



**Your Retailer Needs You:
Retailance and its Marketing Implications**

by

Nada Elnahla

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

Doctor in Philosophy

in

Management

Carleton University

Ottawa, Ontario

© 2021

Nada Elnahla

ABSTRACT

Retailance is surveillance in a brick-and-mortar retail setting. In today's competitive landscape, retailers have moved beyond using surveillance practices and technologies for security reasons to using them to compete for consumers' personal and shopping data, even if this information is not voluntarily reported. Retailance raises ethical questions regarding the differences between the public and the private spheres. Using a pragmatic mixed research methods design that includes an MTurk survey and semi-structured interviews, this exploratory research examines the different retailance channels and systems, and explores retail consumers' awareness of the presence and scope of retailance and of the relevant laws and regulations, consumers' behavioural reaction towards retailance, and the attitudinal and behavioural outcomes of using various surveillance technologies in retailing. Demonstrating the multiplicity and complexity of influences, this research brings together past research by leading scholars from the fields of marketing, consumer behaviour, political science, communications, media studies, science studies, war studies, law, cultural studies, sociology, criminology, and literature.

This research has various contributions. Conceptually, it integrates published literature, synthesizes prior studies, provides definitional clarity and creates a conceptual retailance model that works as a roadmap and opens new avenues for future research. Theoretically, it embraces a multidisciplinary perspective by borrowing theories from other disciplines and integrating them to reveal novel insights when looking at retailance, offers a new theoretical model, and reconciles contradictory reactions to surveillance. In addition, foreseen contributions encompass helping scholars, retail managers, consumers, and policy makers gain a better understanding of the impact of both traditional surveillance and smart retail technologies on consumer behaviour in a brick-and-mortar setting.

Keywords: Retailance; Retail; Surveillance; Surveillance studies; Panopticon; Marketing; Consumer behaviour; Critical marketing; Mixed methods; Pragmatism; COVID-19

ACKNOWLEDGEMENTS

This thesis owes its completion to many people. I record first my deepest thanks to my family: to my husband who has, for the second time, witnessed and fully supported my PhD journey, to my daughter who has become a little marketing expert, and to my family members in Ottawa who have been with me every step of the way. I would also like to express my heartfelt gratitude to my supervisor and mentor, Prof. Leighann Neilson, for her investing her knowledge, expertise and time not only on this research project, but also on many others, and for her willingness to accompany me down every “rabbit hole” I decide to explore. I also appreciate my proposal and dissertation committee members’ continued encouragement and careful readings of this thesis: Prof. Ruth McKay, Prof. Lindsay McShane, Prof. Shaobo Ji, Prof. Sheryl Hamilton, and Prof. Paloma Raggo from Carleton University, and Prof. Leigh Sparks from the Institute for Retail Studies at the University of Stirling. My colleagues at Sprott School of Business have been a tremendous source of support, encouragement and stimulation, and I wish them the best in their own projects and endeavours.

The writing of this thesis saw tremendous changes in my life, from starting a new life in a new country, to changing my field of study, to witnessing a pandemic that is changing the world as we know it. I am, therefore, deeply indebted to my family and several others in my life who listened to me when I was under pressure, giving me their love, support and friendship.

TABLE OF CONTENTS

LIST OF TABLES	9
LIST OF FIGURES	11
CHAPTER 1: INTRODUCTION.....	15
SURVEILLANCE IN TODAY’S WORLD	18
RETAILLANCE.....	23
<i>Your retailer needs you</i>	<i>29</i>
RESEARCH QUESTIONS	30
CHAPTER ORGANIZATION	32
CHAPTER SUMMARY AND CONCLUSION.....	34
CHAPTER 2: LITERATURE REVIEW	36
CONDUCTING THE LITERATURE REVIEW.....	37
AN OVERVIEW OF CONSUMER SURVEILLANCE & DATABASE MARKETING.....	40
THE SURVEILLER: RETAILERS’ GOALS.....	45
(1) <i>To control loss and enhance security.....</i>	<i>46</i>
(2) <i>To create a pleasant and personalized shopping experience.....</i>	<i>47</i>
(3) <i>To enhance profitability.....</i>	<i>49</i>
(4) <i>To ensure safety during the COVID-19 pandemic</i>	<i>50</i>
RETAILLANCE CHANNELS & SYSTEMS.....	51
(1) <i>Direct vs. technologically mediated.....</i>	<i>52</i>
(2) <i>Overt vs. covert.....</i>	<i>53</i>
(3) <i>Real-time vs. over time vs. retrospective surveillance.....</i>	<i>53</i>
(4) <i>Formal vs. informal surveillance</i>	<i>54</i>
<i>Retailance systems</i>	<i>59</i>
(1) In-store surveillance systems	61
(2) Tagging in a retail setting.....	76
(3) Phone number and email	78
(4) Loyalty programs.....	79
(5) Free Wi-Fi and tracking technology	88
(6) Personalized advertising.....	89
(7) Radio frequency identification (RFID).....	94
(8) Tracking returns.....	100
(9) Geo-fencing.....	102
THE SURVEILLED: CONSUMER AWARENESS.....	107
(1) <i>Individual awareness</i>	<i>107</i>
(2) <i>Societal awareness</i>	<i>108</i>
(3) <i>Awareness of government policies and laws.....</i>	<i>110</i>
IMPACT AND OUTCOME: CONSUMERS’ PERCEPTIONS OF SURVEILLANCE	113

THE ETHICAL DILEMMAS OF RETAILLANCE	117
<i>Individual compliance vs. resistance</i>	122
CHAPTER SUMMARY AND CONCLUSION	127
CHAPTER 3: CRITICAL MARKETING & THEORETICAL FOUNDATIONS OF SURVEILLANCE STUDIES.....	134
CRITICAL MARKETING	136
<i>Critical marketing approach to this research</i>	143
(1) Involving different stakeholders.....	143
(2) Power and (in)visibility	144
(3) Understanding vs. mistrust	146
SURVEILLANCE STUDIES.....	147
<i>A brief historical background</i>	150
(1) <i>Panopticism: Bentham, Foucault and Gandy</i>	152
(2) <i>Synopticism: Mathiesen and Andrejevic</i>	160
(3) <i>Post-panopticism: Boyne and Lyon</i>	164
(4) <i>Assemblage: Deleuze and Guattari, and Haggerty and Ericson</i>	166
(5) <i>Virtual identities: Haggerty and Ericson, Poster, Deleuze, Bogard, and Lyon</i>	168
<i>So, is the panopticon dead or alive?</i>	173
<i>Summary</i>	179
SURVEILLANCE, MARKETING HISTORY AND MARKETING RESEARCH	181
CHAPTER SUMMARY AND CONCLUSION.....	185
CHAPTER 4: METHODOLOGY	190
AN INTERPRETIVE APPROACH.....	191
A PRAGMATIC APPROACH TO A MIXED METHODS RESEARCH DESIGN.....	193
THE IMPACT OF THE COVID-19 PANDEMIC ON DATA COLLECTION.....	194
DATA COLLECTION AND ANALYSIS	197
<i>Surveys</i>	197
MTurk survey.....	199
Analysis of survey data.....	202
<i>Semi-structured interviews</i>	202
Post-interview: Transcription, coding and data analysis.....	206
<i>A final, holistic interpretation</i>	211
RESEARCH ETHICAL ISSUES	213
CHAPTER SUMMARY AND CONCLUSION.....	213
CHAPTER 5: DATA ANALYSIS, FINDINGS & DISCUSSION.....	215
DATA ANALYSIS	215
<i>Online surveys</i>	215
<i>Interviews</i>	218

FINDINGS.....	221
<i>First: Consumer awareness and the impact of retailance systems</i>	222
(1) General awareness of the presence and scope of retailance.....	222
(2) Awareness of laws and regulations.....	234
(3) Awareness and reviewing of privacy policies	239
(4) Tracking consumers' purchases	244
(5) Selling consumers' information to third parties	257
(6) Loyalty programs.....	267
(7) Tagging	284
<i>Second: Consumers' behavioural outcomes</i>	295
(1) Acceptance.....	297
(2) Negotiation.....	298
(3) Resistance.....	300
<i>Third: More factors affecting the consumer's behavioural reaction to retailance</i>	322
(1) Political affiliations during crises	322
(2) Consumers' past experiences.....	323
<i>Fourth: Consumers' attitudinal outcomes</i>	325
(1) Consumers for the use of retailance.....	328
(2) Consumers against the use of retailance.....	333
<i>Fifth: Factors affecting the retailer's choice and scope of retailance channels and systems</i>	334
(1) Profiling	335
(2) Retail location.....	340
(3) Size and type of retail	341
(4) Population size.....	342
<i>Sixth: Privacy</i>	343
AN UPDATED RETAILANCE MODEL	351
CHAPTER SUMMARY AND CONCLUSION.....	355
CHAPTER 6: THE IMPACT OF THE COVID-19 PANDEMIC ON RETAILANCE ..	359
THE WORLD OF RETAIL AFTER THE COVID-19 PANDEMIC HIT.....	359
RETAILANCE DURING THE COVID-19 PANDEMIC	363
FINDINGS AND DISCUSSION.....	366
CHAPTER SUMMARY AND CONCLUSION.....	380
CHAPTER 7: CONCLUSION	382
CONTRIBUTIONS.....	386
(1) <i>Conceptual contributions</i>	387
(2) <i>Theoretical contributions</i>	390
(3) <i>Marketing practice contributions</i>	395
(4) <i>Public policy contributions</i>	404

CONCERNS, LIMITATIONS, AND AVENUES FOR FUTURE RESEARCH	408
CONCLUDING REMARKS	411
REFERENCES.....	413
APPENDICES.....	442
APPENDIX 1: SURVEY QUESTIONS	442
APPENDIX 2: SEMI-STRUCTURED INTERVIEW QUESTIONS	456
APPENDIX 3: CONSUMER PRIVACY RIGHTS	464
APPENDIX 4: SUPPORT RESOURCES	469
APPENDIX 5: EXAMPLES OF FACEBOOK ONLINE INVITATIONS	470
APPENDIX 6: SHORT BIOGRAPHIES OF INTERVIEWEES	472

LIST OF TABLES

Table 1 – A matrix of retailance channels and systems.....	60
Table 2 - A chronological summary of the 25 past research studies	133
Table 3 - A representative, though hardly exhaustive, chronological list of surveillance studies	188
Table 4 – Interpretive approach to this retailance research	192
Table 5 - Informants’ demographic profiles	221
Table 6 – Informants’ awareness of retailance systems	223
Table 7 – Chi-square test results of the awareness of retailance systems with the statistically significant associations in red	224
Table 8 – Association between age and the awareness of retailance systems, with the highest percentage under each retailance system in red and the lowest in bold black.....	225
Table 9 – Association between gender and the awareness of retailance systems, with the highest percentage under each retailance system in red.....	226
Table 10 – Association between education level and the awareness of retailance systems, with the highest percentage under each retailance system in red	227
Table 11 – Association between U.S. income and the awareness of retailance systems, with the highest percentage under each retailance system in red, and lowest in bold black	228
Table 12 – The correlation between age and accepting the use of personal information as trade-off, with the highest percentage under each category in red.....	248
Table 13 – The correlation between membership in a minority group and how comfortable informants are with retailers giving their personal information to third parties	260
Table 14 – The correlation between age and the number of loyalty programs informants subscribe to, with the highest percentage under each category in red	271
Table 15 – The correlation between gender and the number of loyalty programs informants subscribe to, with the highest percentage under each category in red	272
Table 16 – The correlation between education level and the number of loyalty programs informants subscribe to, with the highest percentage under each category in red.....	273
Table 17 – The correlation between U.S. income and the number of loyalty programs informants subscribe to, with the highest percentage under each category in red	274
Table 18 – The correlation between age and how comfortable informants are with providing their personal information for reward programs, with the highest percentage under each category in red	276
Table 19 – Chi-square test results of informants’ refusal of retailance with the statistically significant associations in red	304
Table 20 – The correlation between education and refusal of retailance, with the highest percentage under each category in red.....	305
Table 21 – Chi-square tests of the informants’ discovery/detection of retailance, with the statistically significant associations in red	312
Table 22 – The positive correlation between age and discovery of retailance	312

Table 23 – The correlation between age and masking, with the highest percentage in red and the lowest in bold black	313
Table 24 – Chi-square tests of informants’ avoidance of retailance, with the statistically significant associations in red	319
Table 25 – The association between age and avoidance.....	319
Table 26 – A summary of the contributions of this research.....	387

LIST OF FIGURES

Figure 1 – Detailed retailance process model.....	27
Figure 2 – Sources for the surveillance literature review	39
Figure 3 - Publication venues of past academic research	40
Figure 4 - Retailance model.....	45
Figure 5 – How retailers make store surveillance both secure and appealing to shoppers (Bonfanti, 2014).....	49
Figure 6 – Retailance channels	52
Figure 7 - Formal and informal surveillance: Definitions and practical implications at the store level (Kajalo & Lindblom, 2011).....	57
Figure 8 - Comic, credit: Joe Sutliff (Fairchild, 2006)	59
Figure 9 - CCTV cameras (Source: https://advancedoverwatch.com/tips-advice/retail/cctv-systems-retailers-loss-prevention-beyond/)	63
Figure 10 - CCTV counting people (pathmap) (Source: https://advancedoverwatch.com/tips-advice/retail/cctv-systems-retailers-loss-prevention-beyond/)	63
Figure 11 - IKEA, Ottawa, self-serve check-outs (Image: Nada Elnahla, 2019)	65
Figure 12 - Security cameras used overtly in Walmart Supercentres, in Ottawa Train Yards (on the left) and Stittsville, ON (on the right) (Images: Nada Elnahla, 2019)	65
Figure 13 – Asda bodycams (Source: Mirror, https://www.mirror.co.uk/news/uk-news/supermarket-workers-given-body-cameras-12918172).....	66
Figure 14 – How Shopperception works (Source: https://www.shopperception.com/)	67
Figure 15 – A screenshot from Kee Square’s promotional video “The Smart Mannequin is Born” (https://www.youtube.com/watch?time_continue=31&v=9fr9X4f9kXA).....	68
Figure 16 – The US\$ 5,130 surveillance mannequin (Source: Daily Mail, https://www.dailymail.co.uk/sciencetech/article-2235848/The-creepy-mannequin-stares-Fashion-retailers-adapt-airport-security-technology-profile-customers.html)	69
Figure 17 – Presto Vision software (Source: Presto, https://presto.com/2019/10/16/presto-launches-computer-vision-product-for-real-time-restaurant-operations-insights-2/)	70
Figure 18- Thermal imaging camera (Source: Ouellette, 2020).....	71
Figure 19 – The face recognition fact sheet for reducing external shrink (Source: FaceFirst)	73
Figure 20 – Facial recognition used in the A.I. Bar (Credit: CBC News, https://www.cbc.ca/news/science/facial-recognition-london-pub-lineup-1.5317769)	74
Figure 21 – An Alibaba employee demonstrates ‘Smile to Pay’, an automatic payment system that authorize payment via facial recognition (Credit: Alex Wong Staff Getty Images).....	75
Figure 22 – Habitat for Humanity ReStore in Stittsville, Canada (Images: Nada Elnahla, November 3 rd , 2020).....	79
Figure 23 - Advertisement for trading stamps that applauds the wife for her thriftiness and shopping skill (Source: http://www.studioz7.com/stamps.html).....	82
Figure 24 - Canadian Tire money replaced by their Triangle Rewards.....	83
Figure 25 - Loblaw’s loyalty program (https://www.loblaws.ca/loyalty)	85

Figure 26 – Giant Tiger VIP loyalty program (GT VIP) (https://www.newswire.ca/news-releases/tg-vip-giant-tiger-continues-loyalty-program-expansion-833502480.html).....	86
Figure 27 – A screenshot from the 2002 Minority Report film in which John Anderton (played by Tom Cruise) is standing in front of a personalized ad display.	90
Figure 28 - A smart shelf area at Walgreens in Chicago that displays ads along with the cooler’s contents (Source: Teresa Crawford, The Associated Press)	92
Figure 29 – The impact of personalization in retail according to the customer survey study conducted by BCG-Google.....	93
Figure 30 - Mango augmented mirror x Vodafone digital fitting rooms (Source: http://theretailplanner.com/tag/ar/)	94
Figure 31 - The connected #AlwaysOn Midnighter handbag from Rebecca Minkoff (Source: Rebecca Minkoff)	97
Figure 32 – Oversized tags to stem returns (Image: Stores Magazine)	102
Figure 33 - Amazon Go store (Source: Kyle Johnson, The New York Times, https://www.nytimes.com/2018/01/21/technology/inside-amazon-go-a-store-of-the-future.html)	104
Figure 34 - Amazon Go app in the App Store	105
Figure 35 - Retailance systems discussed in this chapter	106
Figure 36 – Loblaw’s \$25 gift card (Source: Richard Buchan/The Canadian Press).....	112
Figure 37 – A post from a Reddit user first brought attention to the facial recognition software running on the information kiosks. (Source: CTV News, https://www.ctvnews.ca/sci-tech/facial-recognition-software-discovered-in-calgary-mall-kiosks-1.4030143)	119
Figure 38 - Steve Mann’s “wearable computer” and “reality mediator” inventions of the 1970s have evolved into what looks like ordinary eyeglasses. (Source: http://www.eecg.toronto.edu/~mann/)	125
Figure 39 - The eight veillances as discussed by Steve Mann (2012).....	126
Figure 40 - The evolution of ideas leading to George Simmel’s “The Metropolis and Mental Life” (1903)	134
Figure 41 – Critical marketing approach to this research.....	143
Figure 42 – Major trends in surveillance studies	148
Figure 43 –Surveillance studies in the context of retailance	149
Figure 44 - Elevation, section and plan of Jeremy Bentham’s Panopticon penitentiary, drawn by Willey Reveley, 1971. Source: J. Bentham, Panopticon Works, Vol. IV, no. 17.	154
Figure 45 - Bentham’s Panopticon; or, The Inspection-Houses book cover (scanned by Google)	155
Figure 46 – Is the panopticon dead?	174
Figure 47 - The standardized ABCD system used in the 1930s (Cited in Arvidsson, 2003)	182
Figure 48 – Three major phases of surveillance studies.....	186
Figure 49 – The mixed methods design employed in this research.....	197
Figure 50 – Survey attention checks.....	198

Figure 51 - A transcribed section of an interview before being prepared for initial analysis.....	209
Figure 52 – The above section after initial coding	210
Figure 53 – The preliminary retailance model introduced in Chapter 1	222
Figure 54 – Chucky in Child’s Play (1988) compared to the EyeSee mannequin which has a camera hidden behind its eye to track shoppers’ behaviour as they browse	232
Figure 55– informants’ awareness of federal institutions that deal with the protection of personal information.....	235
Figure 56 – Informants’ awareness of federal institutions that help deal with privacy and the protection of personal information.....	236
Figure 57 – The association between informants (residing in the U.S.)’ knowledge of the laws that protect their personal information and their average annual income.....	236
Figure 58 – Informants’ belief in the effectiveness of laws protecting their private information held by retail stores	237
Figure 59 – Informants’ reviewing of store privacy policy	240
Figure 60 – Consumers’ reaction towards the tracking of their purchases.....	244
Figure 61 – Informants’ acceptance of retailers’ collecting consumers’ information to inform them of products and/or services that might be of interest.	248
Figure 62 – The association between accepting the use of personal information as trade-off and belonging to a minority group.....	249
Figure 63 – Informants’ acceptance of selling their information to third parties like credit agencies.....	259
Figure 64 –Informants’ acceptance of selling their information to third parties like marketing firms	259
Figure 65 - Consumers’ reactions towards their information being sold to third parties	260
Figure 66 – Number of informants subscribing to loyalty programs.....	268
Figure 67 – Impact of age on the subscription to loyalty programs	270
Figure 68 – Impact of gender on the subscription to loyalty programs	271
Figure 69 – Impact of educational level on the subscription to loyalty programs.....	272
Figure 70 – Impact of U.S. household income on the subscription to loyalty programs.....	273
Figure 71 – Informants’ feelings of comfort when sharing personal information via loyalty programs	275
Figure 72 – Consumers’ reactions towards loyalty programs	277
Figure 73 – Consumers’ reaction towards triggering a false tagging alarm	286
Figure 74 – Consumers’ behavioural reaction towards retailance.....	296
Figure 75 – Survey informants’ resistance to retailance.....	303
Figure 76 – The correlation between consumers’ level of education and their refusal to give their postal/zip code	305
Figure 77 – Informants’ avoidance of retail stores employing retailance	318
Figure 78 – Informants’ overall emotion when encountering retailance.....	326

Figure 79 – Word cloud showing top twenty-five words used by survey informants describing what they think of and how they feel about retailance	326
Figure 80 – The attitudinal outcomes of retailance	327
Figure 81 – Informants’ for/against the use of retailance in general	328
Figure 82 – Informants’ concern about the impact of new technologies used in retail on their privacy.....	344
Figure 83 – Informants’ concern about how their privacy is respected in retail stores	345
Figure 84 – How informants perceive retailers’ protection of consumers’ information	346
Figure 85 – How informants perceive retailers’ protection of consumers’ information	347
Figure 86 – Word cloud showing top twenty words used by interviewees when defining privacy	348
Figure 87 – The retailance model introduced in Chapter 1	352
Figure 88 – The updated retailance model.....	352
Figure 89 – Word cloud showing what retailance means to consumers.....	356
Figure 90 – Surveillance studies (in black) with examples (in red)	357
Figure 91 – Informants working as retail workers surveilling consumers during the pandemic	366
Figure 92 – Informants’ acceptance of more surveillance by retail employees during the pandemic	368
Figure 93 – The association between consumers’ acceptance of increased retailance because of the COVID-19 pandemic and membership in a minority group.....	368
Figure 94 – Word cloud of the 25 frequently used words by informants describing why retailers are using more retailance post the COVID-19 pandemic	369
Figure 95 – The reaction of retail workers, managers and consumers towards the increase of retailance due to the COVID-19 pandemic.....	371

CHAPTER 1: INTRODUCTION

In 2010, Andrew Pole, a senior manager and statistician working for Target (the second-largest department store retailer in the U.S. behind Walmart) delivered a keynote presentation at the Predictive Analytics World Conference (PAW) under the title, “How Target gets the most out of its guest data to improve marketing ROI [Return on Investment].” Toward the end of his presentation, Pole described Target’s project to predict customer pregnancy and its marketing potential (Pole, 2010). In 2012, the *New York Times Magazine* ran a front-page story entitled “How Companies Learn Your Secrets,” by Charles Duhigg, about Target’s pregnancy prediction score, its tone implying wrongdoing. The story was quickly picked up by Kashmir Hill (2012) in *Forbes* and was given a more sensational title: “How Target figured out a teen girl was pregnant before her father did.” By then, the story was explosive, gaining mainstream attention, creating myths around predictive analysis, and questioning the means by which retailers track and manipulate their consumers’ buying behaviour.

But why was Target interested in their consumers’ reproductive health information? What happened was Target’s marketers learned that since consumers’ shopping habits are usually ingrained and incredibly difficult to change, the best moment to intervene and change consumption habits is when consumers go through a major life event, such as, graduating from college, getting a new job, moving to a new town, getting married, or becoming pregnant. At those brief periods in a person’s life, routines fall apart and buying habits are up for grabs. Consumers might not notice or care about their new consumption habits, but retailers pay attention to those vulnerable moments. This desire to collect information on consumers and conducting behavioural research was not new to Target or any other large retailer, however, Target realised that timing is an important element. Once a couple have a new baby, competitive

offers, incentives, and advertisements would come from everywhere, but if the couple are reached earlier, during the second trimester (i.e., before any other retailer knows about the pregnancy), there is an excellent chance that this couple's buying habits could be captured for years. Pole helped Target to figure out if a consumer is pregnant, even if she did not want the retailer to know, by using data mining to create a pregnancy prediction score. As a result, Target has managed to figure out when consumers are expecting babies long before they need to start buying diapers (Hill, 2012). Target's prediction of customer pregnancy in 2010 revolutionized what marketers expect from predictive analytics (PA): instead of predicting a buying behaviour, marketers could predict a wide range of consumers' shopping needs. To build their pregnancy predictive model, Target analyzed data related to baby registry, programs that asked moms-to-be to identify themselves, and other retail customer data such as purchasing baby-related products. Leveraging innovative technology, analytics, and data to optimize their business model, Target succeeded in having a 30% increase in the identification of consumers that could be contacted with pregnancy-oriented marketing material (Siegel, 2013, pp. 38–39).

Duhigg suggests that Target's Mom and Baby sales exploded between 2002 and 2010, and their revenues grew from \$44 billion to \$67 billion. How did they do that?

Target assigns each shopper a unique code—known internally as the Guest ID number—that keeps tabs on everything they buy. “If you use a credit card or a coupon, or fill out a survey, or mail in a refund, or call the customer help line, or open an e-mail we've sent you or visit our Web site, we'll record it and link it to your Guest ID . . . We want to know everything we can.”

Also linked to your Guest ID is demographic information like your age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you've moved recently, what credit cards you carry in your wallet and what Web sites you visit. Target can buy data about your ethnicity, job history, the magazines you read, if you've ever declared bankruptcy or got divorced, the year you bought (or lost) your house, where you went to college, what kinds of topics you talk about online, whether you prefer certain brands of coffee, paper towels, cereal or applesauce,

your political leanings, reading habits, charitable giving and the number of cars you own. (Duhigg, 2012)

But what Target and other retailers have discovered is that although profiling is legal, when consumers realise how closely their lives are studied and how their shopping habits are predicted, influenced and manipulated, they will feel “uncomfortable . . . [and] get queasy” and might even change their retailer.

And we [Target] found out that as long as a pregnant woman thinks she hasn't been spied on, she'll use the coupons. She just assumes that everyone else on her block got the same mailer for diapers and cribs. As long as we don't spook her, it works (Duhigg, 2012).

To Charles Beck, Director of Solutions Consulting, Retail, Restaurant and Grocery at Medallia (a computer software company),

For many retailers—like grocery, convenience stores, cosmetics/skincare and other replenishment businesses—it often takes a significant life event like marriage or children for a loyal customer to switch to a competitor. Tens of millions of consumers are experiencing a significant life event simultaneously. Retailers should take advantage of the opportunity to capture more customers making the switch, while preserving the loyalty of longtime shoppers. (Newport, 2020)

Retailers, therefore, take advantage of the marketing opportunities created by key life events (Chahal, 2016) such as getting married, moving to a new house, or even getting the anticipated COVID-19 vaccine to be administered in retail pharmacies (Silverman, 2021; Terlep, 2021), for when they engage with their consumers during those events, not only do the former have new sales opportunities, but they also increase the likelihood that consumers might switch to their retail stores.

As consumers, we are complicit in the expansion of retailance. Whenever we go shopping, we willingly use our credit cards, provide our emails and postal codes, use the free Wi-Fi, and collect loyalty points. And the more technologically sophisticated the retailer

becomes, the more we are drawn to it (the latest example is Amazon Go which will be discussed in Chapter 2). In the above-mentioned example, Target did not breach any privacy laws, for they utilized customer information and publicly available data, however, the question of how ethical the implications of such analytics are is open to debate. And such scrutiny of consumers is only the tip of the iceberg, for once inside a retail store, consumers could be surveilled by an ever-expanding list of surveillance systems.

Surveillance in today's world

Surveillance has become an intrinsic part of daily life. Torpey (2007) distinguishes two types of governmental surveillance: thin and thick. Everyone is subjected to thin surveillance to some degree; it monitors our daily movements, our business transactions, and our interactions with government, but generally without constraining our mobility per se. Violations detected by thin surveillance usually result in a person's being subject to thick surveillance, which involves a more narrowing of freedom; it occurs in environments such as prisons, military brigades, and prisoner of war (POW) and refugee camps.

While not determinative, technological developments, especially computerization, have been profoundly important in the rise of new forms of surveillance (Haggerty & Ericson, 2006, p. 4). The dependence on communication and information technologies for administrative and control processes has turned societies into "information societies" (Fuchs, 2014; Lyon, 1998) and "surveillance societies" where every day, normal life is closely monitored (Lyon, 2001b, p. 1; 2008). Surveillance may be direct, face-to-face, or technologically mediated (Lyon, 2007), and consequently, is wanted, feared, and/or destigmatized (as in the case of reality shows (Lyon, 2006b)). Agencies, organizations and governments pursue our detailed personal information

(Mordini & Green, 2009); we are constantly asked to fill out forms, produce identification (described by Lyon (2009) as the “starting point of surveillance”), undergo fingerprinting and urine tests, participate in the census, and be manageable—as both workers and consumers—by searchable databases in order to make bureaucratic administration more manageable (Lyon, 2003, p. 161-162). Everyone is now subjected to surveillance. For example, national identification cards (Lyon, 2010b) and immigration cards contain biometric devices such as digitally stored fingerprints. Electronic registers and reports are used in schools, performance monitoring is used in workplaces, and social workers monitor children. To be eligible and entitled to benefits and privileges, individuals living in urban industrial societies, at least, have to be included in medical records, voting lists, housing registries, and tax files, controversially placing power in the hands of those who handle that information (Lyon, 2003b, p. 164).

Connections have been established between technologies and practices of surveillance (marked by the monitoring and attempted disciplining of behaviour), computation (with its construction of data bases) and simulation (with its real-time representations of behaviour and data). Graham (1999) gives three examples of such interrelations in which surveillance, computation and simulation are connected: (1) digital CCTV (Norris, 2003) and electronic tracking, promoted for crime control; (2) home teleservices and cyber-shopping; and (3) road transport informatics (RTI), or the development of smart, digitally controlled highways¹. Such emphasis on the intensifying use of surveillance technology reflects the domination by corporate and institutional concerns with profit, flexibility, and the effective targeting of subjects. National law-enforcement agencies employ surveillance for curtailing and/or preventing terrorist activity,

¹ Some Carleton University researchers are currently involved in various areas of research related to the development of smart cities, including sensor technology, cloud computing, and wireless connectivity (<https://carleton.ca/ips/smart-cities-research/>).

highlighting their authoritarian control, and ultimately, reviving the talk of the panoptic gaze of “Big Brother.” A pre-emptive approach in security and policing is “big data surveillance,” a term introduced by Andrejevic and Gates (2014, p. 190) to denote surveillance that relies upon “control over collection, storage, and processing infrastructures in order to accumulate and mine spectacularly large amounts of data for useful patterns.” Moreover, by targeting vulnerable populations with material that does not serve their long-term interests (a violation of the societal marketing concept), big data and the various tools that accompany it “has the potential to skew existing and future power dynamics between the marketer and customer” (Tadajewski, 2011, p. 14). On 17 January 2014, U.S. President Obama recognized the Big Data/surveillance link when he called for a “comprehensive review of Big Data and privacy.” Later, the U.S. proposed new rules governing bulk data collection by the National Security Agency (NSA) of the phone calling habits of Americans (Bauman et al., 2014; Lyon, 2014).

Michael, Fusco, and Michael (2008) coined the term “überveillance” to describe the human-centric tracking and monitoring services where the person (i.e., subject) is the active node in the network. They defined überveillance as “an *above* and *beyond*, an exaggerated, an omnipresent 24/7 electronic surveillance. It is a surveillance that is not only ‘always on’ but ‘always with you’ . . . [It is an] invasive surveillance” (p. 1198). Two examples of überveillance that monitor humans 24/7 are: the radio-frequency identification (RFID), an embedded technology employed in health applications (for example, RFID-enabled identification bracelets for newborns and patients that have potential privacy implications when linked to identifiable people); and the global positioning systems (GPS), a location-based monitoring technique (for example, a mobile app that tracks its owner’s location even when the app is not used). Such advanced location-based services (A-LBS) bring out the concern that if applied in government-

to-citizen mandated services, the state would be able to collect targeted data or conduct covert surveillance on any given individual.

Retailers protect their stores by investing in various methods of surveillance and shoplifting prevention, including: sophisticated close-circuit television (CCTV surveillance systems); motion detectors; high-tech scanners; Electronic Article Surveillance (EAS) devices, in which detection antennas are installed at the exit of the retail store and hard tags or labels are attached to the articles sold in the store; radio frequency identification (RFID) tags that have revolutionized the efficiency, effectiveness, and security of the supply chain and inventory management (Jones, Clarke-Hill, Comfort, Hillier, & Shears, 2004); and floor personnel and shop detectives (Bonfanti, 2014, p. 302). Gary Marx names such scrutiny of outsiders/customers the “external constituency surveillance” to differentiate it from the “internal constituency surveillance” that scrutinizes insiders/employees (2012, p. xxv).

Another form of surveillance that directly involves the human body is biometric surveillance (i.e., biosurveillance) and it is increasingly found in different sectors, such as: retail loss prevention, transportation security, law enforcement², geo-fencing, and banking security. It includes finger-scanning, retinal scanning, iris scanning (in which the form and coordinates of a person are identified via video cameras), handkey (which verifies users by utilizing the shape and size of a human hand), visual recognition, and genetic testing (Lyon, 2001b, pp. 77–81; Nelkin & Andrews, 2003). In the field of education, since the COVID-19 pandemic hit, there has been a rise in the use of remote proctoring platforms (such as ProctorU, Examity, Respondus and

² One of the first to note the impact of technologized policing was the French sociologist Jacques Ellul who introduced the concept of “la technique,” a totality of methods touching all areas of life, in *The Technological Society* (published in French in 1954 and translated into English in 1964). Ellul’s work would later influence Gary T. Marx’s work on undercover policing and Oscar Gandy’s work on the personal information economy.

Proctorio) that use a combination of human proctors and artificial intelligence (AI) in order to collect students' biometric data (including their unique facial and voice data) and their behavioural data, in addition to capturing their keystrokes, recording their screens and tracking their searches as well as their home environments when they are sitting for their online exams at home (Stewart, 2020). Though security through biology is an enticing idea (for example, implanting microchips in humans for medical and security purposes), it has its ethical implications as a result of its profound threats to the notions of privacy and security. In the context of welfare administration, the use of biometrics can be beneficial for a small group of people (i.e., politicians and those working in the biometrics industry) while situating the poor (i.e., welfare recipients who are usually stereotyped as underserving poor because of their race-, gender-, and class-based identities) in a broader network of crime and criminalization (Magnet, 2009). Thus, instead of eliminating fraud in the welfare system (e.g., when an individual signs up for welfare benefits more than once), people receiving welfare and living on the margins of the state are criminalized, for example, when their fingerprints (taken before they have even committed crimes) are made available to law-enforcement agencies (for example, in the U.S. states—like Massachusetts—where information can be shared). Another type of biometric surveillance is prevention surveillance which is used in public health sectors, for example, the Centres for Disease Control and the World Health Organization use surveillance to avoid or contain pandemics and contagious diseases by monitoring individuals and environmental conditions (an example is the current rise in surveillance practices to predict, observe and report cases and minimize the harm caused by the latest pandemic outbreak, the COVID-19). Protection surveillance includes the electronic location monitoring of abusing former spouses, and banks

and credit card companies monitoring unrelated financial activities of their customers (Marx, 2016b, p. 78).

To sum up, surveillance is pursued by governments, agencies, organizations, businesses and even individuals (for example, when installing home security cameras, using hidden nanny cams, or using GPS bracelets for kids). Its practices can be traced in nearly all aspects of our lives for different reasons, such as: consumption, administrative record keeping, protective services, national law enforcement, crime detection and control, location tracking, and disease/pandemic control. For some, technologies are seen as facilitating, if not producing, a qualitatively different human experience of dwelling in the world, for others, however, the integration of previously separate operations—such as computation, communication, and surveillance—is more daunting.

Retailance

Since this research focuses on the effect of surveillance on consumer behaviour in the retail sector, one must first define the nature of such surveillance. The word “surveillance” itself is rooted in Latin—in which *vigilare* means “to keep watch” and the prefix *sur* refers to “below” (Marx, 2016b, p. 46)—and the French verb *surveiller*, literally to “watch over.” To explain what surveillance is, several researchers have supplied their own definitions of the term. According to Christopher Dandeker (1990), a leading theorist on the subject of surveillance,

The exercise of surveillance involves one or more of the following activities: (1) the collection and storage of information (presumed to be useful) about people or objects; (2) the supervision of the activities of people or objects through the issuing of instructions or the physical design of the natural and built environments. In this context, architecture is of significance for the supervision of people—as for instance in prison and urban design; (3) the application of information gathering activities to the business of monitoring the behaviour of

those under supervision, and, in the case of subject persons, their compliance with instructions (p. 37).

Nearly two decades later, Lyon would define surveillance as the

processes in which special note is taken of certain human behaviours that go well beyond idle curiosity . . . it is the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction (Lyon, 2007, pp. 13–14).

Focusing on the need for mutually beneficial exchanges built on informed consent, Grenville

(2010) defines surveillance as:

an exchange of information between actors. The gatherer obtains data from the subject, these data feed back to the provider of the information. There is an action and a reaction in this exchange (p. 81).

In the *Routledge Handbook of Surveillance Studies*, Gary T. Marx defines surveillance

as:

Scrutiny of individuals, groups and contexts through the use of technical means to extract or create information. This means the ability to go beyond what is offered to the unaided senses and minds or what is voluntarily reported. The new surveillance is central to the emergence of a *surveillance society* with its extensive and intensive (and often remote, embedded) data collection, analysis and networks (Marx, 2012, p. xxv).

The above definition describes what he calls “new” surveillance that is both “decentralized” and “digitalized” versus the older, limited “traditional surveillance” in preindustrial societies, which tended to stay local and compartmentalized, and the centralized “surveillance” that emerged with industrial society and bureaucratic record keeping (e.g., a police officer trailing a suspect). Marx then goes on to identify both the “surveillance agent” (i.e., the watcher/observer/seeker/inspector/auditor/tester) who can be a sponsor, data collector, initial or secondary user, and the “surveillance subject” (i.e., the person about whom information is sought or reported). New surveillance, moreover, could be described as technologies that are:

a broad family of computers, sensors, transmitters, biochemical assays, spectrographs, video lenses, software, and *management practices* [emphasis added] that construct the “new surveillance” and that transcend the senses, space, and time, as well as the traditional borders of the self, the body, and the group. The substance is personal information . . . The technologies offer possibilities for “windows into the soul.” (Marx, 2016b, pp. 1–2).

New surveillance, therefore, has become more comprehensive, intensive, and extensive, and its emphasis has expanded beyond the individual to systems and networks (Marx, 2016b, p. 57).

When it comes to this research, the above definitions are too general to be applied, for they cover the surveillance of all human behaviours and not just consumption behaviours. In the world of business, the term “consumer surveillance” is frequently used though there is no one specific definition. In general, it refers to the monitoring and recording of people’s activities and data, either online or in the physical environment, for commercial purposes, and such data can be shared with third parties. Again, this definition is too broad for this research.

As a result of the lack of a proper definition that would suit this research, I have coined a new term: *retailance* (a combination of the words “retail” and “surveillance”) which I define as following:

Retailance, or surveillance in a brick-and-mortar retail setting, is the focused, systematic, and routine scrutiny of consumers and/or the collection of their personal and shopping data, which goes beyond what is voluntarily reported, for purposes of influence, management, protection, retail crime identification, shrinkage prevention, improving the consumer’s shopping experience, and/or profit. Surveillance may be direct (face-to-face) or technologically mediated (overt or covert in-store security systems).

This definition also serves to bring the research boundaries into focus: (1) the research focuses on consumption in a brick-and-mortar setting (versus online consumption); (2) the routine,

everyday nature of surveillance; (3) the term “consumer” is used throughout the research instead of “customer” to highlight the B2C (Business to Consumer) model, versus the B2B (Business to Business) model, and it denotes “an individual who is pursuing, purchasing or using commodities” which are defined as “objects, services, and other entities that are sold through capitalist means” (Belisle, 2011, p. 9); (4) retailers’ data collection methods could be voluntary (i.e., the consumer willingly gives their information) or involuntary (i.e., collected by the retailer without the consumer’s knowledge); (5) there are different reasons behind the collection of surveillance data; and (6) there are different retail surveillance systems. The last three themes will be expanded upon in the next chapters.

The following retailance model (Figure 1) has been created to provide a conceptual roadmap of how the research proceeded. In this process model, retailance (manifested in surveillance channels and systems) directly influences the relationship between retailers (i.e., surveiller) and consumers (i.e., surveilled). Consumers’ reaction to retail surveillance channels is influenced by their awareness of privacy laws and regulations, and the presence and scope of retailance itself (making “awareness” a moderator of the relationship between surveiller and surveilled). The impact and outcome of such retailance ultimately affects the retailers, creating a never-ending circle. It is worth mentioning that while this initial process model guided the research, it was returned to after the data analysis; its final version has been adapted to the research results (please refer to Chapter 5).

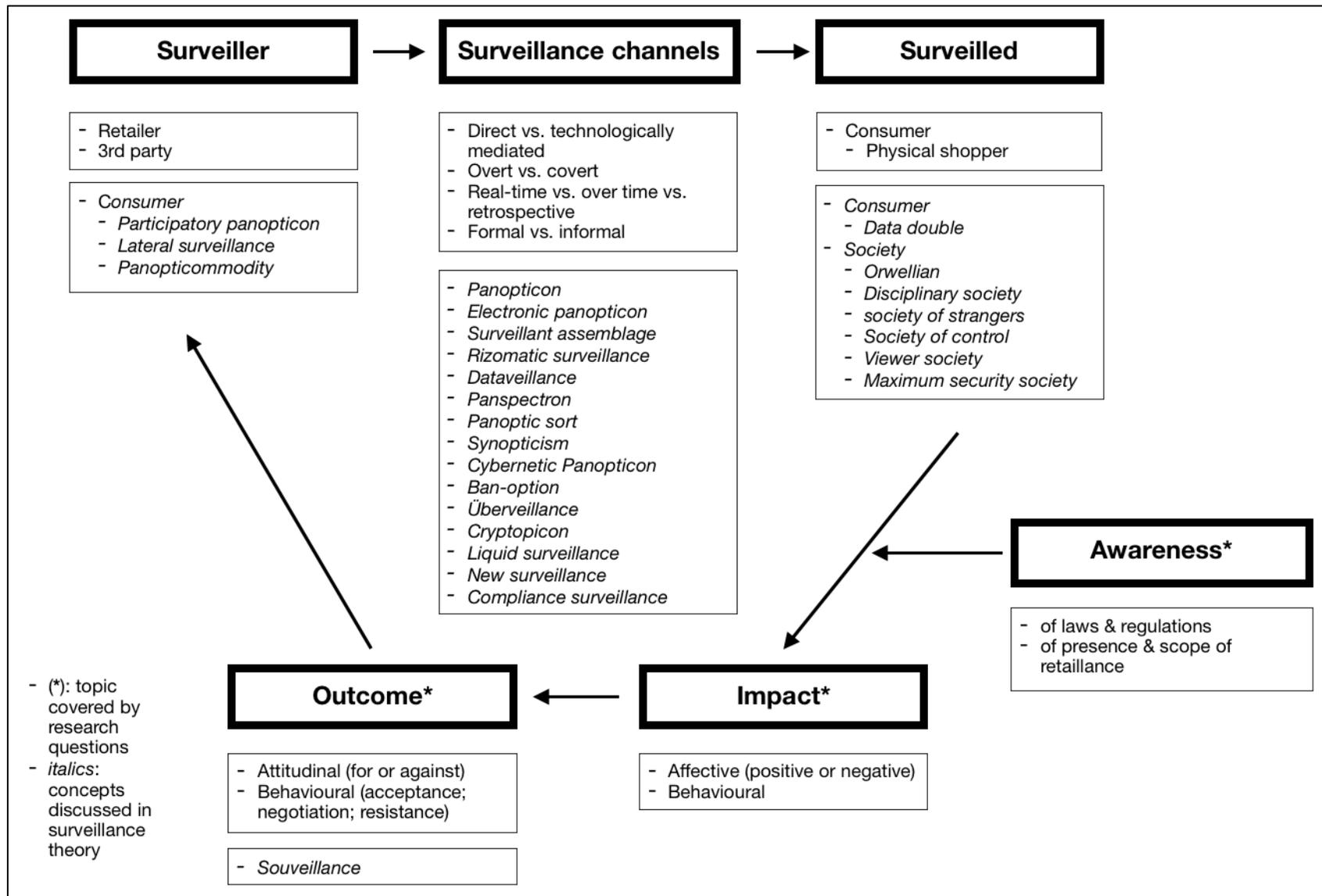


Figure 1 – Detailed retailance process model

Markus and Robey (1988) support the use of process models (in comparison to variance models) when the researcher needs to (1) find patterns in empirical data; (2) retain empirical fidelity of the emergent perspective; and (3) provide richer explanations of how and why the outcomes occur when they do occur. In contrast to the variance approach which focuses on variables that represent the important aspects or attributes of the subject under study, and establishes the conditions necessary to bring about an outcome, a process approach entails explanations that are layered and that incorporate both immediate and distal causation, and shows that entities, attributes or events may change in meaning over time (Van De Ven & Poole, 2005).

It should be noted that this model opens the door to multiple studies whose magnitude is beyond this dissertation research, consequently, the research plan based on the literature review (more details in the following chapters) focused only on parts of the model (mainly the themes of awareness, impact and outcome). In addition, the research conducted (through surveys and interviews) focused on the consumer (although retail workers and retail managers were interviewed to incorporate the point of view of different stakeholders). More importantly, the researcher's stance is neither for nor against the use of retailance; I take a distanced position, for while I believe that marketers, practitioners and policy makers have an ethical and social responsibility to protect their consumers' welfare and privacy, I also believe that practitioners (i.e., retailers) need to survive in an increasingly digital world, and one way to do this is through using retailance.

Your retailer needs you

The title of this research is inspired by the WWI British recruitment poster “Your Country Needs You” designed by Alfred Leete, in which Lord Kitchener, a war hero and the British Secretary of State for War, points his finger at the audience. Although historians now claim that the poster’s vital influence on recruitment is largely a myth (British Library, n.d.; Saul, 2013), it has become an iconic symbol of its age. Some even argue that it caught the attention of the then eleven-year-old George Orwell who would later use it as the basis for his description of the Big Brother posters in his novel *1984* (first published in 1949), however, instead of the poster being a symbol of heroic national resolve, it becomes a symbol of government surveillance and intrusion into the lives of its citizens (Lubin, 2016).

The evolving meaning behind this poster reflects the intricate relationship between the retailer and the consumer in the context of retailance. It also leads to the question of how much consumers are aware of when it comes to retailance. And do they have no other option but to learn to accept, and even welcome, the scrutiny, quantifying, profiling, tracking, and discrimination of retailance? Retailers (like Walmart, Target, Macy’s and many more) are now using increasingly sophisticated electronic monitors that show up first as experiments before becoming ordinary elements of shopping, building a new future for physical retailing (Turow, 2017, pp. 8–9). As a consumer, you may appreciate being the recipient of great service and shopping offers, not realizing the scope of the behind-the-scenes tracking that may have consequences which you might not like. Although discussions of practices related to privacy are widespread nowadays, retailers do not figure much in the debate,

[the] shopping aisle has, in fact, received almost no attention even among academics who focus on the social implications of consumer surveillance—an unfortunate trend, because the traffic that retailers can track through those physical doors is huge. (Turow, 2017, pp. 10-11)

I believe that in a physical retail setting, the impact and outcome of retailance is partly a result of the complex relationship between the retailer and the consumer (this complexity is due to the centre of power that keeps shifting between consumer and retailer, a theme that is discussed later in more details under the critical marketing approach). Thus, as marketing researchers, we need to study how the incorporation of retailance affects the retailer, the consumer, and the larger society. And this is where my research questions come in.

Research Questions

After 9/11 and the subsequent war on terror, the massive development in surveillance capacities paralleled the advancement in technology. The former NSA contractor Edward Snowden described the Five Eyes (FVEY)—an intelligence alliance comprising the United States, Canada, Australia, New Zealand and the United Kingdom—as a “supra-national intelligence organization that does not answer to the known laws of its own countries” (Norddeutscher Rundfunk, 2014), for the collected information is shared to circumvent restrictive domestic regulations on surveillance of citizens. Every person now, especially in urban societies, is subjected to some degree of surveillance, whether by governments, agencies, or corporations. As citizens, workers, or consumers, our information is available in various searchable databases, our images are captured by video surveillance, our conversations could be recorded at any moment—for example, by Amazon’s virtual assistant Alexa and their new Echo Frames (Smith, 2019), or the Wi-Fi-enabled Barbie doll (Lennihan, 2015)—and our bodies (such as faces, fingerprints and blood) are biometrically surveilled. Although data mining for the sake of purchase predictive modeling is under the spotlight, not enough attention is paid to the surveillance employed in the brick-and-mortar retail sector. Retailers invest in surveillance for

different reasons, for example, to monitor in-store activity, maintain low shrinkage rates, and improve marketing effectiveness. Consumers, on the other hand, have expectations of what their shopping experience should be like and they expect to be offered personalized and attractive benefits. However, the collection of consumers' personal data and information related to their consumption behaviour can also be considered an infringement of privacy. Even if such infringements are lawful, retailance reflects on ethical dilemmas, consumer discrimination and policing. Understanding the effect of retailance is definitely important to public policy makers who constantly need to implement new and updated legislative protections. And it is even more important to marketers who need to understand the short-term (e.g., consumers' reaction(s) inside the retail stores at the time of being confronted with retailance) and long-term (e.g., consumers' future choices of which retail stores to frequent) implications of retailance on both consumers and retailers.

The research questions raised by this research are:

- How much are consumers aware of the presence and scope of retailance?
- Are consumers aware of the laws and regulations that protect their personal information?
- What is their behavioural reaction to retailance (i.e., do consumers accept, negotiate or resist retailance)?
- What is the attitudinal outcome of retailance (i.e., are consumers for or against retailance)?

At the beginning of 2020, and during the course of data collection, the retail environment witnessed profound shifts and dramatic changes due to the worldwide spread of the COVID-19 pandemic. Consequently, an additional research question was added:

- What is the impact of the COVID-19 pandemic on retailers' use of and consumers' reaction towards retailance?

Chapter Organization

This dissertation is divided into 7 chapters. In this chapter, Chapter 1, the existence of surveillance practices in the brick-and-mortar retail sector, specifically in North America, was introduced. The retail environment (encompassing department stores, chain stores like grocery stores, discount stores, and big-box stores) present in Canada and the U.S. is strikingly similar, and both American and Canadian retailers benefited from the industrial revolution and the developments subsequent to the Civil War in America (the mid-1860s) (Burns & Rayman, 1995). After looking at the definitions of surveillance in sociology and surveillance studies, a new definition of retail surveillance was provided, a new term, *retailance*, was created to specifically refer to that definition, and an initial *retailance* model was presented. The chapter then ended with a discussion of the research questions which the research aims to answer and a road map.

Because of the many aspects of *retailance* (some of which are not commonly known or noticed), Chapter 2 has a hybrid structure that covers both a review of the relevant literatures and an overview of the various *retailance* technologies. The chapter begins by explaining how the review of the retail and surveillance literature, popular new media, dystopian literature and academic publications (i.e., journal articles, conference proceedings, etc.) was conducted, and then an overview of consumer surveillance methods is presented. Following the *retailance* model, the chapter first focuses on the surveiller and the four major goals of retailers (controlling loss and enhancing security, creating a pleasant and personalized shopping experience, enhancing profitability, and ensuring safety during the COVID-19 pandemic). This is followed by a discussion of surveillance channels and *retailance* systems (including video, audio, biometric, virtual guards, tagging, collecting phone numbers and emails, loyalty cards, free Wi-

Fi and tracking technology, personalised advertising, radio frequency identification, tracking returns, and geo-fencing). Then comes a section about the impact and outcome of retailance on consumers, followed by the ethical dilemmas of retailance. The chapter ends with a summary and conclusion.

Chapter 3 begins by highlighting the interdisciplinary nature of both marketing and surveillance studies and the critical marketing approach that will be applied to the research. Afterwards, my review of surveillance literature is divided into five major theoretical perspectives that are relevant to the retail sector: panopticism (Bentham, Foucault, and Gandy), synopticism (Mathiesen and Andrejevic), postpanopticism (Boyne and Lyon), assemblage (Deleuze and Guattari, and Haggerty and Ericson), and virtual identities (Haggerty and Ericson, Poster, Deleuze, Bogard, and Lyon). The chapter concludes with a discussion of how the progress of surveillance technologies parallels the progress in marketing and consumer behaviour theories.

