geolocation, device IDs, identifying cookies, and browsing history—with dozens or hundreds of different adtech companies" (Cyphers, 2020). In mere milliseconds, data and ad space is auctioned by supply-side platforms or publishers (i.e. websites), bid on by demand-side platforms in the real-time bidding system which are also referred to as the Ad Exchange and the user is served an advertisement once the auction is won (Cyphers, 2020; Olejnik, n.d.). Even if a bidder does not win an auction, they still have access to information on the user such as browsing history (Olejnik, n.d.). This is especially pertinent as Google owns and controls various key players at nearly every level of RTB, including one of the largest third-party ad networks (DoubleClick) and the largest ad server for mobile applications AdMob, with AdMob running inside 94% of

apps in the Google Play store (Cyphers, 2020). In addition, Google controls significant portions of the web at large through its extremely popular products, such as Google Chrome (62% of mobile browser share and 69% of desktop browsers), Android operating system (71% of global mobile operating system share), Google Search (processes 92% of internet searches), YouTube (used by 73% of American adults), Google Analytics (embedded on around 85% of websites) (Cyphers, 2020).

The Nest Mini becomes implicated in RTB if a user asks a query meant to spur further activity (e.g. asking for a coffee shop nearby and further exploring their options). It is also worth noting that the responses given by Google Assistant on either the Home app or the Nest Mini device will keep the user within the Google 'ecosystem' for as long as possible (e.g. location queries will be given a result through Google Maps, others through Google search)[47].

By examining the operating model, it becomes apparent that Google is an organization that derives significant value from its extensive data collection and has a vested interest in continuing to do so. This practice and its implications will be further explored in the technical walkthrough and data sections within the chapter.

5.1.3 Governance

This study of the corporate governance of the Google Nest Mini was conducted by a close reading of three key documents:

1. Google's Privacy Policy
2. Google's General Terms of Service (TOS)
3. Google Nest TOS, specific to the Nest range of smart home products, including the Nest Mini

[47] Similar findings were made by investigative journalists Adrianne Jeffries and Leon Yin, where they found Google privileges its own services in their search results (Jeffries and Yin, 2020).

This section will focus on corporate governance of the Nest Mini, as the meso and macro scale analyses (see sections 6.2 and 6.3) will discuss government regulations and policies. Relevant portions of the Nest TOS include shared governance when using third-party services (e.g. The user is bound to both the third party's TOS and privacy policies as well as Google's), Google's non-liability to dispatch emergency services through its smart home devices and non-liability to guarantee that third party services work as intended (Google Support, 2019). Google's General Terms of Service is organized through five major sections:

1) Your Relationship with Google,

2) Using Google services,

3) Software in Google services,

4) In case of problems or disagreements and

5) About these terms (Google Policies, 2020b).

Specific portions of the General Terms of Service relevant to this thesis include Section 1 and 5. Section 1 states that abusing or harming others (including yourself) or Google's services is against the company's basic rules of conduct (p.1). Google uses "misleading, defrauding, defaming, bullying, harassing or stalking others" as examples of abuse against others. Section 5 states that Google "reserves the right to suspend or terminate your access to the services or delete your Google account" in the following instances: 1) a material or repeated breach of the Terms of Service or Policies (including service-specific additional terms), 2) they are required to do so in compliance with a legal requirement or court order or 3) they reasonably believe that a user's conduct causes harm or liability to a user, third party or Google (hacking, phishing, harassing, spamming, misleading others and scraping content that doesn't belong to you) (p.5) This section also specifies that in the case of settling disputes, California law will prevail regardless of

conflict of laws rules (p.5). The Privacy Policy that presides over all Google services details the information Google collects and why, the user's privacy controls, how and when Google shares the user's information, how they keep user information secure, data retention policies and compliance with regulators (Google Privacy Policy, 2020). Sections of the Privacy Policy relevant to the thesis will be discussed in detail in following sections.

5.1.4 Technical Walkthrough

Registration and Entry

First, the user must purchase a Google Nest Mini. Once purchased, the box includes the device itself, its power cable and three manuals: A Quick Start booklet (blue), a Privacy guide (gray) the Safety, Warranty and Regulatory manual (white) (Figure 14).

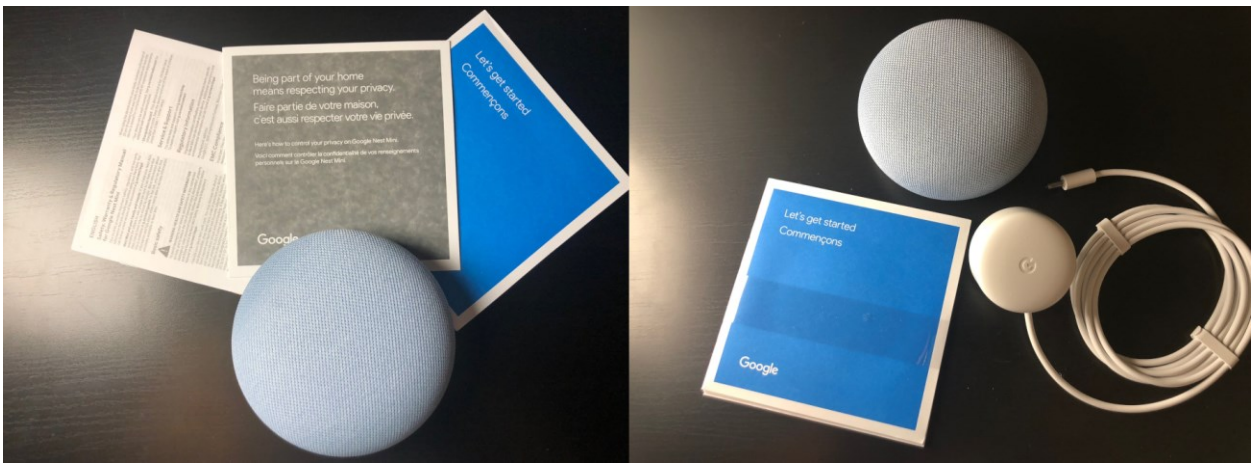


Figure 14: Contents of the Google Nest Mini Box

The first step in activating the Google Nest Mini is plugging it in. When connected to a power source, the Nest Mini's lights will activate, and the device will tell the user to finish setup in the Google Home app. This information is also available in the Quick Start booklet. The Google Home app is available for smartphones and tablets running Android Lollipop (5.0) or higher for Android devices and iOS 12 or higher for Apple devices. Immediately after downloading the app, the user is asked to sign in or create a Google account. The user must have

a Google account to activate any Google Connected Home products. Once activated, anyone in physical proximity to the device may ask the Nest Mini questions, regardless if they have an account. If the user does not have an existing account, clicking “create” will bring them to the Google Account registration webpage. After logging in to their Google account via the Google Home app, the app requests permission for Bluetooth before playing a short demo of what can be done in the Google Home app such as remote thermostat adjustments and home monitoring assuming the user has the accompanying smart home devices. Below is a swimlane diagram I created to summarize this process.

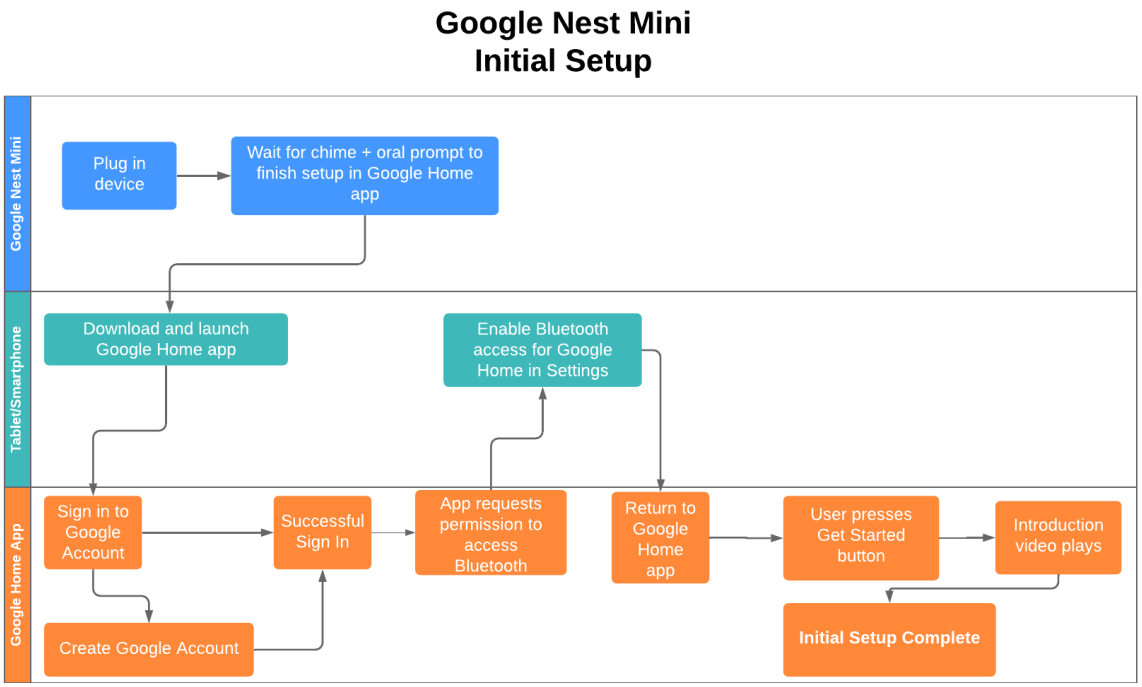


Figure 15: Swim Lane Diagram of Google Nest Mini Setup

Creating a Home

The next step to setting up the Google Nest Mini or any other compatible smart home device by ‘creating a home’. One user may have multiple homes (e.g. Home and Cottage). A ‘home’ simply refers to a group of devices and is the main method of organizing multiple

devices within the app. Once a user has created their 'home', the initial screen in the app will show all of the smart devices the user has linked to their Google Home app as well as 'discoverable' devices in the home (such as an existing smart TV). The user taps "Get Started" and is then asked if they are setting up a new device or linking smart home services. In the case of Google Nest Mini, the user taps "set up new devices". The next screen asks for a home nickname (e.g. Home, Cottage) and address. If a valid address is not entered, a prompt appears warning the user that without a valid address, the Google Nest Mini's location-specific information (e.g. weather, traffic) may be less accurate. The bottom of the prompt includes two buttons: "Continue Anyway" to proceed without entering a valid address and "Try Again" to re-enter an address. Even if a user does not enter their address, the next screen requests permissions to Location Services on their smartphone or tablet to "set up and manage nearby devices". The user is presented with three options: 1) enable Location Services indefinitely, 2) enable Location Services once and 3) Do not allow Location Services, which will terminate the setup. Once Location Services are enabled, the app will attempt to find the smart home device and display a screen if successful, which asks the user if they would like to set up the device now or later. After tapping "Next", the app attempts to connect with the Google Nest Mini. If successful, the Google Nest Mini will play a sound. The app presents a screen asking the user to confirm if they heard the sound and proceed to the next step or to retry. After proceeding, the user is asked if they would like to share device statistics and crash reports with Google to improve their services (below, Figure 16). Either answer will send the user to the next screen, asking which room of the home the device is in for organization purposes (e.g. if the user has two Nest Minis in different rooms, they will be labelled accordingly on the Home screen). Below (Figure 17) is a swimlane diagram I created to summarize this process.

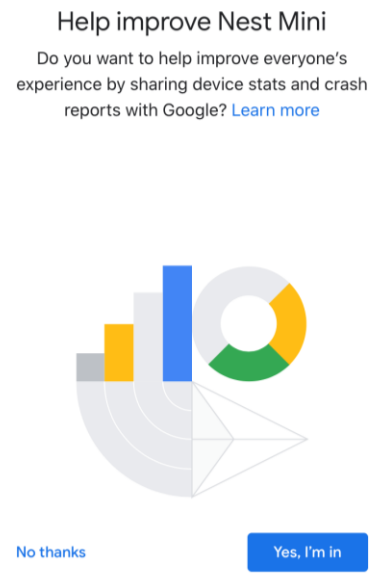


Figure 16: Device Statistics and Crash Report Consent Screen in Google Home app

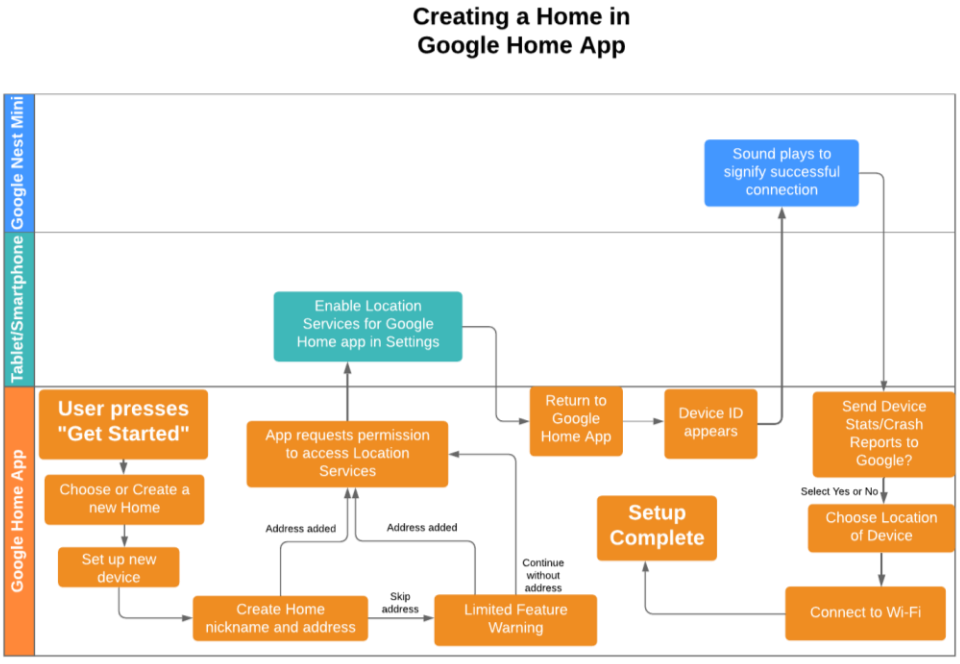


Figure 17: Swim Lane Diagram of Creating a Home in Google Home App

Google Assistant

After establishing the 'home', the next step is for Google Assistant to be configured. Google Assistant is the voicebot AI responsible for answering the user's queries to the Google Nest Mini or Google Home app. Before initiating setup, a sort of 'disclaimer' screen is shown, detailing Google Partners, privacy and how Google Assistant may interact with guests in the home. The user may tap the 'Learn More' hyperlinks to expand one or all these subheadings (Figure 13) or proceed to setup by tapping the 'Next' button. Once pressed, the user must configure "Web and App Activity and Contact Info" settings to gain access to the full features of Google Assistant. The user may change this setting later. Without this setting enabled, certain features such as broadcasting a message to devices are not available. Another setting presented to the user during setup that can be changed later is the option to use Voice Match, Google's speech recognition technology. Voice Match is encouraged for devices that have multiple users to differentiate between voices. To use Voice Match, the user agrees to the Terms and Conditions for Voice Match, including the disclaimer that the device may not be able to discern between two similar sounding voices, potentially causing unwanted access to personal results. Once accepted, the user is prompted to repeat a series of sentences to train the Google Assistant to recognize their voice. If successful, the next screen confirms that Voice Match has been set up and the user can opt to get personalized results through permitting Google Assistant to have access to personal Gmail calendars, contacts, and reminders. This screen is also shown if the user decides to not enable Voice Match and can be toggled later in the user's settings. To enable personalized results, the user taps "Agree" and is later presented with a screen to enter their address for direction purposes but may opt out of this portion by tapping "Not Now" (Figure 18).

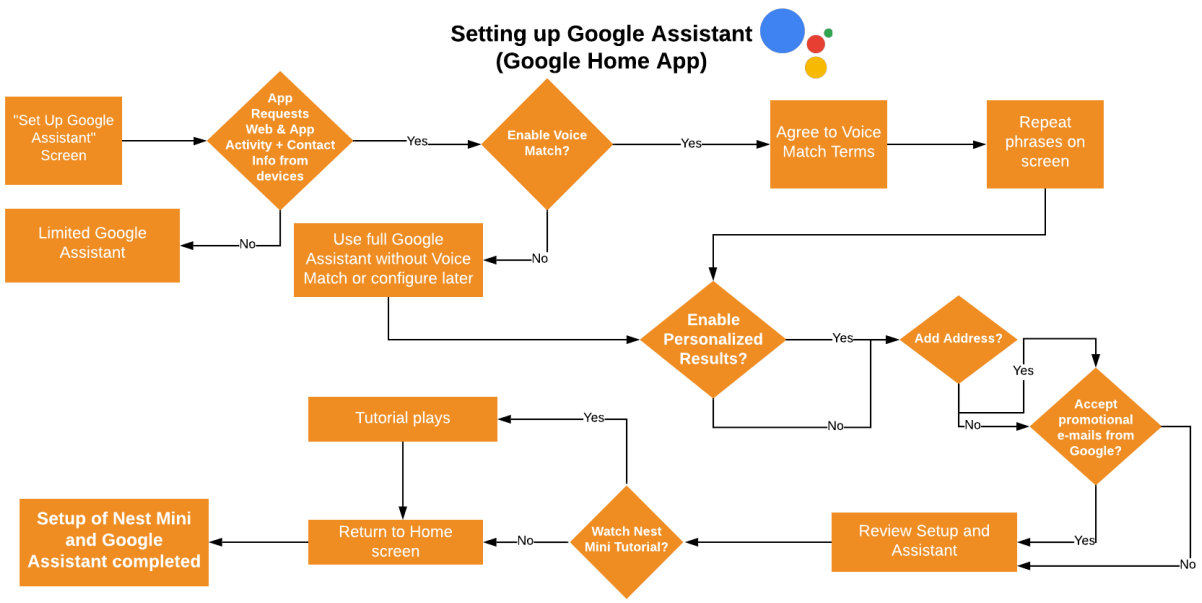


Figure 18: Flowchart of Google Assistant Setup in Google Home app

Using Google Nest Mini – Basic Controls

Once the Google Assistant is configured, the final step is to opt in or out of promotional e-mails from Google. A short tutorial is provided to describe how to use the Google Nest Mini or for whichever device has just been configured. The same information is available in the Quick Start Guide. There are two methods of controlling the Nest Mini: through the Nest Mini itself (touch or voice) and via the Google Home app. If the device is nearby, the user may tap the sides to control the volume and the center to play and pause media; the device will light up to indicate where to tap if media is playing and the sensors detect a hand. These actions may also be done through voice commands (e.g. “Hey Google, turn the volume up to 70%”) to the Google Nest Mini or to the Google Assistant in the Google Home app. The last option is to tap the device in the Google Home app which will present a control screen where the user can manipulate these settings by swiping (see left side of Figure 19). To disable the microphone on the Google Nest Mini, a switch near the bottom of the device can be activated. The microphone is disabled when

the orange indicator lights activate and the device says, “The mic is off”. If the microphone is turned back on, the lights will change back to blue and the device will say “The mic is back on”. To disable the microphone in the Google Home app, the user must configure their permissions (found in the Settings of their smartphone or tablet) to revoke microphone permission from the app. Without the microphone enabled, the user will not be able to talk to Google Assistant and be limited to basic functions such as casting media from their smartphone or tablet. If the microphone is on, users may ask the device or Google Assistant in the Google Home app a variety of queries.

5.2 Modifications to the Walkthrough Method

In the following I provide observations derived from the modifications to the Walkthrough Method required to analyze the Nest Mini (Chapter 4). I include here the unintended uses of the Google Nest Mini, specifically smart home TFV and do so by demonstrating in three main ways how the Google Nest Mini may be misused: 1) through the broadcasting feature, 2) through casting media and 3) through interoperability with other smart home devices. The last subsection will examine the types of data collected by the Nest Mini and by extension, Google services. Following this, the My Activity tab and other user controls over data collection will be discussed.

5.2.1 Unintended Uses

Many of the seemingly useful features of the Google Nest Mini and Google Home app may also be misused for smart home TFV. While abuse is technically against Google’s Terms of Service, it can be difficult to discern if abuse has taken place solely from activity logs, which will be discussed further in sections 5.2.2 and 6.1. The misuses detailed in this section assume that the abuser has access to the Google Nest Mini device, the Google Home app or both and is

focused primarily on families unless stated otherwise. Furthermore, this section does not assume the gender (or any other identity) nor relationship between abuser and victim, as these could vary greatly even within a familial context (ex-partner, technically savvy teenager, abusive spouse or common law partner). Smart home TFV perpetrated by other actors will be mentioned briefly in the meso and macro scale analyses found in Chapter 6, but the methods detailed in this section and their implications are applicable in a multitude of scenarios. The section that follows will discuss the data collected by the app.

The most overt way smart home TFV may occur is through the broadcasting feature in the Google Home app. The broadcasting feature allows a user with access to the Google Home app to tell the Google Assistant by tapping the microphone icon in the app to broadcast a message on all the connected devices in the home. Advertised uses for this feature include notifying family members around the house of mealtimes or traffic delays on a trip home. However, it is also possible for this feature to be misused to broadcast constant harassing, intimidating messages, or other auditory disruptions to home dwellers. Even if the microphone of the Nest Mini is turned off, it will still broadcast messages sent from the Google Home app.

Another way the Google Nest Mini may be misused is through its ability to play media in general. Ferial Nijem, an outspoken smart home TFV survivor described her experience to the CBC and mentioned this ability as one of her abuser's tactics to torment her (Ghebreslassie, 2018). Her estranged ex-partner retained control of the smart home Nijem lived in and would flicker the lights and the television on and off as well as blare rock music in the middle of the night, disrupting Nijem and her pets from sleeping. She described feeling as though she was 'going crazy' in a 'gilded cage' or living in a haunted house. It would be simple for an abuser to

replicate this tactic as it is possible to cast media on the Google Nest Mini (and other compatible devices) in multiple ways if they have access to the Google Home app.

If the app and the Nest Mini are on the same Wi-Fi network, the abuser can cast media through the Google Home app, control the volume and monitor if the device is still playing music (e.g. a dweller muted the speaker). If a dweller unplugs the speaker, the Google Home app will still process and confirm requests as though the speaker is plugged in but will have visual indicators in the app that the request was unsuccessful, such as no animation on the speaker icon and the speaker appearing offline (Figure 18). Furthermore, the abuser may ask Google Assistant "what is playing on the speaker?" and if no media is playing, the speaker will say "nothing is playing on the speaker". Some control over casting is taken away if the app and the Nest Mini are not on the same Wi-Fi network. Through the Google Assistant, media can still be cast, stopped, and controlled for volume on a different Wi-Fi or cellular network, meaning that abusers may still retain the ability to cast media remotely. However, if the Google Home app is on a different network than the Nest Mini, there are no visual indicators of success or failure, meaning the abuser will not necessarily know if a speaker has been muted, paused, or unplugged unless they ask Google Assistant if anything is playing on the speaker, to which the Assistant will respond the same as it would on the same Wi-Fi network (Figure 18). It is important to note that the options for media cast when on a different Wi-Fi or cellular network are limited depending on which services the user has linked to their Google Home app. For example, if a Spotify account (or other compatible streaming service) is linked to the Google Home app, the user will have the ability to cast media from this application on the Nest Mini even from a different network through the Google Home app. However, they will not be able to cast media

directly from the Spotify app. If there is no linked account for streaming, the abuser will still be able to play music from the default service, Google Play Music.

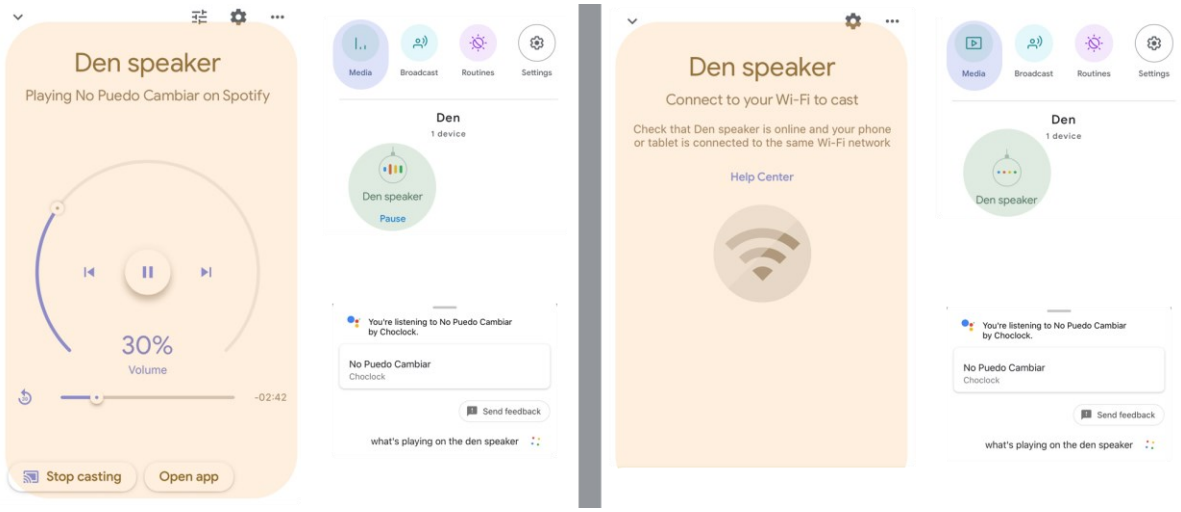


Figure 19: Comparison between phone on same Wi-Fi network (left) and cellular network (right). Differences highlighted in blue, green and yellow

Lastly, the greatest risk for smart home TFV manifests when multiple devices are connected to the Google Home app. As offerings such as smart speakers and security systems gain popularity, an increasing number of household appliances are also becoming 'smart' via compatibility with voicebot AI such as Siri (Apple), Alexa (Amazon) and Google Assistant (Google). Currently, there are thousands of apps and products compatible with Google Assistant, including hundreds in the smart home category. For example, Google Assistant is compatible with Phillips Hue lights, meaning someone can ask Google Assistant if a light is on in a certain room or to turn them on and off remotely. Other actions[48] include remotely locking and unlocking doors, changing air conditioning/heating temperatures, and changing shower or bath

[48] Actions here refers to both the general act of doing something as well as Google Assistant Actions, which refer to code that allows a user to "get things done" via the conversational interface of Google Assistant. Like an app store, Google hosts a directory of over one million Actions in various categories, including for smart homes. Smart home Actions are typically made by their respective vendors but can be created by anyone (all Actions are subject to Google's review) (Google Developers, n.d.).

water temperatures, among others. Thus, the Google Home app acts as a sort of dashboard to control the connected devices in the home, meaning whoever's account is associated with the app has ultimate control over the smart home. Although, this control is contingent on how many apps are used to manage smart home devices, as many other smart home vendors have their own apps, which will be discussed in section 5.2.2. Furthermore, if no other accounts are part of the home, nearly all activity associated with the connected devices will be available via the My Activity tab. The data section will discuss the activity tab in greater detail, but in this instance, the activity tab or the home screen of the Google Home App can be used to monitor occupancy and surveil dwellers of the home (e.g. checking for recent interactions, if any devices are currently in use, contact information), ultimately becoming a form of cyberstalking[49] (Figure 18).

5.2.2 Data

As seen in the operating model (Section 5.1.2.) and technical walkthrough (5.1.4.), smart home devices can collect, process and generate vast amounts of data that are valuable for a variety of actors and some may find this data collection to be "creepy" or obtrusive[50] (Consumers International and Internet Society, 2019). This section will further examine Google's smart home device data practices.

Types of Data Collected

Google mostly divides the data it collects into two categories: information collected through service usage and information voluntarily created or provided by the user. Below is a

---

[49] The risk of cyberstalking could be further exacerbated in a scenario where the device has been configured for one user and they have enabled the setting that grants the device access to their Google calendar and e-mail, among other services. Even if Voice Match is configured (to prevent other users from accessing this information), this info could still be accessed if the abuser has a similar sounding voice, as warned by the Voice Match disclaimer mentioned on page 99.

[50] The survey conducted by Consumers International and Internet Society (2019) found that 63% of respondents were creeped out by smart home data collection. Out of the six countries surveyed, Canadian consumers were in the middle (below US and Australia and above UK, France and Japan) for concerns about smart home data collection.

table summarizing some of the information Google collects as per its Data Transparency page and Privacy Policy (Table 7). As discussed previously, the volume of data Google can leverage depends on how many Google services a user interacts with.

Information derived from use of Google services	Information provided/created by the user
• Searches • Videos watched • Ads viewed and clicked • Location • Websites visited • Apps, browsers, and devices used to access Google services • Purchase activity • Activity on third-party sites and apps that use Google services • Chrome browsing history if synced with Google account • Telephony log information if using Google services to make phone calls • Device type and settings, operating system, mobile network info (carrier name, phone number), application version number • IP address • Crash reports • System activity	• Name • Birthday • Gender • Password • Phone number • Emails written/received with Gmail • Photos and videos saved • Docs, Sheets and Slides created on Google Drive • YouTube comments • Contacts • Calendar events • Payment information

Table 7: Information collected by Google Services (derived from Google Safety, n.d. and Google Policies, 2020a)

The data transparency page also mentions how Google Assistant leverages other Google services to provide the most relevant answers to the user. Lastly, specific Google services such as Google Assistant and Google Maps may access location data including GPS, IP address, Wi-Fi access points and cell towers and sensor information (Google Safety, n.d.).

Pertaining specifically to smart home devices, one of the top concerns with these devices are that they are always listening or recording, even when the user may not necessarily want them to. In its Data Security and Privacy FAQ page, Google states that devices are on standby mode and only come out of standby mode when it detects the 'wake word' (such as "OK Google" or "Hey Google") to fulfill the request. Any audio snippets recorded in standby mode

with no wake word detected are not sent or saved to Google (Google Support, n.d.). When the wake word is detected, audio snippets are processed by Google, but the company does not keep the audio recordings unless the user has enabled this setting, which is turned off by default. What is kept automatically is a transcription of the command (e.g. You asked Assistant "is the drugstore open today") and the Assistant's response, which the user can find in the My Activity tab of the Google Home app (Figure 19; Figure 20). However, some transcriptions are unavailable and will simply state "You used Assistant". Each record includes metadata such as date, time and which technology processed the command (e.g. Google Home or Google app) (Figure 19; Figure 20). As will be discussed further in Chapter 6, these inconsistent records could be a problem if they are used as evidence when reporting to police. For example, if the abuser is sending harassing messages to the household via the broadcasting feature (section 5.2.1; second panel of Figure 21), there may be no solid proof that the messages were harassing in nature if the audio snippet is not kept and the record does not provide a transcription of what was said. Furthermore, depending on whose Google Account is associated with the device (such as an abuser registering the device and being the only person with access to the Google Home app), a victim may not even possess access to these records, including the possibility of deletion by the abuser.

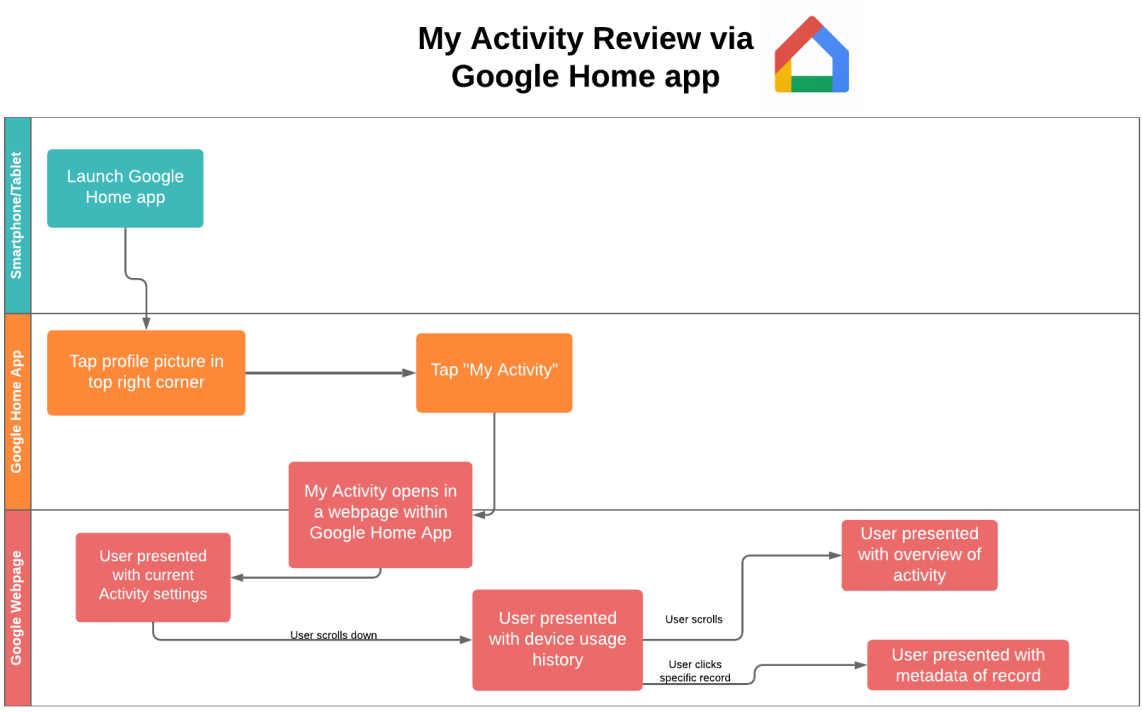


Figure 20: Swim Lane Diagram of My Activity Review

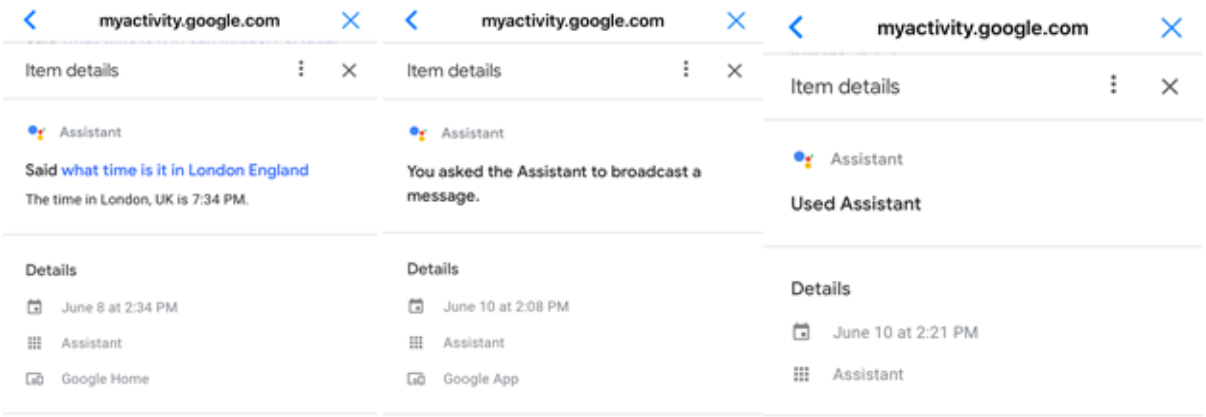


Figure 21: Three Examples of Detailed Activity

Google also provides an information page about the sensors used in its devices, what they measure and examples of what they do (Google Support, 2020b). Relevant sensors for the Google Nest Mini include the microphone which allows user to talk to Google Assistant and emits ultrasonic pulses to detect proximity and display device controls, Bluetooth that detects device tag on other Bluetooth-enabled devices, stream music and Capacitive Touch that is a

close range device control. In its commitment to privacy in the home, Google states that sensor data are only shared with third-party apps and services "if you or a member of your home explicitly gives us permission" and that they will only ask for this permission "in order to provide a helpful experience from an approved partner (such as an energy utility company)" (Google Nest, n.d.). Below is a table summarizing the data specifically captured by Google smart home devices collectively (not solely the Nest Mini) as per its FAQ on Google Nest Privacy in addition to the data from Table 7 (Table 8).