Chapter 4 introduces the mixed methods research design that was used in the subsequent collection of data and the interpretative and pragmatic approaches employed. Data was collected through an MTurk survey and semi-structured interviews (with consumers, retail workers and retail managers). This chapter also discusses the impact of the COVID-19 pandemic on data collection and the research ethical issues. Chapter 5 introduces the collected data and discusses the findings. Based on the themes that emerge and consolidate, an updated retailance model is presented. Chapter 6 discusses the impact of the COVID-19 pandemic on retailing in general and on retailance in particular.

Chapter 7 wraps up the research and presents its contributions and recommendations to the different stakeholders (consumers, retailers, and public policy makers). Conceptually, this

research integrated extant literature, synthesized prior studies, provided definitional clarity, and created a conceptual retailance model that works as a roadmap and opens new avenues for future research. Theoretically, it embraced a multidisciplinary perspective by borrowing theories from other disciplines and integrating them to reveal novel insights when looking at retailance, offered a new theoretical model, and reconciled contradictory reactions to surveillance. Other contributions encompassed helping scholars, retail managers, consumers, and policy makers gain a better understanding of the impact of both traditional surveillance and smart retail technologies on consumer behaviour in a brick-and-mortar setting. The chapter ends with a discussion of the research limitations and avenues for future research. Finally, survey questions, semi-structured interview questions, highlights of consumer privacy rights in North America, and support resources (i.e., contact information of available support to interviewees who could feel stressed out during the interviews when discussing the COVID-19 pandemic), examples of the recruitment tools (online invitations published on Facebook), and short biographies of the interviewees are included in the Appendices.

Chapter summary and conclusion

Brick-and-mortar retailers need to reinvent and reposition themselves in order to compete with the increasing sophistication and importance of e-commerce. To thrive, they need to be efficient, agile, customer friendly, create a brand experience (Retail Council of Canada, 2017) and discover new avenues of advantage over their rival online giants (such as Amazon and eBay). One way to reach their goals is to employ retailance, a decision that can both appeal to and alienate their consumers.

In this chapter, the term “retailance” was introduced, showing how its definition is a better fit for the brick-and-mortar retail setting, and how it brings the research boundaries into focus. A newly created retailance model provided a conceptual roadmap of how the research proceeded, introducing the themes of: surveiller, surveillance channels, surveilled, awareness, impact and outcome. The chapter ended with a list of the research questions raised by this research and how the remaining chapters were organized.

CHAPTER 2: LITERATURE REVIEW

Amid a technological retail revolution, retailers have the potential to enhance both their operations and the experience they can provide their consumers (Grewal, Noble, Roggeveen, & Nordfalt, 2020). The complex retail environment is being shaped by the rise of new competing channels and multichannel shopping behaviour (Singh, 2011). To 21st-century merchants, threatened by new online competitive pressures, consumer tracking has become a strategic imperative in brick-and-mortar stores (Turow, McGuigan, & Maris, 2015). Physical stores now compete with sellers not just in the same city or country, but from all over the world. Even when shopping in a physical store, consumers can access the internet from their smartphones, using them as a competitive weapon, browsing product ratings, price comparisons, comments and feedback on social media, and ads from competitors, in the process becoming “omnichannel shoppers” (Lazaris, Vrechopoulous, Fraidaki, & Doukidis, 2014). Therefore, to ensure their success, retailers need to have tracking abilities at least as good as their online competitors. In addition to retail profitability, one of the main goals of retailers has always been to provide a shopping environment that is both secure and appealing to their consumers. Retailers believe that consumers tend to benefit enormously through relevant, personalized treatment (e.g., when consumers receive discounts and deals that are more relevant to their needs) that will ensue when they let the retailers know of their presence inside the store and when they give up data about themselves (Turow, McGuigan, et al., 2015). Retailers, therefore, need to strike a balance between customer satisfaction and efficient security. Unlike the Orwellian goal of control, the ultimate objective of consumer surveillance is to improve retailers’ profitability, by segmenting consumers for better targeting, increasing their customer loyalty, bolstering sales, and decreasing returns on impulse buys (Pandolph, 2017). With the revolution in surveillance technology, it is

no wonder that surveillance methods and technology are now part and parcel of the retail environment.

Because of the complexity of the interdisciplinary field of surveillance, this chapter covers both theoretical and conceptual works and practical discussions of retailance technologies. The chapter is structured as following: first, using secondary information from the retail and surveillance literatures, popular new media, dystopian literature, and academic publications, the chapter begins by explaining how the literature review was conducted and providing an overview of consumer surveillance. Based on the retailance model introduced in Chapter 1, the following are subsequently discussed: the surveiller and the goals retailers aim for (controlling loss and enhancing security, creating a pleasant and personalized shopping experience, enhancing profitability, and ensuring safety during the COVID-19 pandemic); the four different channels of retailance and the various retailance systems; awareness of retailance (individual, societal, and awareness of government policies and laws); the impact and outcome of retailance on consumers; and the ethical dilemmas of retailance. The chapter closes with a summary and a conclusion.

Conducting the literature review

I first came to the idea of studying surveillance in retailing in 2018 when I came across the news about Amazon opening its first partially automated grocery store in Seattle, Washington, an event that has ushered in a new zeitgeist of retailance and consumption. A starting point for the literature review was reading *Surveillance Studies: An Overview* (2007) by David Lyon, a sociologist and the current director of the Surveillance Studies Centre (SSC) at Queen's University in Kingston, Ontario. Lyon is a good representative of most sociologists who

work in the field of surveillance studies; much of their work takes the form of critique and it is non-empirical (at best, it can be considered conceptual). To build the literature review, therefore, I worked on three fronts simultaneously. First, I reviewed academic papers and books by conducting research on both the Carleton University MacOdrum Library website and Google Scholar online. The library online search engine was used to search both the “header fields” (i.e., titles, keywords and abstracts) as well as the text of the articles (including the reference/bibliography sections) for terms such as: surveillance, panopticon, Foucault, retail, and the various forms of surveillance systems (e.g., tagging, RFID, geo-fencing, etc.). Because of the interdisciplinary nature of the topic, there were no restrictions when it came to publication date or venue. Secondly, I reviewed the reference section of each book and journal paper identified earlier for additional works. Thirdly, I searched online using the Google search engine. As a result, over 520 references (excluding those covering critical marketing and research methodologies) were found relevant to this research, covering the time period from 1791 to May 2021. Those references could be divided into practical and academic categories (Figure 2). Practical resources include reports issued by retail and surveillance businesses and associations, newspaper articles, magazine articles, law guides, forums, and websites of market research and consulting firms, security firms, privacy groups, retail businesses, governments, etc. Academic sources reviewed included journal papers, books, conference proceedings, and a university report (Turow, Hennessy, & Draper, 2015).

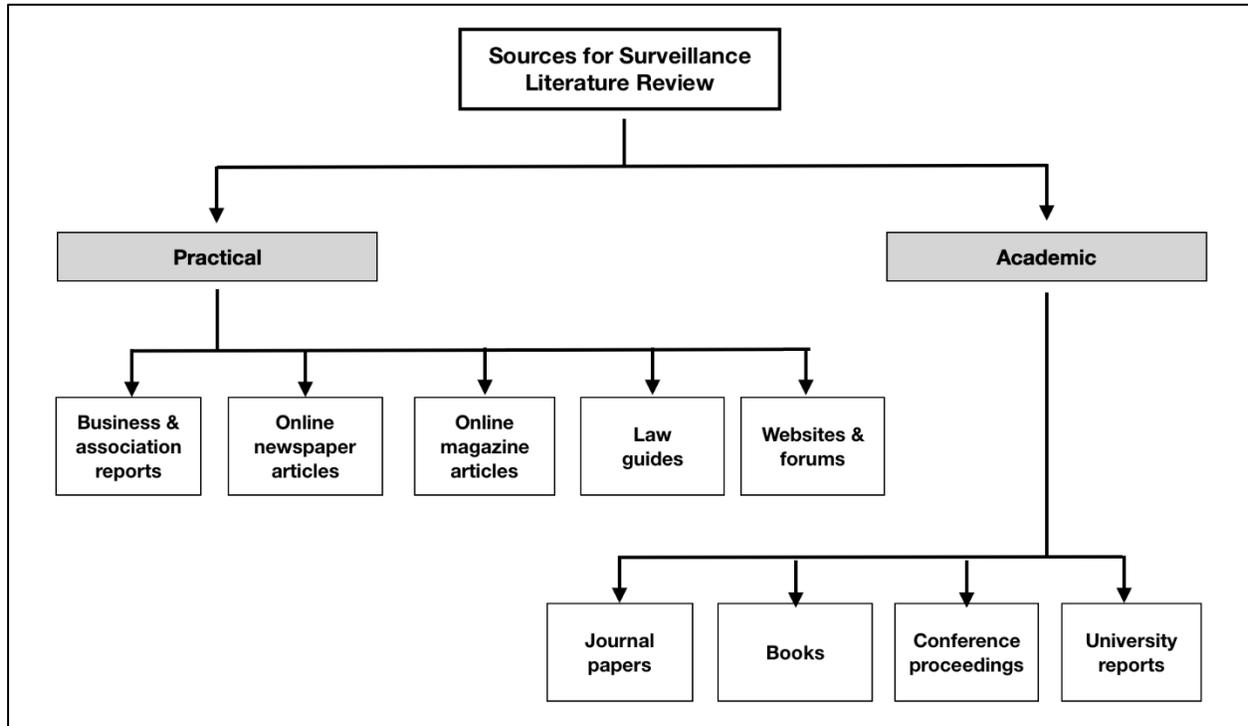


Figure 2 – Sources for the surveillance literature review

Based on the above research, the following observations could be made. First, the lack of scholarly marketing research related to the topic of retailance underscored the necessity to include research from other disciplines. Second, because of the rapidly changing nature of surveillance technology, there is a need for up-to-date research. While some aspects of past research are still valuable (such as theoretical foundations, using previously developed methods as a starting point, or past research results as a point of comparison), a lot of the concepts have to be updated to reflect the capabilities of new technologies. Third, published empirical scholarly research on surveillance in a retail setting is surprisingly quite limited. In fact, although my research project is set in North America, I had to widen the geographic scope to include Europe due to the limited amount of published research. A total of twenty-five academic papers in different publication venues (18 journal papers, 4 book chapters, 2 conference proceeding and 1 university report) have been found relevant (Figure 3). The following selection criteria were

applied: (1) the research had to be already published and not a work-in-progress; (2) the paper had to be academic in nature (e.g., magazines and newspaper articles were excluded); (3) the work had to be relevant to the topic of retailance/marketing, for example, the ultimate focus is on either the consumer and/or the retailer and not on the surveillance technology itself; and (4) the research had to be applicable to a brick-and mortar setting.

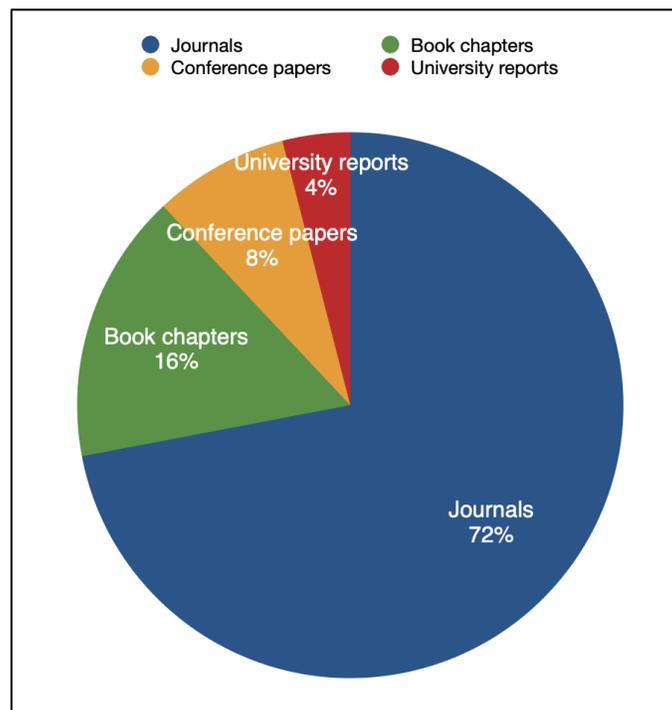


Figure 3 - Publication venues of past academic research

An overview of consumer surveillance & database marketing

While the conducted literature review (as discussed above) covered the topic of surveillance in different fields of study, the focus of this research is on the area of marketing in general, and retailing in particular. It is, therefore, imperative to introduce the connections between surveillance and both consumption and database marketing. Consumption is considered a sphere of surveillance, for “the key traits [of surveillance] are visible, and in the consumer

sphere a particular pattern of growth is evident” (Lyon, 2007, p. 2). Consumer surveillance, therefore, could be viewed as a technologically enhanced development of capitalist management (Lyon, 2001b, p. 43). In my opinion, consumer surveillance has surpassed Orwell’s (1989) dystopian vision of the nation state’s possession of the power of surveillance and control. However, although many consumer surveillance practices may resonate with Taylorist methods—which entailed the use of market knowledge to break down consumer demand into clearly identifiable segments (Arvidsson, 2003, p. 459)—or panoptic methods (which will be discussed in detail in Chapter 3), the leading principle of the consumer order is pleasure, not pain or coercion (Lyon, 1994, pp. 155–157).

Elements of consumer surveillance could be traced back to the early techniques of market research, such as political polls and crude market surveys, that took place in the mid-19th century in the U.S. (Lockley, 1950; D. W. Stewart, 2010). One of the landmarks in early market research occurred in the early 1920s when Alfred Sloan, working for General Motors (GM), used scientific management principles to analyze commodity markets and consumer behaviour, in order to develop an extensive repositioning strategy that was instrumental to General Motors' success over the decades that followed (Powers & Steward, 2010). By gathering information about and from consumers, GM succeeded in estimating consumer demand (Dale, 1956) and discovering the effect of consumer patterns for car sales (e.g., relating buyers’ incomes to cars’ prices, popularity of colours, consumer loyalty, the preferred magazines of car buyers) that could be exploited and thereby boost the number of sales per dealer (Clarke, 1996). By the 1930s, with the help of International Business Machines Inc. (IBM) which was enlisted to provide data services, demographic and socio-economic data on buying habits were collated to build profiles of consumers and manage their activities (Lyon, 2007, pp. 40–41). Such “social Taylorism” was

viewed as a subtle form of social control, for the “corporate capital’s need and desire to control knowledge/information is extending beyond the factory to the society as a whole” (Webster & Robins, 1986, pp. 328–343).

The advent of modern computing later enabled large-scale changes to occur in the marketing industries. Database marketing, a form of marketing surveillance, began in the 1980s when database marketers developed new means of obtaining geo-demographic data (using zip codes and postcodes to cluster populations according to shared spending and lifestyle characteristics) as a means of building a picture of what sorts of people live where so that direct mail could be more accurately sent to them, hence, a system based on the idea that “You are where you live” (Phillips & Curry, 2003). Such collected consumer data revealed the spatial distribution of socio-economic characteristics, tastes, preferences, and lifestyles, providing a solid basis for consumer segmentation (Pridmore & Zwick, 2013, p. 104). Nowadays, PRIZM (an acronym for “Potential Rating Index for Zip Marketers”) is widely used for customer segmentation in the U.S. (“Claritas PRIZM,” n.d.) and Canada (“PRIZM,” n.d.). Used since the 1990s, PRIZM helps businesses and marketers reach, identify, analyze and understand customers and prospects by incorporating the latest demographic, geographic, marketing, consumer behaviour, and media authoritative data. Such database marketing could be considered the first phase of computer-assisted consumer surveillance. A classic study that focused on the growing economic significance of personal data was *The Panoptic Sort* (1993) by Oscar H. Gandy. In his work, Gandy combined analysis of the sorting and classifying aspects of the panopticon with the process of profiling consumers. He discussed how marketers identified individuals who share certain attributes that make them particularly attractive as potential consumers, while

discriminating against and discarding other potential consumers (i.e., what marketers call marketing strategy, consisting of segmentation, targeting, and positioning).

The operation of the panoptic sort increases the ability of organized interests, whether they are selling shoes, toothpaste, or political platforms, to identify, isolate, and communicate differentially with individuals in order to increase their influence over how consumers make selections among these options (pp. 1-2).

The panoptic sort is, therefore, a discriminatory process that sorts individuals on the basis of their estimated value or worth.

The second phase of database marketing was the online monitoring of surfing activities, which started in the 1990s as a result of the commercialization of the internet and the growing possibilities for online marketing, aided by the use of “cookies” and similar devices that allow companies to follow the trails of customer interests (Lyon, 2001b, pp. 43–44). Currently, two of the most noteworthy entities for using data-gathering and collaborative filtering techniques to provide personal shopping suggestions to visitors based on their previous activities are Amazon and Google (Turow, McGuigan, et al., 2015). Thus, obtaining information on the consumer from their current and past purchase history has become an important aspect of marketing practice that has a tremendous potential for improving profitability (Rossi, McCulloch, & Allenby, 1996; Scranton, Berghoff, & Spiekermann, 2012).

But such practices of data mining can have a negative impact. They may exclude classes of consumers from full participation in the marketplace due to price discrimination (when the same goods are sold to different consumers at different prices), weblining (when classes of consumers are excluded from the marketplace, for example, based on geographical location), and segmenting consumers for the purposes of delivering policy-related information (Danna & Gandy, 2002). In national surveys, almost half of adult American consumers are against discount offers tailored to their interest for two reasons: (1) they worry they will not learn about

serendipitous possibilities; and (2) they believe that the algorithm-driven approaches used by retailers divide consumers into “winners” and “losers” when it comes to seeing particular products or prices (Turow, McGuigan, et al., 2015, p. 475). Information (i.e., consumer surveillance using database marketing), therefore, produces discriminatory practices, and plays a crucial role in the development and reproduction of systems of power (Lyon, 2003a).

The third phase of computer assisted consumer surveillance brings the previous two phases together: location-based technologies (also known as “m-commerce,” where *m* is for “mobile”) that trace and track actual movements of consumers, using the data for marketing and other purposes, for example, location-based advertising that targets cellphone users (Lyon, Marmura, & Peroff, 2005). Throughout the development of these three phases, the practice of customer relationship management (CRM) has grown. CRM emerged, with the help of technology in the form of the database, as a fusion of relationship marketing (i.e., enhancing customer relationship) and direct marketing (i.e., the use of customer databases to improve the efficiency of marketing through better targeting) (Neslin, 2014, p. 289). Nowadays, corporations manage the flow of data between service representatives and the marketing department in order to offer differential treatment to different kinds of customers, those whose history (i.e., customer lifetime value) demonstrates greater or lesser profitability for the company (Lyon, 2007, pp. 40–44).

Since this research focuses on the retail sector, the rest of the literature review (compiled below) adheres to the retailance model (Figure 4), discussed earlier in Chapter 1, beginning with the “surveiller.”

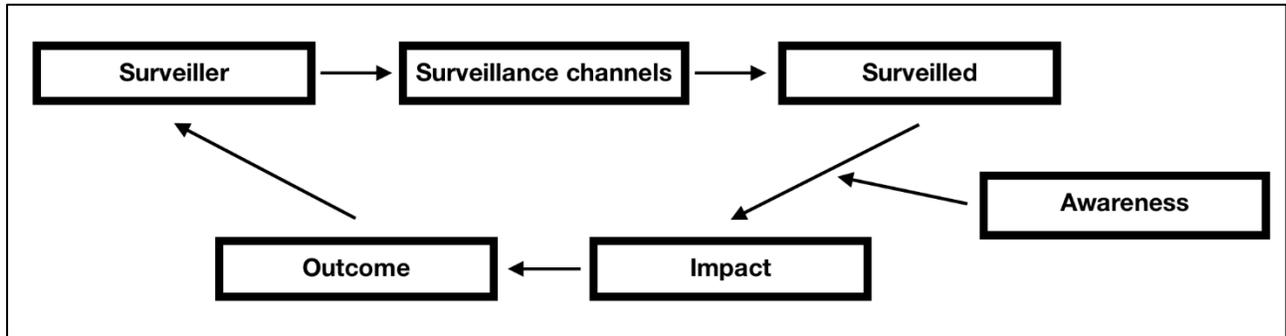


Figure 4 - Retailance model

The surveiller: Retailers' goals

To understand the role that retailers (i.e., surveillers) play in retailance, we should first understand what their goals are, how they align with or contradict the goals of both consumers (i.e., the surveilled) and governments, and the outcome of such retailance and how it affects consumers' attitudes and behaviour. Several factors have contributed to the desire for and ability to gather and use customer information for marketing purposes: (1) with the decrease in operating costs of information and communication technologies (ICTs), the relatively minimal cost of consumer data gathering efforts is seen as providing a potentially large return on investment; (2) fueled by competitive pressures, there is a focus on collecting consumers' personal information, a task made easier by the decreasing costs of data storage and retrieval, the use of new forms of data analytics such as data mining (Turow, McGuigan, et al., 2015) and knowledge data discovery (KDD), and the application of these data within the predominant business strategy of customer relationship management (CRM); and (3) the increased availability of consumer data provided by numerous third-party corporations that sell this information as a commodity and by public distributors of relevant population data (for example, government statistics bureaucracies, such as U.S. Census Bureau, Statistics Canada, and the U.K. Home Office).

Based on academic references, security/surveillance businesses' websites and reports, newspaper and magazine articles, and retailer guides, a more detailed discussion of why retailers employ retail security follows.

(1) To control loss and enhance security

Retail space is not only used for legitimate acts of consumption, but also for illegal forms of shopping behaviour, such as shoplifting (Phillips, Alexander, & Shaw, 2005). To combat retail misbehaviour, retail security is concerned with products, consumers and staff (the last is not covered by this research) (MarchNetworks, 2019). For example, packaging design (Coles & Kirwan, 2011)—in addition to its aesthetic and information functions—plays a role in security, for it helps deter tampering and pilferage, its authentication seal and security printing indicate that its content is not counterfeit, and when combined with anti-theft devices such as RFID (Radio Frequency Identification) tags, it becomes a means of retail loss prevention.

As for safeguarding the security of consumers, a 1995 survey study by Overstreet and Clodfelter of the safety and security concerns of shopping center customers (e.g., parking lot security, robbery, assault, harassment, high-crime areas surrounding the mall, traveling after dark, abduction of small children) concluded that these concerns (especially customers' safety outside the mall) affect shopping frequency and shopping precautionary behaviour (e.g., avoiding shopping after dark or when alone, and avoiding the parking lot). When consumers are afraid of retail crime, they can enact a wide range of avoidance behaviours, such as: reduced shopping activity, limited nighttime shopping, shortened shopping visits, switching to competitors, or turning to alternative shopping formats including the internet or catalogues (Cardone & Hayes, 2012, p. 23; Warr, 2000).

(2) To create a pleasant and personalized shopping experience

The importance retailers place on safety and security should not undermine consumers' shopping experience. The Canadian *Retailer's Guide* ("Retailer's Guide - Vol 1.1," 2018), published by the Retail Council of Canada (RCC), advises retailers to not look at technology as just a way to create an effective omnichannel selling structure, but to also create a unique shopping experience; today's consumers care about their shopping experience as much as finding products and the best prices (both of which could be attained online). Retailers have always leveraged on store environment by manipulating three dimensions: ambient factors (sight, sound, smell, and touch); design elements (functional and aesthetic aspects, such as the layout, design, and décor); and the people component of the space (in which interpersonal interactions take place in the form of customer-to-customer and customer-to-staff interactions) (Baker, 1986). As for employing technology in retailing, from an historical perspective, technology and retailing (specifically the department store invented in the 1850s) have been inextricably linked since the 19th century, both in terms of their development and their ability to facilitate visibility and trialability³, and deliver unique benefits to consumers (Tamilia, 2011; Tamilia & Reid, 2007). Nowadays, retailers' investments in store design, staff training, and technological systems can ensure adequate security levels without compromising consumers' shopping experiences, as long as the surveillance allows them to have contact with the store, its articles, and staff. Retailers have to balance the use of a number of ambient design and social elements—in the hopes of creating a unique, pleasant, and engaging Customer Shopping

³ In his *Diffusion of Innovations* (2003), Rogers identifies trialability and observability as two of the five attributes of innovation that influence the rate of adoption (the remaining three are relative advantage, compatibility, and complexity).

Experience (CSE)—while ensuring that a high level of sales environment surveillance does not interfere with the shopping experience (Bonfanti, 2014). Despite the fact that open merchandising (i.e., an open sales environment in which articles are accessibly displayed) improves the shopping experience and increases sales, it can lead to increased retail “shrinkage” or “shrink” (i.e., the stock loss from crime or waste expressed as a percentage of retail sales), affecting shoppers in a number of ways, such as: reduced on-shelf availability, reduced assortments, defensive merchandising (i.e., a retail practice where the amount of merchandise on display is limited to control theft), and economic losses (Bonfanti, 2014, p. 298). Shoplifting losses and the cost of added security is often pushed on to the consumer; to compensate for the loss in profit, retail prices increase by an average of two to three cents per dollar (Lin, Hastings, & Martin, 1994, p. 24). Thus, since shoplifting is the main cause of shrinkage (Cardone & Hayes, 2012, p. 22), retailers have to monitor shoplifters’ intentions (which can be only achieved by monitoring all shoppers) in order to obtain the most from their security investments, and enhance the store’s attractiveness by ensuring a high level of sales environment surveillance that is also appealing for shoppers (Bonfanti, 2014, p. 298).

To design an attractive shopping experience that is capable of meeting the customers’ latent sensorial, emotional, and psychological expectations without encouraging shoplifting, retailers have to employ surveillance solutions that are both secure and appealing to shoppers, for example: store design (e.g., locating registers in the middle of the store (Lin et al., 1994)), locking and security systems, personnel training, and technological systems. Bonfanti’s (2014) conceptual framework (Figure 7) shows that without providing a feeling of security, a retail store will be less attractive to consumers; it also suggests surveillance solutions that are both secure and appealing to consumers. Thus, appealing store surveillance systems can help in developing

retailer/consumer relationships, making it possible to consider surveillance solutions from the perspective of CSE (customer's shopping experience).

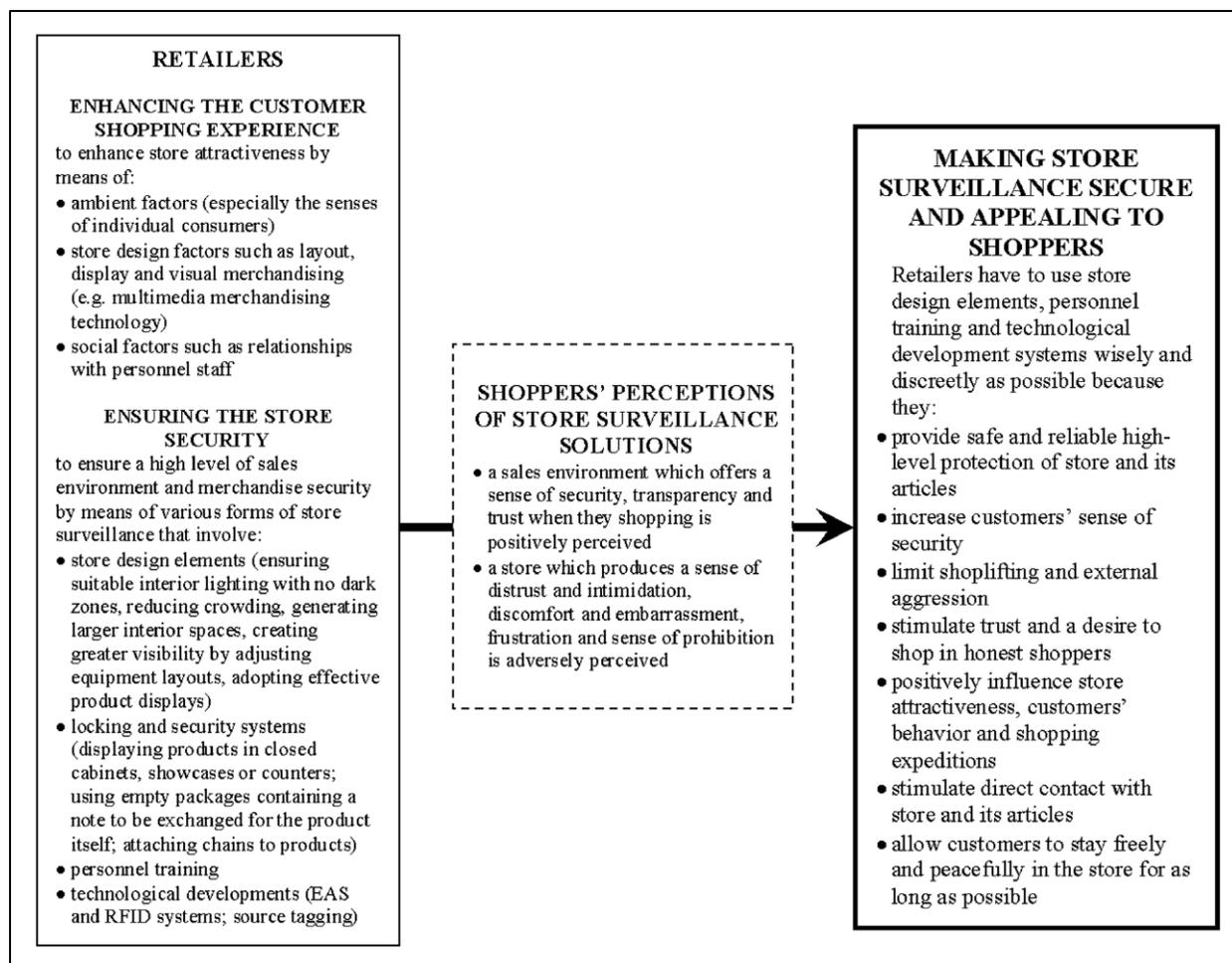


Figure 5 – How retailers make store surveillance both secure and appealing to shoppers (Bonfanti, 2014)

(3) To enhance profitability

To improve their profits, retailers need to provide a good customer shopping experience (CSE) and to use aggregated data (e.g., customer profiles and purchase history). Counting store shoppers (whether in a certain area or moving through a passage), understanding consumer behaviour, and monitoring how shoppers move about in a store's spaces and interact with products is very valuable (Paolanti, Pietrini, Mancini, Frontoni, & Zingaretti, 2020). Shoppers'

behaviour, moreover, can be observed within different store and shelf layouts to provide a fundamental insight for retailers who want to optimize the revenue/cost equation by enriching the in-store experience of their shoppers (Ferracuti et al., 2019). For example, by studying shoppers' in-store navigation and queuing times, retailers can develop a better customer experience, whether by reducing stock outs or queuing times, positioning staff in key store locations at times when customers want it, or improving navigation and layout so that shoppers can find what they are looking for quickly and easily (Ipsos Retail Performance, 2017). Thus, since physical stores need to adapt to shopper dynamics and emerging desires, shopper behavioural analytics have been receiving increasing attention over the last few years. Both individual (e.g., purchase behaviour and customer preferences) and aggregated insights (from movement patterns, hot spots, item popularity, interaction with digital touchpoints, and PoS data) from the collected information help retailers set the foundation for individualization and cost optimization capabilities and improve their service delivery which ultimately enhances their profit (Betzing, Hoang, & Becker, 2018, p. 1675).

(4) To ensure safety during the COVID-19 pandemic

On December 31, 2019, a new coronavirus, named COVID-19, was reported in Wuhan, China and quickly started spreading world-wide. In addition to a rising death toll and health concerns, the economic fallout has affected governments, businesses and consumers (Rae, 2020). The demand for retailance has increased, since retailers need to: secure their stores during temporary closures or reduced operating hours; ensure staff are in compliance with health and safety regulations to avoid government fines and reduce community transmission; and deliver a safe in-store shopping experience in which the retailer can control access and social distancing

and manage queues (Moe, 2020). Thus, retailers need to strike a balance between customer satisfaction and efficient security. To limit the spread of the highly contagious COVID-19 virus, retailers have deployed social distancing requirements, stringent cleaning protocols and capacity limitations as part of their plan to safely remain open. Playing a crucial role in this endeavour is technology that can help identify individuals who do not follow the new procedures and/or may have the virus before that person enters the premises. To assist retailers to operate their stores in compliance with COVID-19 regulations, some types of video surveillance include applications that help with occupancy management (by monitoring multiple entrances and exits to track real-time visitor access through automated displays at entry points), face mask detection (to ensure compliance with prescribed hygiene concepts) and social distancing monitoring (by detecting people and distances between them while providing additional visual analytics that allow retailers to improve current COVID-19 practices) (*SDM Magazine*, 2020). Some retailers have started collecting their customers' personal information to help with COVID-19 tracing, however, many security experts expressed their fear that such information can rarely be deleted securely, could get into the wrong hands, and could be even compromised in an unanticipated way (Macdonell, 2020).

Retail channels & systems

In retail, different surveillance systems (discussed later in detail) could be described in four different ways based on their attributes, and those categories are: direct vs. technologically mediated; overt vs. covert; real-time vs. over time vs. retrospective; and formal vs. informal, as illustrated in Figure 6.

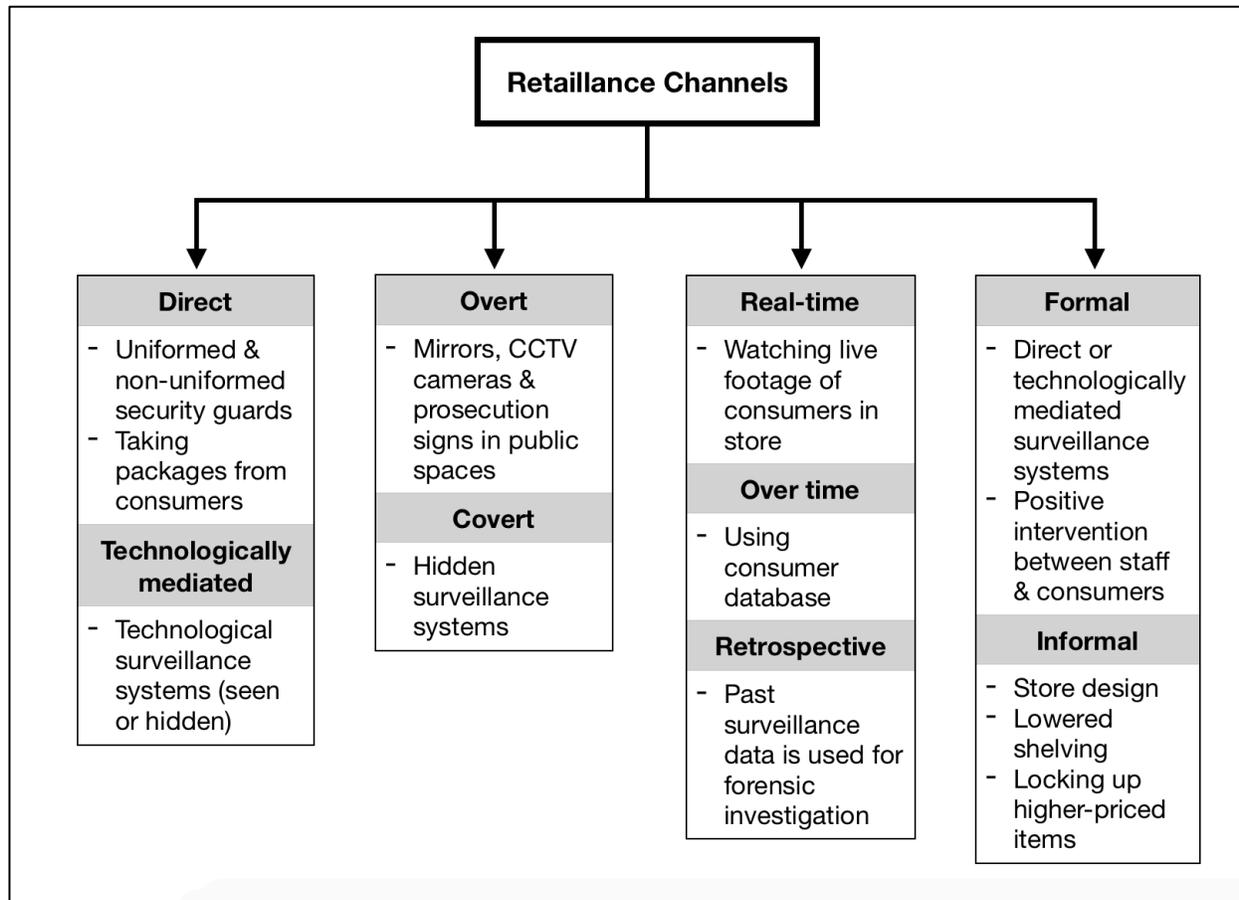


Figure 6 – Retailance channels

(1) Direct vs. technologically mediated

Retailance could be conducted face-to-face (e.g., uniformed and non-uniformed security guards and floor personnel) or through security systems (discussed in depth in the next section). It is worth mentioning that even though there is a human element behind all surveillance systems, surveillance elements will be considered direct only when the consumer is expected to be personally in touch with those operating the technology. For example, video surveillance is considered technologically mediated and not direct because retail consumers do not interact with the security staff operating the system (whether in real-time when the consumer is physically in the store or when the recorded footage is viewed later). On the other hand, there is the tagging

surveillance system. This Electronic Article Surveillance (EAS) consists of three components: the electronic tag, detector gates with built-in radio antennae that are typically located at store exits, and a control unit (DiLonardo, 2018); EAS tags sound an alarm if they pass the detector gates without being removed or de-activated by sales staff after purchase. EAS is considered both direct and technological mediated because when the alarms go on, the consumer is approached by security or store personnel who can ask to check the former's package(s).

(2) Overt vs. covert

Installed retail surveillance could be overt or covert. On the one hand, some retailers prefer not to hide cameras, mounting them visibly in public spaces (i.e., overt), such as check-out counters and common areas, to reinforce the feeling that someone is always watching and to serve as a visual theft deterrent. For example, to deter shoplifting at their new self-checkouts, Walmart uses cameras that reflect consumers' faces back to them, signs that warn people they are under surveillance, and employees positioned within view (Kaitlyn, 2018). On the other hand, some retailers opt to use concealed (i.e., covert) security applications in their retail operations to prevent theft, protect employees, customers and assets, and enhance operational efficiencies, and customer service training. In-store surveillance systems—whether employed overtly or covertly—include: video, audio, biometric, and visual guards.

(3) Real-time vs. over time vs. retrospective surveillance

An example of real-time monitoring, or surveillance, is watching live footage of consumers through video surveillance while they are in the retail store. Surveillance over time, however, is asynchronous, for example, database marketing in which collected consumer data

(e.g., spending habits, preferences and lifestyles) are analysed at a later stage. Retrospective monitoring occurs when past surveillance data is used (e.g., using surveillance CCTV footage for forensic investigations). According to the U.S. NRF (National Retail Federation) *Stores* magazine, retailers can now deter criminals more easily. With the police flooded with surveillance videos to investigate, retailers can now give their high-resolution image of people who committed crimes in their stores to Rite Aid, a U.S. company that uses a criminal identification system (known as “Captis I-4”) since 2017 and on whose website (solvecrime.com) retailers are given the ability to upload their photos and videos into the system, then those photos/videos are blasted out to a 50-mile radius around the area where the crime occurred as well as to multiple cities surrounding the crimes, crowdsourcing them on social media. When retailers offer rewards, tips are expected. This system has led to a 20 to 60% reduction in criminal incidents, usually lasting between four and six months (Stores, 2019a).

(4) Formal vs. informal surveillance

The concept of formal surveillance is based on the idea that increasing observation opportunities decreases crime. This encompasses observations by employees and retail loss prevention (LP) staff, including both uniformed security officers and undercover store detectives. Some studies have indicated that formal surveillance reduces consumers’ safety and security concerns at shopping centres. For example, the study by Overstreet and Clodfelter (1995) found that most consumers believe that a sense of security can be enhanced through formal surveillance, such as security guards. A survey by Pretious, Stewart and Logan (1995) revealed that retail managers perceive formal security systems as effective in reducing crime. Questioning the positive correlation between formal surveillance and security, Lee, Hollinger and Dabney

(1999) studied the relationship between crime and private security at shopping centres in the U.S.A.; they discovered that the level of criminal incidents at the shopping centres did not dictate the level of private security. To prevent consumers from feeling uncomfortable and intimidated while, at the same time keeping them safe, Coleman (2006) and Koistinen and Peura-Kapanen (2009) recommend promoting formal surveillance (such as guard patrols and CCTV cameras) as a discreet element as far as possible.

Informal (or natural) surveillance, on the other hand, is any technique that aids in viewing or observing the retail space, increasing would-be-offenders' sense of risk and their feeling of "being watched," and ultimately having a significant deterrent effect on them. This potential is facilitated by the design of the retail space that supports visual surveillance (Cardone & Hayes, 2012, p. 29) which ultimately yields significant reductions in shoplifting (Farrington, Bowen, Buckle, Burns-Howell, & Burrows, 1993). For example, to pre-empt and/or enhance informal retail security, retailers can plan the arrangement of merchandise and protective design through lighting and mirrors (Phillips et al., 2005, p. 68). Cozens, Saville and Hillier (2005) state that both formal and informal surveillance have proven effective in reducing both crime and the fear of crime.

Kajalo and Lindblom (2010a, 2011a) had a total of 161 grocery store retailers fill in a questionnaire, to create a comprehensive understanding of the ways in which retail entrepreneurs perceive the link between surveillance and customers' and employees' sense of security at the store level. Their study (2010, 2016) employs elements of Crime Prevention Through Environmental Design (CPTED) in their theoretical approach; CPTED is a multi-disciplinary approach to crime prevention that offers a wide range of strategies to prevent crimes (e.g., access control, surveillance, territorial reinforcement, and maintenance of the facility), and it asserts that

the design and management of the physical environment can encourage or discourage opportunities for crime (Kajalo & Lindblom, 2010a, p. 304). Studying how consumers view various surveillance practices in the context of shopping malls, they divide surveillance into “formal” (e.g., CCTV and motion detectors) and “informal” (which maximizes visibility and fosters positive social interaction) forms (Figure 7). Their study reveals that formal surveillance has a negative impact on customers’ feelings of security from the retailers’ point of view, while informal surveillance had positive impacts. In 2011, they used the same theory to study the effectiveness of formal and informal surveillance in reducing shoplifting in the retail store environment, reaching the conclusion that store personnel play a crucial role in preventing shoplifting and that, in general, the human factor remains very important in crime prevention; informal surveillance has a high capacity for crime prevention (Lindblom & Kajalo, 2011). They reach similar results in another research study (Kajalo & Lindblom, 2010b, 2011b) which focuses on Finnish grocery stores: in addition to store environment (e.g., clean and well-lit premises), security guards (i.e., formal surveillance) and activity of the personnel (i.e., informal surveillance) are the most effective ways for reducing crime, vandalism, disturbance and shoplifting. In 2016, Kajalo and Lindblom used data gathered from a survey of 200 shopping mall visitors to show that consumer experience of safe retail environments (i.e., free of crime such as shoplifting, employee theft and vandalism) reflects the distinction between informal, unnoticeable surveillance (e.g., maximizing visibility and well-lit environment) and formal, visible surveillance (e.g., security guards, or security hardware such as CCTV and motion detectors). According to this research, consumers identified five key surveillance practice preferences: clean and well-lit premises, well-designed parking, surveillance technology, sales

personnel and hard crime protection. In this study, Kajalo and Lindblom modified the CPTED theory to reflect the context of shopping malls.

Form of surveillance	Definition	Practical implications at the store level
Formal surveillance	Formal surveillance aims to produce a deterrent threat to potential offenders through the deployment of personnel whose primary responsibility is security (e.g. police, security patrols) or through the introduction of some form of technology, such as CCTV	<ul style="list-style-type: none"> Arrange proper security training for sales staff Hire private security guards Invest in security hardware (e.g. CCTV surveillance systems)
Informal surveillance	Informal (or, alternatively, natural) surveillance limits the opportunity for crime by increasing people's perception that they can be seen. Informal surveillance is promoted using physical features and activities in a way that maximizes visibility and fosters positive social interaction and control	<ul style="list-style-type: none"> Keep store well lit Eliminate hiding spots Place high-risk targets in plain view of sales staff Create a store environment that maximizes visibility Foster positive social interaction between sales staff and customers

Figure 7 - Formal and informal surveillance: Definitions and practical implications at the store level (Kajalo & Lindblom, 2011)

In an exploratory study that used a survey questionnaire (i.e., self-report data) to examine retail managers' attitudes towards shoplifting and identify how they can deal with it, Lin et al. (1994) concluded that although store layout design can reduce shoplifting (for example, informal surveillance by locating registers in the middle of the store), and using security measures—such as guards and taking packages from customers (i.e. direct surveillance); mirrors, TV cameras, and prosecution signs (i.e. overt surveillance); and lowered shelving and locking up certain higher-priced items (i.e. informal surveillance),—can ward off shoplifters, they also make the shopping experience more unpleasant for honest customers. Another empirical research study

(Peek-Asa, Casteel, Kraus, & Whitten, 2006) looked at how strategies to protect employees at the store level, such as protective barriers that isolate employees, could have negative effects on customers and might even leave them vulnerable.

Although it can be argued that formal surveillance may be necessary to combat criminal behaviour, there is a major concern that these investments may make honest consumers feel insecure, and even increase their sense of an environment of hostility within the store. On the other hand, and although some may argue that informal surveillance has only limited utility to prevent crime because potential offenders are not deterred by any noticeable means, in practice, informal surveillance is promoted using physical features and activities that maximize visibility and foster positive social interaction (Welsh, Mudge, & Farrington, 2009). Kajalo and Lindblom (2016) group consumers into four different clusters, based on which surveillance elements most contributed to their sense of security when visiting shopping malls and their preference towards surveillance: (1) formal surveillance; (2) architectural design; (3) well-designed parking; and (4) personnel and hard crime protection. In conclusion, to decrease crime in their stores and ensure that consumers feel secure and, at the same time, have a good shopping experience, retailers have to employ a mixture of formal and informal surveillance.



Figure 8 - Comic, credit: Joe Sutliff (Fairchild, 2006)

Retailance systems

To understand the implications of retailance and its increasing dependence on technology, the following surveillance systems are discussed: (1) in-store surveillance systems (video, audio, biometric and virtual guards), (2) tagging, (3) collecting phone numbers and emails, (4) loyalty programs, (5) free Wi-Fi and tracking technology, (6) personalised advertising, (7) radio frequency identification (RFID), (8) tracking returns, and (9) geo-fencing. A matrix that explains how these systems fall under the various retailance channels is provided in Table 1 below.

Retailance Systems	Retailance Channels											
	Direct	Technological		Overt	Covert		Real-time	Over time	Retrospective		Formal	Informal
Video		X		X	X		X	X	X		X	
Audio		X			X		X	X	X		X	
Biometric		X		X	X		X	X	X		X	
Virtual guards		X			X		X				X	
Tagging	X	X		X	X		X				X	
Phone no. & emails		X		X	X		X	X			X	
Loyalty programs		X		X	X		X	X			X	
Wi-Fi & tracking		X		X	X		X	X			X	
Personalized advertising		X		X	X		X	X			X	
RFID		X		X	X		X	X			X	
Tracking returns		X			X			X			X	
Geo-fencing	X	X		X	X		X	X			X	X

Table 1 – A matrix of retailance channels and systems

(1) In-store surveillance systems

In the U.S., retailers experienced an average shrinkage rate of 1.62% (an all-time high), which cost the economy \$61.7 billion in the fiscal year 2019. Furthermore, shoplifting apprehensions, prosecutions and civil demands are on the rise (National Retail Federation, 2020b). Shoplifting has long been a major problem, to the extent that it was considered a capital offence in 18th-century England (Tickell, 2010, 2015). In 2014, one in eleven people in the U.S. was a shoplifter, and more than 10 million people had been apprehended for shoplifting over the previous five years (National Association for Shoplifting Prevention, 2014). In 2020, Organized Retail Crime (ORC) in the U.S. cost the retail industry an average loss of \$719,548 per \$1 billion in sales, in addition to losses incurred by shoplifting (National Retail Federation, 2020).

Common types of ORC include organized shoplifting, refund or return fraud and counterfeit merchandise, counterfeit money, credit card fraud, traveler cheques fraud, gift card fraud, identity theft, altered or fake receipts, altered or fake price tags, retail e-crimes (e.g., web app attacks, point of sale (POS) attacks, and payment card skimmers), theft of cash, burglary or smash and grabs of quality merchandise, and cargo theft (McGourty, 2015). To combat ORC threat, many retail stores install technologically mediated overt and/or covert surveillance systems which are designed to help in identifying incidents of retail crime, such as shoplifting, employee theft, burglary (i.e., breaking into closed retail stores), and violence that could be either physical (e.g., violent acts between customers or by disgruntled customers towards staff) or verbal (including shouting, swearing, threats and intimidation). In their 2020 survey, the National Retail Federation in the U.S. stated that retailers are “devoting more resources to fight shrink in the coming year, with a majority of those enhancements coming technology

investments,” such as remote monitoring technology, upgraded POS systems, and refund history tracking programs (National Retail Federation, 2020b).

Video surveillance: Retail companies first began adopting video surveillance systems that used CCTV (Closed Circuit Television) cameras in the 1970s. By using video cameras to transmit a signal to a certain location, on a limited set of monitors, these cameras offered visibility into retail crime, but the footage was primarily used for forensic investigations (i.e., retrospectively). Those cameras only contributed to retail crime prevention when complemented with signage (which could potentially deter criminals). In 1976, the use of microchip technology and charge-coupled device (CCD) technology made round-the-clock surveillance in low light situations possible. In 1996, there was a decline of CCTV and the increasing use of IP (Internet Protocol) cameras that could send and receive information across computer networks, and webcams. Although IP cameras offered increased convenience, better resolution, and the ability to save and record without the use of film (since recording could be stored directly to a drive or the cloud), it did not offer greater capacity to deter criminals. Since 2001, internet-based surveillance cameras relying on wireless communication are the most common (Rick, 2013). According to the National Retail Federation, live customer CCTV was one of the top five most-used LP (Loss Prevention) systems in 2020⁴ (National Retail Federation, 2020a). Retail stores now leverage CCTV system capabilities (Figure 9) to achieve more goals beyond loss prevention, such as: heat mapping, people counting (Figure 10), and monitoring queue times. Those surveillance capabilities also improve the consumer’s shopping experience, for example, ensuring they can

⁴ The other four loss prevention systems in use were burglar alarms, digital video recorders, armoured car deposit pickups, and POS data mining.

get through checkout lines faster and avoid crowded aisles. Thus, the function of video surveillance has evolved from mere crime prevention to cover new retailer goals, e.g., to ensure a better shopping experience.



Figure 9 - CCTV cameras (Source: <https://advancedoverwatch.com/tips-advice/retail/cctv-systems-retailers-loss-prevention-beyond/>)



Figure 10 - CCTV counting people (pathmap) (Source: <https://advancedoverwatch.com/tips-advice/retail/cctv-systems-retailers-loss-prevention-beyond/>)

Video surveillance could be either overt (with surveillance cameras mounted visibly and/or consumers alerted to its presence), for example, in IKEA stores (Figure 11) and Walmart (Figure 12), or covert (e.g., when hidden cameras are installed in ceilings and sensors are installed near fitting rooms to learn how many customers pass through the doors and where they tend to go) (Rosenbloom, 2010). Although video surveillance may be viewed negatively by consumers, research shows that it is highly effective in improving the retailer's sales outputs (i.e., profitability) by analyzing consumer behaviour (Cumming & Johan, 2015). In 2018, in an effort to protect their retail employees from increasing in-store violence, Walmart's U.K. supermarket chain Asda began outfitting security guards with body cameras that are quite similar to those used by law enforcement (Figure 13). Compared to CCTV, body cameras offer better evidence-gathering because they are not static and they capture both video and audio from the perspective of the retail employee (Schulz, 2019). Videos are then relayed to Asda's head office in Leeds to help police prosecute offenders (Hayward, 2018).