Category	Examples
Setup information	Device name and type, information about the home including address, ZIP/Postal code and where device is placed
Sensor data	Detected motion, ambient light measurements, temperature, humidity, carbon monoxide and smoke levels
Audio and video data	Facial recognition (if enabled by user), person/object/sound/motion/activity detection information (subject to personal permissions and settings
Device usage data	Manual device interactions (e.g. manually adjusting temperature), heating and cooling usage data, device state, settings and features used. Data from Google service usage or third-party service including voice and touch interactions, long presses on devices, other device interactions and adjustments (device state, settings, features used)
Technical data	Device make and model, serial number, IP and MAC address, Wi-Fi connectivity, signal strengths and settings, device detection on user network/nearby access points, hardware and software version, sensor status, battery charge level, log files from connections, power status, HVAC system capabilities, other technical information such as crash, diagnostics, reliability and performance logs and reports (if user enables this setting)
Services information	Type of service used (such as Nest Aware or an energy service like Rush Hour Rewards and Seasonal Savings), service attributes (such as features used or enabled), service usage data (such as start and end date, service adjustments, and feature settings), how the service performs, and any feedback on the service.

Table 8: Data collected by Google connected home products (Google Support, 2020c)

These devices handle and generate troves of data in exchange for convenience to the user. The next section will discuss some of the privacy controls offered by Google for its smart home devices.

Privacy Controls and Concerns

Another concern with data collection is the retention periods and deletion processes of collected data. In its Privacy Policy, Google states that there are three general timelines for data deletion: automatically, at the user's request and indefinitely in certain circumstances (Google Policies, n.d.). Examples of data that can be corrected or deleted at will by the user include their personal information, specific items from My Activity, photos and documents, removing a product from a Google Account and deleting a Google Account entirely (Google Policies, n.d.).

In the context of its connected home devices, the My Activity tab can be accessed within the Google Home app. In the app, the user can see all the interactions including metadata associated with the devices connected to the app. Some data about these interactions are unavailable or incomplete. For example, even with Voice Match enabled, My Activity does not show who made the query unless the "save audio recordings" setting is enabled, where the voice recording is attached[51]. Furthermore, some activity such as casting audio from a third-party app (such as Spotify) is not captured on the My Activity page at all. For deleting data, the user can delete history directly on the My Activity page or via voice command (e.g. "Hey Google, delete everything I said last week/month). Scheduled deletion of activity is also available (e.g. delete every month). While this may be generally good for privacy, it is easy to see how these might be problematic in the context of smart home TFV, where these details could be used as evidence as further discussed in chapter 6. It is also important to note that Google takes roughly two months to fully delete data and deletion may be suspended or unavailable in circumstances relevant to

[51] To test this, I set up Voice Match with my voice to differentiate it from two different text-to-speech bots. When searching through the My Activity tab, questions I personally asked do not show up differently than the ones asked by the bots. The only exception to this is when the "save audio recordings" setting was enabled; with this enabled, there is no text identifying that I or another voice made a query, but the audio snippets are attached to their respective record. It is important to note that this setting (saving audio recordings) is opt-in, meaning it is turned off by default.

smart home TFV such as abuse prevention and complying with legal requirements like subpoenas (Google Policies, 2020). In terms of technical security, the Google Home device meets the Mozilla Foundation's minimum security requirements of data encryption in transit and at rest, regular security updates, strong password requirements, a system for managing security vulnerabilities and a plain language privacy policy[52] (Mozilla, 2020). While it is true that Google has a plain language privacy policy, the privacy policy is not the only document relevant to the user concerns on data collection and security in order to truly understand how these devices operate, which users often bypass (Office of the Privacy Commissioner, 2016). Second, users with connected home devices by other vendors (e.g. Logitech, Phillips) are also beholden to their terms of use and privacy policies, which may differ from Google's.

Another potential issue with multi-vendor smart homes includes the use of the vendor's app in addition to Google's. For example, if two users are connected to the same 'Home' in the Google Home app (Figure 15), either user may revoke the other's access to the home and control over the devices. It does not matter which user initially configured or set up the devices, and Google does in fact make this clear if a user attempts to delete an account. Thus, if a dweller revoked their abuser's access, the abuser cannot control the devices via the Google Home app[53]. However, if the devices belong to other vendors, the abuser may still retain access and control over the devices through the device-specific apps, especially if it was the abuser who initially set up the smart home and may have administrative privileges. Even in a non-abuse situation, there are valid usability concerns in trying to manage or keep track of the data collected (as well as

[52] As seen in Table 6, the Google Nest Mini and its predecessor the Google Home Mini are very similar; making the analysis by Mozilla on the Google Home Mini still applicable to the Google Nest Mini.
[53] It is important to bear in mind that while this sounds like the ultimate solution to smart home TFV, the victim may not actually have access to the Google Home app and if they do, they may fear retaliation from the abuser should they revoke the abuser's access.

potentially different logins and passwords) for multiple apps, as can be the case for a multivendor smart home configuration. Lastly, it is interesting to note that despite Google's leadership in privacy practices, Google and Amazon now require smart home device manufacturers to constantly send status updates back to them, an arguably intrusive data collection practice. These status updates allow Google/Amazon to know when devices are being used and turned off in real-time (Day, 2019). Privacy concerns with this practice include Google/Amazon learning more about behavioral patterns of home occupancy which can a) become monetized (see Cyphers, 2020) b) used to further develop their products (e.g. Amazon adding a time display to the Echo Dot after realizing the most common voice command to Alexa is asking the time). Another privacy concern with this practice is its inconsistency with data minimization principles as this creates an excess of occupancy data and increases the severity of a data breach should one occur (Day, 2019).

5.3 Summary

This chapter has applied the methodology described in Chapter 4 to the Google Nest Mini suite (device, app and voicebot AI). In addition to step-by-step documentation of four main activity flows (as seen in sections 4.1.4 and 4.2.2), a content analysis was conducted on 33 additional documents (see Table 5) to establish the environment of expected use as well as discuss privacy concerns. The following chapter will analyze these observations as per the hybrid framework outlined in Chapter 3. These observations inform the analysis of smart home TFV in the following section.

Chapter 6: Discussion

In this chapter I will discuss the observations discussed in sections 5.1-5.3, which resulted in the application of the modified Walkthrough Method to the Google Nest Mini suite which included studying the social and technical discourse of the physical device, its software and mobile app, as described in Chapter 4 to understand the following:

- How this device can be misused for the purposes of smart home TFV
- How this device collects data
- Identify broader systems associated with the device by analyzing its environment of expected use.

The analysis of these qualitative data will be informed by the theoretical frameworks described in Chapter 3 which were assemblage theory (section 3.1), actor-network theory (section 3.2) and multi-scalar analysis (section 3.3) as well as by the literature review (Chapter 2). The analysis will be structured into three scales as explained in Chapter 3. While not mutually exclusive groupings, and the boundaries are not fixed, I did apply the following rules when sorting and arranging the various components and contexts (section 3.1):

- **Micro Scale:** Actors within the home (except for an abuser who may be out of the home, but retains access to the technology in the home)
- **Meso Scale:** Condominiums, apartments and rented dwellings, private companies operating outside the home, institutions and organizations including provincial governments
- **Macro Scale:** Federal government, multinational corporations, smart cities and broader ideologies, societal norms, etc.

6.1 Micro Scale Analysis

As discussed in the theoretical framework, the micro scale analysis is primarily concerned with actors within the smart home, such as the materialities and infrastructures that contribute to smart home technology and the practices of those who dwell in the home, and of those who no longer do but have access to the smart technologies in the home.

An important and often overlooked component of smart home technology are its enablers, such as electricity, common communication protocols, hardware miniaturization and Internet access, among others. As seen in Figure 15, a Google Nest Mini requires access to a power outlet. Once plugged in, the user must connect their Nest Mini to Wi-Fi and Bluetooth for the device to function, requiring a smartphone or tablet with the appropriate operating system to establish this connection. Other forms of infrastructure present in the Nest Mini include its connections to the Google Home app via smartphone or tablet and the broader Google ecosystem, as all Google Home app users must have a Google account to register (Figure 15). Once registered, users have the option to connect their Nest Mini and Google accounts to a variety of third-party services (Figure 19). While this thesis focused specifically on the Google Nest Mini, the enablers and infrastructures requirements for this device are the basis of many smart home technologies (SHTs), apart from Google-specific services, as many SHTs have their own respective apps. Even though someone may interact with these infrastructures on a 'micro' scale (plugging their device into their home, registering with their Google account, using the Google Home app on their personal smartphone or tablet), these micro-scale actions are intrinsically connected to their macro level deployments, such as the power grid, cloud computing (e.g. servers) and cell towers, as well as the macro-scale funding, research and development and policies related to infrastructure deployment and technology development (see sections 2.3 and 2.4). In the case of Google products specifically, the ubiquity of its products and

services on the micro scale (individual users) are also reflective of its sphere of influence as a multinational company, seamlessly integrating their products into the most intimate quarters of users' homes due to their trustworthy reputation (see Chapter 5.1). Like Latour's blackbox analogy (Latour 1999), most users do not realize or dwell on these connections until their device stops running smoothly, such as a power outage, weak Wi-Fi signal or failed Bluetooth connection. Nowhere is the link between macro scale infrastructure deployments and SHTs more apparent than in an instance of 'bricking', where technologies cease to function due to malware or companies exerting post-purchase control of their products (Tusikov, 2019). Even without bricking, some smart home technologies are simply not designed to function in any capacity without connection to the internet (Apthorpe et al., 2017). Thus, this linkage raises questions into another potential avenue of smart home TFV (as well as broader innovation agendas associated with IoT deployment) whereby control is exerted via disabling internet access or electrical power, which could be particularly devastating in full-fledged smart homes and for smart technologies installed for the purposes of disability and/or healthcare, whose users may rely on these technologies to a greater extent to improve or facilitate tasks in day-to-day life than able-bodied people who may install these technologies for fun or minor conveniences (City of Cote Saint-Luc, 2019; Birchley, 2017).

In terms of materialities (Table 9), the specific design choices of the Google Nest Mini are reflective of the subjectivities of its designers and the company's wider vision for the product (section 5.1.1.). As seen in Table 6, the Google Nest Mini is the smallest smart speaker available from Google yet one of the most powerful, due to the addition of a machine learning (ML) chip and processor. Not only are these improvements reflective of macro scale advancements in hardware miniaturization, but the addition of a ML chip to decrease query processing time and

improve quality of responses embodies Google's commitment to speed in order to retain users (Vaidhyanathan, 2011, p.69). The aesthetic components of the Google Nest Mini such as its muted color scheme and fabric top also contribute to its vision as an approachable and non-obtrusive addition to the home, a stark contrast to the 'futuristic' design of many SHTs. Google's software interface designs (Google Home app screens), which look and 'feel' like other Google services, also contribute to its ease of use and trustworthiness to users already familiar with Google. These design choices are purposefully made according to the subjectivities of Google as a company. Perhaps more implicitly, as briefly mentioned in Chapter 5, the cultural biases of technology designers are also seen in the device's difficulty in understanding non-Anglo-American accents (Fingas, 2018). In a similar vein, despite Google's connected home products bilingual capabilities, many languages are incompatible with certain devices[54]. On a micro scale, this may be misconstrued as a personal inconvenience for certain users. More broadly, this flaw is reflective of macro-scale cultural biases and individual subjectivities as well as meso and macro scale corporate visions or constructions of idealized or 'typical' users, resulting in misunderstandings of real users, as seen in Chapter 2.1 when discussing the idealized white, middle-class family of post-war electric appliance marketing and home journals (Walker, 2000) and misunderstanding of women's labour by male electric appliance designers (Berg, 1999; Cockburn, 1993; Cockburn, 1997). Directly relating this to smart home TFV, it becomes clear how the risk of unintended uses may be blurred when a technology is created with a specific user (as seen in the family-oriented visions of Google discussed in section 5.1.1.) in mind.

---

[54] For example, I tested the bilingual setting with three languages I speak with intermediate or higher proficiency: Canadian French (advanced), Castilian Spanish (intermediate) and European Portuguese (bilingual). European Portuguese was unavailable for the Google Nest Mini. When set to Brazilian Portuguese, the device sometimes had trouble understanding my regional accent but perfectly understood a text-to-speech bot in Brazilian Portuguese. The device understood my French and Spanish commands with no issues, despite my lower proficiency in Spanish.

The last major component of the micro scale are the practices associated with the Google Nest Mini. Thinking back to conceptions of time-using and time-saving devices (Crowley and Coutaz, 2015; Section 2.1), the Google Nest Mini and similar SHTs effectively blur these distinctions depending on user practices. On the one hand, the Google Nest Mini can be considered a time-saving device as home automation can facilitate tasks (e.g. hands-free control of light switches, near-instant responses to questions and requests). However, it can also be a time-using device when it is used for entertainment purposes, such as streaming music. Either way, these practices are facilitated by Google Assistant's default female voice, which is emblematic of gendered space and design in the home, with smart home tech as the new 'domestic helper' of the 21st century (section 2.1). The other dichotomy present in the practices of the Google Nest Mini, and SHTs more broadly, are the intended versus unintended uses of these technologies as detailed in sections 5.1.4 and 5.2.1. Conducting the modified Walkthrough Method, especially the technical walkthrough portion (5.1.4) illuminated how users do different things with the same features, such as casting media or reviewing activity. In the instance of abuse, these individual actions are also informed by wider societal gender inequalities and norms (Bailey and Mathen, 2017; Parsons et al., 2019). While abuse is technically against Google Terms of Use (see section 5.1.3.), one of the documents all users' practices are governed by a number of factors as listed in Table 9, it can be difficult to discern abusive practices based on the activity logs (see section 5.2.2.). This difficulty in interpreting activity logs as evidence of TFV may also be indicative of a macro scale lack of understanding or belief that smart home TFV constitutes real harm against another person, which will be further discussed in the next two sections. For example, without audio snippets saved (Chapter 5), an activity log full of "Google Assistant broadcasted a message" may not raise any suspicion as the content of the messages are

not displayed (Figure 21). This macro scale lack of awareness and understanding of smart home TFV can make victims of this type of TFV feel as though they are overdramatizing its effects and "going crazy" as described by smart home TFV survivor Ferial Nijem (Ghebreslassie, 2018), potentially opening up the possibility of gaslighting by the abuser as well as less incentive to report to the police.

No matter the intention, any practice associated with the Nest Mini on the micro scale (everyday use or smart home TFV) is also connected to the broader practice of data collection, monetization, and analysis as well as the various interfaces users interact with to enable this collection. As demonstrated in the operating model (section 5.1.2), Google derives significant value from the data its services collect, whether it is through optimizing their own services or real-time bidding. This process is further facilitated by Google's deep integration and interoperability between its services, meaning users stay in the Google 'ecosystem' for as long as possible (Jeffries and Yin, 2020; Table 9), thus the potential for more revenue. As seen in section 5.1.3. and section 5.2.2., users have some control over what and how much data Google collects about them via enabling and disabling certain settings like Web and App Activity or scheduled deletions of activity logs. However, there is a certain amount of data that must be collected in order to register (Figure 15) and as noted by Cyphers (2020), Google's monitoring extends beyond Google branded services, including advertising networks and webpages embedded with Google Analytics across the web (Table 9). Thus, not only does the micro scale expose surveillance practices between current (and possibly former) members of a home (e.g. monitoring activity logs) but also how smart home technologies are connected to broader surveillance apparati like corporate surveillance.