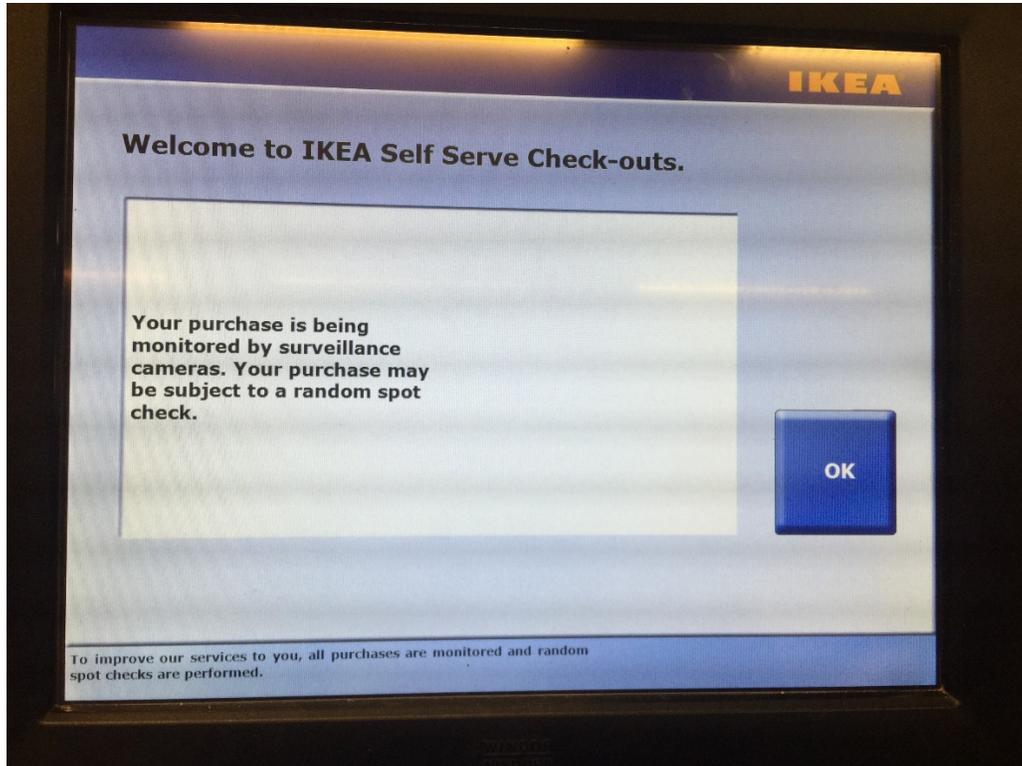


Figure 11 - IKEA, Ottawa, self-serve check-outs (Image: Nada Elnahla, 2019)

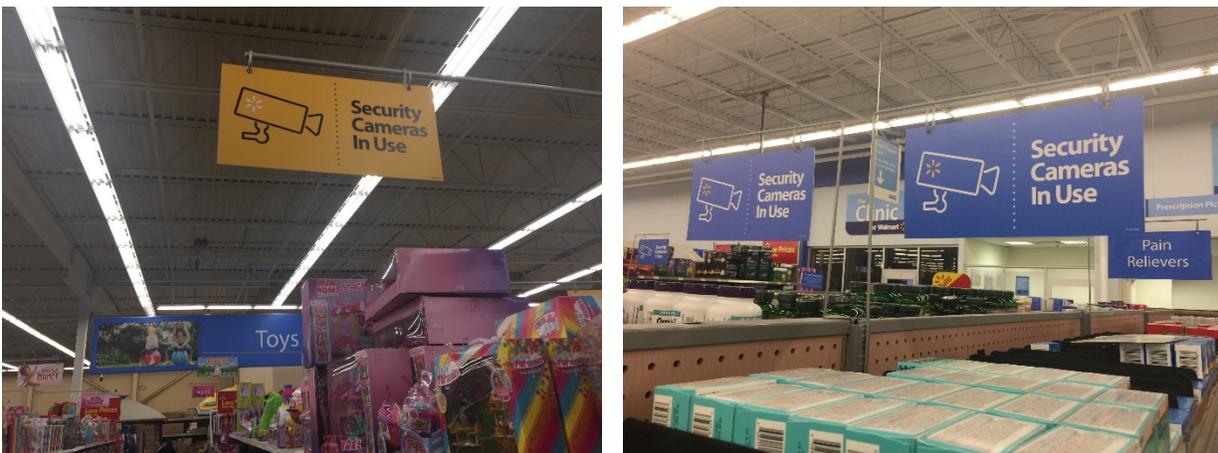


Figure 12 - Security cameras used overtly in Walmart Supercentres, in Ottawa Train Yards (on the left) and Stittsville, ON (on the right) (Images: Nada Elnahla, 2019)



Figure 13 – Asda bodycams (Source: *Mirror*, <https://www.mirror.co.uk/news/uk-news/supermarket-workers-given-body-cameras-12918172>)

A covert surveillance technology (technologically mediated in real-time and over time) is PrimeSense (developed by Shopperception, a small company founded in Buenos Aires with an office in New York City). Working in real-time, it uses 3D sensors and proprietary algorithms to detect shoppers, following them while they are in sensor reach (Figure 14). The technology, therefore, allows retailers to understand precisely what shoppers are doing in front of a retail shelf, in addition to providing advanced and highly personalized offers to customers who opt into loyalty programs (remembering their previous buying habits and predicting what they likely want to buy). The company markets this technology by pinpointing the four advantages it gives to retailers: (1) to improve shopper understanding; (2) to level the battlefield with e-commerce; (3) to boost revenue; and (4) to grow their own brand share (“Solutions for retailers,” n.d.). Knowing that personal privacy is an important feature to most consumers, Shopperception claims that their sensor cameras do not show the actual shopper (only an infrared type blur) and do not record any video. In 2013, Walmart and Heineken started testing this analytics tool in

their Argentinian stores (Israel, 2013). According to the Shopperception website, they now have partners in the U.S., South America, Europe, and Asia.



Figure 14 – How Shopperception works (Source: <https://www.shopperception.com/>)

Luxury stores have also started using EyeSee (sold by Italian mannequin maker Almax SpA in collaboration with Kee Square, a computer vision firm), a mannequin with a camera and facial recognition software embedded in one eye (Figures 15 and 16). This new covert surveillance system offers much data (e.g., consumers' age, gender and ethnicity) since it is closer to shoppers and resides at eye-level with them. When used, these mannequins help retailers shape their marketing, merchandising, signage and promotions; for example, a retailer launched a children's line after noticing that more than half of its mid-afternoon traffic was made up of children, and another placed Chinese-speaking personnel at one of its storefront doors when they learned that a third of the visitors who entered the store after 4 p.m. were Asian (A.

Lee, 2012; Petersen, 2013). So far, Almax has refused to reveal which retailers are trying its “spy” mannequins, and only said that those retailers are in both Europe and the U.S. Meanwhile, they have been working on adding microphones to the mannequins so that they could recognize consumers’ comments about merchandise on display. Fearing that the news of using this technology might backfire and alienate their consumers, some retailers such as Benetton Group, Burberry, and Nordstrom, have denied using EyeSee (*Daily Mail*, 2012).



Figure 15 – A screenshot from Kee Square’s promotional video “The Smart Mannequin is Born” (https://www.youtube.com/watch?time_continue=31&v=9fr9X4f9kXA)

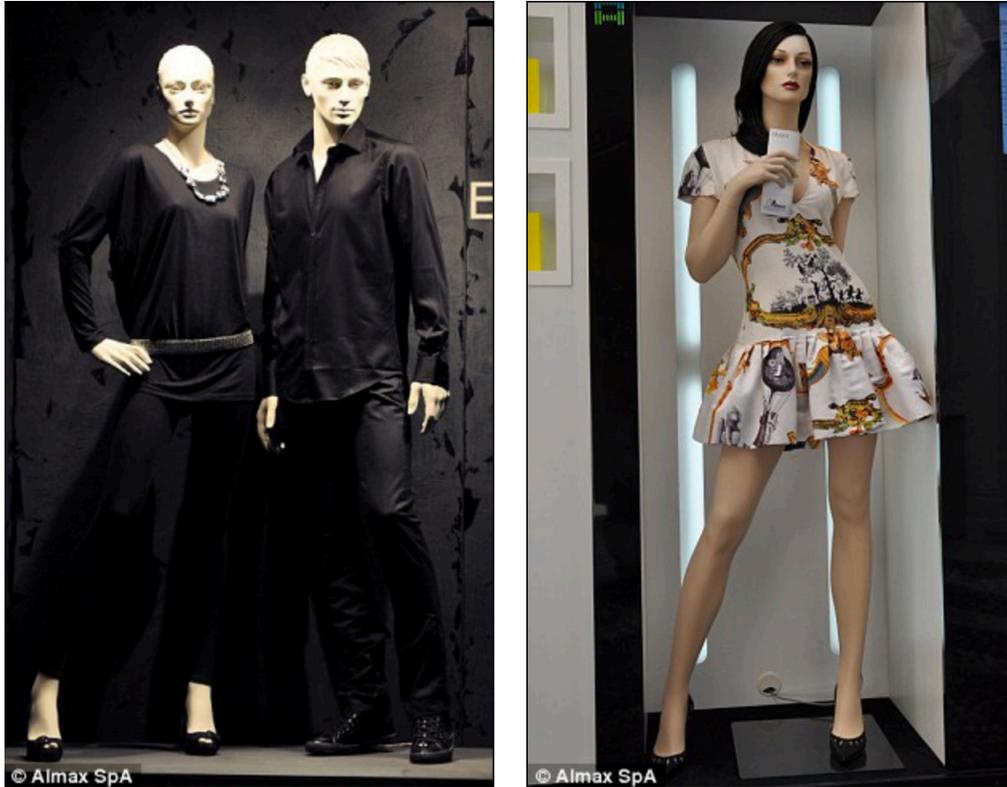


Figure 16 – The US\$ 5,130 surveillance mannequin (Source: *Daily Mail*, <https://www.dailymail.co.uk/sciencetech/article-2235848/The-creepy-mannequin-stares-Fashion-retailers-adapt-airport-security-technology-profile-customers.html>)

Faced with a decline in casual dining, the U.S. Outback Steakhouse franchise has recently announced it would begin testing a new surveillance technology software (called Presto Vision) designed to maximize employee efficiency and performance in its Portland, Oregon, location (Figure 17). Taking advantage of pre-existing surveillance cameras already installed in the restaurant, the system utilises machine learning to monitor and analyze customer traffic in the lobby, determine how many customers leave if tables are not immediately available, calculate wait time for customers to receive their food and determine how attentive staff are to customers (Matsakis, 2019). Obviously, the use of surveillance technology such as this to optimize the restaurant industry has implications for customer satisfaction as well as for the management of

service employees. It also raises important questions about privacy for both customers and employees.

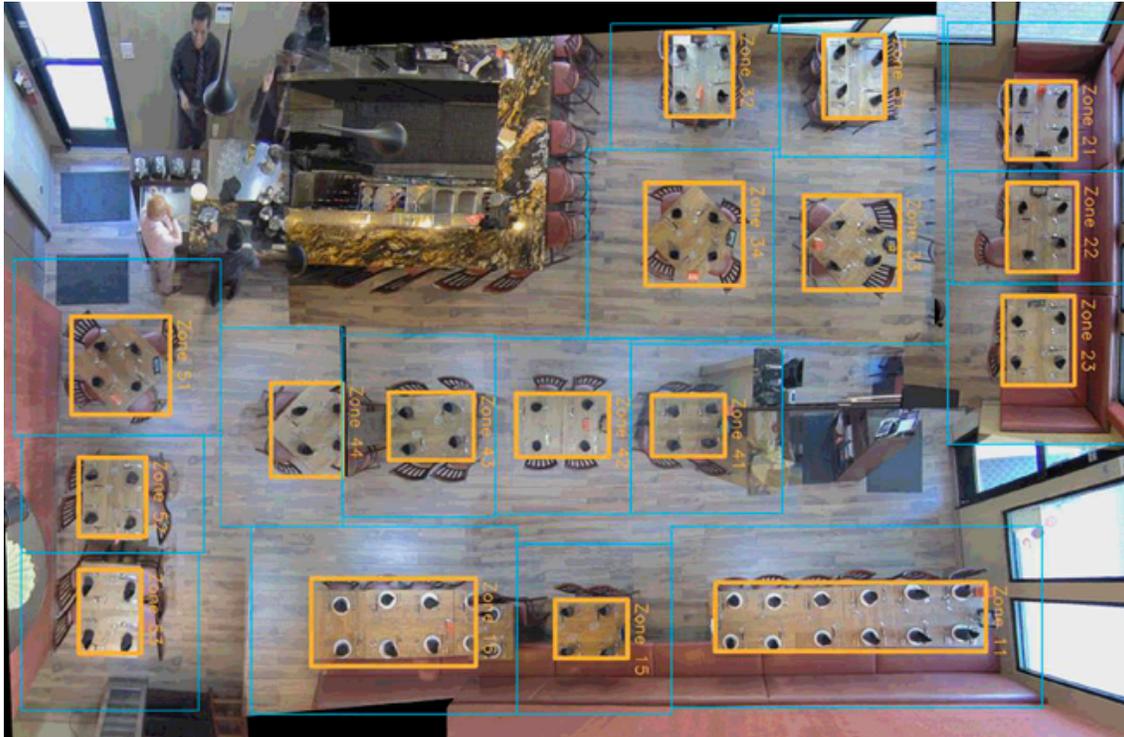


Figure 17 – Presto Vision software (Source: Presto, <https://presto.com/2019/10/16/presto-launches-computer-vision-product-for-real-time-restaurant-operations-insights-2/>)

To help retailers ensure the safety of their consumers and workers during the COVID-19 pandemic, another type of video surveillance, that is both covert and mediated in real-time, is used. Thermal imaging camera systems (Figure 18) have the capability of detecting an elevated temperature in consumers or employees prior to entering the store (Ouellette, 2020).



Figure 18- Thermal imaging camera (Source: Ouellette, 2020)

To sum up, there are different types of video surveillance that can be leveraged in a retail environment, such as CCTV cameras, body cameras, a combination of 3D sensors and algorithms, mannequins with cameras and facial recognition software embedded in their eyes, and thermal imaging cameras. Whether overt or covert, those surveillance systems help retailers boost their revenue through crime prevention, reshaping retailers' marketing, and ensuring a better shopping experience.

Audio analytics: Similar to video analytics, audio analytics aid in responding to situations in real time, triggering alerts when predetermined thresholds are reached. Covert audio surveillance can track whether a gathering of people is turning volatile by monitoring voices for aggression and detect other audible indicators of potential security threats like gunshots or glass breakage (sound intelligence, 2021). In 2018, Walmart patented audio surveillance technology that would focus on minute details of the shopping and checkout experience in their stores (e.g., beeps of item scanners, the rustling of bags, how long shoppers wait in line, and how employees greet customers) but that could essentially spy on cashiers and customers by collecting audio data (i.e.,

conversations). This has raised questions about how the recordings of conversations would be used and whether the practice would even be legal in some Walmart stores (Silverstein, 2018).

Biometric surveillance: Introduced in the 2000s, biometric surveillance technology revolutionized surveillance by offering the ability to automatically identify retail criminals when they walk through the door (in real time). It offers the advantage of being able to automatically match customers against a database of known criminals using a *facial recognition* algorithm (Figure 19). Thus, when a match occurs, the loss prevention team(s) receive(s) instant alerts and it is up to them to monitor the individual, call law enforcement, or take other actions (and that action can take place in real-time when the suspected consumer is still in the store, or over time when an action is taken at a later stage, for example, preventing the same consumer from entering the retail store); this becomes a combination of direct surveillance (real guards are deployed on the scene) and technologically mediated surveillance (through the use of tracking and identification technology). Designed to not only reduce loss but keep customers and loss prevention professionals safer, using facial recognition has been shown to reduce shoplifting by 20% and in-store violence by 91% (“Internal data from FaceFirst,” n.d.). In the wake of the iPhone X launch in November 2017, which enables consumers to use face recognition to protect their own data security, American adults appear to be increasingly becoming more comfortable with similar technology being used to protect private and public spaces (West, 2018).

FACEFIRST FACE RECOGNITION

IDENTIFY THREATS AND PREVENT RETAIL CRIME

With face recognition that is accurate, scalable, private and secure

ALEX WOLF
OFFER CUSTOMER SERVICE
Documented Shoplifter
7 Visits at 3 Locations
• STORE #225
• STORE #223
• STORE #245

THE LEADER IN FACE RECOGNITION FOR RETAIL SECURITY

- Deep Retail Experience**
FaceFirst understands and solves the operational challenges unique to retail deployments.
- Unlimited Locations**
Scale without performance loss, sharing data across unlimited locations and users.
- Camera Agnostic**
FaceFirst works with virtually any camera provider or camera-enabled device.
- Accuracy in the Wild**
Maintains high performance with challenging angles and lighting conditions.
- Real-Time Alerting**
Configurable and actionable match alerts using mobile push notifications, SMS and email.
- Privacy Leadership**
The industry leader in privacy-by-design methodology, best practices and thought leadership.

DESIGNED, DEVELOPED AND SUPPORTED IN THE UNITED STATES

PROVEN RESULTS

34% REDUCTION IN EXTERNAL SHRINK

91% REDUCTION IN-STORE VIOLENCE

Figure 19 – The face recognition fact sheet for reducing external shrink (Source: FaceFirst)

Biometric surveillance has been recently incorporated in the A.I. Bar, a British pub powered by the A.I. firm DataSparQ (DataSparQ, 2019; Filippone, 2019). Using facial recognition to place drinkers in a dynamically intelligent queue (Figure 20), the bar promises better customer service: customers no longer need to physically push in at bar queues, ordering drinks becomes less intimidating for solo drinkers and females, automatic age verification speeds up ID checks, and strain is eased on the bar staff during peak times making the service more efficient. By providing vital data including orders per hour, this facial recognition technology will help pub and bar owners to understand the demand for their service, flag underage customers, optimise their staffing requirements, become more efficient, and ultimately, become

more profitable. However, some consumers worry about the risk to their personal information posed by the technology.

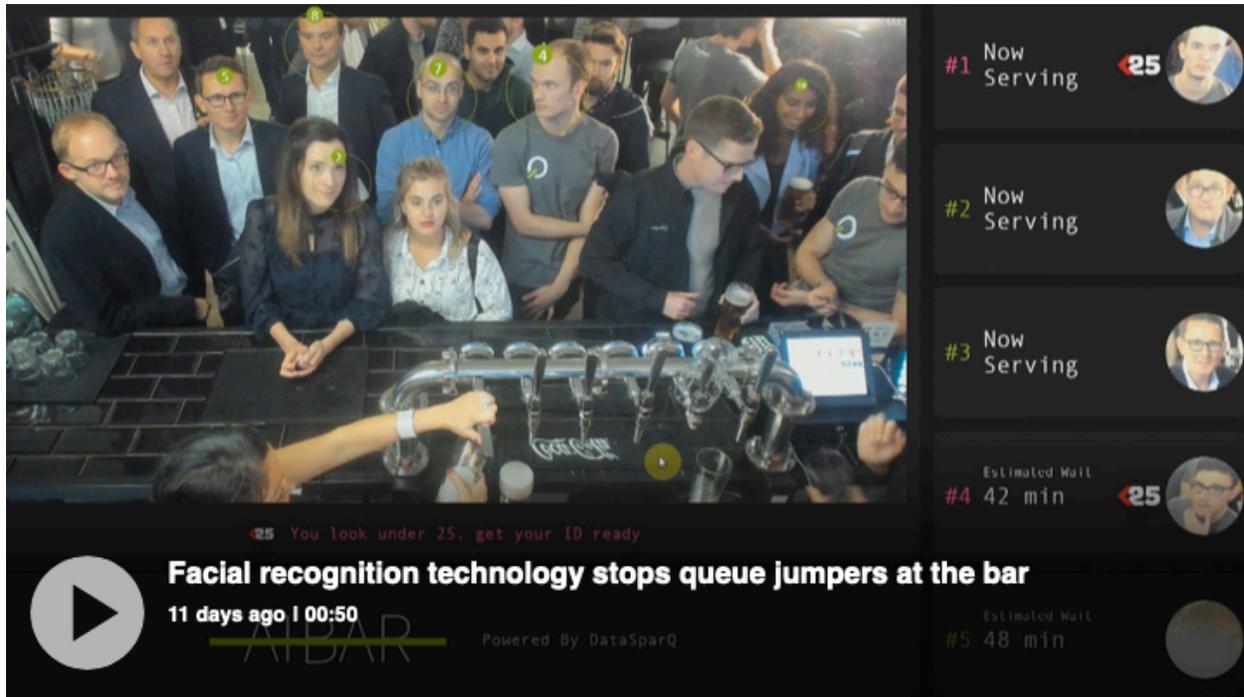


Figure 20 – Facial recognition used in the A.I. Bar (Credit: CBC News, <https://www.cbc.ca/news/science/facial-recognition-london-pub-lineup-1.5317769>)

Another use of facial recognition technology is currently being implemented in China where Alipay—the financial arm of ecommerce giant Alibaba—has been installing facial payment devices in 100 cities (*The Guardian*, 2019). The service has been also debuted in Kentucky Fried Chicken (KFC) in the eastern Chinese city of Hangzhou (Gilchrist, 2017). This technology allows customers to make a purchase simply by posing in front of point-of-sale (POS) machines equipped with cameras, after linking an image of their face to a digital payment system or bank account (Figure 21). The system allows consumers to conveniently pay quickly compared to waiting in checkout lines. Ironically, the reason behind the modest numbers using this technology is not due to the concerns over data security and privacy, but due to vanity, for

60% of poll respondents complained that scanning their faces for payments made them feel “ugly.” In response, Alipay pledged to introduce “beautifying filters” into the Alipay cameras.



Figure 21 – An Alibaba employee demonstrates ‘Smile to Pay,’ an automatic payment system that authorize payment via facial recognition (Credit: Alex Wong | Staff | Getty Images)

The future of biometric in-store surveillance entails implanted devices in consumers’ bodies that would communicate with retailers as they walk down the aisles and inspect various items, signaling whether or not the consumer likes a product (by calculating how long it was held by the consumer) and whether the consumer is cautious or nervous when looking at a product price, leading to the retailer offering a discount on the product in order to reduce the nervousness and lead to the act of purchasing. Although this technology has not been invented yet, Brandon Fischer, director of predictive insights at the influential GroupM Next consultancy, predicted that by 2028, half of Americans (and by 2054 nearly all Americans) will carry such devices in their bodies (Fischer, 2015; Turow, 2017, p. 8).

Virtual guards:

Compared to on-site physical security guards that are usually noticeable by consumers (i.e., overt surveillance), virtual guards are located off-site (i.e., covert surveillance). They are trained operators, on duty around the clock, at a central station who watch over a site (e.g., retail store) remotely to improve security. They observe the location, keep an eye on lone workers (for example, retail workers who have to work alone at night in such places as gas stations with convenience stores), and check in on assigned consumers' locations using video camera feed from their desktop monitors. When a problem is detected, virtual guards can direct intruders to leave the property using pre-recorded messages, strobe lights and sirens, while simultaneously summoning an on-site guard or local law enforcement to respond to the scene (ECAMSECURE, 2021).

(2) Tagging in a retail setting

To face an escalating crime problem, tagging systems (an example of overt surveillance that is also known as electronic article surveillance, or EAS) first began appearing in the 1960s (Dawson, 1993), and since then, have been used in retail settings as a form of subtle control over shoppers, deterring the casual shoplifter from offending, and assisting the detection of shoplifters in the act of theft. Since tagging does not completely stop theft in the sales area, it is usually used in conjunction with other security devices. Compared to other surveillance alternatives—such as CCTVs, loop alarms (which are controllers with a built-in siren connected to a continuous loop of cable that can be passed through the items to be protected, providing security for products exhibited in an open space while allowing consumers to try out potential purchases), and guards—research studies (Handford, 1994) have shown that EAS is not perceived by the public

as a threat. However, when tags are not deactivated at the checkout counter (because of unprofessional staff or technical problems), resulting in the setting off of alarms (i.e., false alarms) in real-time and consumers being stopped by guards and asked to show receipts for the goods in their possession (i.e., a form of direct surveillance), consumers can feel discomfort and embarrassment (for being viewed as likely thieves) (Bonfanti, 2014). In addition, 5% of consumers who have paid for items and yet have been stopped by store guards and asked to show receipts for the goods in their possession become irate and upset at being challenged, which could jeopardize their future shopping habits (but what kind of effect was beyond the scope of this study) (Handford, 1994, p. 180). Based on a survey of 250 individuals, another unintended effect of errant (i.e., false or accidental) alarms is that 16% of consumers may never shop again at a store that subjects them to an errant EAS alarm (Dawson, 1993).

Beyond the direct costs of purchasing, installing, and operating an EAS system, EAS has two major drawbacks. For one, it is not a deterrent to employee theft (itself accounting for a major volume of shrinkage). Secondly, and more importantly, there is a loss of goodwill when shoppers trigger the system through no fault of their own. The unexpected setting off of an alarm can draw unwanted skepticism from other shoppers and questioning from store personnel, leading to unaccounted costs of lowered goodwill, negative word-of-mouth, loss of a future stream of revenue, and even legal actions brought by patrons (Dawson, 1993). In 1994, at the request of and in cooperation with a retailer, Matthew Handford studied and evaluated the effectiveness of the electromagnetic tagging system by reviewing records and stock control audits maintained by four stores in the U.K. and conducting interviews with store managers, stock controllers, and security guards. Handford's study shows that effective administration is a prerequisite for the effective operation of the technology.

(3) Phone number and email

A technologically mediated surveillance system, the collection of consumers' phone numbers and email addresses can be considered both an overt and a covert retailance channel. It can be described as overt because the consumer has to provide the information him/herself, and at the same time, it can be considered covert because most consumers do not know the retailance implications connected to such information. Once a consumer gives up their phone number and/or email, they are handing over all purchasing information to the retailer and allowing the latter to combine this information with internal and external databases to build a more sophisticated and detailed picture of the consumer. It is then up to the retailer's sophisticated software to discover what the consumer's future may hold and to ensure that the former plays a part in it.

After COVID-19 became a pandemic, some establishments started collecting their customers' personal information to help with COVID-19 tracing. For example, in Ontario, Canada, such a regulation came into effect on August 7th, 2020, and is applicable to bars, restaurants and tour boat operators, instructing them to "record the name and contact information of every patron who enters an indoor or outdoor dining area in the establishment . . . [and] maintain the records for a period of at least one month." Although many security experts expressed their fear that such collected information can rarely be deleted securely, could get into the wrong hands, and could be even compromised in an unanticipated way (Macdonell, 2020), some retail stores began to copy this procedure, like the Habitat for Humanity ReStore (Figure 22) in which an unsupervised list of phone numbers is left next to the hand sanitizer station. The only difference is that adding information to that list is voluntarily.

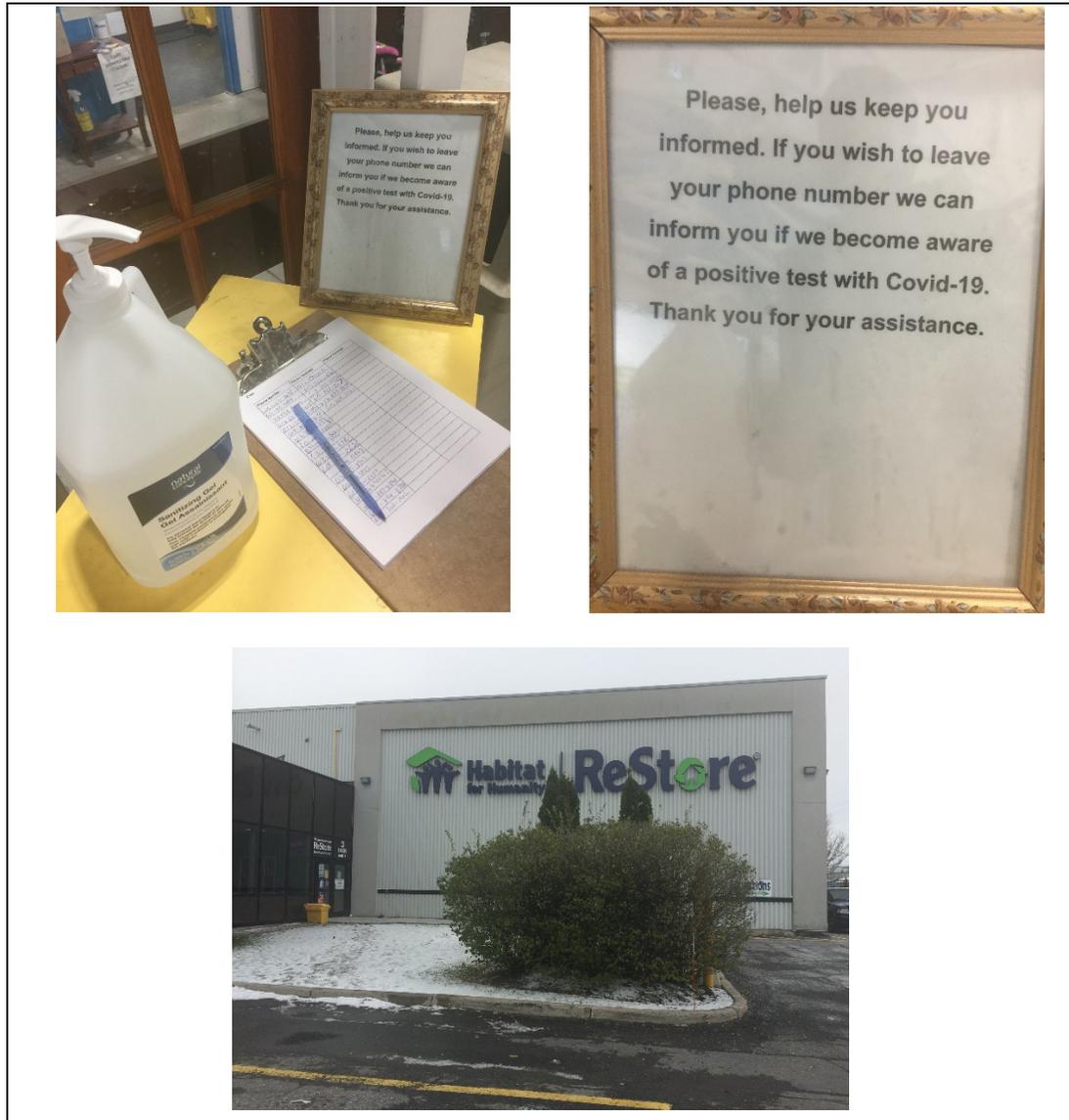


Figure 22 – Habitat for Humanity ReStore in Stittsville, Canada (Images: Nada Elnahla, November 3rd, 2020)

(4) Loyalty programs

The idea behind loyalty programs can be traced back to the desire to reward customers for their patronage. Early examples of programs that provided discounts and encouraged future purchases are tokens, extending credit, trading stamps and proprietary currency.

Tokens: The earliest example of a loyalty program was possibly the “baker’s dozen” as early as 1793, when a merchant in Sudbury, New Hampshire, gave away copper tokens with purchases that could be later redeemed for goods in his store (Nagle, 1971). Nowadays, the “baker’s dozen” is a marketing term that denotes giving thirteen measures of a good when only twelve are purchased⁵.

Extending credit: In the late 19th century, when merchants wanted to find ways to encourage their consumers’ loyalty, one major way was extending credit for their patrons who had exhibited the tendency to buy impulsively and in large quantities and who showed more loyalty to their stores; of course, this offer meant that stores had to profile the consumers to ensure they would pay their bills (Turow, McGuigan, et al., 2015). While retailers first extended credit to their wealthiest patrons, by 1910, virtually all large retailers were promoting “charge” programs to a broader segment of their customers. Some even solicited charge card account holders to recommend up to three friends and acquaintances worthy of “the privilege” of opening a charge account (Leach, 1994, p. 124).

Stamp cards: Retailers have often bestowed frequent shoppers with particular benefits, including punch or stamp cards that require customers to obtain a prerequisite number of punches or stamps through previous purchases in order to receive a free item or a purchase discount (a marketing practice that still exists today). Trading stamps—given to consumers for their purchases and later redeemed in cash or merchandise—were first used in a department store in the U.S. Midwest, as a new method of sales promotion, in 1891 (Strum, 1962). In the second

⁵ The term “baker’s dozen” possibly comes from the 13th-century practice of bakers adding a thirteenth loaf of bread to a batch of twelve loaves in order to avoid punishment for accidentally selling underweight bread.

half of the 1950s, most supermarket chains and groups of independents adopted trading stamps programs (Figure 23) for several reasons: (1) the program helped supermarket chains to differentiate themselves from their non-chain competitors, allowing for “non-price competition” (Barber, 1960); (2) like most premium plans, to the consumers, the value of merchandise traded was greater than a cash discount; (3) it helped consumers to save routinely; (4) it gave chain stores the upper hand over independent supermarkets; and (5) it created a synergistic effect when non-competitive stores (e.g., supermarkets, gas stations, drug stores, laundries, and department stores) distributed a particular trading stamp (Allvine, 1969). By the 1960s, when their effectiveness decreased because most food retail businesses used them, supermarkets increasingly turned to extra stamp give-away programs (e.g., bonus stamps on weekends and/or for featured products). After the peak years of stamp distribution (1962-64), there was a trend amongst shoppers to go back to the basics: “merchandising of groceries at the lowest possible cost” for different reasons: (1) shoppers became more price conscious; (2) the poorly staffed redemption centres were less attractive to shoppers than the then-new convenient suburban shopping centers with wide assortment of merchandise; (3) the licking and pasting of stamps had become more disagreeable to shoppers who saw themselves as part of an affluent and modern society; and (4) the novelty of saving stamps diminished with time (Allvine, 1969, pp. 50–51). By the 1980s, stamp programs were in decline. The period from the mid-1980s through the 2010s represents a period of transition from seeing consumers through a broad demographic lens to monitoring them as individuals who give off streams of data, often in real time (Turow, McGuigan, et al., 2015). By the year 2000, and supported by technology, the reward-for-patronage idea behind stamps evolved into loyalty card programs (GreedyRates, 2018; Withiam, 2000), for example, Shoppers Drug Mart allows its customers to earn points through their PC

Optimum program, and regularly holds events for bonus point collecting and redemption. Thus, with loyalty programs, retailers could not only reward consumers for their loyalty and patronage, but they can also collect the latter's more personal and shopping information.



Figure 23 - Advertisement for trading stamps that applauds the wife for her thriftiness and shopping skill (Source: <http://www.studioz7.com/stamps.html>)

Proprietary currency: Another form of loyalty programs is the distribution of proprietary currency that can be applied directly against the cost of any future purchase, for example, Canadian Tire “money” (CTM), a type of cash bonus coupons used by the Canadian Tire Corporation. This program was first introduced in 1958 at Canadian Tire gas bars but it was so

successful that in 1961, it was extended to their retail stores as well, becoming the most successful loyalty program in Canadian retail history and a collector phenomenon (H. D. Allen, 2006). Starting from April 2018, consumers can collect the digital equivalent of CT Money[®] through the Triangle Rewards loyalty program (Figure 24).

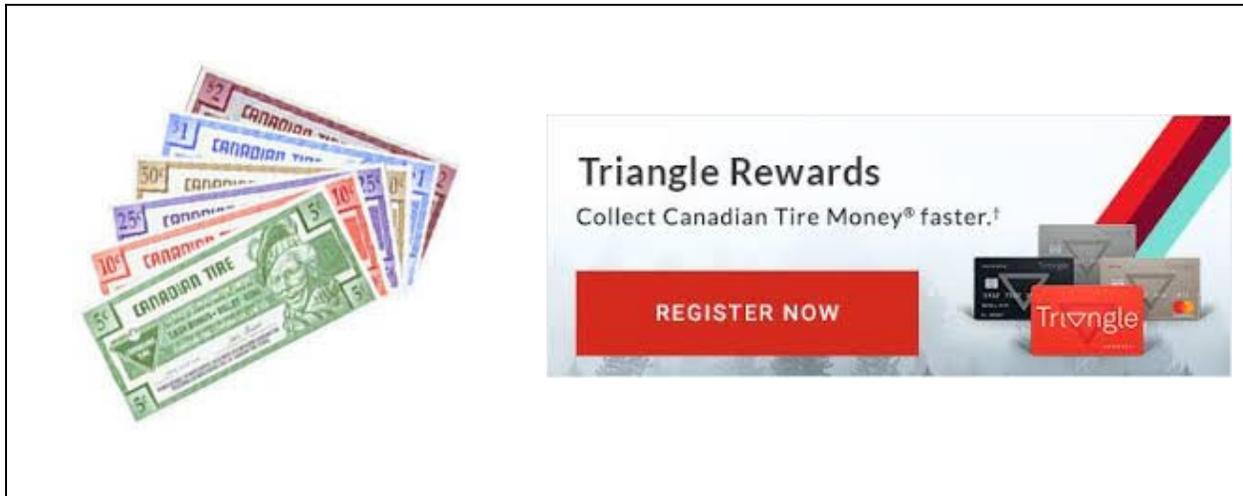


Figure 24 - Canadian Tire money replaced by their Triangle Rewards

Rewarding customers with points:

In any retail loyalty scheme, there are at least three sources of data: first, consumers provide data on the application to join the program (and some consumers believe that this is the only data that retailers hold and use). Secondly, retailers link these personal data with internal and external databases, such as lifestyle and geodemographic data, for example, PRIZM. Thirdly, transaction data from purchasing in store becomes available on a regular basis (Smith & Sparks, 2003). Loyalty programs, therefore, have become a means by which corporations are able to tie transactional data directly to each customer, and those programs range from frequent flyer programs and supermarket discount cards to retail points cards. In addition to the proprietary cards, there are coalition (multiple partner) cards, and both types may themselves be

co-branded with credit cards, such as Visa or American Express, through particular financial institutions. An example is Air Miles, a large coalition program that boasts 69% of Canadian households as members. Given the value that such programs represent to consumers, competition between these programs is relatively fierce (Pridmore, 2010, pp. 296–299).

Loyalty programs are a key means of tracking purchases in a way that connects back to the individual. Thus, the focus shifts from the customer as part of a larger social group or lifestyle segment, to that of the customer as an individual described by dozens, even hundreds, of data points (Turow, McGuigan, et al., 2015). Each time a customer buys goods with a loyalty card (by swiping the card through the Electronic Point of Sale (EPoS) terminal at checkout), an individual profile of consumption habits is built up, and over time, this can be fed into ordering, logistics, and storage and supply chain management, providing raw material for mass customisation and direct marketing. Once the budget, preferences, and shopping times of the customer are known, retailers are able to target customers with offers specific to them, hence, targeted marketing. An example (Graham, 1999) is the supermarket customer loyalty card that provides managing corporations with personalized surveillance and cybernetic customer targeting in the U.K. and U.S. food retail industry, for example, the U.K. retailers Safeway and Tesco.

Another example is Loblaw Companies Ltd. (whose retail network includes corporate-owned supermarkets, Shoppers Drug Mart, Pharmaprix drug stores, and franchised grocery stores) whose PC Optimum program is tailored for each consumer (Figure 25). Loblaw is currently testing a new service that leverages its PC Optimum loyalty program (presently with more than 18 million Canadian members) to personalize advertising for their consumers and

reward them for seeing those ads while browsing online (Redman, 2019). According to Uwe Stueckmann, senior vice president of marketing at Loblaw:

Loyalty programs have historically provided benefits to customers, rewarding them for the information they provide to a company. We're extending that same idea to advertising . . . Our members will see more relevant ads while browsing online, and we will reward them for allowing us to use their data and advertise to them. (Redman, 2019)

To alleviate fears of losing control over their personal information, Loblaw noted that their consumers will have the option to opt out of receiving this advertising at any time.

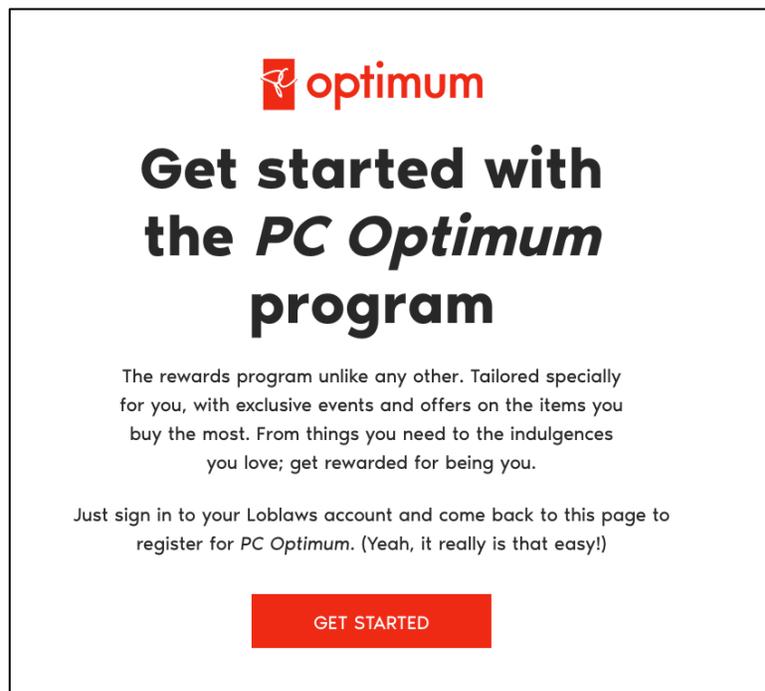


Figure 25 - Loblaw's loyalty program (<https://www.loblaws.ca/loyalty>)

After depending on historic sales to forecast their upcoming merchandise assortment, Giant Tiger Stores Limited, a Canadian owned discount retailer, first launched their loyalty program (available as an app on both IOS and Android devices) to the Ontario region in September 2019, before expanding it to its Quebec stores in February 2020 (Giant Tiger, 2020a, 2020b) (Figure 26).

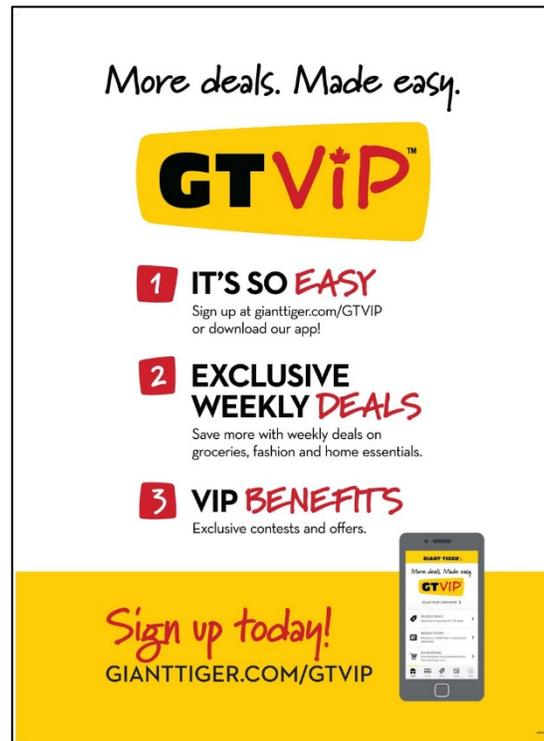


Figure 26 – Giant Tiger VIP loyalty program (GT VIP) (<https://www.newswire.ca/news-releases/tg-vip-giant-tiger-continues-loyalty-program-expansion-833502480.html>)

The number of consumers signing up for loyalty schemes suggests that privacy concerns are not a very powerful disincentive, compared with perceived benefits, or alternatively that consumers are in denial. Moreover, it is worth noticing that unlike other means of consumer surveillance, in loyalty schemes, the consumer is a willing participant and is, therefore, complicit in the use of individual data and any compromise of privacy (Smith & Sparks, 2003). This makes loyalty programs a combination of overt and covert surveillance, for consumers have to accept being part of them even though they might not be aware of the full scope of the programs' surveillance outreach. While loyalty programs give targeted users access to discounts and services directly customised to their consumption patterns, they also raise various concerns, for example:

Where does customised service become a social intrusion? What are the impacts of the reselling of individual dossiers within the “information marketplace,” to support wider direct marketing for financial services and utilities? And what are the implications of direct surveillant simulation of consumer landscapes for retail geographies in the context of the spatial restructuring of grocery networks, the oligopolisation and internationalisation of markets and the increasingly careful exclusion of those groups and areas without the disposable incomes and bank accounts to make them attractive targets of customised services? (Graham, 1999, p. 139)

Also, while shoppers may appreciate knowing about special offers specific to them, they may also find that they are simply not informed about other available merchandise, making it difficult for them to make purchases outside their assigned boxes (Lyon, 2007, p. 13). Others fear that in the not-so-far future, health obligations may oblige supermarkets to prevent certain customers from purchasing a product (for example, customers with tendencies to obesity buying doughnuts) when accessed profiles combine medical with purchase data (Lace, 2005, p. 208).

Pridmore (2010) used the Globalization of Personal Data (GPD) survey data in Canada and the U.S. and focus groups to examine consumers’ knowledge of loyalty profiling, their awareness of possible consumer responses to company attempts to create customer profiles, and their concerns. In the survey, two-fifths of the Americans and two-thirds of the Canadians surveyed said that they carry at least one loyalty card. From the point of view of corporations and retailers, loyalty programs allow them to use detailed customer profiles to improve marketing effectiveness (e.g., targeting specific segments in the market, which ultimately disadvantages the non-targeted consumers) and/or as a source of direct income (e.g., when consumer information is sold to other organizations). Pridmore also demonstrates that the relationship between participation in loyalty programs and willingness to provide consumer data is quite complex, for while there is a customer desire for “privacy” (a North American term

named “data protection” in Europe (Lyon & Zureik, 1996, p. 12)), there is also a consumer desire for purchasing convenience and discounts.

(5) Free Wi-Fi and tracking technology

To compete with e-commerce sites like Amazon, brick-and-mortar retailers have started using tracking technology. When consumers enter a retail environment, they are usually provided with a free Wi-Fi service for which they can sign in. Then in-store equipment picks up consumers’ smartphones’ Wi-Fi cards, consequently, learns their devices’ unique ID numbers and keeps tabs on those devices over time as they move through the retail store. Consumers’ interactions are then logged and uploaded to the databases of third-party companies that specialize in retail analytics (Fung, 2013). Thus, using the Wi-Fi service, bluetooth, and the consumer’s phone to track shopping habits, retailers end up with a research tool that can help them improve the consumer’s shopping experience. Although, in general, no personally identifiable information can be gathered this way, retailers can discover if certain aisles are more successful than others, and if there are areas of overcrowding that need to be fixed. Tracking technology, moreover, helps retailers receive information such as footfall outside the store, engagement (how long consumers spend inside stores), whether consumers are repeat shoppers, and ultimately, how to monitor the efficacy of a particular marketing campaign. National chains like Family Dollar, Cabela’s, the British chain Mothercare, and specialty stores like Benetton and Warby Parker rely on tracking technologies to decide on matters like changing store layouts and offering customized coupons (Cliford & Hardy, 2013).

In fall 2012, Nordstrom started testing a new technology that allowed it to track its consumers’ movements by following the Wi-Fi signals from their smartphones. Nordstrom ended this experiment in May 2013, partly because of the negative comments and complaints of

the consumers. More specific patterns can be deduced if a shopper's phone is set to look for Wi-Fi networks, even if they do not connect to the network, for example, pinpointing where the shopper is in the store within a 10-foot radius. And since mobile devices send unique identification codes when they search for networks, retail stores can also recognize returning consumers, how repeat consumers behave, and the average time between visits. More access to a consumer's profile (e.g., number of recent visits, what products the consumer was looking at online, and their purchase history) is granted when a consumer volunteers some personal information, either by downloading a retailer's app or providing an e-mail address when using in-store Wi-Fi; for example, Macy's uses such technology to provide their consumers with personalized recommendation through their phone the moment they enter the store (Cliford & Hardy, 2013). To conclude, consumers are usually lured to use a retail store's free Wi-Fi, not recognizing that they pay a price for it: sharing their information.

(6) Personalized advertising

Consumers are now used to (or even expect) targeted adverts based on web browsing history, but now, targeted personalized advertising is making its way into our offline life. This includes using consumers' data sources to create personalized messages for them as retailers track them entering the store and proceeding through the aisles (Turow, 2017, Chapter 1). In *Minority Report*, a science fiction film directed by Stephen Spielberg in 2001, an eye-scanning system is used to tailor advertising to the character of John Anderton, played by Tom Cruise (Figure 27), and the content of the advertisement is constrained by the character's embeddedness in the physical environment (Liptak, 2017). Using a *Minority Report*-style technology, video ads playing at retail stores will have the potential to evaluate the consumer, determine their age,

gender, ethnicity, and mood, and ultimately select a message that is best targeted to what some database says the customer wants to know about. Kroger—the largest grocery chain in America which has 2,800 supermarkets—is presently testing cameras embedded in a price sign above shelves in two stores in the suburbs outside Cincinnati and Seattle so that video screens attached to the shelves can play ads and show discounts. Although Kroger is still testing this surveillance system, the company intends to expand it to other locations. According to Kroger, the cameras guess a shopper's age and gender, but the information is anonymous and the data is not being stored (Pisani, 2019).



Figure 27 – A screenshot from the 2002 *Minority Report* film in which John Anderton (played by Tom Cruise) is standing in front of a personalized ad display.

Similar technology is now being introduced to retailers in the U.S. (Pisani, 2019): cameras and sensors installed in cooler doors try to guess the consumer's age, gender or mood as they walk by. The intent is not to deter shoplifting, but to use the collected information to show targeted real-time ads on in-store video screens. An example is Walgreens, with more than 8,000 drugstores in the U.S., which has already installed cooler doors (provided by the Cooler Screens

start-up company using Microsoft cloud technology), with cameras above the door handles, at six locations in Chicago, New York, San Francisco and Bellevue, Washington (Figure 28). Since 75% of shoppers make decisions about what they are going to buy from coolers on impulse, those cooler doors are designed to discern the consumer's gender, general age range, what products they are looking at, how long they are standing there, and even what their emotional response is to a particular product. The doors also use contextual information, like the time of day, to convince the consumer to buy more, for example, frozen pizza near dinner time (Schwab, 2019). Walgreens says that for now, the cameras are only used to sense when someone is in front of the cooler and to count the number of consumers passing by; they decline to say if and when the other functions (i.e., guessing the age and tracking irises to see where the consumer is looking) may be turned on. Cooler Screens has already booked advertising deals with more than fifteen of the twenty top consumer packaged goods companies, including Coca-Cola, Pepsi, Nestle, MillerCoors, and Anheuser Busch.

From a retailer's perspective, the capabilities of such ad-targeting cooler doors bring the digital world to physical retail using a customer-centric approach; they are valuable to companies fighting for consumers' attention on the freezer shelf and anxious to stand out, they provide better product tracking for retailers, and increase revenue (Figure 29). From the consumers' perspective, personalized advertising provides a better shopping experience. According to a study conducted by Boston Consulting Group (BCG) and commissioned by Google, consumers increasingly prefer a shopping experience that is easy and fast and that helps them make purchase decisions (Abraham, Van Kerckhove, Archacki, González, & Fanfarillo, 2019). However, the interaction with this technology can be frustrating to some consumers (e.g., when screens malfunction), and the lack of transparency (i.e., how the users are being watched and

how their behaviour is analyzed) can push some consumers to avoid stores using this technology in order to avoid being targeted by such surveillance (Schwab, 2019).

In 2017, Samat, Acquisti and Babcock developed a scale and investigated the effect of awareness about targeting on users' attitudes towards a targeted ad and behavioural intentions towards the advertised product (i.e., intentions to purchase the advertised product). They defined targeted advertising as "the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests" (p. 299). Although Samat et al. focused on the online platform, the results of their online survey study could be applied to physical retail, specifically personalized advertising employed in stores. According to their study, at least 33% of study participants had negative opinions about targeted ads. The question then becomes: why would the advertising industry be willing to make consumers aware about their targeted advertising practices?



Figure 28 - A smart shelf area at Walgreens in Chicago that displays ads along with the cooler's contents (Source: Teresa Crawford, *The Associated Press*)

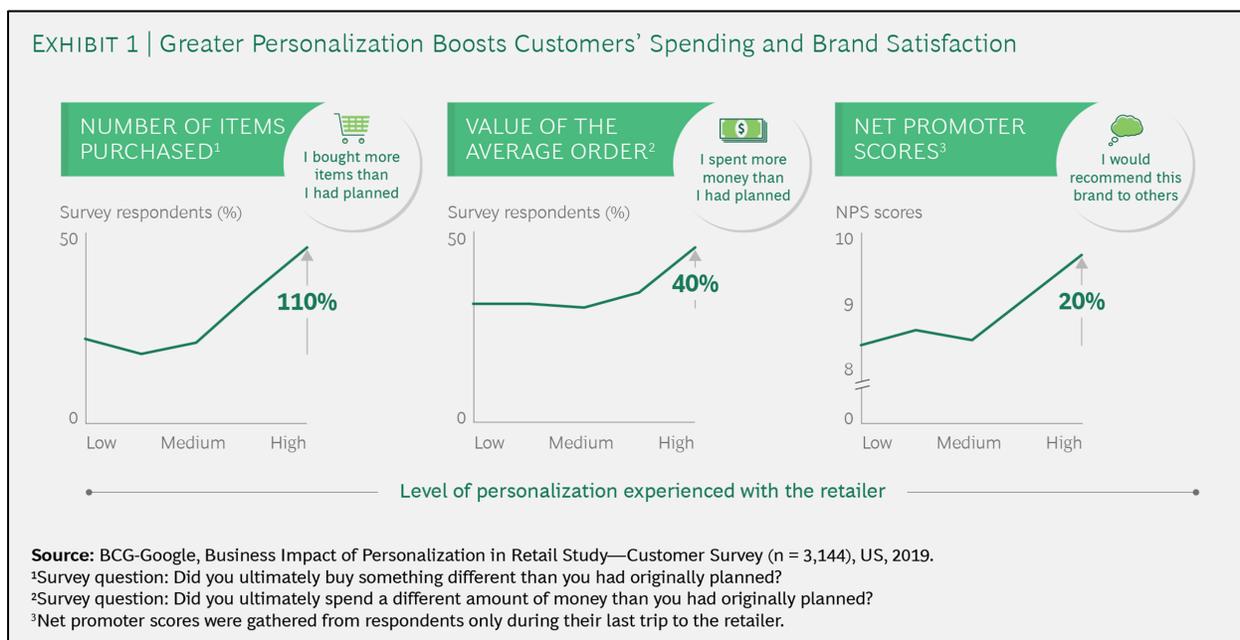


Figure 29 – The impact of personalization in retail according to the customer survey study conducted by BCG-Google

Facial recognition cameras are now fitted to billboard screens (that could be found in places such as retail shops, doctors' waiting rooms, railway stations, airports and gas stations) so that advertising companies can monitor the people viewing adverts at each location (Hudson, 2013). Moreover, combining this facial recognition technology with RFID (Radio Frequency Identification) tags on merchandise can help targeted ad monitors know exactly what the consumer is carrying in anticipation of trying it on. Fashion brand Burberry is already using RFID tags embedded in their latest collections so that when consumers stand in front of the store “magic mirrors” in their London flagship store, they can see how the products looked on the catwalk. Tommy Hilfinger’s Regent Street store, in central London, has dressing rooms (or “digital showrooms”) featuring interactive mirrors equipped with RFID technology to offer fashion advice, and combined with the RFID tags on hangers, can recognise items and suggest complementary items when shoppers are trying them on (Katwala, 2018). The Spanish chain

Mango started using digital fitting rooms (see Figure 30 below) in 2018 in collaboration with Vodafone to blend consumers' online and offline experiences. The near future will also see systems linking Facebook accounts to RFID chips embedded into store loyalty cards to flash up personalized adverts and special offers on screens when consumers visit the shops (Hudson, 2013).



Figure 30 - Mango augmented mirror x Vodafone digital fitting rooms (Source: <http://theretailplanner.com/tag/ar/>)

(7) Radio frequency identification (RFID)

Radio Frequency Identification Technology (RFID) is the “generic name attributed to the technologies that use radio waves . . . for automatic identification of objects, positions or persons located at a considerable distance through electromagnetic answers” (Azevedo & Ferreira, 2009). RFID was first invented in 1948 and had its origins in military applications during World War II.

In the 1950s, the explorations of RFID technology were confined to laboratory experiments while the development of theory and field trials took place in the 1960s. Its commercial applications began to be realised in the early 1980s, and by the 1990s, it became widely deployed (Hossain & Prybutok, 2008). For example, it has been employed on highway and bridge tolls, in tracing livestock movements, in tracking airfreight and in motorcar manufacturing. RFID technologies—usually consisting of a tag and interrogator, or reader, with an antenna that forms a magnetic field—use radio waves to automatically identify items.

Traditionally, within retailing, RFID has been limited to tracking a tagged product and has had no link to the consumers themselves. However, the technology is fast changing and IT services companies are working on the development of RFID applications. According to the *RFID Journal* (Swedberg, 2016),

by linking RFID data to closed-circuit television (CCTV) camera images and social-media sites such as Facebook, a retailer can identify where shopper traffic is heaviest (using a camera-based heat map), understand how an individual responds to a product (by tracking the expressions on his or her face) and monitor comments that its customers make on social media (with their permission), using the store's Wi-Fi network.

Because RFID is limited by the incapability of sound waves to penetrate walls, a new technology has started being integrated and tested in retail environments to collect a large amount of shoppers' behaviour data and to help implement marketing and merchandising strategies: RTLS (Real Time Locating System) which can automatically identify and track objects and people in real time, usually within a building or other contained areas (Ferracuti et al., 2019).

Nowadays, RFID technology provides tighter control and management of the supply chain and of inventory management with attendant cost savings, reduced labour costs, improvements in customer service (Anderson & Bolton, 2015), store operations (e.g., backroom storage and shelf replenishment) (Azevedo & Ferreira, 2009), reduction in shrinkage, out-of-

stock (OOS) issues (Singh, 2011), and clearer targeting of consumers and tracking of their purchasing behaviour (e.g., retailers can put RFID tags on shopping carts and baskets to allow for detailed research on consumer behavior including complete tracking throughout a store). RFID can also accurately track which product shelves consumers have visited to determine in what order certain products were placed in a shopping cart. When consumers can detect the presence of such tags, it is a case of overt surveillance, and when the tags are hidden, it is a case of covert surveillance. Several clothing vendors—such as Benetton, Zara, Prada, and H&M—put RFID tags on clothing to track sales floor inventories, identify hot selling items, and shift production and distribution to accommodate current trends (Clarke III & Flaherty, 2008).

In 2017, as part of their exploration of “the Internet of things” concept, the fashion company Rebecca Minkoff launched ten limited edition bags retailing for U.S. \$295, and dubbed the #AlwaysOn Midnighter style, as part of their #BornDigital concept which aims at digitalizing ten billion items of clothing and accessories (Figure 31). The technology gave each item a digital identity in the cloud, which when accessed, unlocked exclusive offers, e-commerce services, private styling sessions with Rebecca, style recommendations, video content, an invitation to the following show, and elite experiences to enjoy with lifestyle partners. It also automatically qualified the consumer for a loyalty program (Arthur, 2017; Garced, 2017). Deon Stander, vice president and general manager at Avery Dennison RBIS (Rebecca Minkoff’s partner), explained in an interview that beyond consumer experience and satisfaction, Rebecca Minkoff would be able to access consumer analytics that were previously unobtainable, helping to drive key business and marketing decisions (Arthur, 2017).

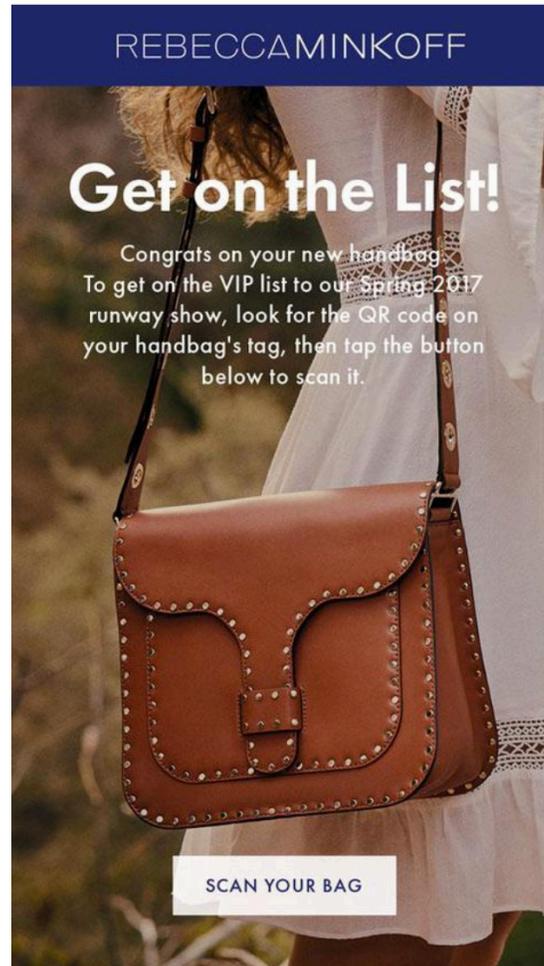


Figure 31 - The connected #AlwaysOn Midnighter handbag from Rebecca Minkoff (Source: Rebecca Minkoff)

RFID real-time data, in addition, provides retailers with up-to-date information on inventory, logistics, and freshness. Within stores, some U.S. clothing manufacturers have indicated as much as a 7% increase in sales when RFID was used because of the greater visibility of the inventory on the shop floor. The use of the technology, moreover, can dramatically reduce shrinkage through theft, reduce check out times (customers can carry their shopped items past a reader and their credit or debit cards then get automatically charged), promote products and stimulate upselling since less time would be spent tracking products, and provide competitive advantage within the marketplace. The Italian fashion retailer Prada has been successfully trialing an RFID system in its New York store, where the technology identifies products a

customer takes to the changing rooms and then automatically displays information about the garment (Jones et al., 2004).

Peslak (2005) identifies three situations where privacy concerns surface in relation to RFID: in pre-sale (when an item is tagged on a shelf and is examined by a customer, the store could, through readers, monitor what items are being examined), during the sale (when the sale transaction takes place, the store can permanently store all personal and shopping information about the consumer and associate it with that specific item), and post-sale (when invasive custom marketing activities could be developed through the active reading of items possessed with RFID tags, or even tracking personal individual movements through their possession of items with RFID tags). It is not surprising, therefore, that the widespread introduction of RFID technology by retailers is generating a range of privacy and public policy issues (Alder, 1998). First, consumers may not be aware, or be given notice, that RFID tags have been attached to products within retail outlets, and in theory at least, such surveillance activity could be even extended beyond the retail outlet itself if the RFID tags are not removed or deactivated. Secondly, when linked to personally identifiable consumer information (e.g., store or credit card number or personal data), aggregated personal information and product purchase information would allow retailers to build up detailed profiles of their consumers and of their purchasing behaviours. Lastly, in theory, linking the consumers' personal identification data with a unique product code could mean that they could not only be profiled, but also physically tracked without their knowledge or consent; if the RFID tags are not removed or deactivated when the consumer leaves a store with their purchases then that consumer can be monitored via the radio signals their purchases continue to emit. Thus, despite the potential benefits of using RFID technology, retailers will have to address a number of operational and strategic issues and challenges and

privacy concerns before they can begin to realise such benefits (Clarke III & Flaherty, 2008; Jones et al., 2004). Incorporating ubiquitous technology, such as RFID, can be a costly failure when retailers face spikes of negative consumer reactions and potential damage to their customer relationships (Davis, 2014; Margulis, Boeck, & Laroche, 2019), as in the cases of Metro and Prada⁶ (J. Blau, 2004; RFID Journal, 2002; Violino, 2004; Wehler, 2003).

Hossain and Prybutok (2008) investigated the factors that affect consumer acceptance of RFID technology, specifically, culture (i.e., societal beliefs, value systems, norms, and/or behaviours influence), privacy and security. Developing a theoretical model that contextualizes the Technology Acceptance Model (TAM)⁷ within the context of RFID technology, the researchers developed new scales and conducted an online survey. Their results show that a higher perceived convenience of RFID technology and cultural influences lead to a greater acceptance of this technology, while a higher perceived importance of and less willingness to sacrifice personal information security led to lower intention to use RFID technology. Margulis et al. (2019) provided a new model of consumer reactions to ubiquitous technology in general, and RFID in particular. They also discussed seven factors that can influence consumer reactions: (1) privacy and security expectancies, (2) previous experience with technology, (3) consumer innovativeness, (4) product and benefits evaluation, (5) social and cultural influences, (6)

⁶ Although not related to the physical RFID system, in 2003, Prada customers were uncomfortable with the level of individual consumer data being recorded and made available to the sales staff (such as the size they wore). In 2004, Metro AG was pressured by anti-RFID activists and decided to drop the use of RFID tags in their customer loyalty cards used at their Extra Future Store supermarket in Rheinberg, Germany.

⁷ TAM is a theoretical lens from the information systems and technology discipline that is commonly applied to understand how users come to accept (i.e., perceived usefulness) and use (i.e., perceived ease of use) a particular technology (Lim, 2018).

consumers' emotional responses to marketing stimuli, and (7) connective proximity (i.e., the metaphysical distance between the consumer and the firm as perceived by the consumer).

(8) Tracking returns

In the first half of the twentieth-century, retailers faced the problem of balancing satisfying their consumers with accepting returns. In 1941, Campbell discussed the retailers' "troublesome problem," saying:

Both agencies concerned with the transaction, store and customer, are responsible for this constant evil of merchandise returns—the store because it has not trained its selling and non-selling staff to perform their tasks with the maximum of intelligence, and the customer because she has not taken sufficient interest to make her purchases with care and discrimination. All types of stores have suffered, large and small department stores, as well as large and small specialty stores. (p. 141)

Not surprisingly, women were blamed then for being "the most frequent offenders" by the stores: they were accused of not being able to make up their minds or for trying to impress their companions by buying items and then returning them later. The problem of merchandise returns persists today. In 2017, U.S. retailers lost more than \$351 billion in sales due to merchandise returns (partly encouraged by the rise of Amazon.com Inc. and its policy to allow returns with little resistance) (Safdar, 2018). Retailers have to inspect all returned products, handle and prepare them for resale, an expensive and time-consuming endeavour, and if there is not an easy and economical way to restock or liquidate returns to a third-party, then retailers end up throwing away those returned products (Ladd, 2018). In addition, 1% of all shoppers were involved in fraudulent and abusive returns (e.g., requesting a refund for items that have been used, stolen, or bought somewhere else), which cost retailers an estimate \$22.8 billion (Safdar, 2018). To combat return fraud, retailers can notify their consumers that their future returns or

exchanges might be limited when no proof of purchase is provided, or when a certain number of returns is exceeded in a specific amount of time (e.g., Victoria's Secret allows shoppers up to seven returns in a 90-day period, or a maximum of \$250 of merchandise over the same time frame without a receipt). Retailers (such as Best Buy, Home Depot, Sephora, and Victoria's Secret) track consumers' returns and exchanges with the help of third-party firms that mine sales data to identify excessive return patterns (Peterson, 2018). Since consumers are usually not aware that their personal and shopping information are being used to control their future buying behaviour, such tracking can be considered a technologically mediated/covert/over time/formal surveillance.

A company that provides artificial intelligence software that can pinpoint people who serially return products and/or show odd patterns of behaviour is Appriss Retail. Another leading third-party firm is Retail Equation based in California; they have developed a "risk score" on each consumer based on shopping behaviour, which can lead to the issuing of warnings and denials. Recently, Best Buy Co. came under fire and was the target of a large share of consumer complaints on Facebook, Twitter, Yelp and other online forums because of their efforts to police returns with the help of Retail Equation; consumers complained about having their shopping monitored and the amount of the merchandise they can return limited (Safdar, 2018). Other retailers, like Bloomingdale, who fear offending shoppers with strict return policies, have started using low-tech solutions such as the one-time-use tag, produced by Alpha Shark Tags in the U.S. and R-Turn in Europe, that stops consumers from returning expensive items (e.g., jewelry returned after wearing it for a special occasion) (Figure 32). Since the tags are bright in colour, three-inches long and usually placed in a conspicuous location on the merchandise, the tags

become a visible deterrent against using the goods before returning them to the store (Stores, 2019b).

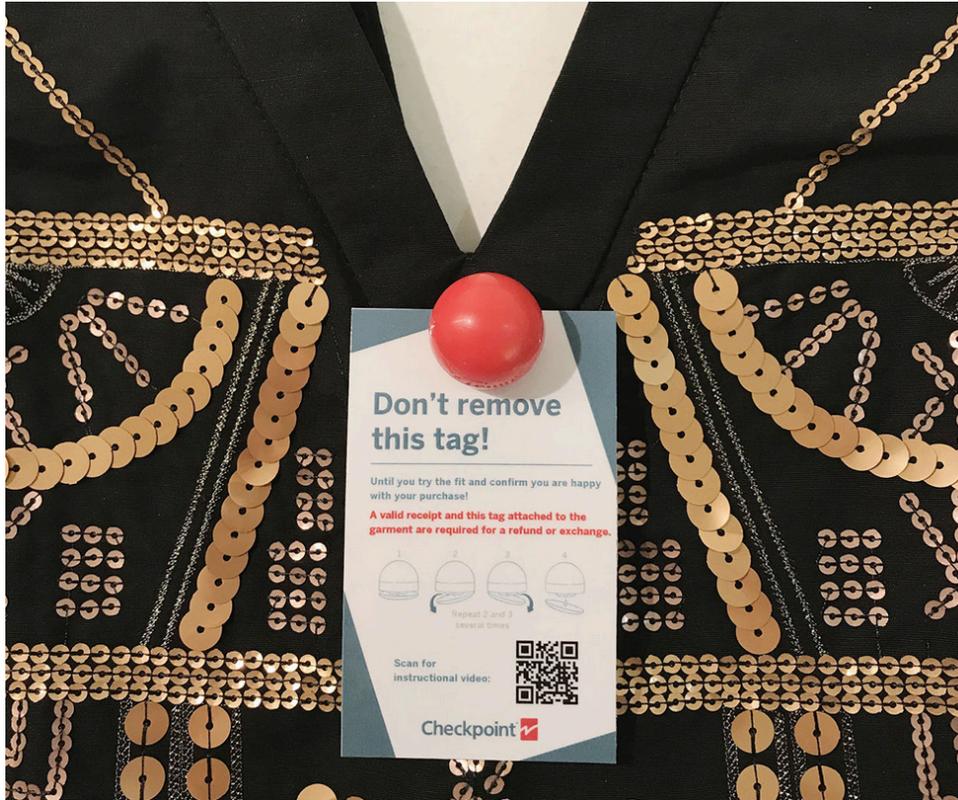


Figure 32 – Oversized tags to stem returns (Image: *Stores Magazine*)

(9) Geo-fencing

Geo-fencing is the use of GPS (Global Positioning System) or RFID (Radio Frequency Identification) technology to create a virtual geographic boundary, enabling software to trigger a response when a mobile device enters or leaves a particular area. To consumers, these smart retail technologies have the potential to improve the consumer retail experience by providing a new, mobile-enabled, real-time, superior, and personalized retail services. For example, consumers can now use the Cartwheel app installed on their smartphone when shopping in Target, one of the retailers on the cutting edge of the geo-fencing technology, which pushes in-

store personalized discount offers based on their previous in-store purchases (Pandolph, 2017). Grocery giant Sobeys Inc. has recently unveiled their “smart” shopping cart at its store in Oakville, Ontario, which features multiple cameras, a scanner, scale, a payment system, and a touchscreen just above the push bar to display on-board items and in-store promotions. The new carts, which have become available to customers in mid-November, 2019, are Sobeys’ latest strategy to compete with other major retailers across North America (Boisvert, 2019; Sobeys, 2021). When it comes to retailers, research findings indicate that smart customer experience directly enhances satisfaction and reduces perceived risk towards smart retail technologies, and as a result, customer satisfaction increases behavioural intentions, word-of-mouth intentions, stickiness to retailer, shopping effectiveness, and customer well-being (Roy, Balaji, Sadeque, Nguyen, & Melewar, 2017).

At the heart of using new technologies to revolutionize the consumer shopping experience and set new expectations of what shopping should be in the future is Amazon (Grewal, Roggeveen, & Nordfält, 2017). On January 22, 2018, Amazon Go opened its first pilot store to the public (Figure 33). A prototype grocery store, Amazon Go has four locations in Seattle, Washington, three in Chicago, Illinois, and two in San Francisco, California as of January 2019; the stores are partially-automated, with customers able to purchase products without using a cashier or checkout station. Amazon Go is the creative coalescence of several “Just Walk Out” technologies that include: 1-click-like Web shopping in retail, a powerful app using location-based services, QR Code IDs, integrated payment, image recognition, multiple sensor technology, artificial intelligence, and machine learning (Ives, Cossick, & Adams, 2019). Thus, when entering the store, consumers swipe their smartphones loaded with the Amazon Go app (Figure 34) and at the same time, hundreds of ceiling-mounted cameras and electronic

sensors work to identify each consumer and track the items they select. With the help of sensors on the shelves, items are added to consumers' Amazon Go account as they pick them up and are deleted if they are put back. When consumers leave the store, purchases are billed to their credit cards; there is no need to unpack the purchases (Johnston, 2018).



A row of gates guards the entrance to Amazon Go. Kyle Johnson for The New York Times

Figure 33 - Amazon Go store (Source: Kyle Johnson, *The New York Times*, <https://www.nytimes.com/2018/01/21/technology/inside-amazon-go-a-store-of-the-future.html>)

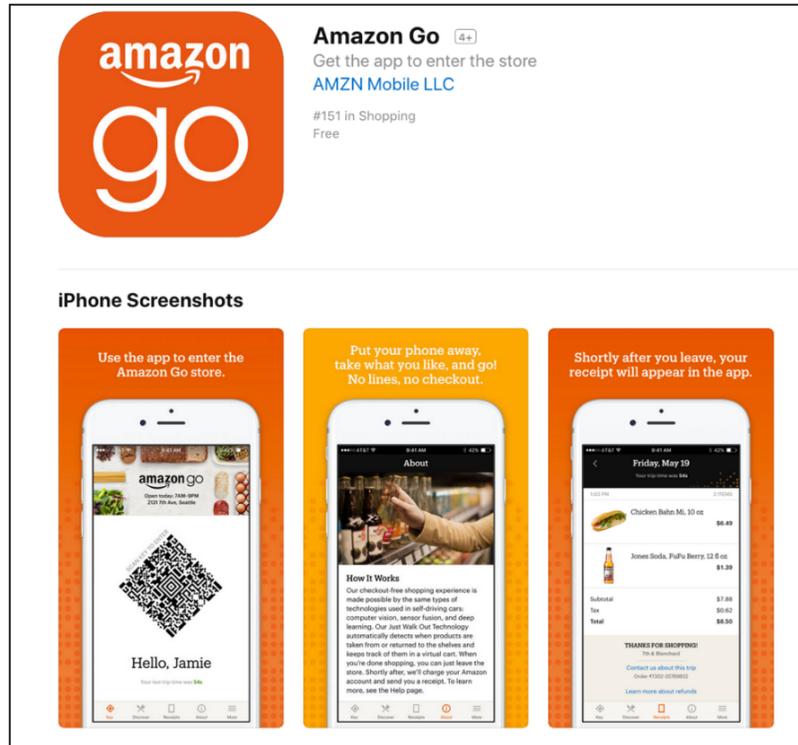


Figure 34 - Amazon Go app in the App Store

However, while this new store concept is seen as a revolutionary model that relies on the prevalence of smartphones and geo-fencing technology to streamline the consumer experience, as well as supply chain and inventory management, the collection of personal data and the constant surveillance highlight the blurred lines between what is considered public and what is considered private. In addition to the expected concerns regarding increased surveillance in the store (i.e., trading privacy for convenience), some worry about the impact of the cashier-less operational model on the workforce—since cashiers represent 30% of the labour task in stores (although a counter-argument is that there would be an increased demand for individuals with computer maintenance skills, and a need for store employees to help customers, prepare meals for sale, and check I.D.s before consumers can take alcohol off the shelves), and the sociocultural implications as a result of eliminating human interaction (Ives et al., 2019; Polacco, 2018).

To sum up, surveillance is an integral part of our world and its emphasis has expanded beyond the realm of politics and policing. In the retail sector, with rapid technological advances, surveillance has become the means to not only monitor in-store activity and maintain low shrinkage rates, but also to provide outstanding and personalized customer service. Figure 35 displays the nine surveillance systems employed in retail stores and discussed above. Out of those nine systems, only video surveillance can be explicitly overt (when consumers can easily see the cameras mounted on walls and ceilings). However, as will be discussed in the next sections, consumers' acceptance of surveillance is not always guaranteed despite what retailers' goals might be.

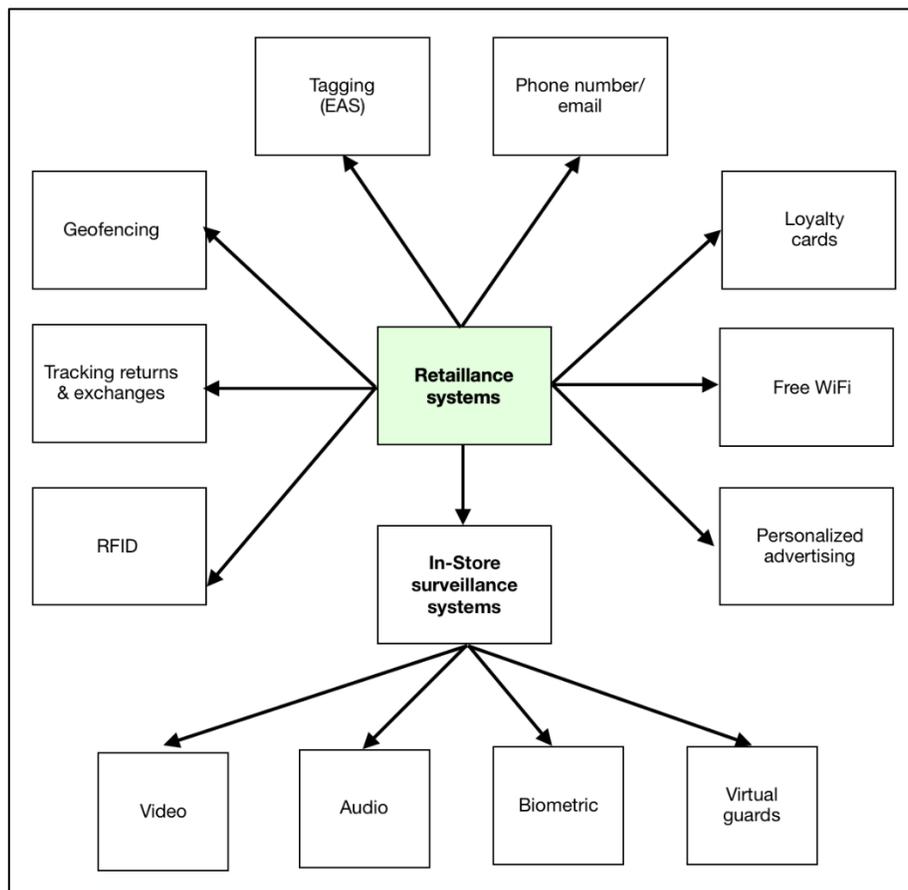


Figure 35 - Retailance systems discussed in this chapter

The surveilled: Consumer awareness

Consumer awareness of retail surveillance is when the consumer knows of the presence of overt store surveillance and when they are aware of the laws, policies and regulations governing surveillance and protecting their rights (note that this knowledge could be partial or complete). As discussed in this section, consumer awareness could include: (1) individual awareness, for example, when a consumer is aware of being watched inside the store in real-time, which could lead to abandoning their purchase or negative opinions about the store's targeted ads; (2) societal awareness, or understanding the broader benefits, challenges and risks posed by surveillance; or (3) awareness of government policies and laws.

(1) Individual awareness

Direct surveillance is when an employee overtly watches consumers in real-time, for example, when retailers employ “defensive merchandising” (i.e., limiting the number of items on display) and/or “restrictive merchandising” (i.e., placing goods behind counters or using locked display booths) in an attempt to control theft (Koh, Schuster, Lam, & Dining, 2003). However, this surveillance practice can have negative outcomes, for shoppers can become simply too embarrassed to ask an employee for access to embarrassing products (e.g., condoms, feminine products, hemorrhoid cream, or foot fungal cream) and end up either abandoning their purchase (Redfeam, 2006) or self-consciously shoplifting (Beck & Palmer, 2009), both of which result in lost revenue for the retailer. Esmark, Noble and Breazeale (2017) conducted four studies to show why an employee watching a shopper can cause the shopper to either permanently or temporarily leave the shopping area as purchase intentions decrease. Using Reactance Theory (i.e., a

psychological motivational state aroused by the threat to a behavioural freedom, for example, shopping in private is threatened through the manipulation of being watched), their research explores why, when shoppers believe an employee is watching them, they feel less in control of their privacy, resulting in negative consequences for the retailer. This relationship is especially important for products that consumers may already feel some level of embarrassment over purchasing in the first place. Additionally, increasing options that allow a consumer to regain control will reduce the overall reactance to the threat to privacy and will improve retailer outcomes.

(2) Societal awareness

A cornerstone in understanding the policy implications of this research is the discussion of societal awareness of the challenges posed by retailance. Lace (2005) calls for moving beyond the traditional demarcation lines of privacy debates to recognise the broader benefits and risks of using personal information.

In the future, policy will be formed less exclusively on the battlegrounds of privacy but on those of risk and of accountability. Privacy itself will need to be promoted as a social (rather than primarily an individual) value that supports democratic institutions (p. 208).

To her, allusions to Big Brother scrutiny are becoming dated, for, instead, we are now moving towards a society of “little brothers” (defined by Tokunaga (2011, p. 705) as a “phenomenon in which organizations and individual Internet users engage in surveillance to gain awareness about the Internet-related behaviors of others”). This creates a need for greater awareness (among governments, businesses, and consumers) of the importance of personal information and the challenges it poses when it comes to: principles of social justice and distributional fairness, quality of life, and the notion that privacy, in particular, can be socially beneficial. The risks

incurred by surveillance include: (1) injustice (when using inaccurate or out-of-date information, making unjust inferences, and function creep—when information is used for a different purpose from that for which it was collected); (2) lack of control of information (such as unjustified surveillance and data collected without consent, and the inability to find out what is held or where data are collected from); (3) loss of dignity and autonomy (resulting from the absence of transparency, and the absence of anonymity or unjustified disclosure); (4) inconvenience (such as making a substantial effort to find out what information has been collected, and how it has been used or to secure the correction of data); and (5) risks to life chances (as the private sector concentrates on people and areas that present the best risks) (2005, p. 211). Kerr and Barrigar (2012) argue that surveillance and privacy are not binary opposites, and that there is a fundamental tension between privacy (a fundamental human right), identity (something that is self-directed and chosen), and anonymity (a basic foundation of political free speech). Thus, the conflict arises between privacy and security, for information must be monitored, collected, and stored with permanence, while assessed continuously in order to prevent significant social threats.

Gotlieb (1996, p. 161) states that “most of the [Canadian] populace really does not care all that much about privacy, although, when prompted, many voice privacy concerns.” A Pew Research Center survey found that up to half of Americans are willing to “share personal information or permit surveillance in return for getting something of perceived value” (Rainie & Duggan, 2016). To achieve a level of mutual benefit, consumers should understand the benefits and risks of providing personal data, so that they can give their informed consent. The second step is building trust, which would lead to a sense of control. Grenville, therefore, advocates that businesses engage in a concerted effort to educate people about both surveillance and resistance.

Culnan and Bies (2003) contend that offering benefits that consumers find attractive is not enough, for there is also a need to be open and honest about information practices so that consumers both perceive disclosure to be a low risk proposition and can make an informed choice about whether or not to disclose, for example, by having an “opt-out” where a consumer’s information will be used for marketing unless they object (pp. 327-328).

(3) Awareness of government policies and laws

Consumer privacy is at the centre of an ongoing debate among business leaders, privacy activists, and government officials (Culnan & Bies, 2003). In the late 1990s, Canadians outside Quebec (since Quebec’s Act respecting the protection of personal information in the private sector came into force in 1994 (LégisQuébec, 2019)) started to take seriously the privacy issues raised by the personal data-gathering activities of private corporations (Lyon, 2003, p. 169). Currently, the Office of the Privacy Commissioner of Canada (OPC)—established in 1977—is responsible of overseeing two federal privacy laws: the Privacy Act, which covers the personal information-handling practices of federal government departments and agencies, and the Personal Information Protection and Electronic Documents Act (PIPEDA), which covers the personal information-handling practices of businesses (“Office of the Privacy Commissioner of Canada,” n.d.). On November 17, 2020, Bill C-11, the Digital Charter Implementation Act (DCIA), was tabled in the Canadian Parliament. If passed, the bill would establish a new private sector privacy law in Canada, the Consumer Privacy Protection Act (CPPA), and a new Personal Information and Data Protection Tribunal. In due course, marketers can expect Canada’s current PIPEDA to be replaced (Canadian Marketing Association, 2020a, 2020b; Office of the Privacy Commissioner of Canada, 2021). The proposed bill recognizes “both the individual right to

privacy and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances” (Canadian Marketing Association, 2020b).

In March 2018, Canada’s Privacy Commissioner launched an investigation after receiving complaints from Loblaw customers who objected to being asked to hand over sensitive personal data (including their name, address, and a copy of a driver’s licence or a utility bill) for a \$25 gift card (Figure 36) which was offered to customers after their bread price-fixing scandal that was made public in December 2017⁸. Loblaw would later revise its communications to customers to make it clear that they could redact sensitive information (such as a photo or a driver’s licence number) when sending a copy of the ID, however, some of the non-compliant customers claimed that they never collected their \$25 gift card. Loblaw was also investigated for transferring their customers’ data to a third-party company in the U.S.A., but the Privacy Commissioner concluded that the shared information was limited and that Loblaw was transparent about the process (Harris, 2019).

⁸ This incident, committed by seven Canadian bread companies (including Loblaw, Sobeys and Metro) who inflated the price of bread by at least \$1.50 over a decade and a half, later came to be known as the “the great Canadian bread price-fixing scandal” (Shaw, 2018). The Competition Bureau of Canada was approached by informants from Loblaw Companies in 2015 and filed the affidavit late in 2017 along with evidence.



Figure 36 – Loblaw’s \$25 gift card (Source: Richard Buchan/*The Canadian Press*)

In February 2012, President Obama introduced a blueprint for the Consumer Privacy Bill of Rights, intended to give Americans the ability to exercise control over what personal details companies collected from them and how the data was used. So far, only a few data controls for consumers have been produced, a testimony to the ongoing clashing visions for American society and commerce (Singer, 2016). In October 2013, the Mobile Location Analytics code of conduct, endorsed by New York Senator Chuck Schumer, was signed. The code calls for companies to have consent if they collect personal information and for a central opt-out site for consumers. This step was praised by the Federal Trade Commission for “[recognising] consumer concerns about invisible tracking in retail spaces and [taking] a positive step forward in developing a self-regulatory code of conduct” (Dato, 2014).

Many consumer polls indicate that consumers cannot trust companies to self-regulate the use of consumer data and that some level of government legislation is needed (Clarke III & Flaherty, 2008; Taylor, 2003), for example, there are no laws that are applicable to the collection of personal data gathered by RFID technology (Shim, 2003). Unfortunately, data protection laws usually have a marginal impact on surveillance societies, for they are constantly challenged by the organizations that desire to amass an ever-increasing level of their customers’ information

(Lace, 2005, p. 215). Some of the major consumer privacy rights in both Canada and the U.S. are listed in Appendix 3.

Impact and outcome: Consumers' perceptions of surveillance

In today's world, technological advancements in the shopping experience come hand in hand with the advancement in surveillance. Many marketers justify data-collection practices with the option of trade-offs (Turow, Hennessy, et al., 2015); consumers trade their personal and consumption information for better service, discounts, personalized offers, or using the store's Wi-Fi without charge. In reality, consumers react differently to retailance:

ordinary people find myriad ways of coping with surveillance—resigning themselves to it, finding modes of settlement that retain some dignity or freedom, or, on occasion, openly objecting to the gaze in whatever shape it takes. (Lyon, 2007, p. 159)

People, therefore, vary widely when they navigate their world of surveillance and infringement of privacy.

Using GPD (Globalization of Personal Data) surveillance data across seven countries, Grenville (2010) posits a model to explain why some resist surveillance (for example, by refusing to give personal details to a business, or by lying to the government), whereas others accept or ignore it. He maps out four basic steps on the path to resistance: knowledge of surveillance, recognition of the experience of being monitored, trust (or mistrust) of the monitors, and finally, the sense of whether or not one has any control over one's personal information (p. 73). According to the survey results, both those who are well informed (i.e., informed resisters) and those who were ignorant of surveillance knowledge (i.e., alienated skeptics) are the most fearful of surveillance. On the other hand, those who believe they know enough to be comfortable that their information is safe (i.e., status quo satisfied) are content with

the status quo and are comfortable with being targeted by commercial enterprises based on analyses of their personal data (p. 76-78). Similar conclusions are stated in a 2009 report about Canadians and privacy (Ekos Research Associates, 2009). The study found, in descending order of importance that: 1) knowledgeable people, as well as those who are least informed, tend to manifest the highest levels of concern; 2) the more transparent the rules are, the less concerned individuals are that their privacy will be violated; 3) having a sense of consent and control over the process of information storage and its release makes people feel comfortable that their privacy will not be violated; 4) those who accept the rationales given for privacy protection, and who see a benefit in it, tend to be less concerned with privacy issues; and 5) perceptions of the legitimacy of institutions that hold information about citizens are correlated with lower levels of concern that these institutions might violate one's privacy. On the basis of a wireline phone survey, American consumers (in general, and not just restricted to physical retail stores) often do not have basic knowledge when it comes to marketers using their information, and they do not believe that "data for discounts" is a square deal (Turow, Hennessy, et al., 2015).

According to Bonfanti (2014), in-store security systems can be either positively or negatively perceived by consumers depending on how they emotionally affect the consumers' shopping experience. On the one hand, positive emotions encompass a sense of security, transparency, and trust, and on the other hand, surveillance could adversely lead to distrust and intimidation, discomfort and embarrassment, and frustration and a sense of prohibition.

When it comes to loyalty programs, consumer concerns centre on issues of trust and personal vulnerability, fearing the prospect of personally sensitive data ending up in the wrong hands, however, information associated with shopping habits and basic demographic information are seen as less of a concern (Pridmore, 2010). An example of such a security breach is the

exposition of private Air Miles data in Canada in 1999 which left the personal data (including names, addresses, phone numbers, emails addresses, types of credit cards held, number of vehicles owned, and other customer loyalty programs subscribed to) of 50,000 online Air Miles registrants freely accessible to all the website visitors. The fact that such data was even collected and resold came as a surprise to many (Gruske, 1999; Lyon, 2001b).

While there are obvious benefits to the use of RFID, particularly at the internet commerce and supply chain level, there are serious implications for personal privacy if the technology is extended to the individual product and retail level (Clarke III & Flaherty, 2008). The four primary privacy concerns are as follows: (1) the hidden undetected placement of RFID tags on almost any item; (2) the hidden placement of RFID readers that could be read from varying distances (depending on the power of the radio signal and the tag's antenna), does not require line of sight, can travel easily through material (the only exception being water), and can be read through packaging, clothing or other objects without a person's knowledge; (3) the potential aggregation of large amounts of consumers' data and purchases; and (4) consumer tracking and profiling (i.e., without the consumer's knowledge or consent, determining the physical location of the consumer, and RFID tags could remain active upon leaving a store). Such concerns could be abated if consumers are (1) fully informed of RFID usage and (2) completely assured of its removal at the point of sale. So far, litigation surrounding RFID technology has focused not on privacy issues, but rather on intellectual property rights arising from disputes over patent rights to the technology.

Marketers often claim that consumers give out information about themselves as a trade-off for benefits they receive (Romele, Gallino, Emmenegger, & Gorgone, 2017). In exchange for sharing their information with a retailer, 54% of consumers anticipate a personalized discount in

a day, and 32% within just an hour of sharing their information (Pandolph, 2017). A 2014 Yahoo report concluded that “more consumers [have begun to] recognize the value and self-benefit of allowing advertisers to use their data in the right way.” Turow, Hennessy and Draper (2015, p. 3) challenge this report that justifies marketers’ data-collection practices, and they argue, on the basis of a representative national cell and landline phone survey of 1,506 Americans age 18 and older, that users are actually resigned⁹ to giving up their data, are not engaged in trade-offs and that they do not believe that “data for discounts” is a square deal;

Resignation occurs when a person believes an undesirable outcome is inevitable and feels powerless to stop it. Rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them. (Turow, Hennessy, et al., 2015)

The survey shows, moreover, that a large percentage of Americans do not often have the basic knowledge to make informed cost-benefit choices about the ways marketers use their information, and many overestimate the extent to which the government protects them from discriminatory pricing (i.e., companies changing prices from person to person based on those individuals’ consumer profiles) (p. 4). People’s inconsistency, and contradictory impulses and opinions when it comes to the safeguarding of their own private information (e.g., shoppers want real-time promotions which often depend on sophisticated commercial surveillance, yet at the same time, they are uncomfortable sharing their browsing history and location) is therefore termed, the “privacy paradox” (Barnes, 2006; Hull, 2015; Turow, Hennessy, et al., 2015). Such a paradox only highlights the complicated nature of the relationship between consumers and retailance.

⁹ What Turow et al. call “resignation,” Romele et al. (2017) call “voluntary servitude” which is a matter of voluntary submission and not coercion.

To summarize, consumers' reactions towards retailance differ, ranging from willing or resigned acceptance, to objection, to resistance (i.e., behavioural reactions). Based on their awareness of retailance, (mis)trust of retailers, and having (or not having) a sense of control over their personal information, consumers can end up being content, concerned, or fearful that their privacy is being violated, hence, being for or against retailance (i.e., attitudinal outcomes). Consequently, retailers have to work on alleviating consumers' concerns over retailance, providing them with a secure shopping environment and more benefits including a better customer experience. Another debatable issue related to retailance is its ethical implications.

The ethical dilemmas of retailance

With the proliferation of retailance, ethical dilemmas (governed by professional and legal guidelines)¹⁰ arise: which information should be considered public and which should be considered private? Should consumers trade their privacy for convenience, better shopping experiences, services and offers? Do consumers even have the knowledge and/or power to oppose retailance? And if they do, what are the forms of such counter-surveillance? Surveillance has always had some ambiguity, consequently, it has become both an intriguing and a highly sensitive topic. It is also increasingly difficult to apply one single set of ethical standards to the rich variations in surveillance behaviour and settings (Marx, 2016b, p. 276). One of the pressing questions when it comes to the darker side of surveillance is how surveillance should be conceived in ethical terms.

¹⁰ This is different from *moral* dilemmas which are related to individual principles with respect to what is right or wrong.

In May 2013, after the American department store Nordstrom put up a sign announcing that they had been piloting technology for tracking customers (by gathering data about in-store shoppers' behavior and moods, using video surveillance and signals from cellphones and apps) for months, they received a number of complaints not just directly to their store but also on social media. Nordstrom might have ended that experiment because of the comments, but the movement by retailers to gather data about consumers' behaviour and moods is gaining momentum (Cliford & Hardy, 2013; Dato, 2014).

A similar incident occurred in the Chinook Centre in south Calgary, Canada, when a visitor spotted a browser window that had seemingly accidentally been left open on one of the mall's directories, exposing facial-recognition software that was running in the background of the digital map (Figure 37). The mall's parent company, Cadillac Fairview Corporation Limited (CFCL), a Canadian company with shopping malls across the nation, said the software, which they began using in June 2018 and which is being used in other malls nationwide, does not record or store any photos or videos from the directory cameras, and only counts people who use the directory and predicts their approximate age and gender in order to understand directory usage patterns to "create a better shopper experience." Nonetheless, mall visitors are given neither an opportunity to opt in nor opt out, and there are no guarantees that the aggregated data would not be used for other purposes, hence, there are negative privacy implications (Heydari, 2018; Rieger, 2018). In this incident, AI surveillance technology was used to collect information, and not for purposes of security, without expressed consent.

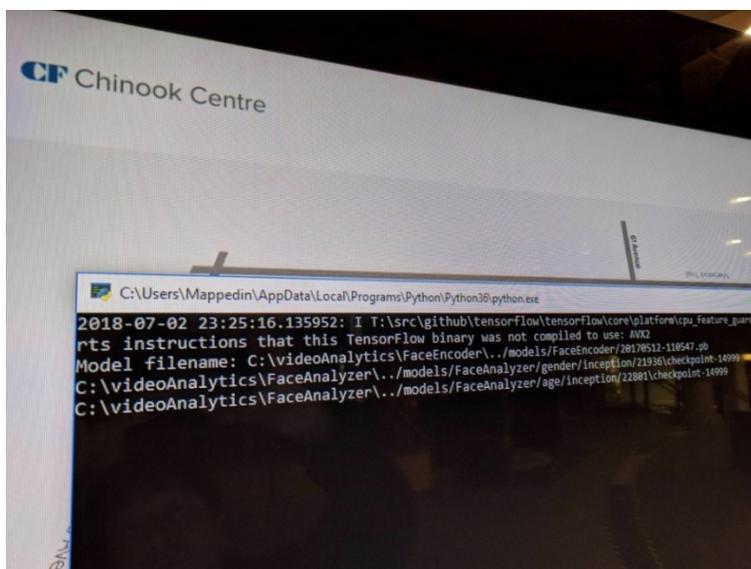


Figure 37 – A post from a Reddit user first brought attention to the facial recognition software running on the information kiosks. (Source: CTV News, <https://www.ctvnews.ca/sci-tech/facial-recognition-software-discovered-in-calgary-mall-kiosks-1.4030143>)

Following up, on October 29th, 2020, the Office of the Information and Privacy Commissioner for British Columbia revealed the results of an investigation conducted by federal, Albertan and British Columbian privacy commissioners that had been prompted by the above news reports questioning the practices of CFCL. The report revealed that CFCL embedded cameras in its digital information kiosks, or “wayfinding” directories, at twelve different Canadian shopping malls, including at Vancouver’s CF Pacific Centre and CF Richmond Centre. Instead of obtaining an “express opt-in consent,” the company’s inconspicuous cameras employed facial recognition technology (or Anonymous Video Analytics (AVA) technology) without the knowledge or consent of shoppers (O’Neil, 2020), collected five million images, and analyzed the biometric information of its customers, which included estimated age and gender. Although the images were deleted, the generated biometric information were stored in a third party’s database. CFCL might have removed the cameras from its kiosks, deleted all information associated with the video analytics technology, and provided privacy-related training to its

employees, but Alberta's information and privacy commissioner, Jill Clayton, still expressed her concern:

This investigation exposes how opaque certain personal information business practices have become . . . Not only must organizations be clear and up front when customers' personal information is being collected, they must also have proper controls in place to know what their service providers are doing behind the scenes with that information. (quoted in Takeuchi, 2020)

Despite Clearview's arguments to the contrary, the Canadian privacy Commissioners (Federal, British Columbia, Quebec and Alberta) found the U.S.-based company had broken privacy law by collecting Canadians' information without knowledge or consent and using it for inappropriate purposes (Retail Council of Canada, 2021b). However, Sharon Polsky, president of the Privacy and Access Council of Canada, said the country's current privacy legislation could not adequately ensure Cadillac Fairview would follow regulations in the future (Herring, 2020).

According to Teresa Scassa, Canada Research Chair in Information Law and Policy at the University of Ottawa (Carleton History, 2020, Nov. 12), the Cadillac Fairview incident raises three questions. First, how can a simple visit to a shopping mall lead to our biometric data getting analyzed and stored for potential future use in AI (i.e., Artificial Intelligence) analytics without us being aware? Secondly, why are similar complaints usually framed as whether we have adequately consented to the collection and use of our data or not? Lastly, does simply entering a public or semi-public space amount to consent to the harvesting of our data? Unfortunately, these questions go beyond the currently applied laws and regulations¹¹. AI is increasingly featuring new technologies of surveillance and control, for example, the COVID-19 pandemic has created new markets for AI-enabled home surveillance (e.g., to remotely monitor

¹¹ In March 2021, the Retail Council of Canada (2021d) reported that the federal Parliament's Standing Committee on Access to Information, Privacy and Ethics (ETHI) has put "The Use and Impact of Facial Recognition Technology" on its agenda for study/activity.

workers and students at home). AI is also behind facial recognition technologies that are increasingly used by public and private sectors, some of them are directed specifically towards assessing, detecting, controlling and even manipulating individuals. Thus, many AI technologies raise privacy issues in their own right, especially since most AI technologies require a vast supply of personal data collected in real time in a multitude of contexts including consumption.

Database marketing—which helps retailers to profile and track current and potential customers by collecting personal data on consumers' spending habits, preferences, and lifestyles (Lyon, 2003, p. 162)—has grown to become a multi-billion-dollar industry. However, this industry raises its own red flags when it comes to ethical issues. Zuboff (2018, 2019) calls the behavioural data collected for more than what is required for product and service improvements “behavioral surplus.” She argues that in an age of “surveillance capitalism,” Google is a frontier example of a surveillance platform that translates its nonmarket interactions with users into surplus raw material for the fabrication of products aimed at its real customers: advertisers. Moreover, with digital assistants like Google's Home and Amazon's Alexa (which fabricate living habits into behavioural predictions of consumption and needed services), privacy rights have become concentrated within the domain of surveillance capitalism. Dataveillance, or the systematic use of personal data systems in investigating and monitoring the actions or communications of one/individual or more persons/mass (Clarke, 1988), is now used to make individuals' data become visible to organizations through data-mining. Consumers' level of awareness of the presence and scope of dataveillance would ultimately affect their reaction towards surveillance in general.

Individual compliance vs. resistance

The right to privacy has become a dominant legal and public discourse positioned against the proliferation of surveillance. A Harris nationwide poll, conducted by telephone within the U.S. in February 2003, found that 80% of respondents felt it was extremely important that someone could not monitor or track them without permission and 79% felt it was extremely important to be able to control what information was being collected about them (Taylor, 2003). However, many advocates are quite pessimistic about the potential of privacy rights (Haggerty & Ericson, 2006, pp. 8–11). The cultural journalist Emily Nussbaum (2007) writes about young people who forsake their privacy on social media:

Young people, one could point out, are the only ones for whom it seems to have sunk in that [the] idea of a truly private life is already an illusion. Every street in New York has a surveillance camera. Each time you swipe your debit card at Duane Reade or use your MetroCard, that transaction is tracked. Your employer owns your e-mails. The NSA owns your phone calls. Your life is being lived in public whether you choose to acknowledge it or not.

So it may be time to consider the possibility that young people who behave as if privacy doesn't exist are actually the sane people, not the insane ones.

Vaidhyathan (2011) calls this disregard of privacy rights a “cryptopticon”:

[The] forces at work in Europe, North America, and much of the rest of the world are the opposite of a Panopticon: they involve not the subjection of the individual to the gaze of a single, centralized authority, but the surveillance of the individual, potentially by all, always by many . . . Unlike Bentham's prisoners, we don't know all the ways in which we are being watched or profiled—we simply know that we are. And we don't regulate our behavior under the gaze of surveillance: instead, we don't seem to care. (p. 85)

Gandy (1993) reasons that people's increasing awareness of the growth of the panoptic machine leads some of them to resist and others to attempt to withdraw; eventually, both responses “invite further attempts at inclusion and containment within the panoptic sphere” (p. 3). Contrary to Bartlett's (1989, p. 101) assumption that “Whenever knowledge is a scarce good,

it confers power on its possessors,” Gandy (1993) argues that economic transactions always take place in the context of substantial inequality, therefore,

...the power that the individual is able to exercise over the organization when she withholds personal information is almost always insignificant in comparison with the power brought to bear when the organization chooses to withhold goods or services unless the information is provided. (p. 19)

Gary T. Marx (2016, pp. 66–69) identifies three kinds of “compliance surveillance”: behavioural compliance (e.g., driving within the speed limit); certification (including licensing and certification for health and safety requirements); and inner compliance (which involves norms about beliefs, feelings, attitudes, and attachments) that leads to contemporary organizations nurturing and rewarding commitment. When applied to retailance, two of Marx’s forms of compliance can explain consumers’ complying behaviour when they adhere to the retailer’s regulations (e.g., no shoplifting or committing acts of violence in the store): “behavioural compliance” because they know (or at least suspect) that they are surveilled inside the store whether overtly or covertly, and “inner compliance” when they follow their inner compass of what is right and wrong and what the society deems acceptable behaviour. Lyon (2007, pp. 165–166) reasons that when compliance is questioned, some sort of negotiation takes place, and surveillance becomes dynamic and amenable to modification, for example, leading to updated and/or new privacy laws. Marx (2003) identifies eleven general strategies of surveillance resistance, all of which could be applied to retailance: (1) substitution (which Marx describes as “switching”, for example, using another consumers’ credit or loyalty card or identity); (2) distorting (manipulating retailance collected data and discrediting its inferences); (3) blocking (e.g., wearing clothes that reveal little about the consumer’s physical appearance, or shoplifters blocking the sensors on electronically tagged consumer goods by using a metallic shield that prevents signal transmission); (4) piggy-backing (avoiding retailance detection by

accompanying or being attached to a legitimate subject or object); (5) discovery/detection (finding out if surveillance is in operation and where it is then behaving accordingly, for example, a consumer does not shoplift because they can see CCTV cameras); (6) avoidance (passive withdrawal from the store where retailance is employed); (7) refusal (saying “no,” for example, the consumer refusing to give the retailer their phone number and/or participate in surveys); (8) masking (misleading the surveillance mechanism by providing useless information, such as a fake email address); (9) breaking (physically disabling retailance systems); (10) cooperation (resisting retailance by colluding with surveillants, i.e., employees working in retail security providing insider information and/or access to restricted areas to consumers/violators); and (11) counter-surveillance (when the consumer starts surveilling the retailer). Marx (2016, pp. 166–168) also argues that countersurveillance can be a form of discovery (and its results can inform other moves, whether defensively or to coerce cooperation) and a tool to uncover questionable practices (which when publicized, may lead to their moderation or cessation)¹².