Below is a table summarizing the elements/content (actors) on the micro scale. Due to the flexible nature and interconnectedness of scales, some actors may also appear on other scales.

The main findings of this section reveal how micro scale phenomena, both human and non-human, are informed, influenced, and shaped by the two broader scales. As seen in Table 9, individual actions in the confined (or territorialized) location of an individual home, whether abusive or not, are informed by broader systems of thought, regulated by various governmentalities and legalities and shaped by various affordances granted through associated material components that contribute to the function of these devices and the subjectivities of those who design SHTs. In this view, it becomes clearer that smart home TFV is intrinsically linked to these elements within a sociotechnical assemblage.

Apparatus/Context	Elements/Content
Systems of thought	SHTs for energy-saving/sustainability; convenience; technological enthusiasm; misogyny and societal norms that perpetuate GBV/TFV; Focus on speed to retain users; gender and racial bias in technology; smart tech as domestic help; smart home tech as part of the family/guest in the home; smart home TFV and TFV as legitimate forms of abuse
Forms of knowledge	Guides included with Nest Mini/SHTs; Google support/FAQ pages
Finance	Sale of device; data monetization
Political economy	Energy incentives; public opinion on smart home tech, trust in tech companies
Governmentalities and legalities	Privacy laws, system requirements for phone/tablet to run Google Home app; Google's Privacy Policy and Terms of Service
Materialities and infrastructures	Design elements of Google Nest Mini, electrical power, Wi-Fi connectivity, Bluetooth connectivity, cellular data; common communication protocols; device hardware and software; tablet and smartphone hardware and software; machine learning chip; sensors; microphones; lights; interfaces and screens; ML Chip, processor, capacitive touch controls, ultrasound sensing, voice match technology
Practices	Individual practices and habits of smart home devices; everyday use; misuse of smart home device features for the purposes of TFV; personal preferences for privacy/device settings; data collection, monetization and surveillance by companies; software bricking; Ability to process requests locally via processor; ML chip to speed response; gaslighting of victims by abusers
Organizations and institutions	SHT vendors; SHT developers
Subjectivities and communities	Individuals in the home; individuals with control of SHT who may be outside of the home; technology developers; technology designers; user interface and user experience designers; Unobtrusive design of Nest Mini; first time smart home device buyers; technological enthusiasts; cultural biases
Places	Individual homes; within apps; servers [data]
Marketplace	Retailers of smart home tech; data monetization methods; ad networks

Table 9: Summary Table of Micro Scale Actors

6.2 Meso Scale Analysis

Like the micro scale, the meso scale includes subjectivities and practices of various actors, but here the focus moves from the individual to organizations and institutions outside of home. The meso scale includes 1) organizations and institutions that respond to and are

concerned with personal security, wellbeing and smart home TFV such as police or social work and 2) the fact that smart home TFV moves beyond the home, such as in a smart apartment complex or condominium development. When an instance of smart home TFV occurs, there are multiple actors who may provide various support services to survivors, if the survivor is able to access them. As part of the federal government's Strategy to End Gender-Based Violence (discussed in Chapter 2.3), the gender-based violence (GBV) knowledge centre was created to provide an online collection of resources across the country, and these can be found on the Department of Women and Gender Equality's (WAGE) website. Some of the resources include:

1) Crisis Lines for family violence or gender-based violence in every province (including some bilingual [Ontario, Quebec] and multilingual [Alberta, British Columbia, Ontario and Quebec])
2) List of provincial and territorial administered resources (province-specific information on family violence leave; province-specific GBV prevention initiatives, strategies and action plans)
3) List of funded projects across the country by the Department of Women and Gender Equality's Women's Program and GBV Program (will be discussed in more detail in macro scale analysis)
4) List of funding opportunities
5) Additional support services by province including additional helplines, shelters (emergency and general), victim services, web applications to access domestic violence services, mental health support, telephone help advice, financial help, social assistance, and housing

Within the list of resources, it is interesting to note the availability of multilingual crisis lines, which may help survivors whose primary language is not English gain access to these services, an important but unfortunately often overlooked segment of survivors (Woodlock, 2017). Moreover, a common feature of websites with information regarding GBV include a 'Quick Exit' button (including WAGE's page), which will exit the webpage and often open an inconspicuous site, such as Google search. While this is helpful in situations of physical surveillance (such as an abuser in the same room), these buttons cannot clear browser history, meaning there can still be a 'trace' if an incognito browser was not used or the user does not

clear their history manually. For webpages that redirect to Google, there may also be an additional risk if the user is signed into their Google account, as any future searches conducted through Google will be recorded in their activity log. Despite these minor flaws, the Quick Exit button is a good example of technology/feature design that is cognizant of different circumstances and risks.

Returning to WAGE's list of resources, it is important to note that governance in Canada is made more complex because of jurisdictional divisions. Although the literature review primarily focused on federal government action, provinces also have the capacity to write legislation, as seen in the GBV Knowledge Centre's list (Section 6.2; Status of Women and Gender Equality, n.d.). And as such, and as it the norm in Canada, there will be differences and inconsistencies between provinces. In a review of select domestic violence policies, legislations and services in Canada, *Women's Shelters Canada* pointed out differences between provinces on a variety of issues including provision pertaining to domestic violence leave and territorial tenancy acts (Martin and Stewart, 2018; Table 10). In an interview with the CBC on barriers in the Canadian legal system in the context of domestic violence, Jennifer Koshan described laws and services as being "patchwork from coast to coast" with a variety of gaps, especially for certain types of abuse such as emotional and financial abuse (Nicholson, 2020). The consequences of this will be further discussed in the macro scale analysis (6.3).

In addition to provincial services listed by the Department of Women and Gender Equality, some municipalities publish their own specific resource list. A good example is the City of Toronto, which published a list of domestic and intimate partner violence resources available in the city, including criminal and family court proceedings services, justices of the peace, legal aid and community legal services, childcare, community support services, distress

centres and a variety of counselling services, including general counselling and specific counselling for assaultive partners (City of Toronto, 2017). The list also includes a variety of culturally specific and multilingual community support services, which again is important in terms of equity of access to support services for non-Anglo-Canadian survivors. Both WAGE and the City of Toronto mention that people in immediate danger should call 9-11. Policing plays an important role in TFV more broadly, as they are often the first point of contact in the justice system should an instance be reported (Saxton et al., 2018). While various police departments across the country have made changes to their practices[55] to better serve those affected by GBV, domestic and sexual violence (see Ottawa Police, 2014; Canadian Chiefs of Police, 2019), it is important to recognize that not all survivors feel comfortable reporting to the police for a variety of reasons, including systemic racial and gender biases in criminal justice (Bailey and Mathen, 2017), a potential language barrier, fear of not being believed, concerns about citizenship or immigration status or past bad experiences with police among others, which further highlights the importance of diverse, accessible and well-equipped community services (as seen in the City of Toronto's list), which may serve as more 'approachable' first points of contact for some survivors. Furthermore, a study of 2,831 intimate partner violence victims conducted at Western University found that out of the 35%+ respondents who reported a crime to the police, perceptions of helpfulness were mixed (Saxton et al., 2018). The same study had similar findings in terms of perceptions of helpfulness of legal services due to challenges with sharing their stories and understanding legal jargon (p.4). Thus, training on TFV and smart home TFV would help these organizations better serve survivors, current and future.

[55] In 2014, Ottawa Police Services held a consultation with frontline workers to discuss police response to intimate partner and sexual violence (Ottawa Police, 2014). In 2019, the Canadian Chiefs of Police created a framework for collaborative police response on sexual violence (Canadian Chiefs of Police, 2019).

When thinking back to the technical walkthrough (4.1.4) and the data section (4.2.2), another possible barrier to reporting smart home TFV specifically are the inconsistent records kept in the My Activity tab. As some actions such as casting audio are not recorded in the My Activity tab, solid evidence may be difficult to obtain, especially if data are captured on a variety of accounts (if there are multiple users registered who all have access via the Google Home app) or if the survivor does not have access to the My Activity page (such as an employee or a household member who may not have an account associated with the device). Moreover, evidence may be weakened depending on certain settings like the capturing of audio or deletion of certain records, opening the possibility of gaslighting by the abuser, as previously mentioned in Chapter 5 and the micro scale analysis (6.1). Further complicating these data as evidence are the information asymmetries inherent in connected devices. As described by Privacy International, smart home technologies create information asymmetries in two ways: 1) through police likely having better ability to extract and interpret digital evidence than its user and 2) through companies keeping much of the data collection process 'invisible' (or blackboxed as per Latour), meaning users are generally unaware of what kind and how much data are being collected about them and generated by their devices (Privacy International, 2019). They also highlight the issue of incomplete activity logs and the technical insecurity of connected devices (e.g. easily hacked) as other contributors to the unreliability of SHT collected data as evidence. These issues are only further exacerbated by police forces' increasing interest and reliance on data captured by smart home technologies not only for instances of TFV, but other crimes committed in and outside of the home (Fussell, 2020). For example, activity logs of a smart speaker could reveal that someone was in the home at a certain time (especially if audio snippets are captured), giving that person an alibi (Fussell, 2020). Google's Transparency Report reveals

that in 2019, 1037 requests for user information were made in Canada by various government agencies, including law enforcement (Google Transparency Report, n.d.), with the number of requests likely to rise as smart home technology continues to proliferate and smart home data being used in courts as evidence (Fussell, 2020). Currently, requests for user information are individually dealt with directly by Google's legal team. However, 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 [Kelley and Guariglia, 2020]) should requests for information increase substantially in the future, which could have a variety of tricky implications for individual privacy and criminal justice. Focusing back on instances of smart home TFV, these types of issues and considerations are just one example of why it is worth distinguishing technology-facilitated violence from other forms (see Chapter 1), as the 'new' technologies used to perpetrate 'old' behaviours (Henry and Powell, 2015) may not be well understood, pose new risks for victims via new methods for abusers to exploit, challenges to current mitigation measures for frontline organizations and are changing at a rapid pace, which may impede legal interventions.

As identified in the literature review, certain Canadian organizations such as the BC Society of Transition Houses and the Citizen Lab have created documents specifically related to TFV and digital security (BCSTH, 2019; Khoo, Robertson and Deibert, 2019; Parsons et al., 2019[56]). Resources related specifically to TFV (especially smart home TFV) are noticeably absent from the GBV Knowledge Centre. While there are TFV resources online from various countries (see Tanczer et al., 2019) especially in terms of managing one's person digital security

[56] Citizen Lab also have a digital security tool called the Security Planner that is meant for broader use but is definitely helpful in terms of TFV as it provides personal cybersecurity recommendations based on a questionnaire, meaning the advice is somewhat tailored to the user's security needs.

or ‘cyber hygiene’, these may be difficult and time consuming to find. It may be advisable for Canadian organizations and institutions on both the meso and macro levels to produce (or reproduce with permission) informational materials like safety guides and pamphlets related to smart home TFV, digital security and TFV more broadly to enhance the accessibility and availability of these resources. Furthermore, as suggested in the literature review (Henry and Powell, 2015; Tanczer et al., 2018; Khoo, Robertson and Deibert, 2019), specialized training for organizations and institutions who serve those affected by smart home TFV and other forms of TFV. Another timely consideration for these resources includes the COVID-19 pandemic, which has resulted in an uptick in domestic violence, including surveillance and technology-facilitated violence (Koshan, 2019). As legal scholar Jennifer Koshan notes, the pandemic has provided enhanced opportunities for surveillance, including increased policing of activities and interactions of others during social isolation (p.1). Part of the reason this is possible is because social isolation orders increase the chances that victims will be home and abusers are “counting on protective legal remedies being more difficult for victims to obtain” during this period (p.3). Sophia Maalsen and Robin Dowling (2020) also describe how the pandemic “reinforces and digitally recalibrates home” as many technologies used to work from home and comply with social isolation orders have the potential to enable heightened surveillance and control creep[57] (p.5).

As organizations and institutions prepare to deal with smart home TFV as explained here, it is useful to consider how smart home TFV will manifest in larger deployments on the meso and macro levels, beyond an individual home. For example, building and real estate industries

[57] ‘Creep’ refers to when something (data, technology) are used for something other than their intended purpose, especially without notice or consent (Mediasmarts, n.d.).

are two major actors in the proliferation of smart homes. In the United States, smart home technologies are increasingly featured at events such as builder trade shows often cast to homebuyers' looking for energy-efficient homes[58] (Norris, 2019). In the Canadian context, home builders have acknowledged the need for tradespeople to have technical competencies (Table 10) so that they may be able to "work in partnership with existing and emerging technologies" (Ontario Home Builders' Association, 2017, p.4). The latest version of the Canadian Home Builders' Manual also includes a section dedicated to smart home automation (Canadian Home Builders' Association, n.d.). One example of a smart apartment in Canada was developed by builder Tridel as part of the Ten York Community of luxury condominiums in downtown Toronto, built in 2018. Some of the technologies included in the Ten York Community include "digital door locks, smartphone-controlled thermostats, automatic license-plate recognition for parking garage, automatic parcel delivery and smart locker system and advanced Wi-Fi as a utility" (Greene, 2019; Tridel, n.d.).

Despite using the example of a luxury condominium, it is important to not misconstrue smart home TFV as a problem that only has the potential to affect the wealthy. Not only do luxury smart homes pose risks for workers within them (cleaning staff, nannies, homecare assistants) (Hall, 2018), but as demonstrated in Chapter 4, smart home technologies can be relatively affordable and will likely become more affordable over time and it may become a way for a property manager to control, monitor and manage their assets at a distance. While this thesis primarily focused on 'consumer-facing' smart home technologies (smart speakers, lights), there are other forms of SHTs including other digital technologies like smart water valves and

[58] One of the major discourses surrounding smart home technology (primarily SHTs that can control lighting, heating/cooling) are that they can help your household be more energy-efficient (Hargreaves and Wilson, 2017).

meters, automated eviction platforms and facial recognition entry systems which are being developed for landlords and property managers (Table 10). These are a new group of smart technologies known as property tech or proptech (Norris, 2019; Maalsen and Dowling, 2020). As discussed in the introduction (Chapter 1), landlords are also installing SHTs such as smart door locks (Doctorow, 2019a; Doctorow, 2019b), which also present new risks for smart home TFV and potentially new challenges to existing privacy legislation related to the tenant and renter relationship (Office of the Privacy Commissioner, 2018). These examples highlight the importance of examining both human and non-human actors equally, as per ANT principles (Chapter 3) because the technologies themselves provide different affordances and implications worthy of study. In the context of smart home TFV, a thorough understanding of these technologies will help to better understand how they can be misused and how to mitigate these risks. More broadly, the accelerated proliferation of new smart home technologies is also illustrative of why it is so important to study technological changes, as the risks we know of right now will likely morph in as little as five years (see OCTEVAW, 2015 in Chapter 2.3).

Outside of Canada, a collaboration between one of England's largest social housing landlord companies *CrossKey Homes*, and digital infrastructure provider *CityFibre* use social housing in Peterborough as a testbed for smart city technology. Through the deployment of various sensors to monitor health, safety and environmental factors, *CrossKey Homes* and *CityFibre* expect outputs such as environmental benefits, increased comfort for tenants and a reduced carbon footprint (Stephens, 2019). While these actions may be based on good intentions, it is critical to consider the risks of misuse, such as predatory inclusion[59] (Maalsen and

[59] Predatory inclusion refers to "wherein financial actors like lenders offer needed products and services to members of marginalized groups but on exploitative terms that limit or eliminate their long-term benefits" (Maalsen and Sadowski, p.5).

Sadowski, 2019) and the use of alternative rationales to normalize surveillance like the green initiatives as seen with Peterborough social housing or in the context of COVID-19, the justification of surveillance for the sake of public health (Maalsen and Dowling, 2020). Moreover, this type of development amplifies the risks found in an individual home, especially matters of consent of technologies placed within the home and surveillance. For example, if a home developer requires smart home technologies to be installed in rentals or social housing as a condition of living in that space, the agency of choosing whether to live with and be monitored by smart home technology may be taken away for a significant amount of people, especially those of already marginalized groups. 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, which would further limit the agency of anyone who may not be able to afford opting out or who have little to no choice in working 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 and 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 and 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) but also strays away from placing accountability onto technology designers and manufacturers to create technologies up to these standards in the first place, lessening the security burden on individual users. Moreover, in the

case of landlords, admin, jurisdiction and responsibility over smart home technology becomes further complicated. 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 and an instance of smart home TFV within a tenant's home, there is an additional risk to a survivor whereby the landlord may deem them high friction and risk, kick them out and further marginalize the survivor. Lastly, there are valid questions as to who the final arbiter is and where a survivor could seek help.