Monahan (2006) suggests that the definition of countersurveillance should include the potential for inherently political acts aimed at correcting asymmetries of power expressed through surveillance activities. In 2012, Steve Mann, the Canadian researcher and inventor—known as the “father of wearable computing” (Mann, 1997)—was kicked out of a McDonald branch in Paris for wearing a computer vision system (Figure 38). Since then, he has been lobbying for the Mann-Wassel Law to counter the concept of McVeillance (i.e., placing people under surveillance while simultaneously forbidding them from using their own cameras). Mann has been also advocating for “sousveillance” (Mann, 1998, 2004, 2012; Mann, Nolan, &

¹² This discussion was integrated into the survey and interview questions that will be used in this research (Appendices 1 and 2).

Wellman, 2003), a “counterveillance,” or a counter-surveillance concept, that denotes the “lower orders” using surveillance technologies and tactics to expose and challenge the surveillance activities of the powerful (Rhee, 1999; Huey, 2009; Mann, 2009). Using what he calls “reflectionism” (i.e., reflecting experiences of being under surveillance back on the surveillers), Mann’s Shooting Back project (2009) was conceived as an art project in places of commerce that appropriates surveillance technologies to challenge their dominant meanings and uses, calling attention to the embodied experience of watching and/or being watched. More generally, Mann (2012) no longer sees a one-dimensional axis of surveillance versus anti-surveillance, but four veillances with eight points, where each can, in principle, be increased or decreased independently of the other (Figure 39).



Figure 38 - Steve Mann’s “wearable computer” and “reality mediator” inventions of the 1970s have evolved into what looks like ordinary eyeglasses. (Source: <http://www.eecg.toronto.edu/~mann/>)

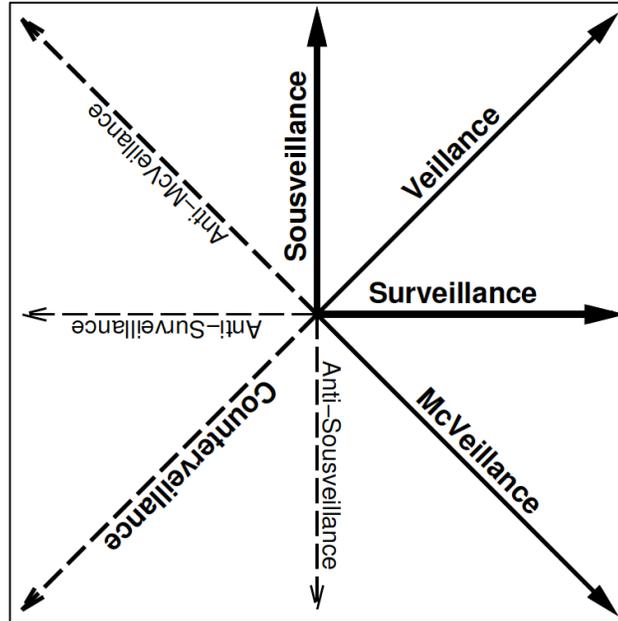


Figure 39 - The eight veillances as discussed by Steve Mann (2012)

Although some countersurveillance activities are intended to be social and to raise social awareness, Monahan (2006), cautions against individualized countersurveillance measures:

The main argument is that activists tend to individualize both surveillance problems and methods of resistance, leaving the institutions, policies, and cultural assumptions that support public surveillance relatively insulated from attack. Furthermore, while the oppositional framing presented by activists (i.e. counter-surveillance versus surveillance) may challenge the *status quo* and raise public awareness, it also introduces the danger of unintentionally reinforcing the systems of social control that activists seek to undermine. (p. 517)

Moreover, in projects like Mann's Shooting Back, Monahan is concerned that focusing on individual agents of surveillance (such as store clerks or security guards) reduces the complexity of the surveillance/countersurveillance problem; those individuals are easy targets but not the best ones, for they might be underpaid and completely dependent upon their jobs, hence, not the best representatives of institutional power.

The above discussion of the ethical dilemmas of surveillance and people's possible (un)intentional (dis)regard of the presence of surveillance in their lives is at the core of some of

the research questions of this research. What is the consumer's attitudinal outcome when faced with retail surveillance: is he for or against retail surveillance? And how does this affect their behavioural reaction? Do they accept (i.e., what Marx describes as compliance), negotiate, or resist (e.g., Marx' strategies of surveillance resistance, one of which describes Mann's counter-surveillance)? Those questions are revisited in Chapter 5.

Chapter summary and conclusion

As mentioned at the beginning of this chapter, despite the fact that surveillance is a hot button issue nowadays, only twenty-five papers (published between 1993 and 2020) employing empirical research relevant to the field of retail have been published (and one of them is more conceptual than empirical). A chronological summary list of this research is provided in Table 3. After compiling the literature review discussed in this chapter, it has become clear that there are numerous research gaps that are worthy of studying in the field of retail surveillance. (1) Although conceptual papers help researchers to conceptualize the topic being discussed, they do not provide empirical evidence that would encourage marketers, retailers, and/or policy makers to take action and make the needed changes. My work, therefore, combines both empirical and conceptual research; (2) There is a need for more detailed, and up-to-date surveillance research that focuses on the brick-and-mortar retail environment; (3) Only 25 empirical published research papers bridge the theme of surveillance and physical retail stores with a marketing perspective, focusing on either the retailer and/or consumer. So far, there is no research that integrates both perspectives; (4) Even when retail surveillance was studied, researchers focused on only one aspect or method of surveillance (e.g., shoplifting, loyalty profiling, physical environment, tagging, EAS false alarms, RFID technology, targeted advertisement, privacy, or

knowledge of surveillance) but there is no research that provides a general and more comprehensive understanding of the consumers' awareness of retailance, the impact of its presence, and their reaction to it, and how such knowledge could impact the retailer; (5) In only one study were interviews conducted (with shoplifting offenders). I, however, believe that listening to the consumer's narrative will provide a richer, more detailed account of how retailance impacts their shopping experience; those stories would open the door to new avenues of consumption studies; (6) Most research papers lacked a theoretical foundation, for only ten papers utilize theoretical frameworks, six of which were conducted by the same researchers (Kajalo and Lindblom). A more solid theoretical foundation should be added to the study of retailance in the field of marketing. Consequently, Chapter 3 is devoted to discussing the intersection of critical marketing and surveillance theory, as a first step in this direction.

In conclusion, filling the gaps in previous research, my work: (1) focuses on the brick-and-mortar retail environment; (2) provides a marketing perspective that is beneficial to retailers (i.e., practitioners), consumers and policy makers; (3) studies retailance in general and does not focus on one particular retailance system; (4) includes semi-structured interviews with consumers in addition to surveys; and (5) provides a solid theoretical background to the study. To sum up, building on previous research, I conduct a more in-depth examination of the consumer in a North-American retail setting, focusing on their awareness of the presence and scope of surveillance, their knowledge of the laws and regulations that protect personal and shopping information (a list of the main consumer rights in North America can be found in Appendix 3), the affective and behavioural impact on the consumer, and the subsequent attitudinal and behavioural outcomes (i.e., acceptance of, refusal of, or resistance to such surveillance practices).

Paper	Discipline	Publication venue	Perspective	Research model	Research location	Theory employed	Research aim(s)
Dawson 1993	Retail	<i>Journal of Retailing</i>	Consumer	Empirical: survey questionnaire	U.S.A.	---	The unintended effect of errant EAS alarms
Farrington et al. 1993	Criminology	<i>Crime Prevention Studies</i>	Retailer	Empirical: experiments	U.K.	---	Evaluating the effectiveness of crime analysis and situational prevention in preventing shoplifting
Handford 1994	Security	Book chapter	Retailer	Empirical: reviewing secondary data & interviewing managers, stock controllers & security guards	U.K.	---	Effective administration of the electromagnetic tagging system
Lin, Hastings & Martin, 1994	Retail	<i>International Journal of Retail & Distribution Management</i>	Retailer	Empirical: survey questionnaire of clothing stores' managers	U.S.A.	---	Examining clothing retail managers' attitudes towards shoplifting & their coping strategies
Overstreet & Clodfelter, 1995	Consumer research	<i>Journal of Shopping Center Research</i>	Consumer	Empirical: survey at twelve enclosed malls	U.S.A.	---	The effect of safety and security concerns on shopping behaviour
Pretious et al. 1995	Retail	<i>International Journal of Retail & Distribution Management</i>	Retailer	Empirical: survey	Scotland, U.K.	---	Surveying retail security methods employed by retailers
Lee et al. 1999	Criminology	<i>American Journal of Criminal Justice</i>	Retailer	Empirical: analysing data on crime	U.S.A.	---	Relationship between crime and private

				incidents, private security measures & demographic measures			security at shopping centres
Smith and Sparks 2003	Marketing/ Consumer research	<i>European Advances in Consumer Research</i>	Consumer	Empirical: case study analysing 2-year purchase records of one individual	U.K.	---	Ethical and privacy issues concerning retailers' use of loyalty card transaction records
Peek-Asa et al. 2006	Public health	<i>American Journal of Public Health</i>	---	Empirical: analysing crime reports	U.S.A.	---	Comparing the frequency and risk factor for employees and customers injured during crimes in retail and service businesses
Hossain and Prybutok 2008	Engineering management	<i>IEE Transactions on Engineering Management</i>	Consumer	Empirical: survey questionnaire	U.S.A.	Technology Acceptance Model (TAM)	Exploring the factors (convenience, culture, and security) that affect consumer acceptance of RFID technology
Grenville, 2010	Law	Book chapter	Consumer	Empirical: GPD survey data	Brazil, Canada, France, Hungary, Mexico, Spain & U.S.A.	---	The effect of the level of surveillance knowledge
Pridmore, 2010	Law	Book chapter	Consumer	Empirical: GPD survey data & consumer focus groups	U.S.A. & Canada	---	Consumers' knowledge of loyalty profiling & their concerns

Kajalo & Lindblom, 2010	Retail	<i>Facilities</i>	Retailer	Empirical: survey of grocery store retailers	Finland	Crime Prevention through Environmental Design (CPTED)	Understanding what kind of surveillance investments can be found from the stores with high consumer and employees' sense of security
Kajalo & Lindblom, 2010 & 2011	Retail	<i>Journal of Retailing & Consumer Services</i>	Retailer	Empirical: survey of grocery store retailers	Finland	CPTED	How retail entrepreneurs perceive the link between surveillance & customers' & employees' sense of security at the store level
Kajalo & Lindblom, 2011	Security	<i>Security Journal</i>	Retailer	Empirical: internet survey of retail entrepreneurs	Finland	CPTED	Retailers' approaches to preventing shoplifting
Lindblom & Kajalo, 2011	Retail	<i>International Review of Retail, Distribution & Consumer Research</i>	Retailer	Empirical: internet survey of store managers	Sweden, Norway & Finland	CPTED	The effectiveness of formal & informal surveillance in reducing shoplifting in the retail store environment
Lindblom & Kajalo, 2011	Retail	<i>Journal of Small Business and Enterprise Development</i>	Retailer	Empirical: internet survey of grocery store retailers	Finland	CPTED	Effectiveness of formal and informal surveillance in reducing crime at grocery stores
Cardone and Hayes 2012	Security	<i>Journal of Applied Security Research</i>	Consumer (shoplifting offenders)	Empirical: content and narrative	U.S.A.	Rational choice theory (RCT), situational crime	Identifying in-store situational (physical)

				analysis of interviews		prevention & CPTED	cues for crime prevention planning
Bonfanti, 2014	Retail	Book chapter	---	Conceptual	---	Customer Shopping Experience (CSE)	Analysis of the development of retailer/consumer relationships by highlighting how retailers can make store surveillance both secure and appealing to consumers
Turow, Hennessy & Draper, 2015	Communication	Report	Consumer	Empirical: wireline phone survey of consumers	U.S.A.	---	Americans' opinions about understanding a variety of online & offline privacy issues
Kajalo & Lindblom, 2016	Retail	<i>Facilities</i>	Consumer	Empirical: survey of shopping mall visitors	Russia	---	The role of formal and informal surveillance in creating a safe & entertaining retail environment
Esmark, Noble & Breazeale, 2017	Retail	<i>Journal of Retailing</i>	Consumer	Empirical: 4 studies (2 field experiments, 1 online scenario-based experiment & 1 behavioural lab setting)	U.S.A. & Amazon's Mechanical Turk platform	Reactance Theory	The impact of shoppers' perceptions of being watched by employees while shopping for embarrassing products
Samat, Acquisti & Babcock, 2017	Security	Conference paper (<i>Symposium on Usable Privacy & Security</i>)	Consumer	Empirical: online survey of consumers	(Amazon's Mechanical Turk platform)	---	The effect of awareness about online targeting on users' attitudes and purchase intentions

							towards the advertised product
Betzing, Hoang & Becker, 2018	Computing	Conference paper (<i>Multikonferenz Wirtschaftsinformatik</i>)	---	Literature review	---	---	Identifying digital capabilities of in-store technologies and relating them to the retailer's profit equation.
Margulis et al. 2019	Marketing/ Consumer research	<i>Journal of Business Research</i>	Consumer	Empirical: online survey of consumers	(Amazon's Mechanical Turk platform)	Seven seminal theoretical models: Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT 1 and UTAUT2), the role of emotions in marketing, and the diffusion of innovations theory	Creating a model that can help managers better forecast consumer reactions to ubiquitous technology (e.g., RFID) when used in marketing

Table 2 - A chronological summary of the 25 past research studies

CHAPTER 3: CRITICAL MARKETING & THEORETICAL FOUNDATIONS OF SURVEILLANCE STUDIES

“Man is born free, and he is everywhere in chains.”
(Jean-Jacques Rousseau’s *The Social Contract*, 1762)

A common characteristic between the fields of marketing and surveillance studies is their interdisciplinary natures. This trait has allowed marketing to borrow theories from other disciplines, a process that at times has involved “taking a concept or theory out of its original social and historical context and using it in another to explain the same or a different social or natural phenomenon” (Murray, Evers, & Janda, 1995, p. 92). On the other hand, surveillance studies are a multidisciplinary enterprise in which sociology offers some distinctive perspectives on empirical grounding (though in general, most of the work takes the form of critique and is non-empirical, hence, the fitting description as “studies” instead of “theories”). Other major disciplines play a role in surveillance studies. For example, early social scientists discussed the modern disciplines of capitalist supervision (Karl Marx), bureaucratic recordkeeping (Max Webber) (Lyon, 2007, pp. 18–24), the individual’s attempts at resistance in the urban metropolis (Simmel, Figure 40) and the disciplinary response to growing social inequality (Durkheim).

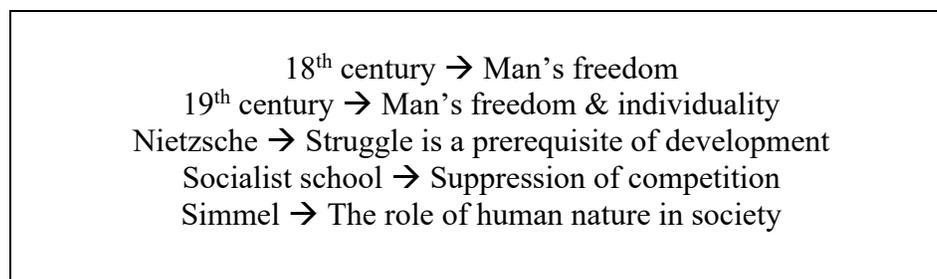


Figure 40 - The evolution of ideas leading to George Simmel’s “The Metropolis and Mental Life” (1903)

While surveillance practices could be traced back throughout history, they took specific forms in the modern world. New approaches and initiatives in theoretical explanation were

stimulated by the work of Michel Foucault and later debated and/or built on. At the turn of the 21st century, routine and systematic surveillance practices evolved from individuation (which reflects a process of differentiation between individuals) and bureaucratic organization (Dandeker, 1990) to become more technological and computer-based. Expanding beyond the study of the control of minorities by police and intelligence services, and initiated by sociologists such as Gary Marx (2012, 2016) and David Lyon, surveillance studies (i.e., theories) are now considered a field of research in sociology. To Lyon (2006b), surveillance theories are situated within and informed by classical, cultural, critical, and post-structuralist debates, as well as being related to history and humanity. To Gary T. Marx (2016),

The growing field of surveillance studies . . . serves as a reminder that while they—whether the state, commercial interests, new public-private hybrids, or free-range voyeurs—are watching us, we are watching them. (p. 320)

However, although there is currently a myriad of studies regarding surveillance, there is a lack of integration among literatures; surveillance theories are varied, fragmented, and scholars often disagree. Marx (2016) calls for “increased communication between fields, improved definition and operationalization of concepts, and nuanced abstractions filled with systematic empirical content” (p. 140). I second Marx’s call for the need of integration and empirical content, consequently, this research will bring together surveillance theories and will ground the findings related to retailance in empirical research.

This chapter is divided into two major sections: critical marketing and surveillance studies. In the first section, I will present a survey of critical marketing, how it differs from marketing criticism, its major concerns (being critical of the present, its ethical responsibility, and involving different stakeholders), its future, and how it shapes my approach to the topic of retailance (specifically the involvement of different stakeholders, power and (in)visibility, and

understanding versus mistrust). Demonstrating the multiplicity and complexity of influences, the second section brings together the ideas and theories of leading scholars of surveillance from the fields of political science, communications, media studies, science studies, war studies, law, cultural studies, sociology, criminology, and literature. In this section, surveillance studies will be grouped into five groups to fit the theme of retailance, and they are: (1) panopticism (Bentham, Foucault, and Gandy); (2) synopticism (Mathiesen and Andrejevic); (3) postpanopticism (Boyne and Lyon); (4) assemblage (Deleuze and Guattari, and Haggerty and Ericson); and (5) virtual identities (Haggerty and Ericson, Poster, Deleuze, Bogard, and Lyon). The chapter concludes with a survey of the rise in popularity of surveillance studies, tracing the link between surveillance and marketing history, and a conclusion.

Critical Marketing

There is no one true definition of critical marketing (Schroeder, 2007, p. 24), and the scholars working in the field have drawn their inspiration from a number of philosophical and theoretical sources, such as Karl Marx (especially his discussion of “commodity fetishism”¹³ and “circulation of capital”¹⁴), the Frankfurt School of Critical Theory (and their critique of late capitalist¹⁵ societies, mass deception, restrictions of individual autonomy, and the dominance of

¹³ According to Marx, when a product is evaluated in relation to other commodities rather than within the social relations in which it was produced it becomes fetishized (Svensson, 2019, pp. 157–158).

¹⁴ Marx’s circuit of capital is designed to produce surplus value and to deliver a return on invested capital. It takes place in three stages: M-C (*monetary capital*, or money, is transformed into *productive capital*), P (commodities pass through the process of *production* so that they have more value than that of the elements entering into the production), and C’-M’ (*commodities are transformed into monetary capital again*) (K. Marx, 1977, p. 153).

¹⁵ Late capitalism refers to modern capitalism after World War II and the perceived absurdities, injustices and crises created by modern business.

technocratic control of consumers), and Michel Foucault (especially the Foucauldian analysis and conceptualization of power, how it is an inevitable and concrete aspect of relations and organizations, and how it can be both repressive of autonomy and a productive force) (Saren et al., 2007, p. xviii; Svensson, 2019). A brief history of the development of critical marketing follows.

The 1920s started witnessing writings against the system of values and practices promoted by the advertising industry that were believed to be harmful, psychologically damaging and unfulfilling (Tadajewski, 2010b, p. 780; 2012, p. 441). Scholars and critical observers, like James Rorty (a major critic of advertising that manufactures what he called a “pseudoculture”) and Robert Lynd (who discussed the power relations between big business and the consumer), first began to scrutinize and critique the marketing system in the 1930s after the burst of the U.S. economic bubble with the onset of the Great Depression. Instead of being seen as contributors to social progress and a rising standard of living, business and marketing practices were found wanting (Tadajewski, 2010b, p. 779). In the early 1940s, scholars, such as Paul Lazarsfeld, became particularly interested in the contribution that critical theory offered to marketing related studies. The period from 1940 until the late 1960s did not see a growth in the use of critical perspectives, for after all, the postwar period was one of economic affluence, rising marketing expenditures and increasing profits were positively correlated, and the rising standards of living did not invite criticism¹⁶. This changed in the 1960s and 1970s when greater

¹⁶ In 1953, Paul Mazur, an investment banker at Lehman Brothers and an authority figure in marketing circles with his development of organization principles for contemporary department stores, published *The Standards We Raise: The Dynamics of Consumption* in which he advocated that the major societal task in the U.S. is to continuously improve the standard of living, a task that can be only accomplished when increasing consumption is accepted and marketing is encouraged (Monieson, 1988, p. 5).

scrutiny was directed towards the environmental and social consequences of marketing (p. 781). During those years, scholars and critical observers witnessed with discomfort how marketing activities helped support the “military-industrial-complex” and the extension of materialistic values to people, which ultimately encouraged them to rethink the relationship between marketing and society. In the 1980s, marketing was influenced by reconstructionists who wanted to remould the discipline along humanist lines, allowing all mankind, rather than a particular sub-set of society, to benefit from it, and by the humanist movement (Tadajewski, 2014, p. 41; Tadajewski & Jones, 2014, p. 1265). Monieson (1988) argued that marketing should become a “human science” governed by ethics and personal responsibility, and Benton (1985) called for an ethical approach to marketing activities that would guide both scholars and practitioners and that would include the well-being of nonhuman nature.

At the turn of the 21st-century and afterwards, critical marketing has been influenced by schools such as critical sociology (and how marketing operates through the manipulation of the human psyche), feminist theory (for example, the exposition of gendered assumptions embedded in marketing and consumption phenomena, as well as the unequal power relations that underpin them), postmodernism, poststructuralism, postcolonialism (which helps in challenging the universality of canonical Western theories about markets and consumers, and situates them within specific spatial, cultural and institutional contexts), psycholinguistics, deconstruction and radical ecology (Maclaran & Kravets, 2019; Svensson, 2019; Varman, 2019). One definition of critical marketing subscribes it to radical philosophies and theories that “explicitly seek to identify and question the ideologies and assumptions underlying the production and consumption of knowledge” (Catterall, Maclaran, & Stevens, 2002, p. 184). Tadajewski and Brownlie (2008, pp. 9–11) outline three criteria for critical marketing: (1) Marketers should be critical of the

notion that the pursuit of profit will automatically satisfy the broader goals of human solidarity, human development, justice, and/or ecological balance; (2) Critical marketing should attempt to question the extent to which specific claims made in support of marketing practice affect society; (3) Critical marketing scholarship should recognise the role of the researcher in the production of knowledge about the marketing phenomena. Within the context of critical marketing, Gould (2008, p. 313) has taken a step further by advocating for the employment of introspection as critical marketing thought. He argues that introspection concerning one's own subjectivity (i.e., "looking within yourself and watching your thoughts and feelings and what your views seem to be aiming at") is a key to the construction and comprehension of critical thought. In other words, when one (i.e., researcher) engages in introspection, one is "taking a critical position in the field, relative to everyone else, including other introspectors." The relation between critical marketing and introspection is then symbiotic.

With such a wide array of influences, I will only focus on critical marketing issues that fit the context of the retail research: (1) its multidisciplinary nature, (2) how it is different from marketing criticism, and (3) some of the concerns it focuses on. First, Gavin Jack, at the University of Leicester, contends that critical marketing involves "the import of multidisciplinary insights into consumption and power into the discipline" (quoted in Schroeder, 2007, p. 24). The same belief in the multidisciplinary nature of critical marketing is echoed by Janice Denegri-Knott, a lecturer at Bournemouth University,

Theoretically then, critical marketing goes beyond marketing theory and adopts a multidisciplinary character in order to appropriate and adapt conceptual tools best suited to understand marketing and a social reality. (quoted in Schroeder, 2007, p. 25)

Secondly, Detlev Zwick, an Associate Professor at York University, Canada, differentiates between critical marketing and marketing criticism, connecting marketing to key social concerns, such as justice, equality and autonomy. To Zwick,

One of the differences between critical marketing and critics of marketing, it seems to me, is that the former accepts the function of marketing as an articulation of the expansion of capital in general but sees room for improving its workings with regard to social justice, gender equality, cultural autonomy etc., while the latter, simply put, reject marketing as one of the root causes of much the contemporary social and cultural ills in capitalist market systems. (quoted in Schroeder, 2007, pp. 21–22)

Thirdly, there are three major concerns of critical marketing: (1) challenging the present marketing concepts to bring change; (2) an ethical responsibility; and (3) influencing policy and practice by involving different stakeholders. A major concern of critical marketing is to “be critical of the present” (Benton, 1985, p. 202) and to help all people/consumers to make sense of the constraints and contradictions they face in their everyday lives (Brownlie, 2007, p. 666).

Tadajewski argues that critical marketing is concerned with

...challenging marketing concepts, ideas and ways of reflection that present themselves as ideologically neutral or that otherwise have assumed a taken-for-granted status. (Tadajewski, 2011, p. 83)

A good example would be surveilling consumers. By tracking, tracing and seducing consumers, marketing can be viewed as “the engine of a vast panoptic system of observation and social control” (Alvesson, 1994; Brownlie, Saren, Wensley, & Whittington, 1999, p. 8). Brownlie et al. further link marketing and surveillance by arguing that:

...the discipline of the market, with its subtle architecture of consumer surveillance, regulated information provision and constrained choice, can be seen as the new panopticon, a revitalized metaphor for a new disciplinary mode of domination. (Brownlie et al., 1999, p. 13)

Broadly speaking, critical marketing studies seek to question the way we think about marketing theory, thought and practice (Tadajewski, 2012). For critique to be effective, it has to bring some

type of change, “not only in ways of thinking, but also in ways of doing” (Saren et al., 2007, p. xxi). Shona Bettany writes that critical doctoral students in marketing have to “tread a very uneasy path” (2007, p. 69) situating themselves as “an oppositional subject” in their research (p. 71), and understanding that the starting point for their critical authorship is the value of “not knowing” (p. 78).

The second concern, voiced by Tadajewski, Higgins, Denegri-Knott, & Varman (2019, p. 2), is that critical marketing should aim to have an “ethical responsibility” to present an accurate, more balanced picture of the marketing discipline, along with the latter’s core assumptions and effects across the world.

The third task is how critical marketing is to carry out the task of influencing both policy and practice as well as having an indirect impact via teaching practices (Wensley, 2007). Critical marketing should not only focus on the consumer, but it should also draw attention to practitioners, for after all, a real marketing change will have to involve different stakeholders (i.e., consumers, retailers, policy makers). I, therefore, agree with Tadajewski that:

Critical Marketing Studies needs to engage with marketing actors and this requires a different relationship between Critical scholars and practitioners than may have been the case previously. (Tadajewski, 2010a, p. 210)

[Critical Marketing] prefers to ask questions about why problematic aspects have taken centre stage, while other more socially beneficial approaches and ways-of-life have been side-lined. (Tadajewski, 2014, p. 41)

[If scholars] start work across thought communities, combining these endeavours with practitioners, public-policy makers and activist groups, they can forge solutions to the pressing problems facing the world. (Tadajewski, 2014, pp. 46–47)

A similar perspective is shared by Ingrid K. Mitchell. Influenced by organizational change theory, Mitchell (2007, pp. 212–215) argues that a marketer should be an “agent of change,” meaning that they should play an important role in creating a vision of a desired future by

seeking to help both organizations and other stakeholders devise strategies for managing the transition from the present to the future. Once researchers position themselves as agents of change, they “begin to acknowledge . . . [their] academic abilities not only to interpret, and respond to the circumstances around . . . [them], but . . . [their] role in shaping those interpretations” (p. 214). In this context,

being critical does not mean standing *outside* marketing exposing its many flaws and weakness, rather it involves an active commitment to improving the abilities of those practising marketing to question the status quo and envisioning alternatives . . . critique is then not something that is opposed to Marketing, but rather seeks to encourage participation and involvement in change by those who are affected. (Mitchell, 2007, p. 212)

A marketer/researcher, therefore, must be able to persuade stakeholders (in this case, retailers and policy makers) that the suggested changes are the logical way to meet their needs. To achieve such a change, marketers need “to think paradoxically,” meaning that they need to realise that no one is capable of knowing in advance what a situation is like, consequently, a “paradoxical” understanding of one’s previous identity would lead to “deframing,” or loss of meaning and old prejudices, which would then make one open to other lines of thought (p. 228).

Writing about the future of critical marketing studies, Svensson concludes that

[it] is not only a matter of being responsive to societal changes. Perhaps more importantly, critical research needs to write itself into relevancy, not only by means of addressing issues experienced as problematic in today’s society, but also by means of problematizing everything in society that seems unproblematic and unquestionable. (Svensson, 2019, p. 167)

The term “critical,” therefore, implies how research can be an emancipatory force capable of changing oppressive social conditions and structures.

Critical marketing approach to this research

My approach to this research is carried out through a critical marketing lens. Prior to the collection and analysis of data, my stance on how to approach the retailance topic could be summarized in three general themes: involving different stakeholders, power and (in)visibility, and understanding versus mistrust (Figure 41). Those three components will serve as undercurrents throughout the research, further explaining the model of theories and shaping how I look at and analyze the collected data.

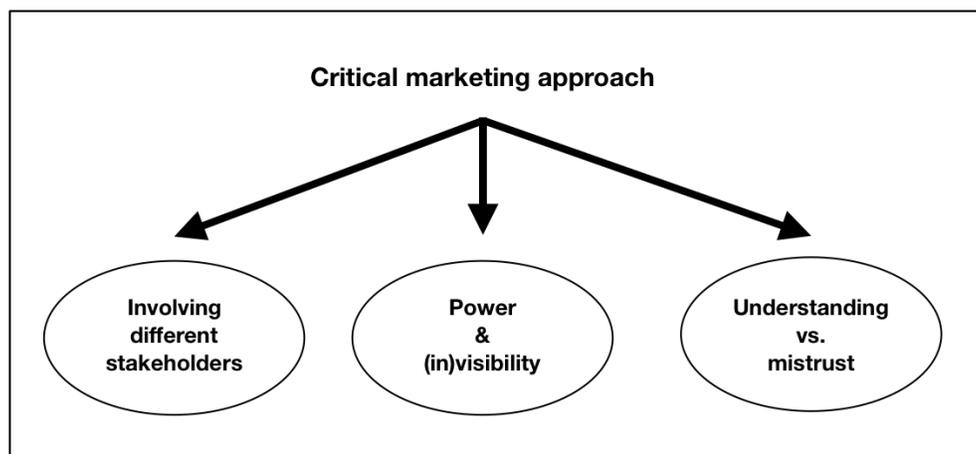


Figure 41 – Critical marketing approach to this research

(1) Involving different stakeholders

I agree with Tadjewski (2010a, 2014) that a real marketing change has to involve different stakeholders (i.e., consumer, retailer/practitioner, and policy maker). I also agree with Mitchell (2007) that a researcher has to play an active role in shaping the interpretation of the context under study (i.e., the effect of retailance on both consumers and retailers). This stance of including different stakeholders stands in open contrast to one of the foundational injunctions to the field of consumer research which is that the critical consumer researcher should “take sides,” specifically the side of the consumer (rather than the manager), a stance that differentiates

consumer research from marketing research (Denzin, Norman, 2001; Earley, 2015; MacInnis & Folkes, 2010). In this research, I argue against choosing between consumer welfare and managerialist research, for my goal is not to differentiate between consumer behaviour research and marketing research, but to find common grounds that would help both parties. Moreover, practitioners are usually put in one of two camps: one that focuses on the bottom line, and one that engages more seriously with ethics and social responsibility. This research, however, stems from the perspective that understanding, respecting and accommodating consumers' ethical concerns related to retailance can also have a positive effect on retailers' profit. A more detailed discussion of the pragmatic and interpretative nature of the research design employed can be found in the next chapter.

(2) Power and (in)visibility

When looking for power in market relations, Denegri-Knott (2019) points out several scenarios, chief amongst them are (1) consumer sovereignty, meaning “power is assumed to rightfully reside in the aggregate, with free choices made by autonomous and self-interested consumers directing the market’s invisible hand” (p. 290); (2) power “inhibits the identification and realization of real needs and instead implants desires and thoughts which serve the long-term interests of a ruling class,” meaning that power operates by elevating “having” rather than “being” as a meaningful mode of existing (p. 294); and (3) based on Foucault’s perception of power as both productive and creative, the study of power requires a general suspicion toward what is believed to be a universal truth (p. 297). Moreover, emancipation in the context of critical marketing is not a final end in itself, but “an ongoing process, a state of mind that needs

to be nurtured and sustained: for one person's emancipation is surely another's imprisonment" (Brownlie et al., 1999, p. 10; Eagleton, 1991, p. 4).

One aim of critical theory (one of the major contributors to critical marketing) is to "make the invisible visible, and to give voice to what has been silenced;" therefore, focusing on the ostracized, critical theory has feminist, racial, political, and social implications (Earley, 2015). Taking a stance against discriminatory practices are Lyon (2003a)—who considers database marketing (a form of consumer surveillance) a source for producing discriminatory practices and reproductions of systems of power—and Poster (1996)—who argues that the development of databases (which will be discussed in the coming sections as the "superpanopticon") serves to refute the hegemonic principle of the subject as centred, rational and autonomous, for the database "directly amplifies the power of its owner/user" (p. 284). Once again, my position is different in this research, for dataveillance is not the only form of retailance. I do not see the surveilled consumer as the Other (i.e., the marginalized) while the retailer is the centre of power. The way I see it, in the retail environment, the relationship between the consumer and the retailer is more complex and the centre of power keeps shifting between them. The consumer is not invisible (whether they know it or not), on the contrary, their visibility is sought after. When it comes to surveillance, it is more difficult (and even impossible) for the consumer to attain a cloak of invisibility. This power struggle happens whether retailance itself is visible (i.e., overt) or invisible (i.e., covert). It should be noted that the word "invisible" in this context has different meanings when it comes to individuals (i.e., consumers) vs. objects/systems (i.e., surveillance). To individuals, (in)visibility is a metaphor that denotes them being either marginalized or the centre of attention. To objects/systems, (in)visibility is a description of their physical presence, and whether it can be detected by individuals or not.

(3) Understanding vs. mistrust

To Foucault, each form of power is accompanied by a form of resistance, a concept that led to his adoption of “hyperactive pessimism” which he exemplifies by the quote:

My point is not that everything is bad, but that everything is dangerous which is not exactly the same as bad. If everything is dangerous, then we always have something to do. So my position leads not to apathy but to a hyper- and pessimistic activism.

I think that the ethico-political choice we have to make every day is to determine which is the main danger. (Foucault, 1982, pp. 231-232)

Craig Thompson adopts Foucault’s hyperactive pessimism, for to the former, overturning one regime of power only brings a new form of power (Earley, 2015). Instead of taking sides, Thompson adopts an agnostic stance of not trusting anything; his perspective of critical work is based on destabilizing regimes of power.

If I had adopted Thompson’s view, my research would have preached about the evils of surveillance and the need to abolish them completely. But that is not the case, for this research is not concerned with juxtaposing the dark and bright sides of marketing. As has been discussed earlier, in addition to maximizing profits, some surveillance techniques used by retailers help them in protecting their stores and ensuring the safety of both their employees and consumers. Consumers, on the other hand, now expect the convenience of “what I want, when, where, and how I want it” (Zuboff, 2018, p. 30). This research, therefore, aims to understand both the pros and cons of retailance from the point of view of both retailers and consumers by studying the lengths to which retailers would go to implement surveillance, and why consumers would accept, encourage, or defy such implementations.

Surveillance studies

One drawback of the interdisciplinary nature and origins of surveillance studies is that the field has become very chaotic. Adopting a chronological approach to trace theory development does not work fully since there are too many readings and interpretations of surveillance, and those interpretations have smoothly developed over time, clashed with each other, or integrated one into another. One of the main contributions of this research, therefore, is surveying surveillance theories, looking at them from a different perspective (i.e., that of their relevance to the field of retail), and synthesizing their relevance to marketing research. Looking at surveillance studies (from the mid-twentieth century and until today) as a progression of trends, I have grouped them into five major trends: Big Brother, panoptic, post-panoptic, beyond the panoptic, and the rediscovery of Foucault (Figure 42). However, although grouping surveillance studies in groups of trends clarifies the development in the field, it does little to explain how those theories/studies can be relevant to retailance. I, therefore, designed a new model in which surveillance studies are grouped based on how they explain retailance, throwing light on important analytical concepts (Figure 43). Those groups are: (1) panopticism developing into (2) synopticism and (3) post-panopticism, (4) assemblage, and (5) virtual identities. The next section will review surveillance studies based on this model, while highlighting how surveillance studies correspond with the retailance model (underlining “surveiller”, “surveilled” and “surveillance channels”) and align with a critical marketing approach.

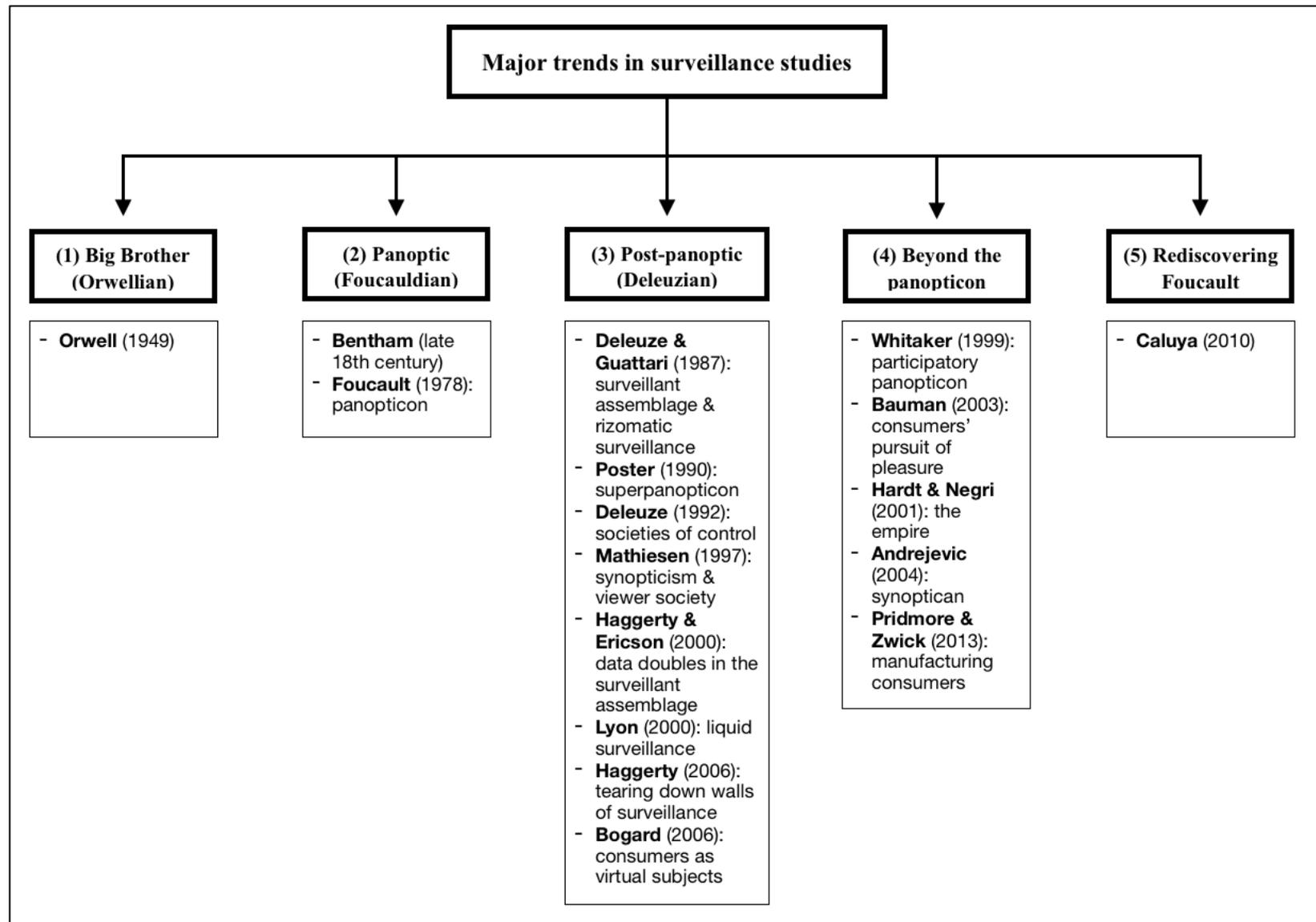


Figure 42 – Major trends in surveillance studies

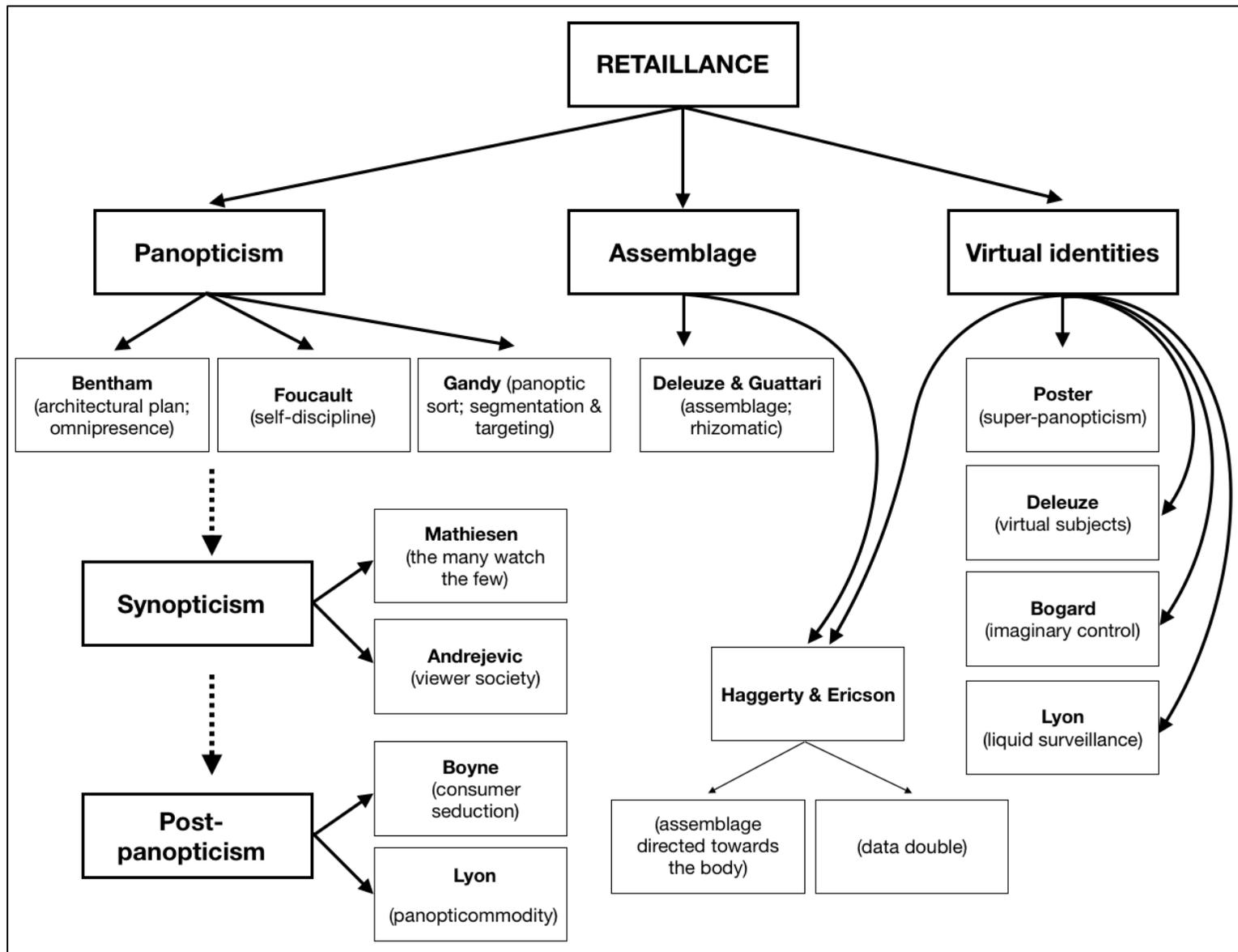


Figure 43 –Surveillance studies in the context of retaillance

A brief historical background

Before reviewing the history of surveillance studies, a very brief historical review of the emergence of surveillance in Western societies should be given. In the 15th century, and under the watch of the biblical God, political and religious surveillance were indistinguishable, and they ranged from keeping basic records of births, marriages, baptisms, and deaths, to the policing of religious consciousness, ritual, and religiously based rules, to the search for heretics, devils, and witches (Marx, 2016b, pp. 40–41). In the 16th and 17th centuries, with the emergence of the nation-state and the spread of secularism, political surveillance became more sophisticated, which led to new fears of being watched and suspected of political (dis)loyalty. The 17th century was also the time of disciplined administration which has its origin in the management of plague outbreaks that produced a temporary counter-society of quarantined sick citizens (Boyne, 2000). During plagues, the procedures of segmentation and surveillance were based on a system of permanent registration, where quarantined citizens in enclosed, segmented, disciplined spaces (i.e., locked inside their houses) were constantly observed until survivors could go through the process of purification at the end.

On the literary front, the early 20th century saw the publication of literary masterpieces that discussed surveillance and its individual, societal and political implications. In Kafka's novella, *In the Penal Colony* (1919), a prison officer invents a sophisticated machine for punishing inmates and is ultimately killed by his creation. Similar to Orwell, Kafka's work describes the shadowy powers that leave people uncertain of anything and focuses primarily on agents of the state. On the other hand, instead of focusing on a Big Brother presence, Kafka portrays the sense of being in a maze. Other works by Kafka that have a surveillance theme are *The Trial* (1914-1915) and *The Castle* (1926). Another dystopian work where surveillance play a

major role is Huxley's *Brave New World* (1932) in which biological and systematic surveillance are featured. Before the advance of surveillance technologies, and in 1949, George Orwell had his dystopian novel, *Nineteen Eighty-Four* (1989), published. It is one of the most significant novels of the 20th century and many of its terms and concepts have entered into common usage since publication, for example, "Big Brother is watching you," "doublethink," "thoughtcrime," "telescreen," "2+2=5," and the adjective "Orwellian." Since its publication, the novel has received critical acclaim and has had cultural, media and linguistic influences. In 2017, the book's sales skyrocketed, becoming the number one bestselling book on Amazon, in the wake of accusations that the Trump administration operated on "alternative facts" which was likened to "doublethink," or the simultaneous acceptance of two mutually contradictory beliefs as correct (Lazzaro, 2017). In Orwell's futuristic nation of Oceania, the "thought-police" is an agent of a centralized totalitarian state that uses surveillance primarily as a means to maintain social order and conformity. Surveillance, therefore, is portrayed as immanent within the totalitarian, bureaucratically organized nation-state. In recent decades, however, Orwell's society of physical discipline and his cautionary tale of "Big Brother" (which has become a metaphor of exercising total control over people's lives) has been surpassed, for he never imagined how rapidly surveillance would extend its global reach and how both state and non-state institutions would be involved in monitoring different populations (Haggerty & Ericson, 2000; Lyon, 1994, pp. 57–63).

The field of surveillance studies in its modern form started being of interest to scholars since at least the 1950s, with the rising awareness of human rights, the appearance of new technologies and their subsequent profound implications for social behaviour, organizations, and societies, and the publishing of literary works.

(1) Panopticism¹⁷: Bentham, Foucault and Gandy

Although the mid-20th century saw the emergence of surveillance studies, an event taking place in the late 18th century marks the beginning of panoptical studies. In the late 18th century, philosopher and social theorist Jeremy Bentham designed the panopticon, an institutional building and a system of control (Figure 44) that could be applied to any penitentiary house (Figure 45). In Bentham's architectural plan,

Each individual, in his place, is securely confined to a cell from which he is seen from the front by the supervisor; but the side walls prevent him from coming into contact with his companions. He is seen, but he does not see; he is the object of information, never a subject in communication. The arrangement of his room, opposite the central tower, imposes on him an axial visibility; but the divisions of the ring, those separated cells, imply a lateral invisibility. And this invisibility is a guarantee of order. If the inmates are convicts, there is no danger of a plot, an attempt at collective escape, the planning of new crimes for the future, bad reciprocal influences; if they are patients, there is no danger of contagion; if they are madmen there is no risk of their committing violence upon one another; if they are schoolchildren, there is no copying, no noise, no chatter, no waste of time; if they are workers, there are no disorders, no theft, no coalitions, none of those distractions that slow down the rate of work, make it less perfect or cause accidents. The crowd, a compact mass, a locus of multiple exchanges, individualities merging together, a collective effect, is abolished and replaced by a collection of separated individualities. From the point of view of the guardian, it is replaced by a multiplicity that can be numbered and supervised; from the point of view of the inmates by a sequestered and observed solitude (Bentham, 60-64). (qtd. in Foucault, 1978, pp. 200–201)

The word “panoptical” comes from the Greek word *pan*, meaning “all”, and *opticon*, which represents the visual (Mathiesen, 1997, p. 217). By having a central observational tower and prison cells arranged around it to increase security and facilitate more effective surveillance, Bentham's design put prisoners under potential observation at any time, however, since prisoners could not see whether they were observed or not, they had to self-monitor their behaviour,

¹⁷ The words “panopticism; panoptic; panopticon” are used interchangeably.

ultimately disciplining themselves (Bentham, 1791). Thus, in addition to its being a system for observation, the panopticon works with explicitly articulated behavioural norms as established by the emerging social sciences (Haggerty & Ericson, 2000). Bentham's work, consequently, emphasized two approaches: first, self-discipline becomes the archetypical modern mode of discipline, supplanting earlier coercive and brutal methods, and second, focusing on classificatory schemes within which sovereign power was capable of locating and differentiating the treatment of different prisoners (Lyon, 2006b, p. 3). Although Jeremy Bentham failed to launch his panoptic enterprise in England (Semple, 1993, p. 244), his architectural plan was first constructed by his brother Samuel, an engineer, in 1787 for a factory at Critchef, Russia (Zuboff, 1988, p. 320). At that time, workplace control was important as "the [labouring] body became the central problem of production" and industrial employers strived to "regulate, constrain, anchor, and channel bodily energies for the purposes of sustained, often repetitive, productive activity" (p. 319).

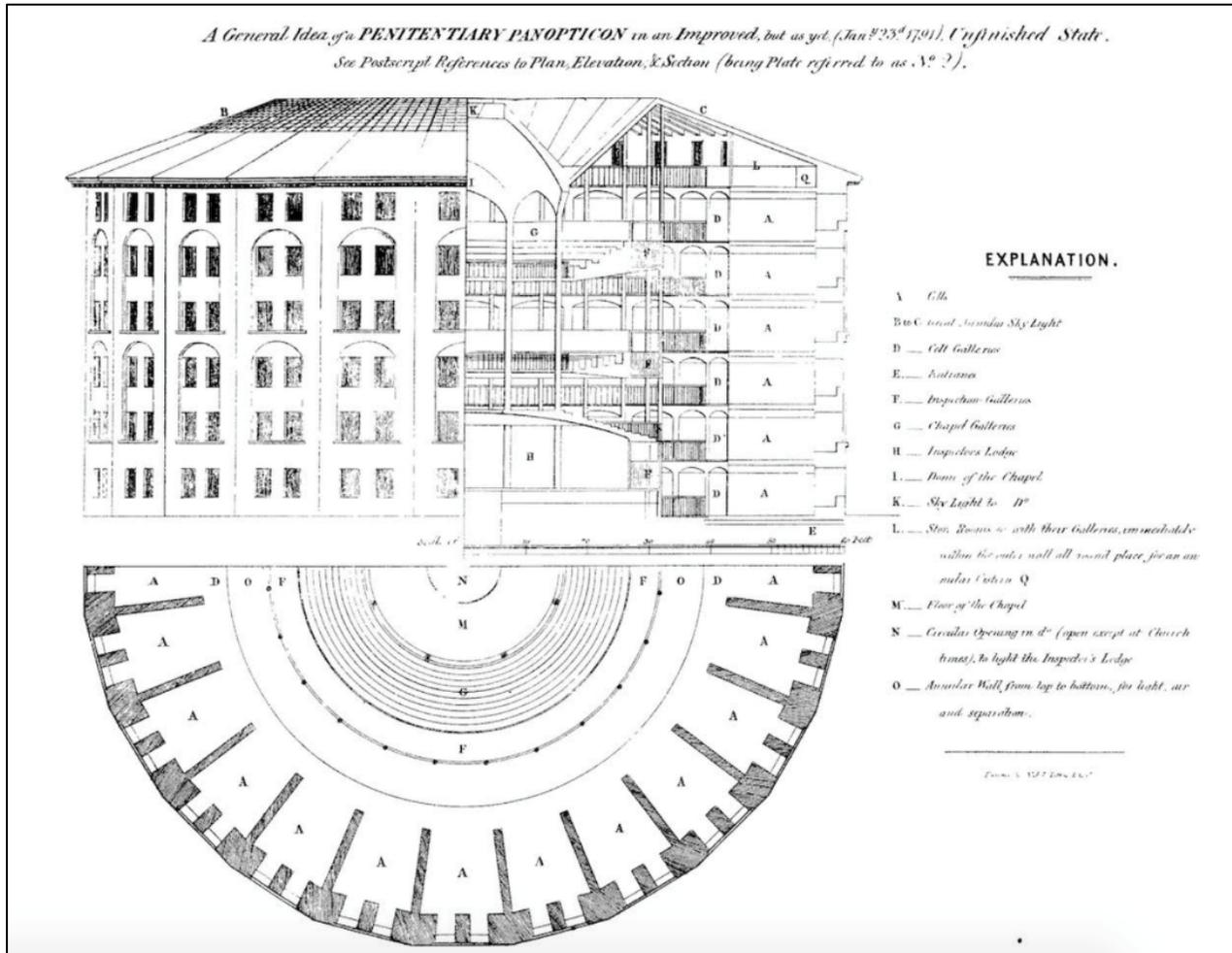


Figure 44 - Elevation, section and plan of Jeremy Bentham's Panopticon penitentiary, drawn by Willey Reveley, 1791. Source: J. Bentham, *Panopticon Works*, Vol. IV, no. 17.

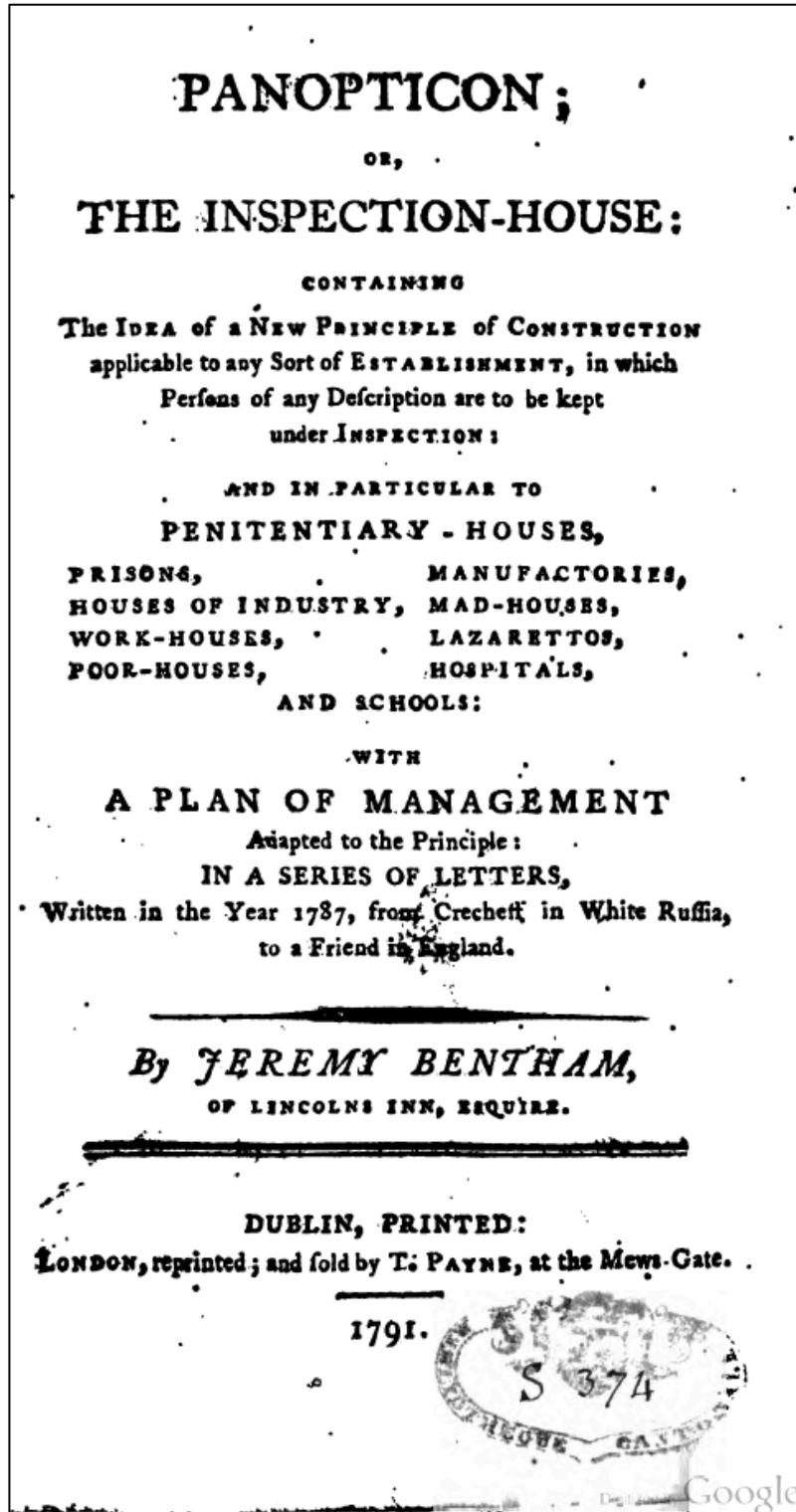


Figure 45 - Bentham's *Panopticon; or, The Inspection-Houses* book cover (scanned by Google)

Although contemporary prisons with their high-security buildings far surpass Bentham's original vision (Rhodes, 1998), his concept of panopticism would later serve as a key theoretical frame of surveillance studies (Elmer, 2012). Through Bentham's design, contagious disease, unruly conduct, and violence could be controlled and disciplined, not by physical violence, but by self-discipline and the fear of being seen¹⁸.

Bentham's architectural design for a prison, centred on the illusion of an omniscient surveillant, became a stepping stone for the French philosopher and social theorist Michel Foucault, whose work on surveillance explicated the metaphor of the panopticon. In his 1975 *Surveiller et punir: Naissance de la prison* (published in English under the title *Discipline and Punish: The Birth of the Prison* (1978)), Foucault argues that being subjected to such disciplinary power has extended everywhere in society, and it is no longer only prisoners who are put under surveillance. To him, surveillance and the strategic use of information are tools of social control.

But the Panopticon must not be understood as a dream building; it is the diagram of a mechanism of power reduced to its ideal form; its functioning, abstracted from any obstacle, resistance or friction, must be represented as a pure architectural and optical system: it is in fact a figure of political technology that may and must be detached from any specific use. (1978, p. 205)

A distinction should be made between Bentham's understanding of surveillance (which focuses on the reality of monitoring by an omnipresent inspector) and the Foucauldian emphasis on discipline (which entails a kind of automatic docility and self-government), hence, a distinction between watching (Bentham) and being watched (Foucault) (Elmer, 2012). With Foucault, the

¹⁸ The context here is the fear of physical visibility, for examples, prisoners fear being literally seen doing something that would merit discipline. In the context of retail, fear of visibility could be either literal (e.g., when consumers fear being seen shoplifting) or metaphorical (e.g., when consumers feel uneasy to be followed around and/or watched closely).

content of punishment has changed, from physical punishment to a transformation of the soul in a democratic capitalist society in which human beings control themselves via self-control

(Mathiesen, 1997, p. 217). To Foucault,

In appearance, it [the panopticon] is merely the solution of a technical problem; but, through it, a whole new type of society emerges. (1978, p. 216)

He, therefore, believed that the concept of confining architectures instills a form of discipline in the individual, making them act independently, and at the same time, conforming to their modern, industrial, democratic society, hence, an illusion of freedom¹⁹.

In Foucault's revisioning of the panopticon, "zones of darkness" (which threaten the transparency of society) are eradicated by the visual power of the disciplinary machine, in other words, the trap of permanent visibility assures the automatic functioning of power²⁰. The Foucauldian panopticon explains why retailers employ overt surveillance systems in stores (e.g., reminding consumers that they are being watched by CCTV cameras in an effort to lessen shoplifting and acts of violence). In other words, retailers control the literal "zones of darkness"

¹⁹ For Foucault, the modern feature of discipline is based on binary oppositions (e.g., self and other, normal and abnormal, or delinquent and non-delinquent), but for Hardt and Negri (2001), what matters most in postmodern forms of control is the "absolute fluidity of identity, the disappearance of the line between self and other, the seamless integration of bodies and information systems" (Bogard, 2006, pp. 63–64). The current retail environment can be easily seen as part of Hardt and Negri's new empire: a world where corporations determine the new geography of the world market and where communication systems and information networks exercise a new power of control.

²⁰ In her study of the lives of inmates in supermax prisons, Lorna Rhodes (1998, 2004) challenges Foucault's reading of the panoptical effect, and comes to the conclusion that disciplinary spaces actually invite and magnify disorder, pollution and noise, allowing prisoners to turn their private and destructive bodily acts into spectacles (for example, when prisoners throw faeces, self-mutilate, and create disturbances). Thus, the docility Foucault describes may reflect the intention of the panopticon, but the reality in which inmates are confined reflects a noisy, smelly, and negative intimacy. This contradiction (between Rhodes and Foucault) is an example of the divergence between theory and practice. Yet while Rhodes' view points out a flaw in the universality of Foucault's concept, it does not fully negate it, for outside prison, and in the retail sector, the panoptic still has a role to play.

(e.g., shoplifting and violence) that threaten the “society” (i.e., consumers and employees in retail stores) by using the power of the disciplinary machine (i.e., retailance). When applied to today’s world of social media, such as Facebook, issues of privacy, exposure and visibility reflect the augmentation of surveillance practices, since users both give up their information and take advantage of the visibility of others (Trottier, 2016). Panopticism, therefore, is the disciplinary society of surveillance:

He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection. (Foucault, 1978, pp. 202–203)

This conflict between privacy (which can be considered a form of invisibility) and visibility is one of the themes critical marketing is concerned with.

Foucault uses the term “panopticon” to describe both the development and the transformation of the Orwellian society from a society of physical discipline to one being managed and monitored by the state (Bigo, 2006). Instead of the Orwellian surveillance that maintained a form of hierarchical social control, Foucault’s panoptic surveillance targeted the masses, forming a system of self-monitoring that was in harmony with the requirements of the developing factory system (Haggerty & Ericson, 2000, p. 615). Thus, his panopticon vision went beyond the prison to include other disciplinary institutions in his era, such as the factory, hospital, military, and school, and it acknowledges the role surveillance plays beyond repression which is contributing to the productive development of modern selves (Haggerty & Ericson, 2000, p. 607). Foucault’s panopticism has been transported “from the penal institution to the entire social body” (1978, p. 298), and his prison becomes the focus for the administrative production of a divided and more easily manipulated working class (Dandeker, 1990, p. 27).

The panoptical spectrum (from rigorous to soft) has invoked analyses of prisons, workplaces, government departments, entertainment, and consumption. In the *Panoptic Sort* (1993), Gandy demonstrates how consumers are filtered through a “triage” that distinguishes and treats them differently based on their worth to the corporation.

[The] “panoptic sort,” [is] the all-seeing eye of the difference machine that guides the global capitalist system . . . I see the panoptic sort as a kind of high-tech, cybernetic triage through which individuals and groups of people are being sorted according to their presumed economic or political value . . . the panoptic sort operates to increase the precision with which individuals are classified according to their perceived value in the marketplace and their susceptibility to particular appeals, the commoditization of information increases the dependence of these interests on subsidized information. (pp. 1-2)

The panoptic sort is the . . . complex technology that involves the collection, processing, and sharing of information about individuals and groups that is generated through their daily lives as citizens, employees, and consumers and is used to coordinate and control their access to the goods and services that define life in the modern capitalist economy . . . [It] is a system of disciplinary surveillance. (p. 15)

Panopticism, therefore, becomes a powerful metaphorical resource for representing the contemporary technology of segmentation (with its negative impact of limiting consumers’ life chances) and targeting that involves surveilling, categorizing consumers and using them in market tests that have the character of experiments (Gandy & Simmons, 1986). It involves three integrated functions or processes: “identification” (which largely depends on the ability of users to reliably identify the objects to be controlled, and this level of identification is indicated by the importance of the transaction that is about to take place), “classification” (which involves the assignment of individuals to conceptual groups on the basis of identifying information), and “assessment” (a particular form of comparative classification where individuals are compared with others through the use of assumptions about normality and the examination of probabilities) (Gandy, 1993, pp. 15–18). The goal of those processes is normalizing behaviour within

categories (i.e., “correct training”) through (1) surveillance or hierarchical observation, (2) normalizing judgement, and (3) examination and evaluation (p. 24).

(2) Synopticism: Mathiesen and Andrejevic

One of the well-cited papers in the post-panoptic literature is Thomas Mathiesen’s “The viewer society: Michel Foucault’s ‘Panopticon’ revisited” (1997). In his paper, Mathiesen highlights three of Foucault’s themes in *Discipline and Punish*: (1) a shift in the nature of punishment (from torture to imprisonment); (2) a shift in the content of punishment (from body to soul); and (3) a change in the social order exemplified by the panopticon. Mathiesen, however, sees this social change not only as a characteristic feature of the modern prison, but also as a movement towards “synopticism.” Mathiesen’s “synopticism” (where the many see and contemplate the few) is the reverse of Foucault’s panopticism (where the few see the many). To Mathiesen, Foucault failed to acknowledge the rise of the spectacle in mass mediated societies where the many watch the few (Caluya, 2010). His concept is based on the Greek word *syn*, meaning “together” or “at the same time,” and *opticon*, which has to do with the visual. In our modern society, Mathiesen writes that mass media (e.g., television) allows for a bottom-up observation where a large number of individuals are able to focus on something in common, such as VIPs, reporters, the stars who have become a new class in the public sphere (p. 219), or non-actors staring in reality TV shows. Consequently, we live in a “viewer society.”

Mathiesen (1997, p. 223), however, does not completely disregard Foucault’s panopticon, for both panopticism and synopticism “*have developed in intimate interaction, even fusion, with each other*” throughout history, starting with the Roman Catholic Church (where the few/priests surveyed the many/town people and where the many listened to the few/Pope), the Inquisition

(which was panoptical in relation to its reaction to heresy and witchcraft from the 1200s on, and synoptical in how many people followed the highly visible Inquisitor), the military (panoptical in the strict disciplinary hierarchy, and synoptical with highly visible military leaders victoriously entering the city after the battle), and, in modern times, in the development of technology.

Orwell's fictional telescreen which performed a two-way function (in that viewers watch while themselves being watched) is now reflected in the field of consumption: consumers synoptically watch TV and order and pay for the advertised commodities, and at the same time, the producers of those commodities panoptically survey and control the consumers and the latter's ability to pay. Although written more than two decades ago (when internet usage was incomparable to today), Mathiesen's argument of the role the media and the internet play in surveillance is still valid, for example, the general public can scrutinize their leaders (Meyrowitz, 1985).

Mark Andrejevic's (2004) study of reality TV (a soft form of panoptic surveillance) shows that a paradoxical docility is achieved in the name of freely chosen self-expression, pervasive monitoring is equated with creativity and self-expression, and close surveillance is destigmatized. But opposite to the panopticon where the few watch the many, in the TV synopticon, the many watch the few:

Today it is technologically entirely possible to have a large number of consumers synoptically watch television and order and pay for the commodities advertised... while the producers of the commodities panoptically survey everyone. (Mathiesen, 1997, pp. 223–224)

[W]atching—is easily accepted because all sorts of watching have become commonplace within a “viewer society,” encouraged by the culture of TV and cinema. As things once “private” have become open to the “public gaze” of many, and as intimate and once-sequestered areas of life are “screened,” so it seems of less and less consequence that this or that bit of once-protected personal data is disclosed. (Lyon, 2006a, p. 36)

Lyon (2006a, p. 41) contends that in such a viewer society, the desire to watch²¹ (whether watching is of the few by the many or of the many by the few) has become a sort of “voyeurism that reduces the rights of the watched.” More importantly, the appeal of the notion of the voyeur gaze²² is critical because it pushes towards an appreciation for the need for normative approaches to surveillance (p. 52). Pecora (2002) examines the contradictory desire for surveillance in popular media like Reality TV and how narcissism is intrinsic to its culture; “Reality TV elaborates surveillance as a sublime object of desire,” instead of a means of social regulation and discipline. In front of the screen, audiences (i.e., consumers) are monitored, profiling their demography and tracking the ratings, a task that has become easier with the advent of cable TV and streaming TV. Reality TV, therefore, has become an example of mass media that fosters a culture of celebrity where fame, and even notoriety, have become valuable in their own right (Haggerty & Ericson, 2006, p. 5). Moreover, in our age of digital, interactive media forms, the relationship between consumers, media consumption, and product promotion has changed, which is illustrated in the rising popularity of the interactive film genre where traditional brand placement (Balasubramanian, 1994; Karrh, 1998; Nagar, 2016; Turow, 2006) is replaced by programmatic advertisement (PA), the automated trading of the audience commodity (Andrew, 2019). PA is now used in different platforms, such as social networks and mobile applications. It is quite invasive (and therefore raises privacy concerns) because of its use of cookies, geolocation, and its algorithms that analyze users’ interests in order to offer related products at a

²¹ The film critic, Christian Metz (1982), coined the word “scopophilia” to describe the love of looking or the voyeur gaze.

²² A more detailed discussion of the voyeur’s gaze can be found in Norman K. Denzin’s *Cinematic Society: The Voyeur’s Gaze* (1995) in which he argues that the “voyeur is the iconic, postmodern self, a product of the cinematic gaze” (p. 1). Marx’s (1996) perspective on popular culture, on the other hand, fosters a kind of “verstehen” (i.e. sympathetic understanding of intentions and contexts) of surveillance experiences.

later time. The continuous developments in fields such as Big Data (Erevelles, Fukawa, & Swayne, 2016), Artificial Intelligence (AI), Data Mining, and Business Intelligence (BI) has allowed companies to continually improve PA targeting (Palos-Sanchez, Saura, & Martin-Velicia, 2019).

Another example of reverse panopticon is social media, where the user stands alone in the middle of the sociotechnical system, while the controllers and other users are all around (Romele et al., 2017, p. 205). Contemporary web 2.0 platforms, like Google or Facebook, are based on identification, classification, and assessment of personal and user behaviour data, turning consumers into “prosumers,” a commodity whose data are sold for advertising purposes (Fuchs, 2011, p. 145). In addition, “web 2.0 surveillance” can be characterized as a system of panoptic sorting, mass self-surveillance and personal mass dataveillance. This phenomenon of reverse panopticism has been given different names: “lateral surveillance” (Andrejevic, 2005), “social searching” or “social browsing” (Lampe, Ellison, & Steinfield, 2006), “social surveillance” (Joinson, 2008; Tokunaga, 2011), and “liquid surveillance” (Bauman & Lyon, 2013).

From a critical marketing perspective, synopticism opens the door to other discussions. By changing the identity of who watches whom, the power of surveillance is no longer in the hands of the traditional surveiller (i.e., the panopticon watcher). For example, while consumers are being increasingly and closely watched by retailers, they now have the technological means (a form of surveillance power) to watch the retailers. For example, writing bad reviews becomes consumers’ means of exercising that power. In their book *The Unmanageable Consumer* (2015, pp. 211–212), Gabriel and Lang argue that we can find the category of the “consumer-worker” all around us:

Indeed, today's supermarket turns the customer into the cashier and security guard too, with self-checkout technology. In a similar way, fast food turns customers into waiters and even table-clearers. IKEA and other stores turn consumers into carpenters by inviting them to assemble their own furniture . . . In spite of the stress they may feel by the time they conclude their purchases, people across social classes, national cultures and age groups appear eager to work hard for their home furnishings . . . Somewhat more controversially, customers are also knowingly or unknowingly used to monitor and evaluate the performance of employees.

Similar to the situation where consumers “assume the position of co-workers who take over specific elements of the productive process, usually unpaid” (Gabriel & Lang, 2015, p. 212), we can argue that consumers also consciously and unconsciously play the part of surveiller inside retail stores. For example, since the beginning of the COVID-19 pandemic, retail consumers are inclined to surveil other shoppers when it comes to following new regulations such as social distancing and wearing a mask. To sum up, with synopticism, the scale of power is tipped and the surveilled (i.e., consumer) can benefit from becoming visible. This change in the classic roles of surveiller/surveilled only highlights the importance of studying the various stakeholders and understanding each of them when studying retailance. This discussion aligns with the three elements in the critical marketing perspective applied to this research: the involvement of different stakeholders (in this case, retailers and consumers), the continuous shift of surveillance power from retailer to consumer and vice versa, and how the retailer/consumer relationship can lead to either understanding or mistrust.

(3) Post-panopticism: Boyne and Lyon

Boyne proposes a new “post-panopticism” paradigm that has the following features: (1) forms of consumer seduction are replacing the panoptic regime; (2) self-surveillance may be carried out so effectively in Western capitalist societies that it makes the original panoptic

impulse redundant; (3) simulation, prediction, and action before the fact may reduce the need for older forms of surveillance; (4) mass media synopticon (where the many watch the few, e.g., following Instagram influencers) acts alongside the panopticon (where the few watch the many), thus, relativizing its effects; and (5) the panopticon's failure to produce docile subjects is a challenge to panoptic theory (Boyne, 2000; Lyon, 2007, p. 60). In the retail sector, not all of Boyne's features of the post-panoptic paradigm are relevant: (1) In the brick-and-mortar retail world, both consumer seduction and the panoptic regime co-exist; the consumer is lured by better services, special deals, and rewards and at the same time, they are under constant physical surveillance (e.g., audio, video, bio) to deter shoplifting and violence and to monitor the movement and consumption patterns inside the store. (2) Self-surveillance has not made the panoptic redundant in Western societies, instead it has made the panoptic more accepted and even sought after, surpassing the limitations first envisioned by Bentham. Today, we do not need physical walls and hidden guards, or even the knowledge of being surveilled, for we have become addicted to voyeurism and the need to surveil others as well as be surveilled, hence, the popularity of social platforms (e.g., Facebook and Instagram) and reality TV programs. On the other hand, one of Boyne's features does apply to the retail sector: prediction before the action (i.e., targeting the needs of consumers with the help of advances in information technology, data gathering and analytics) is aided with advances in retail technology. As for Boyne's last feature (the failure of the panoptic to produce docile objects, for example, in prisons), one of the goals of this research is to discover the effect of the presence of retail technology on the consumers: would they accept, negotiate, or resist it? Would the panoptic in the retail store produce docile or uncooperative consumers?

In the current capitalist economy, the new panopticon is more flexible, subtle, participatory, decentred, and consensual (i.e., voluntary); people are seduced to conform by the pleasures of consuming, which substitutes the predecessors' crudities and brutalities (which brings out the critical marketing question of how ethical that seduction is). To Lyon (2006b, p. 8), the commodification of individuation occurs when consumers customize products to express individuality and creativity, and when they submit to mass surveillance, hence, they get diagnosed by the "panopticommodity." Examples for panopticommodity are reality shows and YouTubers uploading videos of themselves; being watched has become an asset and a social norm, and the more views the better (Galič et al., 2017, p. 27).

(4) Assemblage: Deleuze and Guattari, and Haggerty and Ericson

In an attempt to understand contemporary social and technological developments in surveillance and society, surveillance studies scholars (starting in the late 1980s) began turning their attention away from Foucault (Caluya, 2010). In conjunction with the French psychotherapist and philosopher Félix Guattari, the French philosopher Deleuze introduced a radical notion of multiplicity in the surveillance phenomena, which they called "assemblage" in their iconic book *A Thousand Plateaus* (Deleuze & Guattari, 1987). Assemblage theory provides a bottom-up framework for analyzing social complexity by emphasizing fluidity, exchangeability, and multiple functionalities through entities and their connectivity. To Deleuze and Guattari, these assemblages should be considered assemblages of desire rather than power. For example, in retail stores, surveilling consumers (who might not be the prior focus of routine surveillance) can involve different security personnel and surveillant systems (such as video, audio, biometric, RFID technologies, etc.). Operating across both state and extra-state

institutions, in this assemblage, practices and technologies are combined and integrated into a larger whole, exponentially increasing the degree of surveillance capacity (Haggerty & Ericson, 2000, p. 610) and making it increasingly difficult for individuals to maintain their anonymity (p. 619). When applied to retailance, an example could be the coming together of different institutional and business bodies to create a larger picture of the consumer (for example, combining credit history provided by banks, preferences by social media sites, consumption history by online and offline retailers, and criminal records by police).

Deleuze and Guattari also introduced the concept of “rhizomatic surveillance.” Rhizomes are plants that grow like weeds (think of growing mint as opposed to carrots); they “grow across a series of interconnected vertical roots which throw up shoots in different locations, in contrast with the plants with a deep root structure that grow along branchings from the trunk” (Haggerty & Ericson, 2000, p. 614) .

Any point of a rhizome can be connected to anything other, and must be. This is very different from the tree or root, which plots a point, fixes an order . . . semiotic chains of every nature are connected to very diverse modes of coding (biological, political, economic, etc.) that bring into play not only different regimes of signs but also states of things of differing status . . . A rhizome ceaselessly establishes connections between semiotic chains, organizations of power, and circumstances relative to the arts, sciences, and social struggles. (Deleuze & Guattari, 1987, p. 7)

To Deleuze and Guattari, the rhizome metaphor²³ highlights two attributes of the surveillant assemblage: (1) the phenomenal growth through expanding uses, and (2) its leveling effect on hierarchies, so that the groups which were previously exempted from routine surveillance are now increasingly being monitored (Haggerty & Ericson, 2000). Rhizomatic surveillance,

²³ I am using the “rhizome” metaphor here to describe the assemblage of surveillance channels and systems, and not in the context of thought in which it opposes “arborescent” (a totalizing, binary, dual, tree-like way of thinking).

therefore, allows for the scrutiny of the powerful (i.e., the middle and upper classes in contrast to poor individuals) and their “consumption habits, health profile, occupational performance, financial transactions, communication patterns, internet use, credit history, transportation patterns, and physical access controls” by both institutions and the general population (pp. 617-618). Such scrutiny reflects the creeping and entangling nature of the rhizomes. An example of surveillant assemblage is the social site Facebook which employs various methods of surveillance, such as, monitoring the users’ profiles, social interactions, consumption habits, and geographical locations. At the same time, Facebook allows its users to monitor each other and scrutinize those in power (hence, leveling power hierarchies). According to Haggerty and Ericson, the presence of surveillant assemblage highlights the “disappearance of disappearance,” for it is increasingly difficult for individuals to maintain their anonymity (p. 619) (which brings us back to the theme of (in)visibility in critical marketing).

Drawing on the works of Deleuze and Guattari and their notion of assemblage are Haggerty and Ericson (2000). They direct this assemblage metaphor towards the body, producing a new type of individual whom they call “data double.” A more detailed discussion of their idea is included in the next section on virtual identities.

(5) Virtual identities: Haggerty and Ericson, Poster, Deleuze, Bogard, and Lyon

Describing surveillance as a “major form of power in the mode of information,” Mark Poster (1990, pp. 85–98) wrote about a “Superpanopticon,” a term describing a system of surveillance without towers, guards, walls, or windows, and means of controlling the masses in the postmodern, post-industrial mode of information. In the economic sphere, databases are a postmodern discourse that cancels the public/private distinction: retailers regard the information

they accumulate about their consumers as their property, a valuable asset that they can sell to others, on the other hand, many consumers do not want their information shared, for to them, their economic transactions are private (Poster, 1996, pp. 284–285). Thus, to Poster (1989, pp. 121–123), consumer surveillance amounts to a superpanopticon because the panoptic has no technical limitations, and its power ultimately abolishes the distinction between private life and public life. And this fading out of the private life is achieved with the consumer’s assistance. For example, the consumer’s act of buying something is considered a “private” act of rational choice, however, when they submit a credit card for payment, this private act becomes part of a “public” record; the “unwanted surveillance of one’s personal choice becomes a discursive reality through the willing participation of the surveilled individual” (p. 285). Poster (1990, p. 93) explains that:

The quantitative advances in the technologies of surveillance result in a qualitative change in the microphysics of power. Technological change, however, is only part of the process. The populace has been disciplined to surveillance and to participating in the process . . . Each transaction is recorded, encoded and added to the databases. Individuals themselves in many cases fill out the forms; they are at once the source of information and the recorder of the information. Home networking constitutes the streamlined culmination of this phenomenon: the consumer, by ordering products through a modem connected to the producer’s database, enters data about himself or herself directly into producer’s database in the very act of purchase . . . from the 1920s onward . . . individuals are constituted as consumers and as participants in the disciplining and surveillance of themselves as consumers.

Comparing the panopticon to the superpanopticon, Lyon (2001a, p. 115) writes that the former produces subjects with desires to improve their inner lives, and the latter constitutes objects, individuals with dispersed identities, who may even remain unaware of how those identities are construed by the computer. To Lyon, the spread of consumerist activities after the 1920s should be viewed as a political change (where the population controls itself) rather than an economic change (towards a consumer society) or a semiological change (toward a world of floating signifiers). Poster (1990, p. 97), described databases as “multiplication of the individual” instead

of an invasion of privacy or a threat to a centred individual; this description of an “additional self” would be later echoed in what Haggerty and Ericson (2000) describe as “data doubles” (see below).

In 1992, the French philosopher Gilles Deleuze sketched the shift from the Foucauldian “disciplinary societies” (characterized by discrete physical enclosures) to “societies of control” (a term borrowed from *The Naked Lunch* (1959), a novel by the American William S. Burroughs, to dub the new system of power). According to Deleuze (1992, p. 5), in societies of control, individuals are controlled by “passwords . . . a numerical language of control . . . made of codes that mark access to information, or reject it,” and control relates to “floating rates of exchange” instead of minted money. The capitalism we live in is no longer for production (which is often relegated to the Third World) but for the selling and marketing of products and services. The “factory has given way to the corporation” and “marketing has become the center or the ‘soul’ of the corporation” and the operation of markets an instrument of social control (p. 6) (this “control” can be considered a form of power under critical marketing). In a Deleuzian society, “the point is no longer making bodies docile, but to mould consumers, whose data-bodies become more important than their real bodies” (Galič et al., 2017, p. 20). Moving from discipline to control, Deleuze, therefore, emphasizes the absence of confining spatial arrangements in the exercise of domination afforded by the use of computer technology (Poster, 2005). This switch to digital forms of control where both individuals and masses disappear into pockets of information represents a shift in the history of the exercise of power.

Bogard (2006) argues that we should follow Deleuze and Guattari and study the control society as “a complex socio-technical machine that exerts control through decoding and deterritorializing subjectivity,” in which reality is deconstructed as “hyperreality” (or systems of

simulation) and the subject (or individual) is recreated as a “virtual subject” as is found on computer networks (pp. 62-63). While this argument could be accepted in the context of digital marketing, it cannot stand alone in physical retail, where technology is part (albeit an increasingly big part) of retailance, and where the consumer has both a physical and a virtual presence. Moving away from Deleuze and Guattari’s notion of surveillance assemblage, and in an earlier work, Bogard (1996) reasons that technologies—such as virtual reality, computer reality, artificial intelligence and genetic mapping among others—intensify the role of surveillance beyond which actual control operates toward an imaginary form of control that is capable of seeing and recording every fact of an event prior to the event itself. Bogard’s discussions of surveillance have been heavily influenced by the work of the French sociologist and cultural theorist Jean Baudrillard who wrote about “telematic societies” (i.e., what others call information societies) in an age of “simulation” where symbols and signs replace all reality and meaning, and where human experience becomes a simulation of reality (Lyon, 2001a, pp. 114–118; Raffel, 2004).

At the forefront of the post-panoptic trend is Haggerty and Ericson’s “The surveillant assemblage” (2000), a paper that highlights the disparate, yet connected, arrays of people, technologies and organizations. According to them, although Foucault’s panopticon improves upon Orwell’s Big Brother by situating surveillance in the context of a theory of power, it has failed to capture the effect of rapid technological developments, particularly the rise of computerized databases (p. 607). Echoing Mathiesen, they argue that both Orwell and Foucault view surveillance as a regime in which the few watch the many in top-down scrutiny. Moving forward, they draw on the work of Deleuze and Guattari and the latter’s notion of the “assemblage,” arguing that we have moved beyond discrete surveillance systems to an emerging

surveillant assemblage that is directed towards the “body,” producing a new type of individual, one comprised of pure information, which they called a “data double.”²⁴

A great deal of surveillance is directed toward the human body. The observed body is of a distinctively hybrid composition. First it is broken down by being abstracted from its territorial setting. It is then reassembled in different settings through a series of data flows. The result is a decorporealized body, a ‘data double’ of pure virtuality . . . its movements through space can be recorded, to the more refined reconstruction of a person’s habits, preferences, and lifestyle from the trails of information which have become the detritus of contemporary life. (p. 611)

Haggerty and Ericson’s proposal, therefore, renders visible processes of surveillance in which information is abstracted (i.e., deterritorialized) from human bodies in data flows and reassembled (i.e., reterritorialized) as data doubles (Caluya, 2010, p. 624; Haggerty & Ericson, 2000, p. 600).

Thus, instead of Mary Shelley’s freakish creation assembled from the parts of different corpses in her 19th-century novel, *Frankenstein*, that warned against the potential consequences of unrestrained science and technology, Haggerty and Ericson (2000) draw our attention to data doubles toward which governmental and marketing practices are directed. For example, as consumers, the services we receive (or not) and the discounts we get (or not) are a result of the algorithms that continuously analyze the data defining our doubles.

The notion of data doubles could be also viewed as a departure from Marx’s concept of “surplus value” (i.e., in a labour-oriented discourse, surplus value designates how the owners of the means of production profit from workers’ excess labour power for which the latter are not financially compensated). In a cybernetic world, surplus value refers to “the profit that can be

²⁴ Diana Gordon (1987) used the term “electronic panopticon” to capture the nature of the contemporary situation as exemplified in the far-reaching expansion of government power through the U.S. national criminal records system.

derived from the surplus information that different populations trail behind them in their daily lives” (i.e., the consumer’s personal and shopping information becomes a product that could be sold) which ultimately leads to creating consumer profiles, refining service delivery, and targeting specific markets. Another consequence is the “commodification of the self,” when consumers trade their privacy and personal data for something in return, such as better services, special deals, or rewards. Lyon (2010a) bases his theory of “liquid surveillance” on the creation of data doubles as well as the time-sensitivity of surveillance and the mutated truth. In other words, when the body is reduced to data, life becomes more about the stories of our lives (i.e., data doubles) than about our real lives, an example is the information on social media sites; “today’s surveillance does not keep its shape; it morphs and mutates” both locally and globally (p. 330). Lyon developed the notion of liquidity from Zygmunt Bauman’s (2000) notion of “liquid modernity.” In this post-panoptical world, consumer society is underlined by globalization, nomadism, spatial differentiation (i.e., the loss of public space to privately controlled spaces, an example is the shopping mall which is structured to consumption and movement), and the increasing mobility of capital and social elites. It is worth mentioning that Bauman’s work reflects on dynamics that play themselves out in both North America and the United Kingdom.

So, is the panopticon dead or alive?

In his paper “The post-panoptic society? Reassessing Foucault in surveillance studies” (2010), Caluya argues that Mathiesen, Haggerty, and Ericson’s disregard for Foucault is “rather hasty.” He reminds the readers that Foucault’s discussion of the panopticon is limited to one chapter only (significantly titled “Panopticism”) out of the eleven chapters in *Discipline and*

Punish. Caluya also argues that the interpretation of Foucault’s work is coloured by other writers, for example, Haggerty and Ericson presume that Foucault’s work is an extension of Orwell’s Big Brother (i.e., an instance of the power of the state through an omniscient gaze). As for Deleuze, there was an intellectual friendship between him and Foucault and his concept of assemblages was inspired by Foucault’s corpus of work. To Caluya, Foucault’s “actual target is panopticism rather than the panopticon itself”; Bentham’s panopticon is a penal building, but Foucault’s panopticism is a machine of power that is generalizable across extra-penal domains (Foucault, 1978, p. 205).

Another ongoing argument between surveillance writers is whether the panopticon is still a valid theory, should be laid to rest, or should be integrated with other, more contemporary, theories (Figure 46). There is no one answer to this question, and even a surveillance theorist like Lyon has argued for and against panopticism.

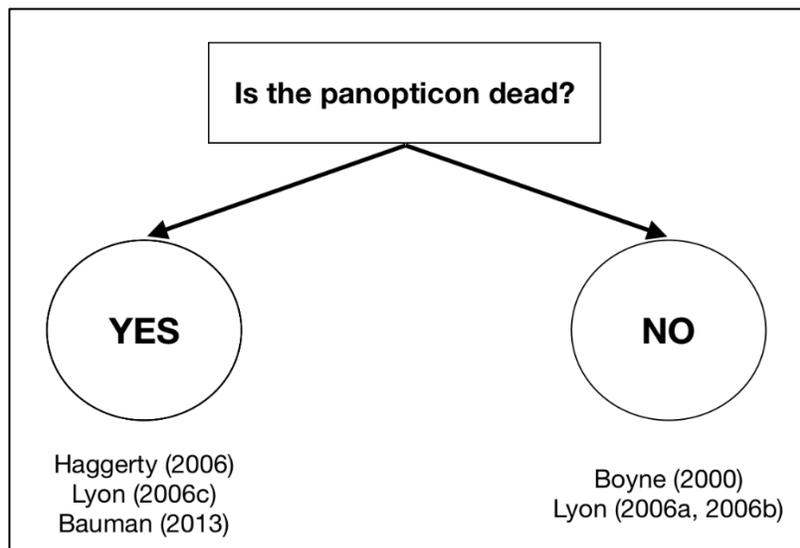


Figure 46 – Is the panopticon dead?

The panopticon is paradoxical; at one end of the spectrum, it can create moments of refusal, resistance, and even militancy, and at the other “soft” end, it seduces participants to

conformity of which they may be even scarcely conscious. Haggerty's (2006) advice is that we need to "tear down the walls" of the panopticon, for not all surveillance attributes can be subsumed under the panoptic rubric. In general, the panopticon stands for surveillance, and each new "opticon" theory points to a distinction or limitation in Foucault's model²⁵. To Haggerty (2006),

Bentham's famous design still retains pride of place in studies of surveillance. My position here is more extreme, as I believe that changes in surveillance processes and practices are progressively undermining the relevance of the panoptic model for understanding contemporary surveillance. Foucault continues to reign supreme in surveillance studies and it is perhaps time to cut off the head of the king. The panoptic model masks as much as it reveals, foregrounding processes which are of decreasing relevance, while ignoring or slighting dynamics that fall outside of its framework. (p. 27)

Thus, to Haggerty, the panopticon has become the leading model or metaphor for analyzing surveillance and in doing so, has become oppressive in the surveillance literature. In *Theorizing Surveillance: The Panopticon and Beyond* (2006c), Lyon, together with an array of surveillance studies scholars, form a growing consensus that Foucault's panopticon should be laid to rest in favour of newer models. Moreover, to Lyon, "the more stringent and rigorous the panoptic regime, the more it generates active resistance, whereas the more soft and subtle the panoptic strategies, the more it produces the desired docile bodies" (2011a, p. 4). In the case of active resistance, Lyon argues that such resistance is not always liberatory and might even invite further

²⁵ Other panoptic theories include: the "polyopticon" which introduced a multiplicity of relations of visibility and the decentralisation of surveillance into everyday routines (M. Allen, 1994); the "panspectron" in which a multiplicity of sensors compile information about all bodies/data at the same time, using computers to select the segments of data relevant to its surveillance tasks (De Landa, 1991, pp. 203–206); the "omnicon" when everyone potentially watches everyone (Groombridge, 2002); "myopic panopticon" and the efficiency issues it raises (Leman-Langlois, 2002); the "pedagopticon" monitoring in the classroom (Sweeny, 2009); and the "fractal-panopticon" which fuses the market and the panopticon to extract labour from the entirety of the social field (De Angelis, 2011).

control. This argument is a good example of why critical marketing is an appropriate approach in this research since it focuses on the themes of power and bringing change.

Bauman (2013, pp. 55–59) argues that the classic panopticon is no longer the universal pattern or strategy of domination; it has been shifted and confined to the margins, the unmanageable parts of society, such as prisons, camps, psychiatric clinics and similar institutions. He reasons that the importance of the panoptic in contemporary society has been reduced, for instead of being socially integrated and subjected to disciplinary surveillance and/or simple repression, people are increasingly viewed as consumers and seduced into a market economy and their consumption patterns are constantly monitored.

[With consumption] Expensive *panoptical* methods of control, pregnant as they are with dissent, may be disposed of, or replaced by less ambivalent and more efficient methods of seduction (or, rather, the deployment of panoptical methods may be limited to a minority of the population; to those categories which for whatever reason *cannot be integrated through the consumer market*). (Bauman & Lyon, 2013, p. 51)

Bauman, therefore, maintains that to the postmodern consumer, experienced reality becomes a “pursuit of pleasure” (p. 50-51) and that synopticism has replaced panopticism through seduction and enticement rather than coercion.

Opposite to the above view that argues for the need to overthrow panopticism, both Lyon (2006b) and Roy Boyne (2000) advocate for accepting the panoptic presence in our post-panoptic world. Although the prison is the most extreme example of panoptic power, they argue that panopticism is still a functioning ideal, metaphor, and a set of practices. Omniscient visibility lies at the heart of military intelligence and urban planning, unseen observation and categorical discrimination are used in CCTV-camera surveillance and call centres. According to Lyon (2006a, p. 45), “consumer desires are created through database marketing, a realm in

which the phenetic is writ large,” consequently, the panoptic and the synoptic be considered together:

The panoptic must be retained in surveillance studies because it helps to highlight a key aspect of surveillance today—social sorting and digital discrimination by means of searchable databases. (Lyon, 2006a, p. 51)

I believe that the panoptic still has a role to play in these post-panoptic times, though that role is more pronounced in the brick-and-mortar retail stores than in digital markets. Retail stores still extensively rely on the Foucauldian self-discipline concept in monitoring both their consumers and employees. Consumers are constantly reminded that their purchases are being monitored and that they could be subject to random spot checks. With the advanced technology used in retailance (such as video, audio, and bio surveillance), there is currently no need to adopt Bentham’s design of the panopticon in respect to the design of retail spaces. I also agree with Lyon that the panoptic and the synoptic should be considered together. In the brick-and-mortar retail environment, retailance intertwines both the Foucauldian panopticon and the synopticon. By entering the retail store and not knowing exactly how, when, and where they are surveilled, the consumer is encouraged to self-discipline their behaviour (panoptic side of retailance). In addition, the consumer is lured into disclosing their personal information and consumption habits which leads to constant monitoring (synopticon side of retailance).

In the field of digital consumption, panopticism and synopticism intertwine, an example is Amazon.com’s Wish Lists. Singh and Lyon (2013) discuss how Amazon.com’s Wish Lists explain various surveillance phenomenon: the Wish Lists present the company with the opportunity to classify consumers into different categories, formulate data doubles, and predict the consumers’ tendencies; they enable peer-to-peer surveillance; their success is derived from their capability to capitalize on the disciplined willingness of consumers to “want” to partake in

the consumption that it promotes. Consequently, this direct collection of consumer information drastically reduces market research expenses, marking an entirely new process of consumer marketing, consumer surveillance, advertising and sales. Therefore, instead of the panoptic “normalized soul training,” the focus is on monitoring market consumption, limiting access to places and information, and/or allowing for the production of consumer profiles through the “*ex post facto* reconstructions of a person’s behaviour, habits and actions” (Haggerty & Ericson, 2000, p. 615).

I disagree with Haggerty’s (2006) belief that every new “opticon” theory only points to the limitation of the Foucauldian model. To me, the fact that the new emerging subcategories are relevant to the present time is an indication that panopticism is still alive and kicking. An example is the commodification of individuation (when people market themselves), dubbed “participatory²⁶ panopticon” by Reg Whitaker (1999), for it is a consumer panopticon based on positive benefits (e.g., facilitating daily life when using credit and debit cards or smart health cards; empowering consumers; and ensuring public safety) where the worst sanction is exclusion:

consumers are being disciplined *by consumption itself* to obey the rules, to be “good” not because it is morally preferable to being “bad” but because there is no conceivable alternative to being good, other than being put outside the reach of benefits. (p. 142)

²⁶ Larsen and Piché (2009) use the term “participatory surveillance” in the context of the long-term public vigilance campaigns, in the wake of the 9/11 attacks, to denote the call for “responsible” individuals to constantly watch for suspicious activity and to immediately convey that information to the authorities. Such campaigns could be also seen in cities that have not directly experienced terrorist attacks, for example, in Ottawa, Canada, the OC Transpo invites citizens to “report to its own security service, which has recently been granted police powers” (p. 191).

Marketing research, therefore, is increasingly directed towards segmentation and identifying individual (paying) consumers' preferences in an attempt to serve their needs and desires; for example, the shift from the availability of a handful of TV channels in the 1950s, to what Whitaker describes as the "500-channel universe" in the late 1990s, to the current proliferating streaming TV providers (such as Amazon Prime Video, Netflix, and YouTube Video) that draw upon the consumer's consumption history to anticipate, suggest, and encourage future consumer behaviour, hence, a fragmentation of mass audiences (pp. 145-146).

Summary

Although Foucault prompted a new panopticism in theorizing surveillance, others had different reactions to his work, such as: (1) Haggerty (2006) critiques Foucault's disregard of the importance of the role played by the "watchers," or the "agents of surveillance," and the effect of their attitudes, predispositions, biases, prejudices and personal idiosyncrasies on the surveilled; to Foucault, surveillance effects are identical irrespective of who the surveiller is. Considering the watcher's background and doubting their objectivity is important, for example, the surveillance carried out by CCTV operators can be coloured by racial prejudices and gender objectification (pp. 32-34). Haggerty (2006) also criticizes Foucault's panoptic model for not containing an image of resistance, however, one can argue that this issue is discussed by Foucault in a later work, *History of Sexuality, Volume I*, in which he states: "Where there is power, there is resistance." (2) Foucault minimized the important role of the class struggle in the case of the factory in which workers and their unions do not succumb passively to the dictates of the industrial panopticon (Giddens, 1981, pp. 171–174). (3) He paid little attention to the growth of mass media and the persistence of the "spectacle" (Lyon, 2007, p. 59), or the many surveilling

the few which Mathiesen called the “synopticon.” (4) Foucault failed to foreground new surveillance technologies in his work, therefore, there is a need to go beyond Foucault’s work to understand the contemporary electronic technology-dependent surveillance (Haggerty & Ericson, 2000; Lyon, 2007; Webster & Robins, 1986; Zuboff, 1988). (5) Marx (2016, p. 64) finds fault with Foucault’s neglect of other surveillance forms (e.g. organizational, interorganizational, and nonorganizational by individuals of each other) and for the fact that the former’s analysis does not give sufficient attention to the multiplicity and fluidity of surveillance goals and the conflicts between them.

When it comes to the analysis of customer databases, Pridmore and Zwick (2013) argue that neither a Deleuzian nor a Foucauldian perspective is enough, for the automated surveillance-based data collection and analysis no longer represent a means to discipline or control consumption, instead, “manufacturing consumers” demonstrates that the consumer population has become

a site for direct economic value creation while the ambition to control consumers, still important to modern marketers, is increasingly giving way to the possibility of manufacturing customers as valuable information commodities themselves in need of marketing. (p. 109)

This “production of customers” perspective proposes that the importance of the database, and data-mining techniques, is not derived from its panoptic capacity, but rather from its ability to produce flexible and reflexive consumer simulations in real time, enhancing the speed and flexibility of the production process.

Because retailance covers both physical (i.e., tracking the consumers themselves when they enter the retail store) and digital (i.e., collecting data for analysis) surveillance, different surveillance concepts (discussed in the above section) apply to it. The ideas of Deleuze (consumers as data-bodies), Bogard (consumers as virtual subjects), Haggerty and Ericson

(consumers as data doubles), and Lyon (liquid surveillance) only partially apply to retailance, for they do not cover the spatial, physical aspects of retailance (for example, monitoring consumers' locations and movements inside the store). Deleuze and Guattari's surveillant assemblage phenomenon, on the other hand, fits the case of retailance, for it expresses the multiplicity of surveillance methods employed in retail stores. Their metaphor of rhizomatic surveillance is also applicable, for (1) there is a phenomenal growth in the use of retailance that crosses geographic boundaries, and (2) the leveling effect on hierarchies is evident in the fact that all retail consumers are being monitored without exemption, a fact that has led to what Pridmore and Zwick describe as the manufacturing of consumers (in which the information collected both digitally and physically about consumers' backgrounds and consumption habits is in itself a commodity). Foucault's image of a world controlled by self-discipline can no longer be the only scenario.

Surveillance, marketing history and marketing research

In marketing history, the progress of surveillance parallels that of marketing and consumer behaviour. In the early 20th century, research based on speculations on consumer behaviour, attitudes and motivations first developed in the field of advertising psychology to study the effectiveness of the medium of persuasion (Arvidsson, 2003, p. 460). Without much scientific backing, the ABCD segmentation system (Figure 47), based on income differences and derived from the structure of the magazine advertising market, was born (pp. 460-462). In the 1940s, "commercial research" (what is currently called market research) and the surveillance of consumers was motivated by a company's intention to align consumer preferences for products and brands with what was being produced, and corporations' need to control consumers, reduce marketing complexities, and improve production efficiencies (Arvidsson, 2003; Elmer, 2004;

Pridmore & Zwick, 2013). By the end of the 1940s, and in the post-WWII (World War Two) era, the ABCD typology was challenged for no longer providing an adequate representation of consumer practice (Arvidsson, 2003, p. 462). The first significant break with the ABCD typology would take place in the late 1950s with the introduction of motivation research (MR), a commercial adaptation of Freudian psychology; consumer decision was then seen as rooted in the unconscious (i.e., psychographics) instead of the social and cultural environment (p. 463). The late 40s and early 50s, however, was not just a time of surveilling consumers, but survey researchers, opinion pollsters and market researchers were also implicated: during the height of the “Second Red Scare” (i.e., the fear of communism during the Cold War phase) in the United States, they were either being spied upon by the FBI and/or dragged in front of hearings with allegations of being covert Soviet spies, or they used their expertise to feed into J. Edgar Hoover’s and Senator McCarthy’s obsessions about communist infiltration of American institutions (Schwarzkopf, 2016). That was an early example of how the researcher as an agent of surveillance can become a “subject of surveillance as a citizen, consumer, communicator, and employee” (Marx, 2008).