Thus, as seen in the summary table below, the meso scale scales up to include larger actors such as proptech, more homes managed by one large company and moving beyond the boundaries of the individual home with a single owner. Meso scale actors interact with some of the same assemblage components operating at the micro scale such as builders with infrastructures and materialities; insurance companies with smart home data, to name a few, as well as the macro scale actors such as government funding for intimate partners, sexual and domestic violence service providers. The significance of the meso scale is that it provides, as the name suggests, a sort of 'middle' ground between individual actions and broader systems that allows for analysis of the broader implications of micro-scale individual practices and actions (the need to find resources related to TFV after an incident has occurred, which services are available, etc.) as well as the efficacy and implications of macro-scale policy and funding allocations (results of funding of provincial initiatives for GBV, jurisdictional issues between provinces). Lastly, this scale is able to identify emerging trends that could be of future interest to macro-scale actors, such as the proptech industry, potentially allowing for earlier intervention.

Apparatus/Context	Elements/Content
Systems of thought	Technological solutionism/enthusiasm; energy-efficient/sustainable homes via SHTs; convenience of remote monitoring of SHTs (efficiency agenda); property management, rationales of environmental benefits in social housing; rationales of public health for surveillance tech during COVID-19;
Forms of knowledge	Multilingual crisis lines; expertise in various frontline organizations; resource lists; digital security tools and guides; Canadian Home Builders' Manual;
Finance	Funding for frontline organizations and GBV-related initiatives; financial help for survivors; insurance incentives for cyber hygiene
Political economy	Strategy to End GBV; GBV Knowledge Centre; Funded Partners of the Strategy to End GBV (Appendix B); Funding of provincial initiatives subject to priorities of current government; public opinion on smart home tech installed in multi-unit
Governmentalities and legalities	Distinctions between provincial and federal jurisdiction; provincial and territorial administered resources (tenancy acts, province-specific info on matters such as family violence leave); discrepancies between provinces on policy administration related to domestic violence broadly; file formats of activity logs including audio snippets; privacy legislation; building code
Materialities and infrastructures	Web applications; internet infrastructure; enablers of and the devices to access online services and resources; Quick exit buttons; device activity logs; metadata; digital door locks; thermostats; automatic license-plate recognition; smart lockers; Wi-Fi as utility in condos;
Practices	Physical surveillance; Quick exit buttons redirecting to inconspicuous webpages; communication barriers to legal services; individual preferences and habits of activity log/privacy settings; gaslighting; cyber hygiene; training for frontline services; surveillance creep; predatory inclusion
Organizations and institutions	Shelters; victim services; web applications; mental health support; social assistance; housing assistance; provincial governments; municipalities; criminal and family court proceedings; justices of the peace; legal aid and community legal services; childcare; community support services; distress centres; counselling services; emergency services (9-11); policing; academia; real estate; construction and housing developers; insurance; technology companies
Subjectivities and communities	Perceptions of policing and legal services; information asymmetries of connected devices; companies keeping data collection 'invisible' to users; renters; homeowners; landlords and property managers; insurance companies, need for increased technological skills in homebuilding; workers within a smart home; technology designers and manufacturers
Places	Municipalities; individual services; apartments and condos; tradeshows, California as the location for dispute resolution for Google
Marketplace	Property tech (proptech); insurance data and policies related to smart homes

Table 10: Summary Table of Meso Scale Actors

6.3 Macro Scale Analysis

As discussed in section 2.3, macro scale actors such as governments, policy and legislation are important when it comes to preventing and mitigating the impacts of smart home TFV experienced at the micro and meso scales. Two major ways that macro scale actors interact with the micro and meso scale is through governance and funding. As seen in the meso scale analysis (5.2), governance in Canada is made more complex because of jurisdictional divisions and the autonomy of provinces. When thinking about TFV and smart home TFV, jurisdiction is further complicated as they may cross provincial or international borders (Gladu, 2017), especially in the context of data storage (Table 11) as many multinational corporations may store data on a number of servers around the world, the location of dispute resolutions being in California as in the case for Google (see chapter 5.1.3) and smart home technology data increasingly being used for evidence (see section 6.2).

There are only a few items in the Strategy to End Gender-Based Violence related to prevention and support for TFV. As seen in Appendix B, there are only 3 initiatives specific to TFV such as preventing cyberbullying, enhancing capacity to combat online child sexual exploitation and awareness of online child sexual exploitation, which primarily focus on forms of TFV against children and well-known forms of TFV. Furthermore, most of the initiatives fall under pillar 2: supporting survivors and their families. Similar patterns emerge when reviewing projects funded by Women and Gender Equality Canada. Out of the 156 funded projects across the country, 97 (62%) of them are under pillar 2. Across the three pillars, only 7 mention cyberviolence in some capacity. The common thread between these 7 initiatives are that they all involved some sort of multi-stakeholder collaboration with goals ranging from creating local strategies to mitigate or eliminate cyberviolence, establishing knowledge exchange hubs and

creating peer networks for girls in schools and youth groups among others ('Funded Projects' – Status of Women and Gender Equality Canada, n.d.). It is advisable that the Strategy continues to fund similar initiatives dealing with cyberviolence but also be mindful of where these projects are funded, as a majority of the cyberviolence initiatives are within the Greater Toronto Area (5 out of 7) and only represent three provinces (Ontario, Quebec and Nova Scotia). While it is natural for a large urban centre like Toronto to have more initiatives than other places in the country, cyberviolence and smart home TFV can happen in any city or province, meaning all provinces should be well-equipped to deal with these issues. Moreover, as the development of smart homes and cities require forward thinking, more initiatives could be funded under the prevention pillar to create proactive responses to emerging forms of TFV like smart home TFV rather than being purely reactive. As mentioned in the literature review (Chapter 2.3), there is a need for national awareness, action and recognition of emerging forms of TFV such as stalkerware, spyware and smart home TFV (Tanczer et al., 2018; Khoo, Robertson and Deibert, 2019). Potential policy and legislative actions from the literature review include modernization of existing legislation (such as PIPEDA) (Khoo, Robertson and Deibert, 2019; Citizen Lab, 2017), increased training (and funding for training) of frontline organizations and law enforcement on TFV (Tanczer et al., 2019c; Gladu, 2017) and the broadening of definitions of domestic violence to fully encompass new and emerging methods such as smart home TFV (Violence Abuse and Mental Health Network, n.d.). Thus, while the Strategy to End Gender-Based Violence is a step in the right direction, some have argued that a national action plan on domestic violence (Martin and Stewart, 2018) or a federal act similar to the United States' Violence Against Women Act (Nicholson, 2020) must be created in Canada to mitigate provincial discrepancies and provide better access to funding for frontline organizations and

training for national, provincial and local police forces to have the mechanisms to address it when it is reported (Table 11).

Another important macro consideration for smart home TFV is the acknowledgement that smart homes are important sites for cybersecurity intervention. In Canada, federal government action on cybersecurity is largely focused on protection and deployment of critical infrastructure (Public Safety Canada, 2019). Furthermore, the Cyber Centre's current publications on IoT security are largely targeted towards organizations rather than individuals and require some level of technical knowledge as their recommendations are not fully explained and likely targeted towards users with a solid base of technical knowledge (Table 10) . Of course, the protection and securing of critical infrastructure is integral as their security will ultimately affect the security of citizens (see section 6.1), but increased action and guidance on cyber hygiene for individuals is necessary. As demonstrated in the technical literature (Atzori et al., 2010; Geneitakis et al., 2018; Apthorpe et al., 2017) and acknowledged by Public Safety Canada, IoT deployment is known for its security vulnerabilities. As these devices begin to proliferate in individual homes, let alone entire cities, individuals will require enhanced guidance and knowledge on how to keep themselves and their information safe. In addition, there is merit in trying to develop methods to ease some of the burden of security from the user, such as improvements in the technology design process (Freed et al., 2018). For example, a GBA+ analysis conducted on a smart home technology could reveal issues related to TFV as a GBA+ analysis would likely take into consideration an abusive ex as an important threat model for technologies in the home.

In the context of smart home TFV, part of this problem could be remedied through policy action of enhanced training on TFV for frontline organizations, as training could increase the capacity for both meso scale actors (provincial gov, frontline orgs) and macro level to develop

and disseminate relevant resources such as safety guides, pamphlets and lists of community services. There is also potential for cross-sectoral collaboration and knowledge mobilization in this area, as so many different organizations contribute certain knowledge and expertise on these issues. For example, a frontline organization (or even the Department of Women and Gender Equality) could collaborate with the Cyber Centre to develop public facing guides, infographics, and safety tips on smart home TFV. Another example could be a federal department such as Women and Gender Equality Canada or the Social Sciences and Humanities Research Council (SSHRC) (depending on the participants) funding macro level initiatives similar to the computer security clinics of the IPV research group at Cornell Tech in the US, where technical experts meet with survivors of TFV and help uncover and mitigate any abuse they are facing in conjunction with other meso level actors like social workers and police (Clinic to End Tech Abuse, n.d.; Havron et al., 2019; Table 10). However, these sorts of solutions are highly contingent on the priorities of the current government in power (Table 11).

Despite Sidewalk Toronto pulling out of the Waterfront Toronto Project (2020), discussions and consultations on what citizens want to see in the future of their cities is warranted as these kinds of developments are not disappearing anytime soon. As many of the SHT vendors also create technologies on the smart city scale (such as Alphabet Inc. with Sidewalk Labs and Google connected home products), it is valuable to view the smart home as a sort of miniaturized version or testbed for smart city technologies. One of the most important practices that must be analyzed further is data collection and monetization by technology companies. In this current time of 'techlash', it is worth examining and questioning the value that private companies derive from data collection, especially considering the increasingly intimate data they are able to collect through IoT devices (see section 5.2.2 and section 2.4) and how to

regulate them, and the mistrust people of have of these big companies in general (The Economist, 2018) which is also fueled by COVID-19 contact tracing apps (Rabson, 2020; Geist, 2020) (Table 11). Not only are the data collected becoming more intimate but are appearing in more scenarios where consent may be blurred (social housing, health and eldercare to name a few). Data collection is further problematized via partnerships and acquisitions of other meso and macro level actors, such as Amazon's Ring (smart doorbell) partnership with US police departments (Kelley and Guariglia, 2020) and Google's $450 million investment in security company ADT (Porter, 2020), which ultimately extend corporate power, their respective spheres of influence and surveillance. In a smart city scenario, this power is further amplified as a private company may be the sole provider of a city's technology via government contracts, granting access to a vast trove of data, much of which is collected and generated 'behind the scenes' unbeknownst to some citizens in addition to data collected from smart homes (Table 11). While various power dynamics can be seen on the previous two scales (abuser/victim, landlord/tenant, police/survivor, technology company/user, individual/legal system, etc.), the macro scale is the locale of the broader systems of thought that inform and sometimes reinforce these dynamics. Just as the smart home can be viewed as a miniaturized smart city, the smart city can be viewed as a glimpse into society at large. While this thesis has focused on the implications, risks, and effects of smart home TFV, it is important to acknowledge the disproportionate effects of smart home TFV, surveillance and violence on marginalized people. As writer Lorraine Chuen (2018) succinctly states, "Communities at the margins have always been watched. Discussions about the rise of surveillance technology must acknowledge the histories and ongoing surveillance of those who are racialized, poor, migrants, incarcerated, queer, women. We cannot talk about surveillance without talking about power" (p.1). Both Chuen (2018) as well as Murakami Wood

and Mackinnon (2019) highlight how hiding behind the shiny slide decks and utopic promises (or innovation agendas) of projects like Sidewalk Labs may ultimately exacerbate already existing inequalities by further adding to the data collection and subsequent data dehumanization of marginalized people[60]. Not only do we see similar power dynamics present on the micro scale (consider the 'watching' or monitoring of activity logs and cyberstalking by abusers in Chapters 2.3, 2.4 and 5), but it is easy to imagine how a survivor may become further entangled in broader systems of data collection (such as applying for financial or housing assistance [Chuen, 2018], having their location inadvertently revealed or monitored due to phone settings, etc.), exacerbated by the smart city. Considering this, some scholars and experts have proposed the need for a national data strategy. Legal scholar 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, with all needing consensus at both federal and provincial levels to maintain consistency in enforcement across the country[61] (Scassa, 2019). Tying back to the literature review (Chapter 2), the examples put forth in the macro scale analysis also illustrate the importance of tools such as GBA+ being integrated into various macro scale processes such as smart city design and the creation of public policy, as these types of analytical tools help designers, policy makers and planners consider the impacts of their work from varied perspectives, mitigate potentially harmful biases that may otherwise be overlooked and highlight issues such as smart home TFV, thus inching closer to inclusive and equitable design[62].

---

[60] It is also helpful to think back to Schiller and McMahon (2019)'s work on the racial and gendered biases encoded within voice assistants mentioned in Chapter 5.
[61] A detailed discussion of a data strategy is out of scope for this thesis but a potential avenue for future work.
[62] It is important to note here that the thesis does not intend to imply techno-solutionism here and that I am cognizant that technologies will not singlehandedly solve societal issues.

As seen in this chapter and the summary table (below), it becomes clear that interventions on the smart home (or micro) and meso levels are necessary and the identification of issues at these scales have the potential to mitigate the risk of their reproduction on a macro scale, when they could reach the point where it is hard to change embedded and ubiquitous practices (Hughes, 1993). Moreover, as our homes and cities become increasingly digitized, the distinctions between online and offline harms are further blurred. Being surrounded by 'always on' devices in everyday life, whether in the home, the workplace or in a city, means that cybersecurity becomes increasingly linked with personal security and safety (especially for marginalized people), further amplifying the importance of cyber hygiene and awareness of how technologies can be misused, including smart home TFV. The actors within the macro scale occupy an interesting space in the sociotechnical assemblage as this scale is 'home' to some of the root problems and causes of smart home TFV via various systems of thought (biases, misogyny, patriarchy, surveillance) as well as the scale with the most power to enact meaningful, sweeping changes to mitigate smart home TFV (funding for meso scale organizations/local initiatives, creating policies and smart city designs with equity and inclusive principles in mind, 'techlash' against technology companies) as experienced on all three scales.

Apparatus/Context	Elements/Content
Systems of thought	Pillars of the End Gender-Based Violence Strategy; rationale for increased awareness of smart home TFV; rationales for cybersecurity; 'techlash'; innovation agendas of smart cities; misogyny and societal norms that perpetuate GBV/TFV; gender and racial bias in technology
Forms of knowledge	Cyber Centre publications; policies; laws; technology design; public consultations and discussions on smart cities
Finance	Project funding for GBV initiatives; funding for smart home TFV training; capital for smart cities
Political economy	Complexities of jurisdictional divisions and autonomy of provinces; cross-border data flows; modernization of existing privacy legislation; matters of data privacy and security of smart cities; government contracts to multinational tech companies
Governmentalities and legalities	Privacy legislation (such as PIPEDA); need for national action plan or federal act on domestic violence; creation of a national data strategy
Materialities and infrastructures	Server (farms); stalkerware; spyware; internet infrastructure; power grid; 5G networks
Practices	Enhancing cybersecurity habits and hygiene; creating policies to address smart home TFV; connection between cyber and personal security; mass data collection; mass surveillance; knowledge mobilization
Organizations and institutions	Federal government departments; frontline organizations; multinational technology companies
Subjectivities and communities	Priorities of current government in power; citizens of a smart city; technology designers and manufacturers
Places	Individual homes; individual organizations; apartments; condos; entire cities; server farms
Marketplace	Mergers and acquisitions of smaller companies by multinational technology companies; governments seeking smart city solutions; partnerships between organizations; SHT vendors

Table 11: Summary of Macro Scale Actors

6.4 Summary

In summary, this section discussed the findings of the literature review (Chapter 2) and the technical walkthrough (Chapter 5) according to the hybrid theoretical framework developed in Chapter 3. As seen in the previous tables (Table 9, Table 10, Table 11), smart home TFV is comprised of a wide assemblage of human and non-human actors that exist in a multi-scalar reality. While the scales used in the analysis are not rigid, the use of scale was helpful to both

organize the findings (illuminated via assemblage theory and the Walkthrough Method) as well as represent spheres of influence. When unpacked in this way, it becomes clear that instances of smart home TFV are not isolated, one-on-one disputes. Rather, it is a practice that is enabled, mitigated, and ultimately shaped by a variety of contexts (Kitchin, 2014) as well as its interactions with other components (Kitchin, 2014). For example, this method not only traces the potential 'journey' of a survivor from how the abuse occurs (6.1) and where they might seek help (6.2) but also creates an understanding of how this process is influenced by and intrinsically related to perhaps seemingly disparate phenomena like technological change and design, data collection and privacy policies and corporate surveillance among others (6.1, 6.2, 6.3). 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 Nest Mini in a home on a micro scale versus living in a smart city) By doing so, this further territorializes the site of the smart home as an important part of broader networks such as smart cities and infrastructure deployments, even though it may not initially seem so.