- | |
|--|
| <p>A. Homes of Substantial wealth above the average in culture that have at least one servant. The essential point, however, in this class is that the persons interviewed shall be people of intelligence and discrimination.</p> <p>B. Comfortable middle class homes, personally directed by intelligent women.</p> <p>C. Industrial homes of skilled mechanics, mill operators or petty trades people (no servants)</p> <p>D. Homes of unskilled labourers or in foreign districts where it is difficult for American ways to penetrate.</p> |
|--|

Figure 47 - The standardized ABCD system used in the 1930s (Cited in Arvidsson, 2003)

In the 1950s and 1960s, market researchers such as Sidney Levy (1959) and management theorist Peter Drucker (1950, 1954) posited that the primary challenge for the firm lies in identifying and responding to consumers’ changing needs and wants in the market, and in

satisfying not controlling them for maximum sales. It was in the 1970s when marketing icon Philip Kotler (1972) advocated for “customer satisfaction.” Kotler advocated that a concern with production efficiencies should be subordinate to discovering what consumers want, a strategy that would help secure market share and maximize profits (Pridmore & Zwick, 2013, p. 103). In the 1980s, and with the growth of the media industries and the rise of cable television and VCR, consumers appeared as fragmented, nomadic individuals, and Customer Relations Management (CRM) proliferated (Arvidsson, 2003; Turow, 1997). In the late 1990s, marketing went through what has been retrospectively known as the “branding revolution;” brand value was no longer seen as an extension of the product itself, but derived from the “experience or emotion that resulted from the inter-textual links that brand managers constructed around the product” (Arvidsson, 2003, p. 466). This led to the rising importance of digitized information and customer database at the turn of the 21st century. By examining all those adjustments throughout the years (Blankenship, Chakrapani, & Poole, 1985; Scranton et al., 2012), marketing researchers can understand and study the current monitoring and measuring of consumers and their consumption practices, drawing links between the consumer and the commercial surveillance practices (Pridmore & Zwick, 2011, 2013). The consumer now is viewed as:

...a complex entity whose desire to consume may be boundless (as maintained by the economic branch) but whose motivations to consume (the what and why of consumption) are not well understood and require continuous scrutiny. (Pridmore & Zwick, 2013, p. 103)

Since this research aims to further the marketing practice, a question poses itself: can marketing research itself be considered a form of surveillance? To answer that question, a distinction has to be made between academic marketing research and practical marketing research (conducted by corporations, business owners, retailers or third parties). Such a distinction could be traced in the answers to the following questions:

- Who does the research serve? How objective are the results?
- What is the research agenda?
- Who determines the questions, who gets questioned, and to what use is the collected data put?
- Is anything offered to the disadvantaged and beyond-the-mainstream subjects of the research?
- Are the potential research subjects aware of the research and the reasons behind seeking the collected information?
- Have there been any coercive, secret, involuntary and/or passive means of data collection that could harm the research subjects?
- Who can access the research results?
- Is the collected data treated as the property of the collector and is it unavailable to the subject who cannot review and/or question its use?
- Are the goals of the body behind the research in conflict with the legitimate interests and goals of the subjects?

Most marketing (specifically consumer) research has a trace of surveillance in it, although how strong that element is depends on the above-mentioned questions. However, there are three distinct perspectives when it comes to marketing research. (1) Those wary of surveillance, such as sociologists and surveillance theorists, have a negative view of the integration of surveillance in marketing research and practice. To them, marketing research is definitely a form of surveillance no matter how benign it is. In his discussion of surveys and surveillance, Marx (2008) encourages readers to look at the implications of research and to “analyze the *structure* of surveillance settings and characteristics of the *means* used, *data collected* and *goals* sought, and

a concern with ethics.” He describes researchers as “more spies than spied upon, even if for academics this is usually in benign contexts.” (2) Marketing practitioners, on the other hand, have a much more positive perspective. To them, marketing research focused on consumers is about gathering information about consumers, their needs and the constantly changing marketplace in which they operate, providing businesses with descriptive, diagnostic and predictive answers (Lamb et al., 2016, pp. 69–70); such efficient marketing should ultimately lead to higher profits for businesses (and, at least in theory, a more prosperous economy) and more satisfied consumers. (3) To academic marketing researchers, marketing research run by academics can be considered less problematic than that run by practitioners. When rooted in an academic context, marketing research is governed by standards, reviews and procedures, and research subjects (i.e., informants) can opt out when contacted, refuse to answer, or even terminate their participation at any point. I personally believe that any human interaction (whether for personal, academic, or business reasons) carries an element of surveillance. Consequently, the real issue that should be focused on is not the mere presence of surveillance itself, but rather the other party’s awareness of its presence and scope and its impact on their privacy rights.

Chapter summary and conclusion

This chapter introduced the critical marketing approach the research followed, highlighting its major concerns and expected future. This was followed by an overview of key theoretical frameworks and conceptualisations in surveillance studies in relevance to the field of retail. Although surveillance studies should not be viewed from a strict chronological perspective, they can be roughly grouped into three phases (Figure 48). The first phase, featuring

Bentham and Foucault (i.e., panoptic/Foucauldian trend), revolves around the panopticon structure and metaphor. The second phase (i.e., post-panoptic/Deleuzian trend) moves away from panoptic metaphors and shifts the focus to networked surveillance that relies primarily on digital rather than on physical technologies, and on dealing with data doubles rather than physical persons, going beyond panoptic effects of self-disciplining, and discovering the assemblages of surveillant concepts. Lastly, the new types of surveillance associated with new marketing and consumer behaviour trends, online social media platforms, and popular media are presented (i.e., the beyond the panopticon trend). A chronological list of the major surveillance studies/theories discussed in this research is compiled in Table 4.

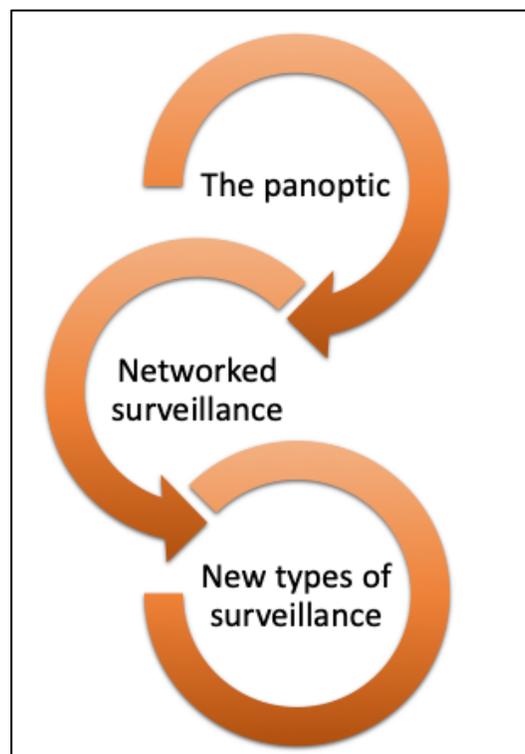


Figure 48 – Three major phases of surveillance studies

Writer(s)	Surveillance Studies	Published Work
Jeremy Bentham	- Panopticon (an architectural design)	<i>Panopticon; or, The Inspection-House</i> , 1791
George Orwell	- Big Brother - Orwellian society (social control)	1984, 1949
Michel Foucault	- Panopticon (the few see the many; disciplinary society)	<i>Discipline and Punish</i> , 1978
Diana Gordon	- Electronic panopticon	"The electronic panopticon," 1987
Gilles Deleuze & Félix Guattari	- Surveillant assemblage (practices and technologies combined to increase the degree of surveillance capacity) - Rizomatic surveillance	<i>A Thousand Plateaus: Capitalism and Schizophrenia</i> , 1987
Roger A. Clarke	- Dataveillance (the systematic use of personal data systems in investigating and monitoring the actions or communications of persons)	"Information technology and dataveillance," 1988
Christopher Dandeker	- Bureaucratic surveillance (society of strangers)	<i>Surveillance, Power and Modernity</i> , 1990
Mark Poster	- Superpanopticon (the panoptic view with no technical limitations)	<i>The Mode of Information</i> , 1990
Manuel De Landa	- Panspectron (using computers to select segments of data relevant to surveillance tasks out of all compiled data)	<i>War in the Age of Intelligent Machines</i> , 1991
Gilles Deleuze	- Societies of control (marketing is the soul of the corporation, and the operation of markets is an instrument of social control)	"Postscript on the societies of control," 1992
Oscar Gandy	- Panoptic sort (consumers are filtered through a triage based on their worth to the corporation)	<i>The Panoptic Sort</i> , 1993
Thomas Mathiesen	- Synopticism (the many see the few; viewer society)	"The viewer society: Michel Foucault's Panopticon' revisited," 1997
Reg Whitaker	- Participatory panopticon (when people market themselves) - Cybernetic panopticon	<i>The End of Privacy</i> , 1999
Kevin D. Haggerty & Richard V. Ericson	- Data double (the individual comprised of pure information)	"The surveillant assemblage," 2000

Roy Boyne	- A post-panopticon paradigm	“Post-panopticism,” 2000
Michael Hardt & Antonio Negri	- The nation state is replaced by a new empire that changes societies of discipline to societies of control.	<i>Empire</i> , 2001
Zygmunt Bauman	- People are viewed as consumers and seduced into a marketing economy.	<i>Intimations of Postmodernity</i> , 2003
Steve Mann, Jason Nolan, & Barry Wellman	- Neo-panopticon - Sousveillance (using counter-surveillance technologies and tactics to expose and challenge the surveillance activities of the powerful)	“Sousveillance: Inventing and using wearable computing devices,” 2003
Mark Andrejevic	- Lateral surveillance (peer-to-peer monitoring)	“The work of watching one another,” 2005
David Lyon	- Resistance to panopticism - Panopticommodity	<i>Theorizing Surveillance</i> , 2006
Didier Bigo	- Ban-opticon (profiling technologies determine who is to be placed under surveillance)	“Security, exception, ban and surveillance,” 2006
M. G. Michael, Sarah Jean Fusco, & Katina Michael	- Überveillance (an omnipresent electronic surveillance facilitated by technology that makes it possible to embed surveillance devices in the human body)	“A research note on ethics in the emerging age of überveillance,” 2008
Siva Vaidhyanathan	- Cryptopicon (knowing of and accepting being surveilled by the many)	<i>The Googlization of Everything</i> , 2011
Zygmunt Bauman & David Lyon	- Liquid surveillance (the transformation of ordinary citizens into suspects and their relegation to consumer status across a range of life-spheres)	<i>Liquid Surveillance</i> , 2012
Gary T. Marx	- New surveillance (decentralized and deigitalized; maximum security society) - Compliance surveillance (which identifies behavioural norms, certification, and norms about beliefs and feelings)	<i>Windows into the Soul</i> , 2016

Table 3 - A representative, though hardly exhaustive, chronological list of surveillance studies

In general, surveillance is conceptualised through other lenses such as dataveillance, access control, social sorting, peer to-peer surveillance and resistance. With the datafication of

society, surveillance has become a combination of the monitoring of both physical spaces and digital spaces, in which government, corporate and self-surveillance can be found. Not only are we watching and being watched, but we also voluntarily share our data. The panopticon remains a powerful metaphor, but “disciplining forces have altered in shape, place visibility and dynamics” (Galič et al., 2017, p. 33). Following a critical marketing approach, the main concern of this research is not the simple exposure of retailance flaws, it is rather understanding the status quo (e.g., who watches whom? In which setting(s)? For what reasons?), from the perspective of all stakeholders (retailer, consumer, and policy maker), and envisioning alternative(s) that would be beneficial to and meet the needs of all concerned parties. The following chapter lays the groundwork for the research methodology that was employed.

CHAPTER 4: METHODOLOGY

One of the early questions posed before designing a research methodology for this thesis was what would best suit its exploratory nature: a qualitative, quantitative or a type of mixed methods research design? While a qualitative methodology helps the researcher collect stories from their informants about their lives and experiences (Creswell, 2014, p. 13) and interpret complex phenomena (Leedy & Ormrod, 2010, pp. 135–136), its perspective-based method does not provide an opportunity to measure collected responses. On the other hand, the positivist nature of the quantitative methodology, reflected in the scale items that go into the questionnaire and the statistical analysis, clashed with this research's interpretive nature (discussed below in more detail). Tadajewski and Brownlie (2008, p. 10) argue against a positivist perspective when employing critical marketing research:

...critical marketing scholarship should exhibit a degree of reflexivity. It should refuse the positivist injunction that 'reality' exists external to the researcher. Instead, critical marketing scholarship should recognise the role of the researcher in the production of knowledge about marketing phenomena.

Moreover, when it came to the survey questions used in the research, although I mainly relied on questions/scales used in past research, it is doubtful whether all the instruments to measure the constructs were well validated (for example, those employed in the Ekos report on privacy (2009)), and developing new constructs was beyond the scope of this exploratory research. It, therefore, became obvious that a pragmatist methodology combining both quantitative (using an MTurk survey) methods and qualitative (by conducting semi-structured interviews) would best suit the interpretive nature of this research.

An interpretive approach

To Hudson and Ozanne (1988), interpretivism is crucial as a methodological approach in the following cases: (1) The researcher needs to study individuals who have multiple realities that are constantly changing and whose meaning is based on context. Instead of reducing people to variables, the researcher needs to be interested in describing multiple realities and to not believe that there exists only one single reality; (2) The primary goal of the research is to understand behaviour and not predict it, consequently, understanding—or what Wax (1967) calls “*verstehen*” (i.e., shared meaning), an active process in which language, customs, meanings and culture are continuously being created by the joint activities of people—is more of a hermeneutic process than an end product. This understanding has to be comprehensive, and to cover both individual meanings and shared meanings; (3) Rather than the positivist approach that endeavours to identify time- and context-free generalizations or nomothetic statements, interpretivism is about seeking “motives, meanings, reasons, and other subjective experiences that are time- and context-bound” (p. 511). Thus, detailed (i.e., “thick”) descriptions are expected by focusing on the particulars of the studied phenomenon, hence an idiographic approach that focuses on the individual and their unique experience; (4) Opposite to the positivists who prioritize the identification of causal linkages (e.g., causes of individuals’ behaviours), interpretivists view the world holistically and do not distinguish a cause from an effect; (5) Lastly, the interpretive researcher has to adapt to emerging research designs and interact cooperatively with the people involved in the research (called “informants” instead of “subjects” or “respondents”). How those points are reflected in this research is explained in Table 5 below.

Assumptions		Interpretive approach	Retailance research
Ontological	Nature of reality	Multiple realities that are changing and contextual	Consumers have different reactions to retailance, and those reactions are receptive to change.
	Nature of social beings	People actively create meaning and interact in order to shape their environment	Not all consumers react passively to retailance, for some are expected to negotiate and/or resist.
Axiological	Overriding goal	A comprehensive, hermeneutic/interpretive process of understanding shared and individual meanings	The research aims at understanding consumers' reactions towards retailance, and how these reactions are shaped by individual, societal and political awareness.
Epistemological	Knowledge generated	Idiographic outcomes that are time-bound and context-dependent	The research focuses on the current consumer (i.e., time-bound to the present) in a brick-and-mortar retail setting (physical vs. online context)
	View of causality	A holistic view of a dynamic world	The retailance research model shows that the relationship between the surveiller and the surveilled is not one of cause and effect, rather, they mutually affect one another.
	Research relationship	Interactive, cooperative relation with informants	One-on-one interviews will be conducted with consumers.

Table 4 – Interpretive approach to this retailance research

To conclude, using an interpretive approach when addressing a novel question, researchers are free to chase new insights that emerge (Edmondson & Mcmanus, 2007), for interpreting and making sense of what they see is critical for understanding any social

phenomenon (Leedy & Ormrod, 2010, p. 135). Since this approach requires an evolving research design capable of adapting to changes in perceived reality (Hudson & Ozanne, 1988), a pragmatic research methodology in which initial understanding of the collected data can be modified and developed at a later stage was employed.

A pragmatic approach to a mixed methods research design

Pragmatism accepts the existence of two realities: the single (i.e., positivist) and multiple (i.e., interpretivist), and is, therefore, a valuable research approach to study practical problems in real world situations (Creswell & Plano Clark, 2018; Feilzer, 2010; Rorty, 1999). Pragmatist principles are also particularly relevant for dealing with and “understanding the contemporary challenges of change and complexity especially as they play out across multiple levels of analysis” (Farjoun, Ansell, & Boin, 2015, p. 1787). Pragmatists view individuals as “plural and paradoxical: they have multiple and often contradictory selves; they are capable of both following rules and doubting or questioning them” (p. 1790). Since consumer behaviour is complex and cannot be separated from the context in which it occurs, and since new retailance systems and channels are constantly being introduced in retail with varying degrees of impact on different stakeholders (i.e., consumers, retailers/practitioners, marketers and policy makers), a pragmatic research approach was employed.

According to Morgan (2007), the pragmatic approach is associated with abduction, intersubjectivity and transferability. First, the pragmatic approach relies on abduction instead of induction (associated with qualitative research) or deduction (associated with quantitative research) which begins by building theories out of observations and testing them on a wider sample. Second, a pragmatic approach helps introduce the notion of intersubjectivity (denoting

that the existence of unique subjective interpretations of the world is not mutually exclusive) instead of the polar views represented by the subjective/objective dichotomy, hence, a more representative middle-ground of reality. Third, a pragmatic approach requires transferability, which is working back and forth between the qualitative research's specific and context-dependent knowledge, and the quantitative research's general knowledge.

To summarize, this research undertook the pragmatic perspective by employing a mixed methods research design that included both quantitative (i.e., surveys) and qualitative (i.e., interviews) analysis techniques. The interviews were designed to follow the survey research sequentially to explore in more detail the survey findings; in other words, data collection followed a sequential, or two-phase, mixed methods design (Feilzer, 2010; Johnson & Onwuegbuzie, 2004; Johnson, Onwuegbuzie, & Turner, 2007). To glean insights into the collected data, both the quantitative and qualitative findings were integrated and brought together (Bryman, 2007). More details about the collection and analysis of data are discussed later in this chapter.

The impact of the COVID-19 pandemic on data collection

Because of the coronavirus pandemic and with social distancing becoming the new norm, data collection procedures for academic research have been impacted. For example, in-person interaction with participants has been either replaced by online means or suspended (Office of Research Ethics, 2020). Consequently, the design of this research was altered to accommodate the new data collection restrictions and new procedures. The pre-coronavirus data collection plan

was designed to include two pilot studies, the first of which was to be a student survey²⁷. Because of the disruptions caused by the pandemic which led to the closure of the university campus, the pilot student survey was changed into a second MTurk pilot survey. Since MTurk informants are recruited online through Amazon, the pandemic presented no issues when it came to them filling out the online surveys. The research plan was approved by the Research Ethics Board at Carleton University (CUREB, project number 112372).

As for the interviews, I recruited informants through the MTurk survey and through social media, specifically Facebook (Kozinets, 2020, pp. 252–254). I also postponed interviews with retail managers till late Summer and early Fall 2020 since, understandably, sitting for an interview was not on any manager's to-do-list during the beginning of the pandemic. Interviews were conducted using the online platform Zoom (using online platforms for interviewing has been discussed by Janghorban, Roudsari, & Taghipour, 2014; Lupton, 2020; Salmons, 2011). Online interviews, or e-interviews, are defined by Salmons (2011) as “in-depth interviews conducted using CMC [computer-mediated communication]” (p. 5). Like face-to-face interviewing, online interviews must be conducted in accordance with accepted ethical research guidelines and in relation to the research focus and question. Kozinets (2020) recommends that when conducting online interviews via a teleconferencing program, it would be better to stick to one platform in order to maximize comparability (p. 252). Online interviews can also include

²⁷ Undergraduate students are recruited using the Sprott Behavioural Research Participant Pool, by inviting them to participate in behavioural research in exchange for 0.5% bonus course credit (in general, students can earn 1% for each hour of participation in a research study, up to a potential maximum of 2%). Invitation emails (with a short description of the study, information about confidentiality, and a link to the survey hosted on Qualtrics), sign-up for the study and bonus credit tracking is managed via the Sprott SONA research registration system. University students were deemed an appropriate population to study due to their awareness of the current surveillance technologies compared to older generations.

screen sharing, and most platforms allow for recording, saving and even basic transcription of the conversation, freeing the researcher from routine note-taking or transcription concerns, allowing them to focus fully upon the interview and building rapport (p. 254).

Figure 49 (below) shows the updated research design. It is worth noting in this research, all retail environments (e.g., different store types and sizes) will be treated as one.

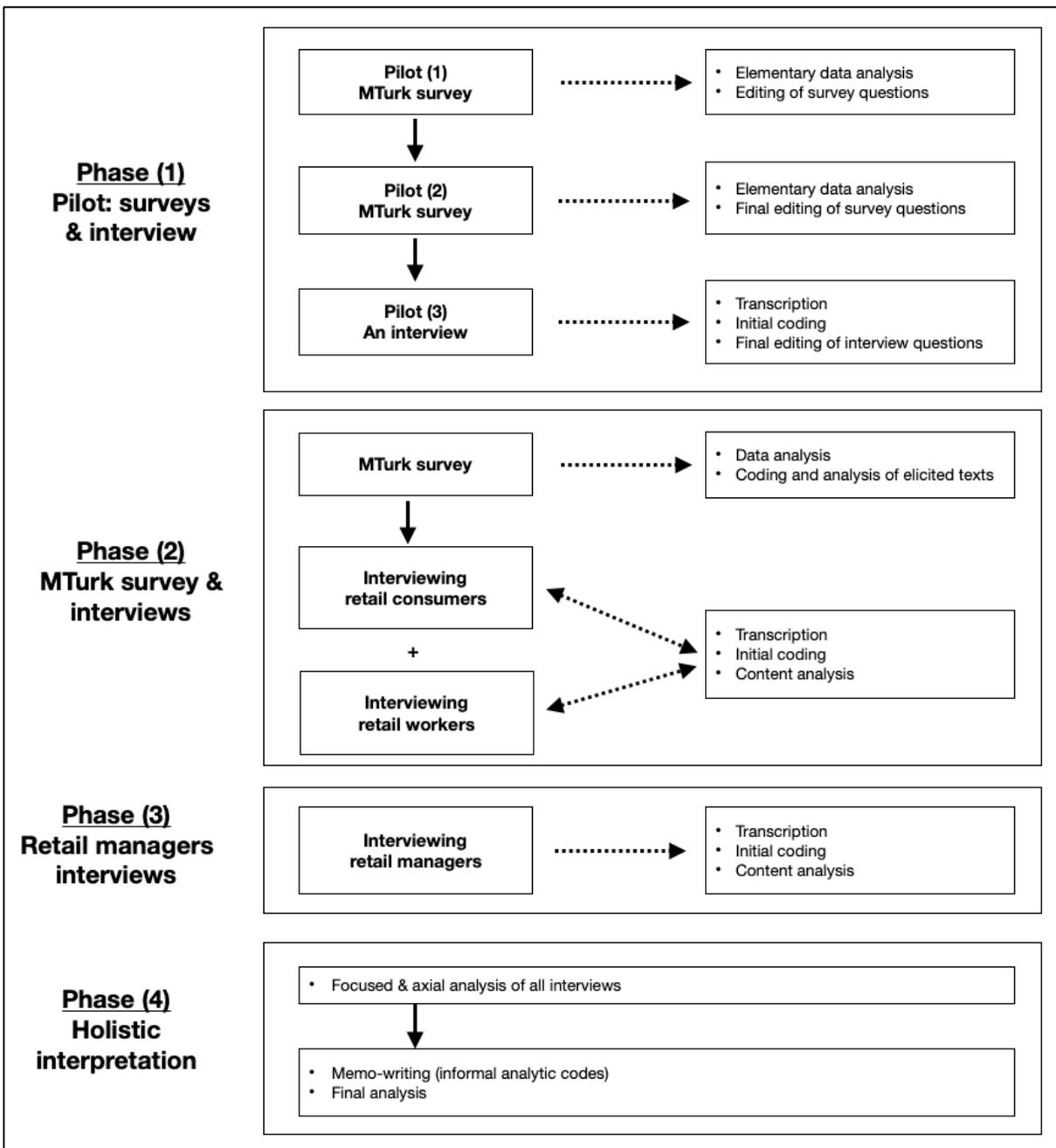


Figure 49 – The mixed methods design employed in this research

Data collection and analysis

Surveys

In this research, the survey questionnaire was designed to explore consumers' awareness of the presence and scope of retailance and of the relevant laws and regulations, their behavioural reaction, and the attitudinal and behavioural outcomes of using various surveillance technologies available in retailing. The survey also covered the impact of the COVID-19 pandemic on the acceptance/refusal of retailance. Questions asking for demographic data (such as gender, age, income, and ethnicity) were added at the end of the questionnaire in an attempt to explore whether they influence the consumer's awareness of and reaction to retailance. The survey also included open-ended questions (i.e., elicited texts) that would enhance the collected data, and ended with an invitation to be interviewed. A complete list of the survey questions is available in Appendix 1.

A cause for concern when conducting informant-driven surveys online is the quality and level of informants' attentiveness to survey questions, for they can either pay little attention to the questions or their responses, or they may deliberately misrepresent their behaviour or preferences. This lack of attentiveness could lead to bias and response error, increase the amount of noise in the data, and produce inaccurate estimates (Alvarez, Atkeson, Levin, & Li, 2019). To avoid inattentive informants and reduce noise, screeners should be added to the survey questions (Berinsky, Margolis, & Sances, 2013), for example, attention checks (also called trap or red herring questions) such as instructed-response items and instructional manipulation checks (IMCs) which instruct respondents to answer a survey question in a specific way to prove that

they are paying attention (Alvarez et al., 2019). For example, attention check 2 in Figure 50 below.

Attention check 1 (logical statement):

I would rather eat a piece of fruit than a piece of paper.

A five-point Likert-type scale (from 1=strongly agree to 5=strongly disagree)

Attention check 2 (directed query):

When you urgently want to buy some milk, you often choose to go to the nearest retail store. We want to know which one you choose. We also want to know if people are paying attention to the question. To show that you have read this much, please ignore the question and select none of the above as your answer.

Which retail store do you choose when you urgently want to buy milk?

- Supermarket
- Drug store
- Discount store
- None of the above

Attention check 3 (response pattern/time):

A post-hoc evaluation of response consistency, pattern, and effort evaluated as a function of timing.

Figure 50 – Survey attention checks

Once the survey results are collected, and the shirkers (i.e., inattentive informants) and workers (i.e., attentive informants) are identified, the question then arises: should this noisy data be included or excluded from the analysis? On one hand, dropping, or discarding, inattentive survey informants from the sample reduces noise but decreases sample size and alters its composition (e.g., age, education, and race), losing one of the main benefits of online collection of data, namely the ability to collect a diverse sample; therefore, it risks producing an unrepresentative sample and inflated results which threaten external validity (Berinsky et al.,

2013; Berinsky, Margolis, & Sances, 2016). On the other hand, keeping all respondents in the sample and ignoring attentiveness in data analysis can threaten the survey internal validity. To reconcile these two points, transparency regarding the presence of shirkers, who offer careless and haphazard survey responses, can be presented with the results. Thus, instead of dropping informants who fail the screeners, which might skew the sample and produce severely biased estimates, stratified results can be presented, showing how the culled sample affects the findings (Berinsky et al., 2013)²⁸.

Researchers caution against using only one screener question (i.e., attention check) as an accurate measure of attention and recommend using multiple items to measure attention (Abbey & Meloy, 2017; Berinsky et al., 2013, 2016). Since the presence of multiple screeners can lead to generating “various unwanted emotional responses, such as annoyance, irritation, and even fear” (Abbey & Meloy, 2017, p. 68), only three screeners were used in the survey. In addition to the logical statement check and the directed query check, the researcher looked at the inattentive responses in relation to the reasonable response duration (Alvarez et al., 2019) and the completion of survey questions. More details regarding which survey responses were deemed inattentive and discarded are in Chapter 5.

MTurk survey

The objective of the MTurk survey was to reach a more diverse pool of informants (i.e., participants recruited from the Amazon Mechanical Turk survey panel). In addition, it was hoped that informants’ written responses to the open-ended survey questions (i.e., elicited texts) would

²⁸ The argument of whether to use or not use noisy data is relevant to the use of surveys in both qualitative and quantitative research, hence, a positivist overtone in the discussion.

enrich the data to be analyzed. It is worth mentioning that the use of MTurkers in marketing and consumer behaviour research is not new (e.g., Hamby, Brinberg, & Daniloski, 2017; Kupor & Tormala, 2015; Kwan, Dai, & Wyer, 2017; Raghurir, Morwitz, & Santana, 2012).

There are three main concerns regarding the use of MTurk. The two threats pertinent to internal validity are: whether its population is dominated by subjects who participate in numerous experiments, and whether its subjects are effectively engaged with the survey stimuli. The third concern is about external validity and the nature of the subject pool. According to the study run by Berinsky, Huber and Lenz (2012), MTurk is a valuable subject recruitment tool and its benefits are: (1) facilitating low-cost experiments with a diverse subject pool that involves nonstudent adult subjects; (2) the demographic characteristics of its domestic users are more representative and diverse than the corresponding student and convenience samples; (3) the estimates of its average treatment effects have been proven to be similar to original convenience and nationally representative samples; and (4) the potential limitations and concerns about heterogeneous treatment effects, subject attentiveness and prevalence of habitual survey takers have proven to be not large problems in practice. Despite those advantages, some aspects of MTurk should engender caution in general, particularly: (1) MTurk subjects are notably younger and more ideologically liberal than the general public; (2) they appear to pay more attention to tasks compared to other informants; and (3) habitual responding may pose more of an external validity problem. Harms and Desimone (2015) highlight other problems associated with the use of MTurk: (1) the problem of representativeness is more magnified when using non-U.S. samples (however, since this research focuses on the North-American region, this concern is eliminated), (2) the majority of the participants tend to be underemployed or unemployed, and (3) having non-English speakers as informants. Ford (2017) raises more concerns regarding the

use of MTurk respondents. First, the presence of “cheaters” (i.e., those who lie or misrepresent themselves in order to take surveys and make money) and “speeders” (i.e., those who quickly go through the questions paying too little attention to the questions being asked, producing flawed or misleading data) in the pool. However, such a concern is not limited to the MTurk pool. Secondly, Ford also draws attention to the fact that even if Amazon tracks respondents’ location by checking their internet protocol (IP) addresses, some international MTurkers (from 5% to 10% of the total number of respondents) will set up a variety of fake addresses and accounts to allow themselves to appear to be U.S. respondents. Lastly, he cautions against the “Super Turkers,” the small group of heavy survey takers who may greatly skew data, by creating the potential for significant experience effects.

For this research, participating in the survey was controlled by the following eligibility requirements: (1) the “requester” (i.e., researcher) specified that each “worker” (i.e., participant) could undertake the task only once; (2) the country of residence of the workers had to be either Canada or the U.S.A. (verified by checking the IP addresses, even though this method is not completely reliable); (3) prior approval rate followed the recruitment recommendations established by previous researchers (Berinsky et al., 2012; Ford, 2017; Harms & Desimone, 2015; Samat et al., 2017), implementing a minimum of 5,000 approved HITS with a minimum of 97% of HITS approval rating (i.e., the percent of prior Human Intelligence Tasks submitted by the respondent that were subsequently accepted by requesters); (4) adding a question that checks if the worker’s first or second language was English. Two 50-response trials were followed by recruiting a minimum 500 respondents. At the end, 678 MTurk respondents filled out the survey, out of which 593 cases were retained. More details are included in the data analysis in Chapter 5.

Analysis of survey data

To aid in the analysis of the survey data, IBM SPSS Statistics Premium software (version 26) was used to analyze the standard questions (i.e., multiple choice, ranking and yes/no questions). To explore the statistical associations between two or more of the categorical variables, Pearson's chi-square test for independence was used (Mchugh, 2013; Singleton & Straits, 2005) using a 95% confidence interval (du Prel, Hommel, Röhrig, & Blettner, 2009; Singleton & Straits, 2005, p. 124) and focusing on the values of the chi-square (X^2), the sample size (N), degrees of freedom (df), and p values $< .05$ (i.e., the chosen significance level was $\alpha = 0.05$ (Meyers, Gamst, & Guarino, 2006; Rosenthal & Gaito, 1963)). The chi-square test is useful when analyzing cross tabulations of survey response data (i.e., contingency tables that group variables together to enable researchers to understand the correlation between the different variables). An independent t-test (Singleton & Straits, 2005, pp. 499–500) was not run on SPSS because it utilizes only two independent/categorical groups (e.g., gender: male and female) while at least three groups are used in the research survey (e.g., gender: male, female, other). For the open-ended questions (i.e., elicited texts), NVivo 12 qualitative data analysis software was used. A more detailed explanation of the statistical analysis employed is in Chapter 5.

Semi-structured interviews

Conducting semi-structured interviews represented the qualitative phase in this research. To Eileen Fischer, a professor of marketing at York University, the nature of critical research invites a qualitative approach, for

...critical research . . . challenges the status quo. That is, it holds up for examination assumptions and ideologies and power structures and practices that are taken for granted and that tend to reinforce patterns of stratification or privilege. Critical research is thus differentiated from constructivist (or

hermeneutic) traditions of research that focus more on understanding understandings harboured by particular groups or individuals. Critical research looks at individuals or groups in social context and is concerned with the ways that the social context valorizes some practices, assumptions, interpretations of reality, etc. over others, often in ways that protect vested power interests. It doesn't have to advocate an alternative set of assumptions or practices, though some critical research does. Critical research need not be, but may be, qualitative. (quoted in Scott, 2007, pp. 9–10)

Creswell (2014) writes that one of the chief reasons for conducting a qualitative study is when the study is exploratory. This usually means that not much has been written about the topic or the population being studied, and the researcher seeks to listen to participants and build an understanding based on what is heard. This description fits this research perfectly: so far, there has been limited focus on retailance (i.e., not much has been written), past research tends to focus on the retailer rather than the consumer (i.e., population studied), and interviews will be conducted (i.e., listening to participants). Resonating with Creswell is Becker (2018) who argues that to capture the multi-dimensional and context- and situation-specific nature of consumer experiences, qualitative methods are more appropriate for such research endeavours.

Thus, this phase of the research was designed to explore the views of participants (Deshpande, 1983) and delve into the consumers', retail workers' and retailer managers' understanding of and/or reaction to retailance in detail. Each interview was expected to last for approximately one hour. Both structured and unstructured interviews were considered but not chosen. Structured interviewing is a rigid form that does not allow departure from pre-formulated questions usually asked in a specific order, which did not suit the exploratory and iterative nature of this research. Moreover, since all the interviews were to be conducted by myself, there was no need to ensure consistency across multiple interviewers (which could be problematic when different researchers conduct the same set of interviews). As for unstructured interviews, they were not chosen (despite their flexibility) because they yield different

information from different people, hence, the inability to make comparisons among the interviewees (Leedy & Ormrod, 2010, p. 148). Semi-structured interviews, on the other hand, are favoured because they allow for both structure (since they involve the use of some pre-formulated questions) and improvisation (by not adhering strictly to those pre-formulated questions), giving “the interviewee the opportunity to add important insights as they arise during the course of the conversation, while . . . previously prepared questions provide some focus” and “consistency across interviews” (Myers, 2013, Chapter Ten, Loc. 2817).

At the beginning of the interview, the purpose of the research was explained to the interviewee, and they were asked to sign a consent form. It was explained to the participants that the interviews would be video- and audio-recorded, that they could decline answering any question(s), that they were free to withdraw their agreement to participate (by a specified date), that they could decide at that time if the researcher could use any of the data collected or if it should be destroyed, and a pseudonym would be used should the research be written up for publication or presentation at academic conferences. Participants were assured that data, including recordings, would be securely stored by the investigator. No interviewees withdrew their participation and pseudonyms were used in this presentation and subsequent publications.

Although an interview is similar to a conversation (both being informal and loose in structure), an interview is still different, for the interviewee is the one who does the talking. Accordingly, interviewees were encouraged to follow a “stream of consciousness” approach to telling their stories; they were allowed to talk and lead the conversation without interruption for as long as they wanted to, leading to more free association of thoughts and deeper responses. The interviewer, moreover could choose to play two roles: the role of a guide (looking for signals about when to ask another question or when to ask more about what has already been said, or

was meant to be said , and when to go on to a new topic), and the role of a follower (when the interviewee exhibits a new level of excitement in what is being talked about) (Atkinson, 1998, p. 31-33). The prompts that were used during the interviews followed those discussed by McCracken in *The Long Interview* (1988, pp. 35–37). Prompts were either “floating” or “planned.” Floating prompts include the use of facial expressions (e.g., raising one’s eyebrow at the end of the respondent’s utterance), repeating a key term of the respondent’s last remark with an interrogative tone, and being forthcoming without being obtrusive. Planned prompts give the respondent the opportunity to consider and discuss a phenomenon that does not come readily to mind or speech, and they include: (1) contrast prompts (e.g., asking about the difference between two things); (2) category questions (that account for the formal characteristics of the topic under discussion); and (3) asking respondents to recall exceptional incidents in which the research topic was implicated. McCracken’s fourth planned prompt, auto-driving (i.e., asking the respondent to comment on a picture, video, or some other stimulus, and to provide his or her own account of what they see there), was also used in this research. Ideally, emotionally laden questions should be asked at the end of the interview, to give the interviewee time to get used to the idea of talking about their experience(s) (Atkinson, 1998, p. 35). At the end of the interview, the interviewer expressed their gratitude for being given the opportunity to share the interviewee’s stories and experiences.

Asking what the optimum number of interviewees is always produces the evasive answer “it depends” or “until saturation” (Baker & Edwards, 2012). I anticipated conducting 12-15 interviews, or more until saturation was reached (i.e., no new data emerges during analysis). I ended up conducting a total of 38 interviews. To gain more insight into the reason behind

retailers' use of retail systems, different stakeholders were included (16 consumers, 18 current retail workers and 4 current retail managers).

Post-interview: Transcription, coding and data analysis

Interviews were conducted on the Zoom platform. Carleton University's license allows for automatic transcription of the recorded audio file, therefore, preparing interview data for analysis included revising, editing and proofreading the transcription. In addition, the NVivo 12 qualitative data analysis software (which also facilitates the coding of data) was employed. NVivo helps in the creation of word clouds, a form of charting qualitative data which "allows the recognition of more common or prominent words, and thus can lead to discerning patterns of overall or comparative word use that might otherwise go undetected" and helps in the evaluation of "whether a given text is relevant for a particular information need" (Kozinets, 2020, p. 351).

The transcription process essentially consisted of: (1) leaving out the interviewer's questions (so that the collected data could be read as one coherent narrative); (2) using standard spelling (without changing word usage, order or meaning); (3) creating sentence and paragraph structure; (4) leaving out extra things for ease in readability (e.g., deleting extraneous or unnecessary words or phrases such as "um" or "er" or "uh" that are used as fillers, false starts, or backing-and-filling); (5) adding missing things (e.g., adding a word or phrase, in brackets, if an answer to a question is incomplete, for ease in readability); (6) clarifying a word or phrase by using correct spelling or some other grammatical correction; (7) adding "stage directions" when they played a significant role in the conversation (e.g., laughter, sigh); and (8) possibly reorganizing certain sections to keep common subject matter together (Atkinson, 1998, pp. 54-57).

The steps taken after gathering the data up to writing the final report followed the standard procedures for coding qualitative data outlined by Spiggle (1994) in her seminal article. The procedures for coding data that were followed are: (1) the processes of categorization (i.e., the process of classifying or labeling units of data during the process of coding); (2) abstraction (i.e., collapsing more empirically grounded categories into higher-order conceptual constructs by grouping previously identified categories into more general, conceptual classes); (3) comparison (i.e., employing the principles of logic in making inferences from data); (4) dimensionalization (i.e., exploring the relationships across categories and constructs); and (5) integration (i.e., identifying patterns, themes, or unrelated propositions, and mapping relationships between conceptual elements).

Complementary to Spiggle's work is Charmaz's strategies of data coding adopted in her constructionist version of grounded theory (Charmaz, 2008). To Charmaz, using grounded theory methods provides a "valuable set of tools for developing an analytic handle on . . . work" and helps make the qualitative analyses of interviews "more insightful and incisive" (Charmaz, 2006, p. xii). Although this research does not employ grounded theory per se, it is common for qualitative researchers in business and management to employ grounded theory methods when coding and analysing data (Myers, 2013, Chapter Nine, Loc. 2444).

[I]f all you want to do is use some of the grounded theory coding techniques for your qualitative data analysis, and some other theory as an overarching framework for your study, then I believe that is acceptable. All qualitative research methods require the researcher to be critical and creative and grounded theory studies are no exception (Myers, 2013, Chapter Nine, Loc. 2451).

Grounded theory coding that was conducted in this research consisted of three phases: “initial coding,” “focused coding” and “axial coding” (Charmaz, 2006, pp. 42–71; Gibbs, 2015)²⁹.

Initial coding: The first phase of initial coding keeps coding open-ended while acknowledging that the researcher holds prior ideas and skills. In general, it takes segments, words, lines or incidents of data apart, names them in concise terms, and proposes an analytic handle to develop abstract ideas for interpreting each segment of data. Since the data to be coded was from interviews and elicited texts (i.e., written responses to some of the survey questions), “line-by-line coding” method was used³⁰. This type of coding helps the researcher to (1) identify implicit concerns as well as explicit statements, (2) question the respondents’ views and look at the data critically and analytically, (3) refocus later interviews, (4) spark new ideas to pursue, and (5) refrain from imputing their motives, fears, or unresolved personal issues in the collected data. Initial coding, moreover, helps the study to “fit” the empirical world (since the developed categories reflect participants’ experiences) and to have “relevance” (since the analytic framework interprets what is happening and makes relationships between implicit processes and structures visible). The codes applied were close to the data (for example, coding with gerunds helps in detecting processes and sticking to the data), and were simple, short, and open to what

²⁹ Axial coding is sometimes followed by “theoretical coding” families, introduced by Glaser, which specify possible relationships between categories already developed in the phase of focused coding. Charmaz argues that although theoretical codes may lend an aura of objectivity to an analysis, they “do not stand as some objective criteria about which scholars would agree or that they could uncritically apply” (p. 66).

³⁰ The two other coding methods are “word-by-word”, which is particularly helpful when working with documents and internet data, and “incident to incident”, or a comparative study of incidents described in field notes.

the material suggests. To preserve participants' meanings of their views and actions, their telling terms were also adopted as *in vivo* codes, hence, an interactive process of coding.

To analyze the interviews, I updated Charmaz's initial coding method that relies on line-by-line coding, instead, I divided the text into short segments (Figure 51). In comparison to transcriptions that are either hand-written or typed, filling out every line on the page, interviews that are auto-transcribed by a software, such as Zoom (Figure 52), are divided into short sentences and lines based on screen shots (to provide timely captions). In addition, the number of words in every line is dependent on the type of chosen font and its size.

208
00:25:09.360 --> 00:25:12.480
#5: So it doesn't affect you coming back to that store or anything.

209
00:25:13.530 --> 00:25:16.920
#5: No, I mean, these are human beings that are working behind

210
00:25:18.060 --> 00:25:25.770
#5: that register. Who knows? I mean, especially if it's really busy and they're just trying to get to do, especially if there's a line of people

211
00:25:25.830 --> 00:25:26.850
#5: trying to check out.

212
00:25:27.570 --> 00:25:37.230
#5: It's going to happen and it's okay. They don't make enough money for me to yell at them for it. It's . . . it's just a human mistake, it happens.

Figure 51 - A transcribed section of an interview before being prepared for initial analysis

<p>No, I mean, these are human beings that are working behind that register. Who knows? I mean, especially if it's really busy and they're just trying to get to do, especially if there's a line of people trying to check out. It's going to happen and it's okay. They don't make enough money for me to yell at them for it. It's . . . it's just a human mistake, it happens.</p>	<p>Nada Elnahla <ul style="list-style-type: none"> •Behavioural impact on consumer •Treating store workers </p>
--	---

Figure 52 – The above section after initial coding

Focused coding: In the second phase of focused coding, the most useful, significant, and/or frequent initial codes are selected and tested against extensive data. Through focused coding, the researcher can move across interviews and compare people’s experiences, actions and interpretations. It is worth noticing that moving to focused coding is not entirely a linear process, and the researcher “may return to earlier respondents and explore topics that had been glossed over, or that may have been too implicit to discern initially or unstated” (Charmaz, 2006, p. 58).

Axial coding: The purposes of axial coding are to sort, synthesize, and organize large amounts of data and to reassemble them in new ways, giving coherence to the emerging analysis. It develops subcategories of a category and shows the links between them. Although axial coding “helps to clarify and to extend the analytic power of your emerging ideas,” Charmaz cautions that too much reliance on axial coding “may limit what and how researchers learn about their studied worlds and, thus, restricts the codes they construct” (Charmaz, 2006, pp. 62–63).

In conclusion, I believe that grounded theory coding methods were a fitting choice for this research because they reflect its exploratory nature, for unlike quantitative logic that applies preconceived categories or codes to the data, grounded theory “codes emerge as you scrutinize your data and define meanings within it . . . [and] may take you into unforeseen areas and new research questions” (Charmaz, 2006, p. 46). To Charmaz,

...coding is a heuristic device for engaging with the data and beginning to take them apart analytically. I emphasize coding in gerunds, when they fit and doing

line by line coding with early data, particularly with data from interviews and such texts as personal accounts. These practices help the researcher to take a fresh look at the data and to move it forward analytically. They are simply strategies that help researchers begin to see processes in their data. These strategies foster taking an active stance towards the data, which ultimately expedites analytic work (Charmaz & Keller, 2016).

It is worth noticing that grounded theory coding is an activity of constant comparison and it progresses along with data collection (i.e., interviews); in other words, analysis and data collection overlap (versus data analysis coming after data gathering) (Myers, 2013, Chapter 9, Loc. 2526). To analyse the subtle inferences to be found in the interviews, content analysis was applied to the interviewee's own language and mode of expression. This helped in examining the language used by the interviewees, as well as the social and cultural contexts in which these communications occurred (Berg, 2009, p. 353). Such an analysis can lead to understanding other people's cognitive schemas (Duriau, Reger, & Pfarrer, 2007).

An expected output of the above-described qualitative phase would be a deeper understanding of the level of consumers' awareness of the presence of retailance and their subsequent reaction to it.

A final, holistic interpretation

During the analysis of data collection, coding was conducted to give a focused way of viewing data, route the work in an analytic direction, and help make discoveries and gain a deeper understanding of the empirical world. After data collection, coding, and initial analysis, the final phase of analysis was dedicated to memo-writing (i.e., informal analytic notes), developing a holistic interpretation of the collected data, and writing up the findings.

Interpretation "seeks informed conclusions and meaning from data or analysis, and encompasses its critique, as well as its extension into new and additional inquiries" (Kozinets, 2020, p. 359).

At this final stage of analysis, the researcher adopted a bird's-eye view of the emergent data, themes and concepts, in light of the relevant literature and theory, in order to find out if there were precedents and/or discover new concepts (Gioia, Corley, & Hamilton, 2012). To sum up, in this third phase, all the collected data (from interviews and surveys) were integrated, common themes were identified, and the research questions were answered. This led to a revision of the retailance model to ensure that all the essential concepts and themes discovered and the relational dynamics among those concepts were well represented.

In addition to coming up with a discussion that reflects the developed retailance model and where qualitative data is supported by the quantifying elements collected in the surveys, visual elements, such as charts and tables, were employed³¹. In the past, extended text has been the most frequent form of display for qualitative data, however, charting—or data display which can include tables, maps, charts, graphs, matrices, networks and word clouds—is now considered a major component of analytic activity (Kozinets, 2020, pp. 347–348). Moreover, using tables in qualitative research complements the content of the main text, helps to organize and display the data effectively, and enhances transparency about data collection, analysis and findings (Cloutier & Ravasi, 2021).

³¹ According to Kozinets' (2020, pp. 332–355), there are five analytic operations of netnography research, which are: (1) “collating” (i.e., preparing various types of data for coding), (2) “coding” (i.e., detecting repeated patterns across the various elements of the dataset), (3) “combining” (i.e., uniting conceptually-related codes to form a new, higher-order element in analysis, a “pattern code” or abstract conceptual relationships), (4) “counting” (i.e., quantifying elements identified in the qualitative data), and “charting” (i.e., the visualization, mapping, organization and display of data).

Research ethical issues

Most ethical issues in research fall into one of four categories: protection from harm, informed consent, right to privacy, and honesty with professional colleagues (Leedy & Ormrod, 2010, p. 101). Consequently, this research conformed to the current Tri-Council Policy Statement (Government of Canada, 2014). In preparation for applying for ethics clearance from CUREB, I successfully completed the TCPS-2 (latest edition of the Tri-Council Policy Statement) Course on Research Ethics (CORE).

I also contacted the Office of Research Ethics to discuss the choice of participant pools. As a result, I taught neither BUSI2004 (Basic Marketing) nor BUSI2008 (Introduction to Marketing) courses in Winter 2020 in order not to risk the voluntariness of the students' consent, since course instructors have access to the list of students who participated in available research studies. As for the MTurk pool, the Office of Research Ethics did not object to employing them. Unfortunately, although researchers from different faculties and departments in Carleton University employ the MTurk in their surveys, no records are kept of the total number of approved ethics applications for research studies that utilize MTurk.

Chapter summary and conclusion

This chapter discussed why a pragmatist mixed methods research design best suits the interpretive nature of this exploratory research. In order to explore consumers' awareness of the presence and scope of retailance and of the relevant laws and regulations, their behavioural reaction to retailance, and the attitudinal and behavioural outcomes of using various surveillance technologies available in retailing, data collection and analysis were divided into four phases. In the first phase, two pilot MTurk surveys were followed by a pilot semi-structured interview. In

the second phase, in addition to an MTurk survey, semi-structured interviews of both retail consumers and workers were conducted (until data saturation was achieved). In the third phase, retailer managers were interviewed. And finally, in the fourth phase, a holistic interpretation of all the collected data and analysis was conducted and the retailance model was updated.

CHAPTER 5: DATA ANALYSIS, FINDINGS & DISCUSSION

Data analysis

As explained earlier, because of the exploratory nature of this study, a pragmatic, mixed methods research design was employed. Two forms of data collection were used: online self-administrative questionnaires and semi-structured interviews. This chapter proceeds as following: first, the collected data and how informants were recruited is explained. Second, the findings are then divided into six sections based on the retailance model introduced in Chapter 1: (1) consumer awareness and the impact of retailance systems (general awareness of the presence and scope of retailance, awareness of laws and regulations, awareness and reviewing of privacy policies, tracking consumers' purchases, selling consumers' information to third parties, loyalty programs, and tagging); (2) consumers' behavioural reactions (acceptance, negotiation, and resistance); (3) more factors affecting consumers' behavioural reaction (political affiliations during crises and consumers' past experience); (4) consumers' attitudinal outcomes (being for or against the use of retailance); (5) the factors affecting the retailer's choice and scope of retailance channels and systems (profiling, retail location, size and type of retail, and population size); and (6) privacy. Third, based on the findings, the retailance model is updated. Lastly, the chapter ends with a summary and a conclusion.

Online surveys

To create the questions for a self-administered online survey, previous research (e.g., Ekos Research Associates, 2009; Zureik et al., 2010, pp. 361–382) was used as a guide. In addition to updating the questions to include new technologies, more exploratory questions were added to address the dissertation research questions (discussed in Chapter 1). Demographic and

general surveillance questions were included (for example, what surveillance in a brick-and-mortar retail store means to the consumer, and how confident they feel about having enough information to know how new technologies used in stores might affect their personal privacy). The questionnaire was designed to explore the topics of retailance awareness, impact, outcome, ethics, and the current and expected future impact of the COVID-19 pandemic on retailing. A complete list of the survey questions is available in Appendix 1.