The subsequent chapter will summarize the findings of the thesis, restate its theoretical contributions, discuss its limitations, and highlight areas of future work and research.

Chapter 7: Conclusion

The goal of this thesis was twofold: 1) to understand how smart home technologies are misused for the purposes of smart home TFV and 2) to examine how smart home TFV can be conceptualized as a part of a large sociotechnical system and the benefits of this approach. This chapter will summarize each of the previous chapters and their contributions to answering the research questions and state its theoretical contributions. The later portion will discuss its limitations, future areas of work and research and any final thoughts or takeaways.

To begin, chapter 1 introduced the issue of smart home TFV, defined what a smart home is and provided the rationale of using the term "smart home technology-facilitated violence" or smart home TFV. As stated previously, the "technology-facilitated" prefix was chosen as it is commonly used as a differentiator between violence enacted through digital media, less ambiguous than prefixes such as 'cyber' which have other connotations and allows for critical exploration of the new affordances and risks provided by technologies to perpetuate 'old' behaviours. Since TFV has multiple forms, focusing on TFV mediated through smart home technology enabled the examination of a new, emerging, and understudied form of TFV while also situating it within the broader sociotechnical implications of smart homes. By not narrowing the definition to intimate partner violence (IPV), this recognized that smart home TFV may occur in other relationships besides intimate partners, and this was primarily discussed in the

meso scale analysis (section 6.2). Chapter 1 also provided brief context into wider IoT deployments and the burgeoning popularity of smart home devices in Canada to further illustrate the urgency of addressing smart home TFV and presented the two main research questions of this thesis.

To expand on the context given in chapter 1, in chapter 2 an interdisciplinary literature review was provided, and it incorporated a variety of relevant concepts, issues, projects, viewpoints and subjectivities. The literature review was divided into four main categories: 1) history of home automation and gendered design, 2) the state of current TFV research, 3) Canadian policy and legal environment, 4) technical research on smart home tech safety and security. Upon reviewing 77 documents academic and grey literature (Table 1), it was discovered that there was an established, gendered history and linkage between the smart home of today and 20th century domestic home technology (section 2.1), little academic research and legislative action in Canada on smart home TFV and a general lack of acknowledgment in the technical literature (section 2.4) of an abusive (ex)-spouse as a serious threat actor. This thesis addressed some of the shortfalls of the literature by conducting a study on smart home TFV in the Canadian context, drawing parallels to the implementation of smart cities and mobilizing knowledge from a variety of disciplines and methods.

Chapter 3 provided the theoretical framework of the thesis which was purposely designed to enable the analysis of smart homes and smart home TFV understood as large sociotechnical systems. The hybrid theoretical framework developed in this chapter included Rob Kitchin's iteration of assemblage theory (Kitchin, 2014), principles of actor-network theory such as agnosticism of human and non-human actors and blackboxing (Latour, 1999) and multi-scalar analysis as developed by Paul Edwards (2003). Together, these render the heterogeneous content

and context components of smart homes and smart home TFV (actors) visible, their relationships between them for analysis and for the components and their relationships to be organized, contextualized and understood within a contemporary multi-scalar reality.

To complement the theoretical framework, chapter 4 discussed the methodological approach adopted to study smart home TFV in Canada, which was a modified version of the Walkthrough Method developed by Ben Light, Jean Burgess and Stefanie Duguay (2018). In its original form, the Walkthrough Method combines step-by-step technical walkthrough methodology with the 'analytical power' of cultural studies and actor-network theory to illustrate the mutual shaping of technology and society via examination of an app's vision, operating model, and governance (the environment of expected use) and its everyday uses (via the step-by-step documentation of screens) (p.2-4). The Walkthrough Method was modified in this thesis to include two additional sections pertaining to 1) issues of data collection 2) environment of 'unexpected use' or smart home TFV. These modifications further facilitated the Walkthrough Method's ability to illuminate how issues such as smart home TFV materialize through smart home technologies themselves, working in tandem with the theoretical framework.

The subsequent chapter applied the modified Walkthrough Method on one smart home technology, the Google Nest Mini, a smart speaker. As stated in Chapter 5:, this device was chosen for analysis because of its low price point, popularity in Canada and ease of use, so that the findings are more likely to be generalizable than highly specialized, in lieu of custom smart home solutions or more expensive 'off the shelf' counterparts. After applying the methodology to the Google Nest Mini suite (device, app and voicebot AI), providing step-by-step documentation of four main activity flows (sections 4.1.4. and 4.2.2.) and a content analysis of 31 additional documents (see Table 5), key observations and findings included:

1) identification of various components relevant to the discussion section, such as intended and unintended uses of smart speakers, data collection practices and various infrastructures,
2) two ways in which the Nest Mini can be misused for smart home TFV,
3) privacy concerns with data collection practices of smart home technologies and
4) an enhanced understanding of Google's operations, including the value it derives from data collection practices and how their technologies are marketed to the public.

Overall, this section was integral to answering the first question of the thesis, regarding how smart home technologies are misused for smart home TFV. Furthermore, it can be argued that this exercise of walking through a smart home device such as the Nest Mini and examining how it can be misused not only legitimizes smart home TFV as an issue deserving of attention and awareness but also acts as an illustrative example as to why researchers and subject matter experts separate technology-facilitated violence from other forms of violence by describing and analyzing the specific device's risks and affordances (Chapter 1). Methodologically, the walkthrough method and the modifications additions coupled with assemblage theory (Kitchin, 2014), illuminated the various components and contexts that comprise smart homes and smart home TFV, laying the groundwork for them to be unpacked at the three scales in the discussion section.

Chapter 6 discussed the findings of sections 5.1 and 5.2 as well as the literature review (Chapter 2) informed by the theoretical framework, including the use of micro, meso and macro scale analysis. As previously stated, the following flexible rules were applied to the three scales when sorting and arranging the various components and contexts (section 3.1):

- **Micro Scale:** Actors within the home (except for an abuser who may be out of the home, but retains access to the technology in the home)
- **Meso Scale:** Condominiums, apartments and rented dwellings, private companies operating outside the home, institutions and organizations including provincial governments
- **Macro Scale:** Federal government, multinational corporations, smart cities and broader ideologies, societal norms, etc.

The use of multi-scalar analysis helped to unpack the various contexts and components (Kitchin, 2014) identified in previous chapters, ultimately making them actionable. Action on smart home TFV and related issues cannot be taken if one cannot see the interconnectedness of these heterogeneous components or how the same components scale up in different deployments (such as data collected from individual device's being part of wider systems of surveillance, which are informed by broader systems of thought and power dynamics). Moreover, examining the linkages between these components (via principles of actor-network theory) helped to identify various interdependencies like the relationship between enabling infrastructures and the technologies that use them, all of which are benefits to using these methodological and theoretical frameworks. Lastly, the equal weighting (or agnosticism) given to human and non-human actors ultimately allowed for this thesis to fully explore how the social and technological components of smart home TFV are intrinsically linked and mutually inform each other. Overall, the discussion successfully contributed to answering the second part of the thesis question concerned with how smart home TFV can be conceptualized as part of a large sociotechnical system by illustrating the assemblage of human and non-human actors associated with smart homes and smart home TFV and the subsequent benefits derived from this conceptualization.

Thus, the main contributions of this thesis include: 1) a study of smart home TFV in the Canadian context, 2) an interdisciplinary approach to examine this issue and 3) a modified methodological approach that added unintended use and data and applied the study a smart home and not just an application and 4) a hybrid theoretical framework that situated smart home TFV in its complex social and technical ecosystem and to assess sociotechnical implications of technologies and associated practices. The methodological approach and the theoretical framework including how the results were arranged into different scales, was not only useful for

this study, but these could translated beyond the academy to help facilitate action on smart home TFV within individual organizations and different levels of government as their respective 'roles' and potential action items are highlighted via this method.

To conclude, it becomes clear, that the governance of smart home TFV will require a multi-stakeholder approach as its impact is embedded within a vast network of both public and private institutions and is not an issue to be dealt with solely by social workers, police officers or technology designers.

7.1 Limitations, Future Work and Final Thoughts

The two most significant limitations of this thesis were time and scope. As a master's thesis, there is a finite period of time for a project to be completed, ultimately narrowing its scope. Thus, only one technology (Google Nest Mini) was studied in-depth, with only brief mentions of other configurations of smart home technologies. While it can be argued that this thesis took a slightly instrumentalist view[63] of smart home TFV, it is important to restate that the purpose of this thesis was not to thoroughly examine issues of violence, domestic violence, or feminist theory, but more so to recognize that smart home TFV is another form of violence that merits attention, study and early action so as to pre-empt its negative consequences as it is being developed and rolled out. While I was cognizant of some of these issues as I was conducting the literature review, the discussion remained contained within the parameters of a case study of one common smart home technology as the purpose was to illustrate how TFV in a smart home context can occur, and by exposing multiple vulnerabilities at the micro, meso and macro scales and address the sociotechnical assemblage related to TFV, I think was able to do so and

[63] Instrumentalism refers to a philosophy of technology whereby technologies are neutral or whose only purpose is to fulfill the user's tasks (Quan-Haase, 2016, p.268)

developed a methodology and a hybrid theoretical framework that could be applied to the study of different types of smart homes. With more time and resources, the project could have been further improved by examining multiple smart home technologies (including a fully automated home) and multiple walkthrough scenarios, including scenarios with collaborations from various stakeholders such as a women's shelter, police officers or a property management company. I would also have liked to have been able to conduct interviews with experts in key industries such as frontline organizations, real estate, and technology experts, and with the knowledge gained from the research done here, I think it would be possible in a future study to conduct a set of interviews and also to experience a smart home. Alternatively, future research could focus on in-depth analysis of smart home TFV potential in single industries like healthcare (which was not fully explored in this thesis) and property management technology (proptech). Another avenue of future work could be a deeper examination of smart home data flows and their various sociotechnical implications of these, especially as smart homes and smart cities proliferate.

Reflecting upon the theoretical framework and methodology chosen for this thesis, they were effective at answering the two research questions posed but there is still room for improvement. For example, the development of the multi-scalar analysis could be tailored towards the subject of smart cities and the boundaries between scales could have more effectively encompassed how actors exist at multiple scales. Nonetheless, the framework and methodology did enable a broad overview of the sociotechnical systems of smart homes and smart home TFV in Canada, identified the multiple actors associated and presented them in an actionable way, hoping to inspire future research and action in this understudied area across various disciplines.

Next steps might include collaboration between academia and frontline organizations to develop guides and resources for cyber hygiene and help with smart home TFV in Canada (see Tanczer et al., 2018; Havron et al., 2019), deeper examination of the construction and real estate sector's impact on smart home TFV including building codes and regulations pertaining to smart homes or legal analysis of the various jurisdictional issues with smart home TFV.

Appendices

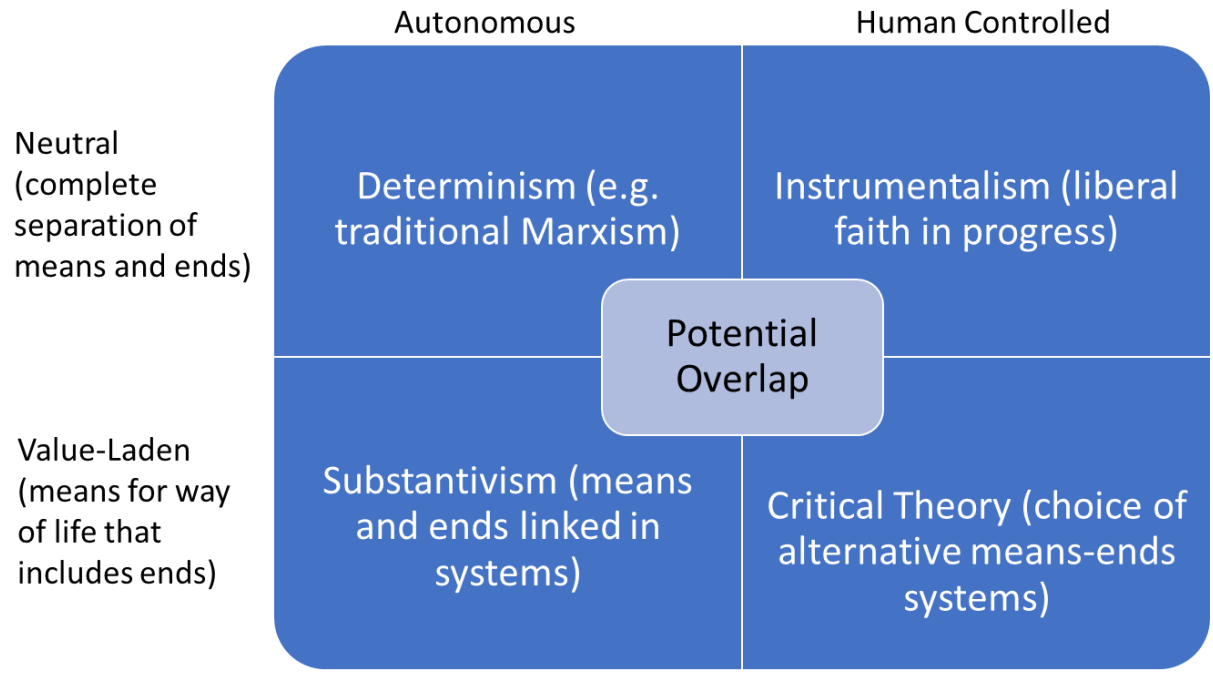
Appendix A : Charlevoix Commitment (G7 Nations, 2018)

1) Promote legal regimes, national anti-violence strategies, educational approaches and existing mechanisms, as appropriate, that keep pace with technological development. **2)** Work to strengthen sex and age-disaggregated data collection and publication, consistent with the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, so as not to further marginalize those at risk. **3)** Strengthen the effectiveness of existing and new violence, abuse and harassment prevention and response strategies at international, national and local levels, ensuring that they are informed by gender-based analysis. **4)** Support awareness-raising initiatives on the gravity of sexual and gender-based abuse, harassment and the threat of violence in digital contexts, as well as on their impacts on civic discourse and the enjoyment of human rights. **5)** Share approaches and support global efforts aimed at addressing gender inequality and at preventing and countering sexual and gender-based based abuse, harassment, violence and threat of violence in physical and digital contexts. **6)** Mobilize the international community, including through working with the private sector, civil society and women's rights organizations, to develop strategies to improve prevention of and response to sexual and gender-based abuse, harassment and the threat of violence in digital contexts and learn lessons from current models of industry-government collaboration on emerging digital challenges **7)** Encourage everyone, particularly men and boys, to speak out strongly against sexual and gender-based violence, abuse, harassment and discrimination. **8)** Work together to improve our responses to breaches in data privacy and the criminal misuse of online platforms and connected technologies. We will ensure the appropriate confidentiality of survivor information and promote efforts to educate law enforcement, judges and other legal actors. **9)** Coordinate efforts and share best practices on preventing the misuse of the internet to facilitate trafficking in persons, recognizing that girls and women make up the majority of victims and survivors of trafficking for sexual exploitation. **10)** Support removing gender biases in the development of digital platforms and connected technologies from design to end-use.

Appendix B : Funded Initiatives under the Strategy to Prevent Gender-Based Violence (derived from Department of Women and Gender Equality, n.d.).

Pillar	Initiative Name	Federal Organization	Funding and budget year
Pillar 1: Preventing gender-based violence	National Youth Awareness Strategy on Gender-Based Violence	Department of Women and Gender Equality Canada (WAGE)	$5.7 million for five (5) years; $1.3 million per year ongoing (Budget 2017)
	Developing a Framework to address gender-based violence in post-secondary institutions		$5.4 million for five(5) years (Budget 2018)
	Awareness of online child sexual exploitation	Public Safety Canada (PS)	$1 million for five (5) years; $0.3 million per year ongoing (Budget 2017)
	Preventing bullying and cyberbullying		$4 million for five (5) years; $1 million per year ongoing (Budget 2018)
	Developing and testing innovative practices in parenting support programs to prevent child maltreatment	Public Health Agency of Canada (PHAC)	$6 million for five (5) years; $1.3 million per year ongoing (Budget 2017)
	Developing and testing innovative practices in youth/teen dating violence prevention		$3.5 million for five (5) years; $0.7 million per year ongoing (Budget 2017); $26.7 million for five (5) years; $6.2 million per year ongoing (Budget 2018)
Pillar 2: Supporting survivors and their families	GBV Program: Identify, pilot and adapt interventions to address gaps in supports for Indigenous and underserved groups of survivors in Canada	Department of Women and Gender Equality Canada (WAGE)	$29.4 million for five(5) years; $6.2 million per year ongoing (Budget 2017); $25.6 million for five (5) years; $6 million per year ongoing (Budget 2018)
	Enhance Family Crisis Teams	Department of National Defence (DND)	$4 million for five (5) years; $0.8 million per year ongoing (Budget 2017)
	Support to Sexual Assault Centres near Canadian Armed Forces Bases & Wings		$2 million for five (5) years (Budget 2018)
	Enhance Settlement Program	Immigration, Refugees and Citizenship Canada (IRCC)	$1.5 million for five (5) years (Budget 2017)
	Training health and allied professions	Public Health Agency of Canada (PHAC)	$4.5 million for five (5) years; $1 million per year ongoing (Budget 2018)
	Support for the Canadian Centre for Child Protection	Public Safety Canada (PS)	$5 million for five (5) years; $1 million per year ongoing (Budget 2017)
Pillar 3: Promoting Responsive Legal and Justice Systems	Cultural Competency Training for RCMP employees	Royal Canadian Mounted Police (RCMP)	$2.4 million for five (5) years; $0.6 million per year ongoing (Budget 2017)
	Enhance capacity to combat online child sexual exploitation and transnational child sex offenders		$19.3 million for five (5) years; $5.8 million per year ongoing (Budget 2018)
	Support for the Sexual Assault Review Team and Victim Support Action Plan (RCMP)		$10 million for five (5) years (Budget 2018)
Gender-Based Violence Knowledge Centre	Lead and coordinate the Strategy	Department of Women and Gender Equality Canada (WAGE)	$12.3 million for five (5) years; $2.5 million per year ongoing (Budget 2017)
	Develop multifaceted approaches to knowledge mobilization		
	Report on the Strategy's progress and results		
	Create and manage the GBV Knowledge Centre's online platform		
	Undertake data collection and research in priority areas		$30.1 million for five (5) years; $6 million per year ongoing (Budget 2017)

Appendix C : Theories of Technology and Society (derived from Feenberg, 1999 as adapted by Quan-Haase, 2015)



Works Cited

Alaa, M., Zaidan, B. B., Zaidan, A. A., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, *97*(Journal Article), 48–65. https://doi.org/10.1016/j.jnca.2017.08.017

Aldrich, F. K. (2006). Smart Homes: Past, Present and Future. In R. Harper (Ed.), *Inside the Smart Home* (p. 19). Springer Science and Business Media.

Ali, S., & Yusuf, Z. (2018). *Mapping the Smart Home Market*. Boston Consulting Group (BCG). https://www.bcg.com/en-ca/publications/2018/mapping-smart-home-market.aspx

Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (n.d.). Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. *ArXiv Preprint*. arXiv:1708.05044

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, *56*(Journal Article), 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004

Auditor General of Canada. (2009). *2009 Spring Report of the Auditor General of Canada*. Auditor General of Canada. https://www.oag-bvg.gc.ca/internet/English/parl_oag_200905_01_e_32514.html#hd5a

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

Bailey, J., & Mathen, C. (2019). Technology-Facilitated Violence against Women & Girls: Assessing the Canadian Criminal Law Response. *Canadian Bar Review*, *97*(33).

Barber, M. (1985). Help for Farm Homes: The Campaign to End Housework Drudgery in Rural Saskatchewan in the 1920s. *Scientia Canadensis*, *9*(3), 3–26.

Beatty Refrigerators. (1956). *Tappan Ranges [Advertisement]*. Maclean's Magazine. https://archive.org/details/Macleans-Magazine-1956-06-09/page/n19/mode/2up

Beatty Refrigerators. (1958). *Beatty Refrigerators [Advertisement]*. Maclean's Magazine. https://archive.org/details/Macleans-Magazine-1958-05-24/page/n31/mode/2up

Bell. (1962). *Bell Extension Cord [Advertisement]*. Maclean's Magazine. https://archive.org/details/Macleans-Magazine-1962-04-07/page/n21/mode/1up

Bell, G., & Dourish, P. (2007). Back to the shed: Gendered visions of technology and domesticity. *Personal and Ubiquitous Computing*, *11*(5), 373–381. https://doi.org/10.1007/s00779-006-0073-8

Bennett, B. (2019, December). Google Play Music/YouTube Premium subscribers eligible for free Google Nest Mini. *Mobile Syrup*. https://mobilesyrup.com/2019/12/14/google-play-music-youtube-premium-subscribers-free-google-home-mini/

Berg, A.-J. (1999). A Gendered socio-technical construction: The smart house. In J. Wajcman & D. Mackenzie (Eds.), *The Social Shaping of Technology* (2nd ed.). Open University Press.

Bijker, W. E., Hughes, T. P., & Pinch, T. (2012). *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Anniversary). The MIT Press.

Birchley, G., Huxtable, R., Murtagh, M., Ter Meulen, R., Flach, P., & Gooberman-Hill, R. (2017). Smart homes, private homes? An empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies. *BMC Medical Ethics*, *18*(1), 23–13. https://doi.org/10.1186/s12910-017-0183-z

Bivens, R., & Hasinoff, A. A. (2017). Rape: Is there an app for that? An empirical analysis of the features of anti-rape apps. *Information, Communication & Society*, *21*(8).

Bivens, R., & Hoque, A. S. (2017). Programming Sex, Gender, and Sexuality: Infrastructural Failures in the "Feminist" Dating App Bumble. *Canadian Journal of Communication*, *43*(3).

Blackwell, A. F. (2006). Gender in Domestic Programming: From Bricolage to Séances d'Essayage. *CHI'2006 Workshop on End User Software Engineering*. CHI 2006.

Bohn, D. (2019, September). Google is reducing how much audio it saves for human review. *The Verge*. https://www.theverge.com/2019/9/23/20878710/google-assistant-audio-recording-policy-hotword-human-review

Bowker, G., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. MIT Press.

Bowles, N. (2018, June 23). Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. *New York Times*. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Buckley, D. (2019). New types of answers from your Google Assistant on Android. *Google Product Blog*. https://www.blog.google/products/assistant/new-types-of-answers-your-google-assistant-on-android/

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.

Callon, M., & Law, J. (1997a). After the Individual in Society: Lessons on Collectivity from Science, Technology and Society. *Canadian Journal of Sociology*, *22*(2), 165. https://doi.org/10.2307/3341747

Callon, M., & Law, J. (1997b). After the Individual in Society: Lessons on Collectivity from Science, Technology and Society. *Canadian Journal of Sociology*, *22*(2), 165. https://doi.org/10.2307/3341747

Canadian Centre for Cyber Security. (n.d.). *Cyber Security Glossary*. https://cyber.gc.ca/en/glossary

Canadian Centre for Cyber Security. (2019a). *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. (2019b, October). *Internet of Things Security for Small and Medium Organizations*. https://cyber.gc.ca/sites/default/files/publications/ITSAP.00.012-en.pdf

Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c11 Citation in text: (Canadian Charter, 1982, s 6(2)(b)). https://laws-lois.justice.gc.ca/eng/const/page-15.html

Canadian Chiefs of Police. (n.d.). *Canadian Framework for Collaborative Police Response on Sexual Violence* (2019). https://www.cacp.ca/crime-prevention-committee.html?asst_id=2059

Canadian Home Builders' Association. (n.d.). *Builders' Manual*. https://www.chba.ca/CHBA/Publications/Builder-Manual.aspx

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

Carter, A., & Rieti, J. (2020, May 7). Sidewalk Labs cancels plan to build high-tech neighbourhood in Toronto amid COVID-19. *CBC News*. https://www.cbc.ca/news/canada/toronto/sidewalk-labs-cancels-project-1.5559370

Cavoukian, A. (2011). *Privacy By Design: The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices*. Information and Privacy Commissioner of Ontario. https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

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

Cisco. (2016). *Internet of Things: At a Glance*. https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf

Citizen Lab. (n.d.). *About—Citizen Lab*. https://citizenlab.ca/about/

City of Cote Saint-Luc. (2019). *Executive Summary: City of Cote Saint-Luc, Quebec*. Infrastructure Canada. https://www.infrastructure.gc.ca/cities-villes/exec-summaries-resumes/exec-cote-saint-luc-eng.html

City of Toronto. (2017). *Domestic/Intimate Partner Violence Resources*. https://www.toronto.ca/wp-content/uploads/2017/12/8c17-R1-Domestic-Intimate-Partner-Violence-Resources-FINAL.pdf

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

Cockburn, C. (1993). The Circuit of Technology: Gender, Identity and Power. In E. Hirsch & R. Silverstone (Eds.), *Consuming Technologies: Media and Information in Domestic Spaces*. Routledge.

Cockburn, C. (1997). Domestic technologies: Cinderella and the engineers. *Women's Studies International Forum*, *20*(3), 361–371. https://doi.org/10.1016/S0277-5395(97)00020-4

Coffield. (1947). *Coffield Appliances [Advertisement]*. Maclean's Magazine. https://archive.org/details/Macleans-Magazine-1947-01-01/page/n19/mode/1uphttps://archive.org/details/Macleans-Magazine-1947-01-01/page/n19/mode/1up

Coletta, C., & Kitchin, R. (2017). Algorhythmic governance: Regulating the 'heartbeat' of a city using the Internet of Things. *Big Data & Society*, *4*(2).

Crowley, J., & Coutaz, J. (2015). *An ecological view of smart home technologies*. 1–16.

Cyphers, B. (2020, March 19). Google Says It Doesn't "Sell" Your Data. Here's How the Company Shares, Monetizes, and Exploits It. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and

Dahlqvist, F., Patel, M., Rajko, A., & Shulman, J. (2019). Growing opportunities in the Internet of Things. *McKinsey & Company*. https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things

Davis, A. (1993). 'Valiant Servants': Women and Technology on the Canadian Prairies 1910-1940. *Manitoba History*, *25*. http://www.mhs.mb.ca/docs/mb_history/25/womenandtechnology.shtml

Day, M. (2019, May). Your Smart Light Can Tell Amazon and Google When You Go to Bed. *Bloomberg*. https://www.bloomberg.com/news/articles/2019-02-12/your-smart-light-can-tell-amazon-and-google-when-you-go-to-bed

DeKeseredy, W. S., & Dragiewicz, M. (2014). Woman Abuse in Canada: Sociological Reflections on the Past, Suggestions for the Future. *Violence Against Women*, *20*(2), 228–244. https://doi.org/10.1177/1077801214521325

Delanda, M. (2006a). *A new philosophy of society: Assemblage theory and social complexity*. Continuum.

Delanda, M. (2006b). Deleuzian Social Ontology and Assemblage Theory. In M. Fuglsang (Ed.), *Deleuze and the Social*. Edinburgh University Press.

Delanda, M. (2011). *Assemblage Theory, Society, and Deleuze*. https://www.youtube.com/watch?v=J-I5e7ixw78

Delanda, M. (2016). *Assemblage Theory*. Edinburgh University Press.

Deleuze, G., & Guattari, F. (1987). *A thousand plateaus: Capitalism and schizophrenia*. University of Minnesota Press.

Deleuze, G., & Parnet, C. (2007). *Dialogues II* (H. Tomlinson & B. Habberjam, Trans.). Columbia University Press.

Department of Women and Gender Equality. (n.d.). *Funded Projects—Strategy to End Gender-Based Violence (GBV)*.

Department of Women and Gender Equality (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-rapport2018-en.html

Dimond, J. P., Fiesler, C., & Bruckman, A. S. (2011). Domestic violence and information communication technologies. *Interacting with Computers*, *23*(5), 413–421. https://doi.org/10.1016/j.intcom.2011.04.006

Doctorow, C. (2019a, 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

Doctorow, C. (2019b, May). “Smart” doorlocks have policies that let landlords and third parties spy on you. *Boing Boing*. https://boingboing.net/2019/05/03/surveillant-tenancies.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

Dragiewicz, M., Harris, B. A., & Douglas, H. (2019). Technology-facilitated Domestic and Family Violence: Women’s Experiences. *British Journal of Criminology*, *59*(3), 551.

Duguay, S. (2017). Dressing up Tinderella: Interrogating authenticity claims on the mobile dating app Tinder. *Information, Communication & Society*, *20*(3), 351–367.

Dworkin, G. (2020). Paternalism. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. https://plato.stanford.edu/archives/fall2020/entries/paternalism

Edwards, P. (2003). Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems. In T. Misa, A. Feenberg, & P. Brey (Eds.), *Technology and Modernity*. MIT Press.

ELAN. (n.d.). *About—Elan*. https://www.elanhomesystems.com/connect/elan-and-nortek-security-control

Estevan-Reina, L., de Lemus, S., & Megías, J. L. (2020). Feminist or Paternalistic: Understanding Men’s Motivations to Confront Sexism. *Frontiers in Psychology*, 10, 2988.

European Commission. (n.d.). *EU Data Protection Rules*.

Fairbairn, J., & Black, D. (2015). *Cyberviolence Against Women and Girls*. Ottawa Coalition to End Violence Against Women. https://www.octevaw-cocvff.ca/sites/default/files/CyberViolenceReport_OCTEVAW.pdf

Feenberg, A. (1999). *Questioning Technology*. Routledge.

Finestone, S. (1995, September 6). *STATEMENT BY THE SECRETARY OF STATE (STATUS OF WOMEN AND MULTICULTURALISM) OF CANADA, THE HONOURABLE SHEILA FINESTONE AT THE FOURTH UNITED NATIONS WORLD CONFERENCE ON WOMEN*. https://www.un.org/esa/gopher-data/conf/fwcw/conf/gov/950906204201.txt

Fingas, J. (2018, July 19). Voice assistants still have problems understanding strong accents. *Engadget*. https://www.engadget.com/2018-07-19-voice-assistant-problems-understanding-accents.html

Finn, J., & Atkinson, T. (2009). Promoting the safe and strategic use of technology for victims of intimate partner violence: Evaluation of the technology safety project. *Violence against Women*, *15*(11), 1402. https://doi.org/10.1177/1077801209346723

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

Geist, M. (2020, August 2). Why I Installed the COVID-19 Alert App. *Michael Geist*. https://www.michaelgeist.ca/2020/08/why-i-installed-the-covid-alert-app/

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

General Electric Appliances. (1953). *General Electric Appliance Gifts [Advertisement]*. Maclean's Magazine. https://archive.org/details/Macleans-Magazine-1953-12-01/page/n25/mode/2up

General Electric Company. (1921). *General Electric Sovereign Electric Iron [Advertisement]*. Maclean's Magazine. https://archive.org/details/Macleans-Magazine-1921-11-01/page/n2/mode/1up

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

Gilchrist, A. (2016). *Industry 4.0: The Industrial Internet of Things* (1st ed.). Apress.

Gladu, M. (2017). *Taking Action to End Violence Against Young Women and Girls in Canada*. Parliament of Canada. https://www.ourcommons.ca/Content/Committee/421/FEWO/Reports/RP8823562/feworp07/feworp07-e.pdf [

Global Affairs Canada. (2018). *Playbook for Gender Equality in the Digital Age*. Government of Canada. https://www.international.gc.ca/world-monde/issues_development-

enjeux_developpement/human_rights-droits_homme/playbook-manuel_instructions.aspx?lang=eng

Google. (n.d.). *Google Products*. https://about.google/intl/en_us/products/?tip=autofill

Google. (2020). *Privacy on Google Assistant*. https://www.youtube.com/watch?v=ZaqZcDOoi-8&feature=emb_logo

Google Assistant. (n.d.). *Google Assistant—Explore*. https://assistant.google.com/explore

Google Developers. (n.d.-a). *Actions on Google Assistant*. https://developers.google.com/assistant/

Google España. (2018, October 4). *Google Home, el Asistente de Google para tu casa*. https://www.youtube.com/watch?v=TT_uhXjkYi4

Google France. (2017, December). *Google Home Mini—Petit et grand à la fois—Google France*. https://www.youtube.com/watch?v=_ubhauvtgtE

Google France. (2019, October). *Découvrez le nouveau Nest Mini. Un son de qualité, un allié de taille. - Google France*. https://www.youtube.com/watch?v=a9e0icMRwBo

Google France. (2020, May). *Apprenez en famille avec Nest Mini—Google France*. https://www.youtube.com/watch?v=LFYGotas8QA

Google Mexico. (2018a, July). *El Antojo*. https://www.youtube.com/watch?v=AcixoJTGejA

Google Mexico. (2018b, July). *La Tarea*. https://www.youtube.com/watch?v=c9g4SK-iYKM

Google Nest. (n.d.). *Our commitment to privacy in the home*. https://store.google.com/magazine/google_nest_privacy

Google Nest. (2019a, October). *Introducing Nest Mini*. https://www.youtube.com/watch?v=XaTh42Srgcg

Google Nest. (2019b, November). *Disney's Frozen 2 Stories on Nest Mini*. https://www.youtube.com/watch?v=xuRWUwUSlZk

Google Nest. (2019c, November). *How to get big help from a little Mini*. https://www.youtube.com/watch?v=16ZTti6nl0I

Google Policies. (2020a). *Privacy Policy*. https://policies.google.com/privacy

Google Policies. (2020b). *Terms of Service*. https://policies.google.com/terms

Google Safety. (n.d.). *Data Transparency*. https://safety.google/privacy/data/

Google Store. (n.d.-a). *Google Nest Mini—Brazil*. https://store.google.com/br/product/google_nest_mini?hl=pt-BR

Google Store. (n.d.-b). *Google Nest Mini—Canada*. https://store.google.com/product/google_nest_mini

Google Support. (n.d.). *Data security and privacy on devices that work with Assistant*. https://support.google.com/googlenest/answer/7072285?hl=en

Google Support. (2020a). *FAQs on privacy: Google Nest*. https://support.google.com/googlenest/answer/9415830?p=privacyfaqs&visit_id=637299124375817422-1927119034&rd=1

Google Support. (2020b, May). *Google Nest Terms of Service*. https://support.google.com/googlenest/answer/9327735?p=nest-tos&visit_id=636960429306365222-1263716351&rd=1

Google Support. (2020c, May). *Sensors in Google Nest devices*. https://support.google.com/googlenest/answer/9330256?p=sensorglossary&visit_id=637299103686635163-395926385&rd=1#topic=7029677

Google Transparency. (2019). *Google Transparency Report*. https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts,compliance;authorit

y:CA;time:&lu=legal_process_breakdown&user_data_produced=authority:CA;series:compliance&dlr_requests=authority:CA;time:&legal_process_breakdown=expanded:

Google UK. (2019a, October). *Google Nest Mini—Cooking*. https://www.youtube.com/watch?v=TE_mZwUhhEc

Google UK. (2019b, October). *Google Nest Mini—Help with the washing up*. https://www.youtube.com/watch?v=gdS5TaGOmRw

Greene, K. (2019, October). SMART tech and smart design critical for OHBA award winner. *Mortgage Broker News*. https://www.mortgagebrokernews.ca/news/smart-tech-and-smart-design-critical-for-ohba-award-winner-306876.aspx

Hall, M. (2018). Beware the Smart Home. *Autonomy Think Tank*. http://autonomy.work/portfolio/beware-the-smart-home/

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

Hargreaves, T., & Wilson, C. (2017). *Smart Homes and their Users*. Springer International Publishing. https://doi.org/10.1007/978-3-319-68018-7

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

Henry, N., & Powell, A. (2014). The Dark Side of the Virtual World: Towards a Digital Sexual Ethics. In *Preventing sexual violence: Interdisciplinary approaches to overcoming a rape culture*. Palgrave Macmillan.

Henry, N., & Powell, A. (2015). Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence. *Violence Against Women*, *21*(6), 758–779. https://doi.org/10.1177/1077801215576581

Hoover. (1958a). *Hoover [Advertisement]*. Maclean's Magazine. https://archive.org/details/Macleans-Magazine-1958-09-27/page/n21/mode/2up

Hoover. (1958b). *Hoover [Advertisement]*. Maclean's Magazine. https://archive.org/details/Macleans-Magazine-1958-12-06/page/n27/mode/2up

Hou, A., Tops, J., & Ou, C. (2019). *2018 Charlevoix G7 Interim Compliance Report 10 June 2018-10 December 2018*. Munk School of Global Affairs and Public Policy, University of Toronto. http://www.g7.utoronto.ca/evaluations/2018compliance-interim/20-2018-G7-interim-compliance-violence.pdf

Hughes, T. P. (1993). *Networks of power: Electrification in Western society, 1880-1930*. JHU Press.

Humphry, J., & Chesher, C. (2020). Preparing for smart voice assistants: Cultural histories and media innovations. *New Media & Society*. https://doi.org/10.1177/1461444820923679

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

Infrastructure Canada. (n.d.). *Smart Cities Challenge*. https://www.infrastructure.gc.ca/cities-villes/index-eng.html

International Standards Organization. (2018). *Internet of Things*. International Standards Organization. https://www.iso.org/obp/ui/#iso:std:iso-iec:20924:ed-1:v1:en

IPV Tech Research. (n.d.-a). *About*. https://www.ipvtechresearch.org/about

IPV Tech Research. (n.d.-b). *Resources*. https://www.ipvtechresearch.org/resources

Jeffries, A., & Yin, L. (2020, July). Google's Top Search Result? Surprise! It's Google. *The Markup*. https://themarkup.org/google-the-giant/2020/07/28/google-search-results-prioritize-google-products-over-competitors

Kaspersky. (2019). *The State of Stalkerware in 2019*. https://media.kasperskydaily.com/wp-content/uploads/sites/92/2019/11/18053214/Kaspersky_Coalition_The-state-of-stalkerware-in-2019_ENG_fin.pdf

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.

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures & their consequences*. Sage Publications Ltd.

Kitchin, R., & Dodge, M. (2019). The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*, *26*(2), 47–65. https://doi.org/DOI:10.1080/10630732.2017.1408002

Kitchin, R., & Lauriault, T. P. (n.d.). *Kitchin, R., & Lauriault, T. (2014). Towards critical data studies: Charting and unpacking data assemblages and their work.*

Kitchin, R., Lauriault, T. P., & McArdle, G. (2015). Knowing and governing cities through urban indicators, city benchmarking and real-time dashboards. *Regional Studies, Regional Science*, *2*(1), 6–28.

Koshan, J. (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/

Latour, B. (1987). SCIENCE IN ACTION: HOW TO FOLLOW SCIENTISTS AND ENGINEERS THROUGH SOCIETY. In *Cambridge, MA: Harvard U Press, 1987* (Vol. 1–Book, Section).

Latour, B. (1988). *The pasteurization of France*. Harvard University Press.

Latour, B. (1996). On Actor-Network Theory: A Few Clarifications. *Soziale Welt*, *47*(4), 369–381.

Latour, B. (1999). *Pandora's hope: Essays on the reality of science studies*. Harvard University Press.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.

Lauriault, T. P. (2012). *Data, Infrastructures and Geographical Imaginations: Mapping Data Access Discourses in Canada* [Ph.D Thesis]. Carleton University.

Law, J. (1991). *A sociology of monsters: Essays on power, technology, and domination* (Vol. 38). Routledge.

Light, B. (2016). The rise of speculative devices: Hooking up with the bots of Ashley Madison. *First Monday*. https://doi.org/10.5210/fm.v21i6.6426

Light, B., Burgess, J., & Duguay, S. (2018). The walkthrough method: An approach to the study of apps. *New Media & Society*, *20*(3), 881–900. https://doi.org/10.1177/1461444816675438

Livingstone, S. (1993). The meaning of domestic technologies: A personal construct analysis of familial gender relations. In E. Hirsch & R. Silverstone (Eds.), *Consuming Technologies: Media and Information in Domestic Spaces*. Routledge.

Maalsen, S. (2019). Revising the smart home as assemblage. *Housing Studies*. https://doi.org/10.1080/02673037.2019.1655531

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

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

Made by Google. (2018, October). *Read along with Google Home Mini and Disney's Little Golden Books*. https://www.youtube.com/watch?v=NH7HI2BW6aE

Made by Google. (2019, October). *A Phone Made the Google Way | Introducing Google Pixel 4*. https://www.youtube.com/watch?v=0gizLT97cKo

Marshall, A. (2020). Alphabet's Sidewalk Labs scraps its ambitious Toronto project. *WIRED*. https://www.wired.com/story/alphabets-sidewalk-labs-scraps-ambitious-toronto-project/

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

Mediasmarts. (n.d.). Surveillance: Why worry, if you have nothing to hide? *MediaSmarts*. https://mediasmarts.ca/privacy/surveillance-why-worry-if-youve-got-nothing-hide

Misa, T. (1994). Retrieving Sociotechnical Change from Technological Determinism. In M. R. Smith & L. Marx (Eds.), *Does Technology Drive History*. MIT Press.

Mozilla Foundation. (2020). *Google Home—Privacy Not Included*. https://foundation.mozilla.org/en/privacynotincluded/products/google-home/

Murakami Wood, D., & Mackinnon, D. (2018). Partial Platforms and Oligoptic Surveillance in the Smart City. *Surveillance & Society*, *17*(1/2). https://doi.org/10.24908/ss.v17i1/2.13116

Nail, T. (2017). What is an Assemblage? *SubStance*, *46*(1), 21–37.

National Network to End Domestic Violence. (2018). *Home Automation: Survivor Privacy Risks and Strategies* (Tech Safety Project). https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/5b3e46501ae6cf89cc3b4398/1530807889950/NNEDV_IoT+Home+Automation+Safety_2018.pdf

Ng, G. (2019). Spotify Offer: Free Google Home Mini Speaker in Canada with Premium Plan. *IPhone in Canada*. https://www.iphoneincanada.ca/news/spotify-google-home/

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

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

Norris, A. (2020, February). How Real Estate Will Drive Smart Home Adoption. *Forbes*. https://www.forbes.com/sites/aaronnorris/2020/02/27/how-real-estate-will-drive-smart-home-adoption/#2c4068434d4e

Office of the Privacy Commissioner of Canada. (2016a, May). *10 privacy tips for the rental housing sector*. https://www.priv.gc.ca/en/privacy-topics/landlords-and-tenants/02_05_d_66_tips/

Office of the Privacy Commissioner of Canada. (2016b). *2016 Survey of Canadians on Privacy*. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/

Olejnik. (n.d.). *Selling Off Privacy At Auction in less then 100 ms, for less than $0.0005*. http://lukaszolejnik.com/rtbdesc

Ontario Home Builders' Association. (2017). *An Apprenticeship Skills Agenda– Executive Summary*. https://www.ohba.ca/apprenticeship-skills-agenda-executive-summary/

Oster. (1953). *Oster Kitchen [Advertisement]*. Maclean's Magazine. https://archive.org/details/Macleans-Magazine-1953-11-15/page/n43/mode/2up

Ottawa Police. (2014). *Violence Against Women Consultations*. https://www.ottawapolice.ca/en/about-us/resources/ops_vaw_consultation_27nov2014_final_f.pdf

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.

Phillips, J. (2006). Agencement/Assemblage. *Theory, Culture & Society*, *23*(2–3), 108–109. https://doi.org/10.1177/026327640602300219

Porter, J. (2020, August). Google Invests in ADT, will integrate its Nest devices into smart home business. *The Verge*. https://www.theverge.com/2020/8/3/21352360/google-adt-investment-nest-smart-home-security-alarms-machine-learning-alerts

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

Powell, A., & Henry, N. (2018). Policing technology-facilitated sexual violence against adult victims: Police and service sector perspectives. *Policing and Society*, *28*(3), 291–307.

Privacy International. (2019, June). *With my fridge as my witness?!* https://privacyinternational.org/long-read/3026/my-fridge-my-witness

Public Health Agency of Canada. (2019). *Canada: A Pathfinding Country: Canada's Road Map to End Violence Against Children*.

Public Safety Canada. (n.d.). *Departmental Plan 2020-21*. Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2020-21/dprtmntl-pln-2020-21-en.pdf

Public Safety Canada. (2018a). *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

Public Safety Canada. (2018b, September 26). *Government of Canada Announces New National Cyber Security Strategy and the Creation of the Canadian Centre for Cyber Security*. https://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2018/in18-003-en.aspx

Quan-Haase, A. (2016). *Technology & Society: Social Networks, Power, and Inequality* (2nd ed.). Oxford University Press.

Rabson, M. (2020, June). Privacy concerns raised as made-in-Canada contact tracing app ready for testing in Ontario. City News Toronto. https://toronto.citynews.ca/2020/06/18/privacy-concerns-raised-as-made-in-canada-contact-tracing-app-ready-for-testing-in-ontario/

Ribes, D., & Jackson, S. J. (2013). Data bite man: The work of sustaining long-term study. In L. Gitelman (Ed.), *"Raw Data" is an Oxymoron.* MIT Press.

Rip, A., Callon, M., 1945, & Law, J., 1940. (1986). *Mapping the dynamics of science and technology: Sociology of science in the real world*. Macmillan.

Ritzer, G. (2007). *The Blackwell encyclopedia of sociology*. Blackwell Pub.

Rode, J. A., Toye, E. F., & Blackwell, A. F. (2004). The fuzzy felt ethnography—Understanding the programming patterns of domestic appliances. *Personal and Ubiquitous Computing*, *8*(3–4), 161–176.

Saxton, M., Olszowy, L., MacGregor, J., MacQuarrie, B., & Wathen, C. (2018). Experiences of Intimate Partner Violence Victims With Police and the Justice System in Canada. *Journal of Interpersonal Violence*, https://doi.org/10.1177/0886260518758330.

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

Sidewalk Toronto. (2019). *Toronto Tomorrow: A New Approach for Modern Growth*. https://storage.googleapis.com/sidewalk-toronto-ca/wp-content/uploads/2019/06/23135619/MIDP_Volume1.pdf

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/

Spillett, R. (n.d.). Jealous husband "who spied on his wife through smart house" is jailed. *Daily Mail*. https://www.dailymail.co.uk/news/article-5958005/Jealous-husband-spied-wife-smart-house-jailed.html

Status of Women Canada. (n.d.-a). *Additional support services for those affected by gender-based violence*. https://cfc-swc.gc.ca/violence/knowledge-connaissance/add-supp-en.html

Status of Women Canada. (n.d.-b). *Funded Projects*. https://cfc-swc.gc.ca/violence/knowledge-connaissance/previous-precedent-en.html

Status of Women Canada. (n.d.-c). *Provincial and Territorial Resources*. https://cfc-swc.gc.ca/violence/knowledge-connaissance/canada-en.html

Status of Women Canada. (n.d.-d). *The Gender-Based Violence Strategy—GBV Knowledge Centre*. https://cfc-swc.gc.ca/violence/knowledge-connaissance/strategy-strategie-en.html

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. (2018a). *A Year in Review (2017-2018): Canada's Strategy to Prevent and Address Gender-Based Violence* (No. 1). Government of Canada. https://cfc-swc.gc.ca/violence/strategy-strategie/report-rapport2018-en.html

Status of Women Canada. (2018b). *Status of Women Canada—Homepage*. https://cfc-swc.gc.ca/index-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, November 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/

Sunbeam Appliances. (1938). *Sunbeam Appliances [Advertisement]*. Maclean's Magazine. https://archive.org/details/Macleans-Magazine-1938-12-01/page/n22/mode/1up

Sweeney, L. (2013). Discrimination in Online Ad Delivery. *Communications of the ACM*, *56*(5), 44–54.

Tanczer, L. (2018). *Tech Abuse Policy Brief*. Department of Science, Technology, Engineering and Public Policy. https://www.ucl.ac.uk/steapp/sites/steapp/files/giot_policy_.pdf

Tanczer, L. (2020). *Gender and Internet of Things: Futureproofing Online Harms legislation* (p. 1). Department of Science, Technology, Engineering and Public Policy.

https://www.ucl.ac.uk/steapp/sites/steapp/files/ucl_g-iot_online_harms_tech_abuse_one_pager_-_feb2020.pdf

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.

Tanczer, L., Lopez-Neira, I., Patel, T., Parkin, S., & Danezis, G. (2019). *Gender and IoT (G-IoT) Resource List* (pp. 1–7). Department of Science, Technology, Engineering and Public Policy. https://www.ucl.ac.uk/steapp/sites/steapp/files/g-iot-resource-list.pdf

Tanczer, L., Patel, T., Parkin, S., & Danezis, G. (n.d.). *Written evidence submitted by the 'Gender and Internet of Things' Research Team University College London (UCL)*. https://www.ucl.ac.uk/steapp/sites/steapp/files/g-iot_home_affairs_committee_submission_final.pdf

Tasca, N. (2019). Doing more to protect your privacy with the Assistant. *Google Product Blog*. https://www.blog.google/products/assistant/doing-more-protect-your-privacy-assistant/

The Economist. (2018). A member to big tech: The techlash against Amazon, Facebook and Google—And what they can do. *The Economist*. https://www.economist.com/briefing/2018/01/20/the-techlash-against-amazon-facebook-and-google-and-what-they-can-do

Townsend, T. (2017). Google Assistant will make money from e-commerce. *Recode*. https://www.vox.com/2017/5/23/15681596/google-assistant-ecommerce-revenue

Tridel. (n.d.). *Tridel Ten York Toronto Condo*. https://www.tridel.com/tenyork/

Tusikov, N. (n.d.). Regulation through "bricking": Private ordering in the "Internet of Things". *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1405

United Nations. (1995). *Beijing Declaration*.

Vaidhyanathan, S. (2011). *The Googlization of Everything: (And Why We Should Worry)*. University of California Press.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Vanek, J. (1974). Time Spent in Housework. *Scientific American*, *231*(5).

Walker, N. A. (2000). The Ladies' Home Journal, "How America Lives" and the Limits of Cultural Diversity. *Media History*, *6*(2), 129–138.

Westinghouse. (1951). *Westinghouse Laundromat [Advertisement]*. Maclean's Magazine. https://archive.org/details/Macleans-Magazine-1951-12-15/page/n25/mode/2up

Westinghouse All Electric House (Color). (n.d.). [Video]. https://www.youtube.com/watch?v=jyrTgtPTz3M

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus*, *109*(1), 121–136.

Wong, R. (n.d.). *Technology Safety and Privacy Toolkit for Canadian Women Experiencing Technology Facilitated Violence* (Technology Safety Project). BC Society of Transition Houses. https://bcsth.ca/wp-content/uploads/2019/03/BCSTH-A-guide-for-Canadian-women-experiencing-technology-facilitated-violence-2019-1.pdf

Woodlock, D. (2017). The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women*, *23*(5), 584–602. https://doi.org/10.1177/1077801216646277

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