MTurk pilot test (1): This pilot survey was administered to test the survey questions and their clarity. 49 participants (between the ages of 18 and 65 or older, with 67.4% male) completed the study in April 2020. All of them identified as U.S.A. citizens. The average length of time to completion was approximately 29 minutes and 25 seconds. Each participant was paid US\$1 as compensation (in addition to 40% paid to Amazon). This test led to the discovery of a few typographical errors and the re-adjusting of the response scales. As a result, in the following surveys, for the Likert-type questions, a five-point scale was used instead of a seven-point scale since it has been proven to reduce the frustration level of respondents and would thereby increase the response rate and the quality of the responses (Babakus & Mangold, 1992, p. 771; Buttle, 1996; Devlin, Dong, & Brown, 2003; Marton-Williams, 1978). All answers to the question asking about the clarity of the survey questions were positive. The responses from this pilot test were not included in the analysis for two reasons: (1) the scales of some of the questions were changed in the following surveys; and (2) after the COVID-19 pandemic hit, a decision was made to add more questions to the following surveys.

MTurk pilot test (2): 50 participants (between the ages of 18 and 65 or older, with 62% male) completed the study in May 2020 and all of them identified as U.S.A. citizens. This second pre-test was needed to add questions related to the COVID-19 pandemic and to ensure their clarity. Because of the addition of questions related to the impact of the COVID-19 pandemic, the average completion time of the survey was approximately 33 minutes and 35 seconds (i.e., higher when compared to the first pilot test). Each participant was paid US\$2 as compensation (in addition to 40% paid to Amazon). Since all informants indicated that the questions were clear to understand, no changes were administered to the following survey and those 50 cases were included in the data analysis.

Third MTurk survey: In late May 2020, 589 informants participated in the survey. Only 11 informants (1.87%) identified themselves as Canadians and the rest were Americans. The average time for completing the survey was 25 minutes (the reason behind a lower completion time is that this average was calculated based on all submissions, including incomplete ones that were later removed). Each participant was paid US\$1.75 as compensation (in addition to 40% paid to Amazon).

In total, 639 responses (the total of 50 responses from the second pilot survey and the 589 responses from the third MTurk survey) were collected via MTurk. Before the analysis of data, and to avoid inattentive informants and reduce noise (Abbey & Meloy, 2017; Alvarez et al., 2019; Berinsky et al., 2014, 2016), each informant had to pass at least two of the three screeners (i.e., attention checks): (1) a post-hoc evaluation of response consistency, pattern, and effort evaluated as a function of timing; (2) a logical statement; and (3) a directed query. No cases were dismissed because of the screeners since not one respondent failed the three screening tests (1

informant failed 2 screeners and 17 informants failed only 1 screener). However, 46 responses were judged to be unusable: 1 response answered no demographic questions, and 45 responses were incomplete (i.e., leaving most of the questions unanswered). A total of 593 cases out of 639 cases (92.8 %) were retained for analysis. They included: 424 retail consumers, 77 current retail workers and 92 consumers who had worked in retail within the past five years, between the ages of 18 and 65 or older, with 51.5% female. Only 11 informants (1.85%) identified themselves as Canadians; their responses were not excluded because they matched those of the American informants (i.e., geographical location had no undue influence on the observations). To aid in the analysis of data, NVivo 12 qualitative data analysis software was used in analyzing the open-ended questions (i.e., elicited texts) and IBM SPSS Statistics Premium software (versions 26) to analyze the survey questions (i.e., multiple choice, ranking and yes/no questions).

Interviews

A total of 38 semi-structured interviews were conducted, with each interview lasting for approximately 40 minutes. Three online platforms were used for recruitment: MTurk, Facebook and LinkedIn.

MTurk recruitment: A question was added at the end of the three MTurk surveys (the two pilots and the main survey) asking informants to provide their email if they were interested in participating in an interview for which they would be compensated by an Amazon Gift Card or an MTurk bonus payment (between US\$5-15). A link to a second Qualtrics survey was provided to ensure anonymity of the data in the main survey. Out of 326 informants who provided their email address, only 12 agreed to be interviewed when contacted (3.7%); one of the reasons behind such a small acceptance rate could be the low payment offered as

compensation when compared to minimum wage (which is US\$7.25/hour) or to the even high hourly rate offered by marketing firms for interviews (one informant wrote back saying he typically gets paid US\$60 for an hour for interviews).

Facebook recruitment: Recruitment on the social media platform Facebook had a much higher acceptance rate; out of 49 Facebook users who showed interest in being interviewed, 25 were interviewed (49%), and they were compensated by CAD 10-25 paid through an Interac e-Transfer. Recruitment posts (see Appendix 5 for examples) were published on my personal Facebook page where I changed the setting of the post to “public” to enable its sharing. I also published them on different public and closed Facebook groups, and they were:

- Bancroft buy and sell
- Barrhaven Costco Friendly Shoppers (unaffiliated)
- BMGCA – Buying / Selling/ Free Stuff / Advertising
- Buy & Sell Brampton
- Buy & Sell Ottawa Gatineau
- Buy, Sell or trade Sudbury
- East Windsor/Tecumseh Ontario Buy & Sell
- Gloucester Costco Friendly Shoppers (unaffiliated)
- Kanata – Buy, sell and trade
- Kanata & Stittsville Area Buy and Sell
- Kanata Costco Friendly Shoppers (unaffiliated)
- Ottawa and Area Bu, Sell + Swap Shop
- Ottawa buy, sell and trade anything
- Ottawa Market

- Windsor Buy and Sell

Recruitment of retail managers: Out of the four recruited retail managers, two were recruited via Facebook (a Store Manager for a wireless provider in Ottawa and a Planning Manager in TJX Canada). One manager (who worked as an Assistant Account Manager for Product Services in the ALDO Group head office at the beginning of the pandemic) was recruited via LinkedIn by Prof. Leighann Neilson (the supervisor of this thesis). I was introduced to the fourth retail manager (an Associate Vice President of Business Transformation, Giant Tiger Stores Limited) by the Sprott staff member responsible for alumni liaison.

All thirty-eight interviews were conducted on Zoom, with the majority of interviewees opting for a “video meeting.” Seven informants chose to participate with only audio and the reasons behind their choice were: technical difficulties (a webcam was not available, the internet was unreliable, or children in the house were using all computers and tablets for their online school), convenience (one of the informants was in his pajamas), or shyness (some felt more comfortable when the webcam was closed despite sometimes having their personal photo uploaded with their username). The following (Table 5) shows all informants’ demographic profiles:

	MTurk survey (n = 593)				Interviews (n = 38)						Total (n = 631)	
	Consumers (n = 424)		Current & past workers (n = 169)		Consumers (n = 16)		Current workers (n = 18)		Managers (n = 4)			
	No.	Percent	No.	Percent	No.	Percent	No.	Percent	No.	Percent	No.	Percent
Age												
18-24	19	4.48%	8	4.73%	2	12.5%	8	44.44%	---	---	37	5.86%
25-34	120	28.3%	61	36.09%	4	25%	4	22.22%	4	100%	193	30.59%
35-44	130	30.66%	50	29.59%	4	25%	5	27.78%	---	---	189	29.95%
45-54	79	18.63%	25	14.79%	3	18.75%	---	---	---	---	107	16.96%
55-64	43	10.14%	19	11.24%	1	6.25%	---	---	---	---	63	9.98%
65 or older	31	7.31%	5	2.96%	2	12.5%	1	5.56%	---	---	39	6.18%
Not disclosed	2	0.47%	1	0.59%	---	---	---	---	---	---	3	0.48%
Gender												
Female	194	45.75%	87	51.48%	11	68.75%	10	55.56%	4	100%	306	48.5%
Male	225	53.06%	80	47.34%	5	31.25%	8	44.45%	---	---	318	50.4%
Other	5	1.18%	2	1.18%	---	---	---	---	---	---	7	1.12%
Country of residence												
Canada	9	2.12%	2	1.18%	7	43.75%	15	83.33%	4	100%	37	5.86%
USA	415	97.88%	167	98.81%	9	56.25%	3	16.67%	---	---	594	94.14%
Education												
High school	98	23.11%	54	31.95%	3	18.75%	4	22.22%	1	25%	160	25.36%
College	45	10.61%	23	13.6%	2	12.5%	2	11.11%	---	---	72	11.41%
Current college/ university student	11	2.59%	7	4.14%	2	12.5%	8	44.44%	---	---	28	4.44%
Bachelor	205	48.35%	68	40.24%	5	31.25%	3	16.67%	3	75%	284	45%
Master's	53	12.5%	16	9.47%	3	18.75%	1	5.56%	---	---	73	11.57%
Ph.D.	5	1.18%	---	---	1	7.69%	---	---	---	---	6	0.95%
Other	7	1.65%	1	0.59%	---	---	---	---	---	---	8	1.27%
Average income												
CAD 20,000 or less	30	7.08%	6	3.55%	3	18.75%	3	16.67%	---	---	42	6.66%
CAD 20,000- 39,999	58	13.68%	30	17.75%	1	6.25%	3	16.67%	---	---	92	14.58%
CAD 40,000- 59,999	70	16.5%	36	21.3%	2	12.5%	2	11.11%	1	25%	111	17.6%
CAD 60,000- 100,00	146	34.43%	58	34.32%	2	12.5%	4	22.22%	1	25%	211	33.44%
Over CAD 100,000	106	25%	36	21.3%	7	43.75%	3	16.67%	2	50%	154	24.41%
Not disclosed	14	3.3%	3	1.78%	1	6.25%	3	16.67%	---	---	21	3.33%
Minorities												
Black American	16	2.7%	4	0.67%	1	7.69%	---	---	---	---	21	3.33%
Hispanic	5	0.84%	4	0.67%	1	7.69%	---	---	---	---	10	1.58%
Asian	13	2.19%	4	0.67%	5	31.25%	7	38.89%	---	---	29	4.6%
Middle Eastern	---	---	---	---	1	7.69%	---	---	---	---	1	0.16%
Latino	2	0.34%	2	0.34%	---	---	1	5.56%	---	---	5	0.8%
Indigenous/aboriginal	6	1.42%	7	1.18%	---	---	1	5.56%	---	---	14	2.22%
With a disability	21	4.95%	11	1.85%	---	---	---	---	---	---	32	5.07%
Not disclosed	4	0.67%	2	0.34%	---	---	---	---	---	---	6	0.95%

Table 5 - Informants' demographic profiles

Findings

In Chapter 1, a preliminary retailance model (Figure 53) was introduced based on the synthesis of readings from different fields, such as marketing, consumer behaviour, sociology, political science, communications, media studies and law. This model is used to guide the discussion of the research results (see below). For each theme, Bryman's (2007) advice is

followed by discussing the results of the quantitative and qualitative and components of the research in such a way that they are “mutually illuminating.”

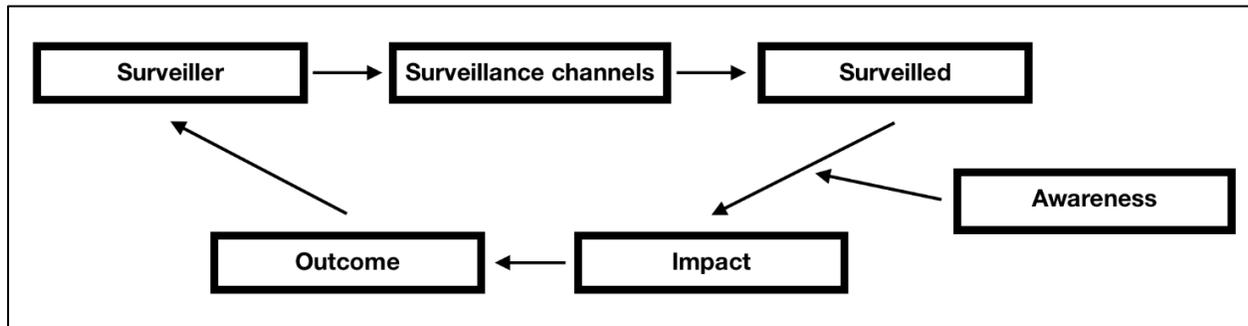


Figure 53 – The preliminary retailance model introduced in Chapter 1

First: Consumer awareness and the impact of retailance systems

(1) General awareness of the presence and scope of retailance

In a retail environment, consumers are exposed to different overt/covert and direct/technologically mediated retailance systems at the same time (which creates an assemblage of retailance). When those systems are combined with other bodies (e.g., credit card information provided by banks, or data collected from online shopping platforms or social media sites), a larger picture of the consumer is created. Consumers, therefore, would find it increasingly difficult to maintain their anonymity (what is described as “invisibility” in critical marketing) and protect their privacy, hence, a rhizomatic surveillance that scrutinizes consumers.

To understand how aware consumers are of the presence and scope of retailance systems, survey informants were given a list of twelve different surveillance systems and asked to answer a dichotomous yes/no question: “Which of the following surveillance systems have you come across in retail stores?” Their answers (Table 6) are listed from the highest to the lowest percentage of awareness of each retailance system. As expected, on the top of the list

(96.46%) is awareness of one of the most widely used overt retailance system, CCTV (or video surveillance), while biometric surveillance (whose use as a retailance system is relatively new) comes at the bottom of the list (15.51%).

Retailance			YES answers (from a total of 593)	
Systems	Channels		N	Percentage
	Overt	Covert		
Video surveillance	X	X	572	96.46%
Tagging	X	X	527	88.87%
Customer loyalty card	X		526	88.7%
Free Wi-Fi	X	X	477	80.44%
Tracking returns		X	440	74.2%
Collecting phone numbers and emails	X	X	414	69.81%
Personalized advertising	X	X	311	52.45%
Virtual guards		X	263	44.35%
Radio frequency identification (RFID)	X	X	189	31.87%
Audio surveillance		X	157	26.48%
Geo-fencing	X	X	108	18.21%
Biometric surveillance	X	X	92	15.51%

Table 6 – Informants' awareness of retailance systems

Running the Chi-square test of independence, to discover if awareness of the various retailance systems was associated with gender, age, education level, income level and/or membership in a minority group, statistically significant associations were discovered with all of the above (which are marked red in Table 7) except membership in a minority group.

Retailance system	Chi-Square test																			
	Gender				Age				Education				Income (U.S.A.)				Minority			
	X ²	df	N	p	X ²	df	N	p	X ²	df	N	p	X ²	df	N	p	X ²	df	N	p
Video surveillance	1.118	3	593	.773	1.334	6	593	.970	7.571	6	593	.271	7.844	6	582	.250	2.843	2	101	.241
Tagging	3.009	3	592	.390	13.628	6	592	.034	5.726	6	592	.455	15.778	6	581	.015	.893	2	100	.640
Customer loyalty card	11.997	3	591	.007	20.349	6	591	.002	5.737	6	591	.453	6.721	6	580	.347	4.674	2	101	.097
Free Wi-Fi	1.472	3	592	.689	25.213	6	592	<.001	6.406	6	592	.379	12.343	6	581	.055	.275	2	101	.871
Tracking returns	3.113	3	592	.375	11.847	6	592	.065	12.863	6	592	.045	6.014	6	581	.422	.781	2	100	.677
Collecting phone numbers and emails	3.973	3	592	.264	4.783	6	592	.572	2.605	6	592	.857	7.553	6	581	.273	5.619	2	101	.060
Personalized advertising	8.806	3	590	.032	5.393	6	590	.495	9.539	6	590	.145	14.623	6	579	.023	4.199	2	101	.122
Virtual guards	2.198	3	593	.532	12.565	6	593	.050	8.018	6	593	.237	14.278	6	582	.027	.113	2	101	.945
Radio frequency identification (RFID)	11.006	3	593	.012	2.036	6	593	.916	4.455	6	593	.615	9.187	6	582	.163	2.652	2	101	.266
Audio surveillance	3.588	3	592	.310	15.565	6	592	.016	8.898	6	592	.179	4.947	6	581	.551	2.679	2	101	.262
Geo-fencing	1.742	3	592	.628	6.544	6	592	.365	14.753	6	592	.022	7.153	6	581	.307	2.867	2	101	.238
Biometric surveillance	3.886	3	592	.274	9.266	6	592	.159	16.321	6	592	.012	5.174	6	581	.522	2.668	2	101	.263

Table 7 – Chi-square test results of the awareness of retailance systems with the statistically significant associations in red

Looking closely at the statistically significant associations (shown in red in the above table), the following was revealed:

Age: The association between Age (Table 8) and five of the twelve retailance systems is statistically significant at the 0.05 level: tagging ($X^2(6, N = 592) = 13.628, p = .034$), loyalty programs ($X^2(6, N = 592) = 20.349, p = .002$), free Wi-Fi ($X^2(6, N = 592) = 25.213, p < .001$), virtual guards ($X^2(6, N = 593) = 12.565, p = .050$), and audio surveillance ($X^2(6, N = 592) = 15.565, p = .016$). The analysis shows that more older consumers (aged 55 and above) are aware of overt retailance systems (e.g., tagging and loyalty programs) than younger consumers (aged 18 to 54), while more younger consumers are aware of covert retailance systems (e.g., audio surveillance and free Wi-Fi) than older consumers. This result is consistent with the idea that older adults are selective in the technologies they use and likely to be slower to adopt (Olson, O'Brien, Rogers, & Charness, 2011).

Age	Percentage of awareness of retailance systems				
	Tagging	Loyalty programs	Free Wi-Fi	Virtual guards	Audio surveillance
18 to 24 (n = 27)	85.19%	88.89%	85.19%	44.44%	33.33%
25 to 34 (n = 181)	83.98%	83.24%	82.32%	41.99%	35.36%
35 to 44 (n = 180)	93.89%	91.67%	85.56%	37.22%	25.14%
45 to 54 (n = 104)	89.42%	92.31%	83.65%	57.7%	22.12%
55 to 64 (n = 62)	87.1%	95.16%	68.85%	31%	16.13%
65 or older (n = 36)	97.14%	88.89%	58.33%	44.44%	33.33%

Table 8 – Association between age and the awareness of retailance systems, with the highest percentage under each retailance system in red and the lowest in bold black

Gender: The association between gender (Table 9) and awareness of three retailance systems is statistically significant at the 0.05 level: loyalty programs ($X^2(3, N = 591) = 11.997, p = .007$), personalized advertising ($X^2(3, N = 590) = 8.806, p = .032$), and RFID ($X^2(3, N = 593) = 11.006, p = .012$). The results indicate that female consumers are more aware of loyalty programs and personalized advertising while male consumers are more aware of the retailance systems employing RFID technology, which suggests that women are more aware of retailance systems directly related to the activity of shopping.

Gender	Percentage of awareness of retailance systems		
	Loyalty programs	Personalized advertising	RFID
Male (n = 303)	87.45%	47.19%	37.38%
Female (n = 281)	91.1%	58.57%	26.7%

Table 9 – Association between gender and the awareness of retailance systems, with the highest percentage under each retailance system in red

Education level: The association between consumers' level of education (Table 10) and awareness of three retailance systems was statistically significant at the 0.05 level: tracking returns ($X^2(6, N = 592) = 12.863, p = .045$), geo-fencing ($X^2(6, N = 592) = 14.753, p = .022$), and biometric surveillance ($X^2(6, N = 592) = 16.321, p = .012$). Looking at the chi-square test results, consumers with a post-secondary education are more aware of those three retailance systems. This result suggests that consumers educated beyond high school are more aware of the latest retailance technologies (geo-fencing and biometric which are both overt and covert systems) while consumers with a high school diploma are more aware of retailance that is directly related to the items they buy (the tracking of returns).

Education level	Percentage of awareness of retailance systems		
	Tracking returns	Geo-fencing	Biometric surveillance
High school (n = 152)	69.74%	9.87%	13.16%
College diploma (n = 68)	69.11%	14.7%	10.29%
Enrolled in a bachelor's degree (n = 18)	66.67%	27.78%	44.44%
Bachelor's (n = 273)	66.67%	21.69%	16.54%
Graduate (Master's & Doctorate) (n = 74)	64.86%	21.62%	16.22%

Table 10 – Association between education level and the awareness of retailance systems, with the highest percentage under each retailance system in red

Income: The association between consumers' income level (Table 11) and three retailance systems was statistically significant at the 0.05 level: the overt/covert tagging ($X^2(6, N = 581) = 15.778, p = .015$), the overt/covert personalized advertising ($X^2(6, N = 579) = 14.623, p = .023$), and covert virtual guards ($X^2(6, N = 582) = 14.278, p = .027$). The chi-square test results show that consumers who earn less than USD 29,000 are less aware of those three retailance systems, while consumers who earn over USD 77,000 show the highest percentage of awareness. Although it is beyond the scope of this research, the association between having a high-income level and being aware of tagging and personalized advertising is worth studying, for example, if this association is related to a high purchasing volume and/or purchasing high-priced items. Another point worth future investigation is that although the education and income variables are typically related, according to the MTurk survey, the retailance systems with significant statistical associations to both variables are different.

U.S. income	Percentage of awareness of retailance systems		
	Tagging	Personalized advertising	Virtual guards
USD 14,999 or less (n = 34)	91.43%	35.29%	51.43%
USD 15,000 to 29,000 (n = 85)	80.23%	41.18%	32.56%
USD 30,000 to 44,000 (n = 103)	92.31%	48.54%	37.5%
USD 45,000 to 76,000 (n = 200)	88.44%	56.5%	45.5%
USD 77,000 and over (n = 141)	93.62%	60.28%	52.48%

Table 11 – Association between U.S. income and the awareness of retailance systems, with the highest percentage under each retailance system in red, and lowest in bold black

While all interviewees admitted to being aware of at least some type of retailance in retail stores, they dealt with that knowledge differently. Some consumers said they do not worry about being surveilled because why would they complain if they were doing nothing illegal? Solove (2011) calls this privacy-security debate the “nothing to hide argument,” when individuals contend that they have no reason to fear or oppose surveillance programs (especially governmental), unless they are afraid it will uncover their own illegal activities. An example quotation from an informant is:

Jason (M, early 50s, College, USD 124,000): I just ignore it [surveillance]. Like I said, usually the store I go into is Walmart all the time . . . Soon as you walk in the door, they have a camera and a monitor showing your face that's on camera, that they see you. I just ignore it because I know I'm not gonna do anything wrong. I'm going to go buy what I'm going to buy. [Then] I'm going to leave.

Some consumers simply ignored the presence of retailance:

Michael (M, late 40s, MBA, USD 105,000): Honestly . . . sometimes it [surveillance] worries me, sometimes it doesn't. But I know it happens. But I try not to think about it and it just happens in the background.

Jennifer (F, 50 yrs, BA, USD 99,000): I guess everyone's mind might see a camera or something. But it's not [on] top of my mind really ever when I enter [a store].

Others are aware of the presence of retailance, however, they do not take it seriously:

James (M, 70s, PhD, USD 14,000): [My reaction to surveillance in stores] kind of varies on my mood. If I'm in the mood to do it if I think I've been surveyed. Oh, I'll stick my tongue or something [laughs].

Others are constantly aware of the presence and scope of overt retailance, such as CCTV cameras, tags attached to products, and personnel watching shoppers.

Maria (F, early 40s, HS, USD 36,000): And when this whole COVID thing started, several locations [in the U.S.] had a police officer to help because what they were doing is they were only allowing one person in for every person that came out. So, there was a policeman there to tell people to get in line, to wait to come in, and to keep order, make sure that people are not trying to step in front of others or do anything like that. So, there's been more surveillance than usual now. But the cameras, I've been aware of for a while.

This constant awareness pushes some consumers to even change their behaviour when shopping:

Mary (F, 60s, BA, USD 50,000): In every, every store you walk into no matter how small, you are very much aware that there's surveillance and of course we all know there's surveillance in the casinos [in Reno, Nevada]. So, I think about it constantly. And I made a conscious effort not to pick things up unless I'm going to buy them.

Mary's conscious decision "not to pick things up" for fear of being surveilled is a negative outcome of retailance. In the Retail Dive Consumer Survey, the "ability to see, touch and feel products ranks highest among the reasons consumers choose to shop in stores versus online" (Skrovan, 2017). Retailers, therefore, should think about encouraging their consumers to touch the products and get more familiar with them (i.e., employing haptic marketing that uses tactile sensations to influence purchasing (Magnarelli, 2018)) and/or employ more covert retailance systems in order not to alienate their consumers.

Many interview informants also mentioned that although they do not see them, they expect that there are “mystery shoppers” (i.e., undercover store security in plain clothes going around the store). Sarah has been aware of retailance since she witnessed a family member caught by security after shoplifting:

Sarah (F, late 20s, MA, CAD 63,000): Yeah, I do [think about surveillance] . . . because there was an issue in my family with shoplifting. It's just sort of something like I'm hyper aware about . . . just like where there are cameras but, you know, how sometimes stores have those kind of like fake shoppers that are just going around and watching you . . . Not in like any store, but like a fancy high-end retail store . . . It was just a close family member who [was] . . . caught taking a perfume, but like they didn't stop them in the store. It was actually just as we were getting onto the streetcar. This was back in Toronto [in a Saks Fifth Avenue attached to The Bay] . . . And then, all of a sudden, I turn around, I'm like, “Where's this person?” . . . After I got off the streetcar, [I] notice that they were in handcuffs and being taken away and then I wasn't allowed to talk to them. And so, it was just a very confusing experience. And so now, that's just kind of in my head.

Rachel talked about how as a store worker in The GAP herself, she is more aware of retailance and more understanding of why store employees have to keep a closer eye on store customers.

Rachel (F, early 20s, MSc, earns minimum wage): I think it depends on the store . . . I'm now working retail and knowing that a lot of times management kind of pushes you to talk to people and kind of trail them a little bit . . . I find, especially since working retail, I tried to be like a lot more polite about things and really trying to, you know, engage and like not mess up the shelf and clothing store and like talk to the people working. So, I've noticed that change since I've been in their shoes, so to speak.

The same reaction is conveyed by Taiba who works in Farm Boy:

Taiba (F, early 20s, HS, CAD 24,000): I did think of being watched. Because as an employee, I watch customers to see what they do, what they throw onto the floor, or something like that. But I also put myself on their shoes sometimes when I go into stores. So, I try to respect the work circumstances or like the store circumstances as well.

During the interviews, and after talking about the retailance systems they are aware of, the interviewees were shown pictures (by sharing the interviewer's screen with them through the

Zoom platform) of the latest retail systems currently being introduced in some of the stores in both Europe and North America (all of which are mentioned in Chapter 2). Some consumers were positively interested in trying new technology:

Jennifer (F, 50 yrs, BA, USD 99,000): I think the initial shock of some of them, you're like, "Oh my gosh!" like I can't believe, you know, that that's the thing, or that that's whatever. But then on the other side, technology is a pretty cool thing. Like the one where you don't have to try on the clothes and you can just see it. Like, that's pretty convenient, you know . . . So, I think all of that takes . . . getting used to . . . But then once you're exposed to an interest[ing] kind [it] becomes the norm. I mean, some of it seems a little over the top but and I think some will catch on and some wouldn't catch on, you know.

Myint (F, early 30s, BA, CAD 125,000): The one where you could try on a dress seems amazing, and I have a medical condition where like, if I change positions very quickly, I faint. So, like taking things off, putting them on, like sitting down in the changing room, standing up again . . . That's a pain and I hate doing it and I feel terrible doing it. So, I think that's awesome. I would like to go to that store.

Therefore, for some consumers, like Jennifer and Myint, retailance systems can be used not just for surveillance, but also to improve customer experience.

Some consumers had no concern when it comes to up-to-date retailance systems:

Jason (M, early 50s, College, USD 124,000): Whatever they're gonna do, they're gonna do. Maybe you'll make life better, make products cheaper. I don't think so, because they got to pay for those cameras and the doors and stuff.

Michael (M, late 40s, MBA, USD 105,000): I've seen them to some degree. I don't have a problem with none of those . . . The only thing about it is that it is equal kind of surveillance, everyone. The only question is, on the other hand, is how the information is used . . . the introduction of human bias would be my only concern, but none of those systems I think I will have a concern with, just on their own.

Michael's words highlight two important points. First, his reference to "human bias" is a reminder of the profiling of consumers which, from a critical marketing perspective, is a discriminatory practice that marginalizes some of the consumers. Second, another concern of

Michael is not encountering one retailance system on its own, but an “assemblage” of surveillance systems and/or individuals.

On the other hand, other consumers were quite shocked and used words like “gross; horrible; uncomfortable; creepy” to describe those new retailance systems. However, some were resigned to the fact that at one point in the future, they will have to accept all those types of surveillance, for they will become the new normal.

Maria (F, early 40s, HS, USD 36,000): Lies, lies, lies . . . So gross! . . . Oh, the mannequins! Oh, that's something out of a nightmare . . . I mean, that's seriously . . . that makes me think of Chucky, you know, *Child's Play* [Figure 54] . . . It's horrible. That's horrible. And then the scan bag. That's ridiculous.

This resignation to accept retailance turns consumers into what Foucault described as “docile bodies” that are constantly surveilled and controlled (Foucault, 1978; Norris, 2003, p. 250).



Figure 54 – Chucky in *Child's Play* (1988) compared to the EyeSee mannequin which has a camera hidden behind its eye to track shoppers' behaviour as they browse

Christopher (M, 38 yrs, HS, USD 17,000): I do not like it. I think that, you know, it's kind of like that in drones or something that really scares me for the future because on one hand, I love technology, but on the other hand, I just feel like we're getting into a place in society where we can just be watched all the time, which is very much that Big Brother thing . . . It's like there's not only no consent but there's just not really any real privacy either. And you know it's scary to think about.

Sarah (F, late 20s, MA, CAD 63,000): [Body cams] That's sneaky . . . [Mannequins] That's creepy . . . [Pay with smile] Oh my gosh! . . . [Freezer doors with cameras] That's wild . . . [Augmented mirrors] I didn't realize that was real, like you see that in movies and stuff all the time [laughs] . . . Honestly, and a lot of those things you showed me are things I thought would all be in movies like spy movies. Like oh, put this like fake eyeball in the mannequin. Like, yeah, obviously that's going to happen in the movie, but not in real life! Dang, that's creepy. I'm not a fan. Or like in the purse? Unlock your offers? No, just email me.

Ishita (F, early 20s, BA, CAD 15,000): So, there's certain things that I think are very neat and definitely will help, but things like the Alibaba ID, like paying with your smile is a huge invasion of privacy . . . Anyone can try to copy that or . . . I think you're more at risk . . . I know it's very interesting. I think everyone has a different opinion out there and that's totally valid . . . I think we're also leaning towards a very highly technical dependent environment now, where we depend so much on these things and people want to make their life easier. So, I understand these things coming out in the future. But at the same time, I think some of them are a bit too much.

The different reactions to new retailance systems that are technologically mediated show that each consumer has a tipping point after which they cannot accept those retailance systems.

Retailers, therefore, need to weigh the benefits when they introduce new retailance systems, for one of their goals is to provide their consumers with a memorable customer experience and not to make them “uncomfortable” or “gross” them out.

To conclude, the above section looked at consumers' general awareness of the presence and scope of retailance systems. It is worth noting that all of the discussed retailance technologies are already in use (or at least in the trial phase) and not simply future predictions. As expected, not all respondents were aware of the latest retailance technologies and some of

them focused on well-known systems that are familiar to them (i.e., not imagined), such as CCTV cameras and RFID tags on merchandise. The analysed data showed that consumers are more aware of the widely used overt retailance systems (e.g., video surveillance, tagging and loyalty programs) and less aware of the relatively new, technologically advanced retailance systems (e.g., geo-fencing and biometric surveillance). Varying degrees of relevant statistical associations were discovered between awareness of retailance systems and age (older consumers are more aware of overt systems while younger consumers are more aware of covert systems), education level (consumers with a post-secondary education are more aware of retailance), and income level (consumers with an annual income equal to above USD 77,000 are more aware of retailance). Interview informants described different reactions to this awareness, for example, they accepted it since they do nothing illegal, ignored it, did not take it seriously, or changed their behaviour inside the store. When introduced to some of the technologically advanced retailance systems, their reactions ranged from being interested in the new technologies to being creeped out. In the coming sections, two of the above discussed retailance systems (tagging and loyalty programs) are discussed in more detail.

(2) Awareness of laws and regulations

In the MTurk survey, three five-point Likert-type questions/statements were included to ask about consumers' awareness of the laws and regulations that protect their privacy and their effectiveness. The first statement read, "I am aware of Canadian or American federal institutions that help deal with privacy and the protection of personal information from inappropriate collection, use and disclosure." Only 47.8% of informants either strongly or somewhat agreed that they were aware of institutions that deal with the protection of personal information (Figure

55); no statistically significant associations were discovered with gender ($X^2(12, N = 592) = 12.966, p = .372$), age ($X^2(24, N = 592) = 30.011, p = .184$), education level ($X^2(24, N = 592) = 34.127, p = .082$), income level ($X^2(24, N = 581) = 31.948, p = .128$), or membership in a minority group ($X^2(8, N = 101) = 7.357, p = .499$).

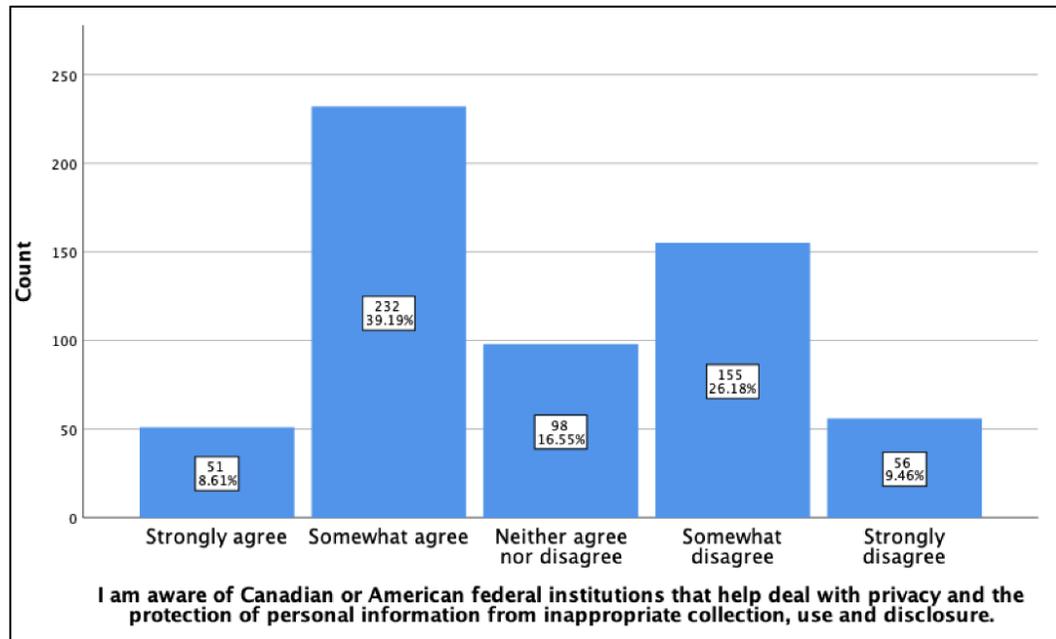


Figure 55– informants’ awareness of federal institutions that deal with the protection of personal information

The second statement was, “I am knowledgeable about the laws in Canada or the USA that deal with the protection of personal information,” and only 42.16% of informants either strongly or somewhat agreed that they were aware of laws that help deal with privacy and the protection of personal information from inappropriate collection, use and disclosure (Figure 56). The only statistically significant association discovered was between this awareness and the income level of informants residing in the U.S. ($X^2(24, N = 582) = 44.365, p = .007$). A closer look at this association (Figure 57) shows a positive association between such awareness and the average annual household income (for example, 25.7% for informants with an average income of

USD 15,000 compared to 49.5% for informants with an average income between UDS 45,000 and USD 76,000). The reason for this association was not immediately apparent and would make a good topic for future research. No statistically significant associations were discovered related to gender ($X^2(12, N = 593) = 14.024, p = .299$), age ($X^2(24, N = 593) = 13.488, p = .957$), education level ($X^2(24, N = 593) = 24.782, p = .418$), or membership in a minority group ($X^2(8, N = 101) = 7.253, p = .510$).

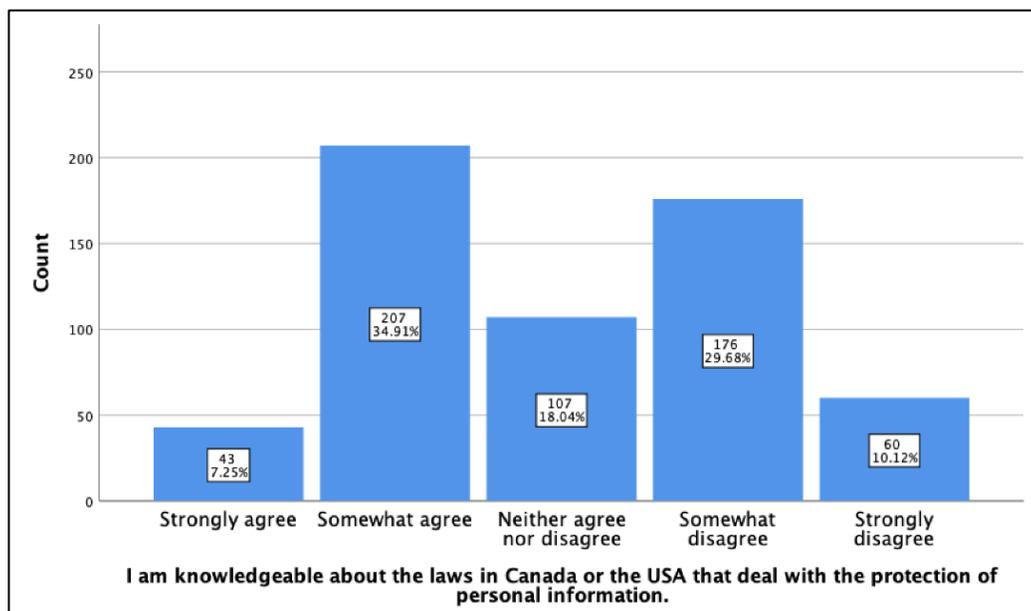


Figure 56 – Informants’ awareness of federal institutions that help deal with privacy and the protection of personal information

		What is your average household income in the USA?						Total	
		USD 14,999 or less	USD 15,000 to 29,000	USD 30,000 to 44,000	USD 45,000 to 76,000	USD 77,000 and over	Do not know		Prefer not to say
I am knowledgeable about the laws in Canada or the USA that deal with the protection of personal information.	Strongly agree	2	4	6	17	13	0	0	42
	Somewhat agree	7	27	36	82	49	0	2	203
	Neither agree nor disagree	7	10	22	41	22	1	2	105
	Somewhat disagree	9	34	33	43	46	2	6	173
	Strongly disagree	10	11	7	17	11	2	1	59
Total		35	86	104	200	141	5	11	582

Figure 57 – The association between informants (residing in the U.S.)’ knowledge of the laws that protect their personal information and their average annual income

The third statement read, “I believe that laws are effective at protecting my personal information that is held by retail stores.” Only 44.51% of informants either strongly or somewhat agreed that such laws are effective at protecting their information held by retail stores (Figure 58); no statistically significant associations were discovered with gender ($X^2(12, N = 593) = 17.835, p = .121$), age ($X^2(24, N = 593) = 34.018, p = .084$), education level ($X^2(24, N = 593) = 18.369, p = .785$), income level ($X^2(24, N = 582) = 21.424, p = .614$), or membership in a minority group ($X^2(8, N = 101) = 6.142, p = .631$).

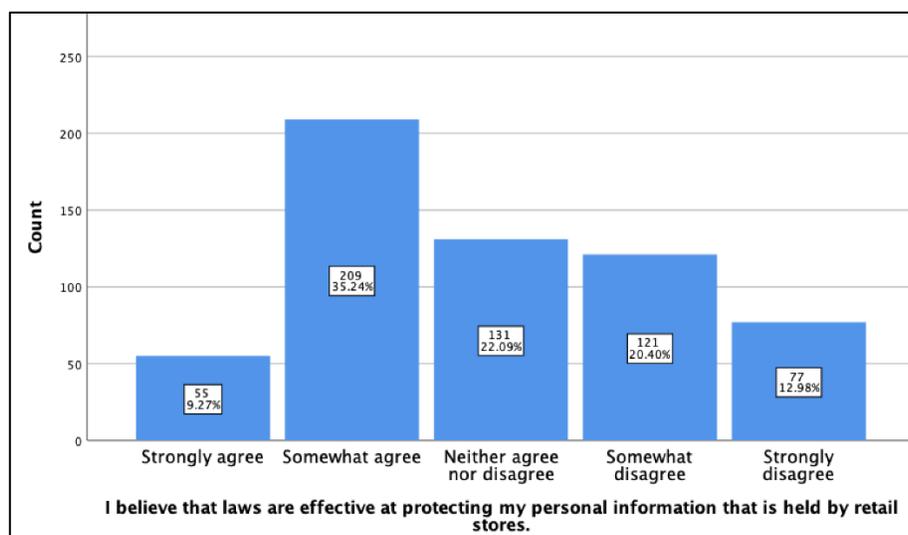


Figure 58 – Informants’ belief in the effectiveness of laws protecting their private information held by retail stores

Taking these three questions together, it seems that the majority of informants were not aware of legislative protections. Furthermore, most had doubts about or even no faith in the type of protection those laws and regulations can offer. This may lead to a “vicious circle” where lack of belief in the effectiveness of legislation leads to consumers not bothering to learn about legislative protections. Quotations from interview data demonstrate a feeling of hopelessness and a “defeatist attitude” on the part of informants, who describe the situation as a “hopeless cause” because “the genie is out of the bottle” and there is no going back.

Michael: I think that to some degree, we need better laws in terms of protections of privacy and regulations, but with the power of the tech companies and [their] ability to take information, it is gonna be very difficult. The genie is kind of out of the bottle on that.

Maria: [In the U.S.] it's pretty much on a company-by-company basis. And so, you have to look at each one individually, but there's not really any strong legal protections. At least that I'm aware of. It's pretty much letting corporations do what they want.

David: I'm aware of HIPAA [Health Insurance Portability and Accountability Act in the U.S.] laws, medically speaking. I know there are online privacy laws and with websites they have to have the private privacy policy publicly stated, but I'm not really sure where the laws go after that. I feel like it's a hopeless cause really with the internet. I guess I feel like those laws, you know, some companies may follow them. Some might not. I just almost feel like it's pointless because once there's certain information like that you give to companies out there, there's really no telling what they do with it. I'm sure there are laws. I'm not familiar with them and I imagine I should be. But you know, I just have a defeatist attitude in that regard.

Ashley: I would hope they would be enough. But unless there was someone monitoring or someone that knew what the law was, there might be loopholes.

Sarah: The legislative process is so slow. Yeah, we're always like a step behind.

Rachel: I mean, I would like to hope so. Personally, I suppose one part of me does like to believe in that, and hope that these policies and laws are put in place to help protect us as citizens supporting the economy and moving forward. But I guess another little part of me, like the devil on my shoulder, likes to believe that maybe it doesn't do everything it says it does.

Joshua: I think, yeah, they probably do something on the large scale. But on a more personal one-on-one scale, not really. I think that if I give my information to a company, the government should have to approve the sale or the distribution of my information. I feel like the government should have control over where it's going, because this is like selling my information. That's how I get dumb scammer calls, dumb emails, all that stuff. And I think if the government could step in and maybe just . . . I don't know . . . approve where everything's going? I think it would solve stuff.

Looking at the above discoveries—having more than half the consumers (no matter their age, gender or educational background) not aware of the laws and institutions that protect their privacy and personal information collected in retail stores, and not believing in the effectiveness

of such regulations—is a red flag for public policy makers that warrants further research (Jenkin, 2018). In a telephone survey of Canadians on privacy-related issues (Office of the Privacy Commissioner of Canada, 2019), roughly two-thirds (64%) of Canadians rated their knowledge of their privacy rights as good or very good. This increase in the percentage of consumers' general awareness of their privacy rights indicates that compared to other businesses and government departments, consumers may be less aware of their privacy rights related to the retail sector. This, therefore, becomes another reason why public policy makers should focus on informing consumers about their retail privacy rights.

(3) Awareness and reviewing of privacy policies

One of the survey questions was “Have you ever reviewed a store/retailer’s privacy policy?” Given the choice of a yes or no answer, 45.19% of informants maintained that they have never reviewed a retailer’s privacy policy (Figure 59). This percentage is even higher than the one published by the Pew Research Center (Auxier et al., 2019a) which stated that 36% of American adults never read a company’s privacy policy before agreeing to it. Performing the chi-square test for independence, a statistically significant association was found between reviewing the privacy policy and minority identity ($X^2(2, N = 101) = 9.257, p = .010$) which required further investigation. Out of the 593 informants, 101 (17%) identified themselves as belonging to a visible minority, being indigenous or having a disability³². Admitting that they have never reviewed a privacy policy were 51.8% of informants who identified as belonging to a visible minority (29 out of 56), 34.4% of indigenous informants (1 out of 13), and 65.6% of

³² Respondents were asked to identify if they have a disability in general; no data was collected to differentiate between visible and hidden disabilities.

informants with a disability (11 out of 32). On the other hand, 84.7% of non-minority (i.e., white) informants (227 out of 268) admitted to never reviewing a privacy policy, which is the highest percentage. Surprisingly, the relationship between education and the review of privacy policy was not statistically significant ($X^2(6, N = 593) = 1.841, p = .934$). There were also no statistically significant associations with gender ($X^2(3, N = 593) = 1.532, p = .675$), age ($X^2(6, N = 593) = 2.903, p = .821$), or income level ($X^2(6, N = 582) = 6.565, p = .363$).

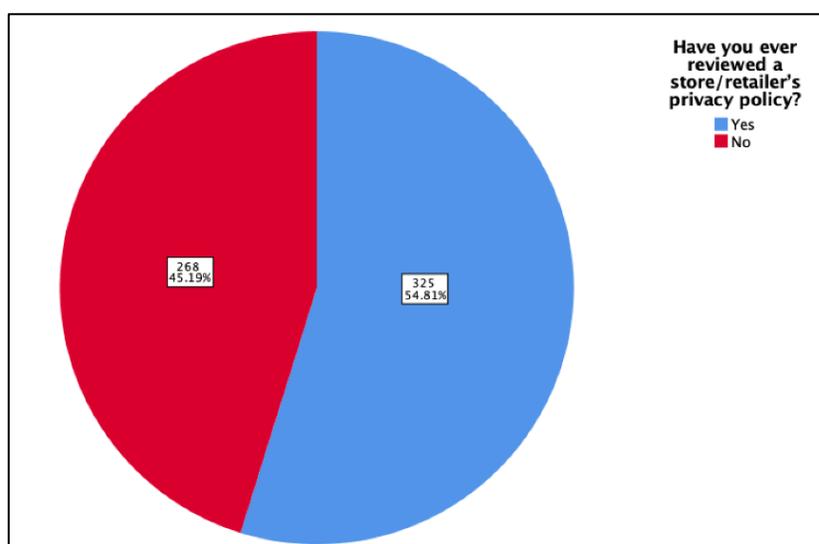


Figure 59 – Informants’ reviewing of store privacy policy

Since the survey results indicated that consumers’ disregard of reading privacy policies is prevalent, informants were asked during the interviews about how often they disregard reading those privacy policies and how they feel about that. They described their behaviour as “embarrassing” and “shameful.” Some interviewees admitted that they have read a privacy policy only once but they gave up soon afterwards.

Mary (white American): Okay, so this is embarrassing. But I will tell you that may be once way back when they first started doing all this stuff, I read one. And I was just kind of blasé about it.

Paulo (Brazilian in Canada): Privacy policy! I read [one] once in my life. And that's it. I never read anymore.

Some informants confessed that skimming privacy policy texts is the best they can do before signing off on them.

Ashley (white American): I have skimmed it [privacy policies], but some of them are so long and the wording is so tiny. Sometimes I just put "I agree," and I know I should probably read a lot more. I think they do that on purpose. They make it so long. That way you won't, you know . . . you just sign it.

Jennifer (white American): I mean I skim it [privacy policy] very lightly. I've never sat in like reading, word for word. And then like decided not to do it because of what it said. Yeah, I mean I just skim it a little and then click the box.

Christopher (white American): I try. I'm not perfect about it. I admit that I'm more likely to go in and adjust my settings and read the information if I've heard that a particular site or company is involved with like a data leak or if they've been accused of sharing data or manipulating data in a way that users are not happy about. So, I do try, but there's just so many sites and so much, you know, interaction with them that it's very difficult to keep up with all that.

Myint (Burman Canadian): I don't read every word, I'll admit. I'm sure you hear that answer a lot. But I definitely skim them . . . just to make sure everything is good. From the ones I've skimmed and all the ones I've seen with my husband [a data analyst] working in them, there's nothing that bothers me. I mean, I have a very positive spin on the world a lot of the time. And research and data collection can be used for some very good things.

Ishita (Indian Canadian): So initially, when I [moved out and] started doing things for myself, I would read them. But that was probably only for a few months or a year. After that I just scroll through it very briefly, I don't actually read the whole thing. And now, like being 23 years old, I find that I've had to do this multiple times to the point I don't read them. I just hit "I agree."

And some informants sign off on privacy policies without even reading them:

Michael (Black American): I just have never taken the time to look at it. I just pretty sign off on it and move on to be honest. I just feel like . . . [it's] something I can't control anyway, so I just kind of just signed off on it.

David (white American): I can't say that I've ever thoroughly read one front to back. Boy, it'd be [a] tough read, I think.

Jason (white American): I don't [read privacy policies] because I never worry about anything going wrong with my identity or anything getting stolen from me.

Matthew (white American): You can do whatever you want . . . I don't think my data is particularly valuable, you know.

Taiba (Afghani Canadian): I'm sorry, but I never read them. If possible, I would just read the first line saying, "I accept the conditions." [laughs]. I accept all the conditions. That's it. That's probably how far I've read all these policies too. And I quickly go into "I accept" or "I agree." And that's it.

Then how can consumers be encouraged to review privacy policies before signing off?

According to Sarah, they need to be written in plain language with no jargon.

Sarah (white Canadian): I mean, though they list the terms and conditions when you sign up for these programs, I'm pretty sure they are also well aware that people don't actually read them very thoroughly very often, like a small percentage will most likely. So, it's sort of blind consent that they're getting. Whereas if they . . . if they were really trying to be ethical about it, they might try to simplify it. I mean with technology these days, I'm sure there's some way to like actually get people to read it in plain, like three bullet points about their privacies and what they're going to do with your information. So no, I don't think it's ethical. Because there's no true consent. It was just sort of haphazard in the moment. Also, because usually when you're signing up for these things, it's like just to get to the next step so you can finish your purchase or whatever.

Joshua, on the other hand, argues that the sheer length of most privacy policies is to blame for not having consumers read them.

Joshua (white Canadian): I've gone through some of them [privacy policies] before. Obviously not everyone [in] my life because I see a ton of them a day, but yeah. I know that there's a reason they're long as they are and they are basically getting permission to do whatever they want with your information and sell it to whoever they want. That long text is just them saying "We got every right to buy and sell your name, email address and phone number."

A similar recommendation has been voiced by Bashir, Hoff and Jeon (2014) when studying online consumer privacy: "If policies better accommodated the preexisting knowledge levels of diverse individuals (e.g., across age, gender, and education), readership rates might increase."

According to the Office of the Privacy Commissioner of Canada (OPC), meaningful consent is

“an essential element of Canadian private sector privacy legislation . . . However, advances in technology and the use of lengthy, legalistic privacy policies have too often served to make the control—and personal autonomy—that should be enabled by consent nothing more than illusory.” (Office of the Privacy Commissioner of Canada, 2018).

Out of the thirty-eight interviewees, only one, Robert (a fourth-year law student), described how he reads every single privacy policy before accepting it, and that is because of his past and current experiences.

Robert (white Canadian): I actually do sit down and read them because of having the law background and [I] took a consumer law course at Carleton. And one of the professors told us that every time we sign up for something, we're supposed to read the contract or the agreement or the stipulation, so that if anything comes up, we know how to get out of it, instead of having it fall back on us, like, “Oh! You should have done this.”

In addition, he has prior experience of what is involved in signing a contract:

Robert (white Canadian): The reason why I'm also aware of what a contract says and doesn't say is when I worked for some cell phones. You have to know your contracts in and out and make sure that you're not fluffing any part of that contract. Because I had a close friend of mine that worked at Bell and she sort of fluff information to a family that she was selling cell phones to, and the family didn't like what she was saying because it wasn't in the contract and she lost her job because of it. So, it's one of those things where anytime I'm talking about a product or, you know, signing up for something, I make sure I read everything before I sign.

To sum up, it is apparent from the above findings that consumers' awareness of laws and regulations and their attempts to protect their privacy (by reviewing privacy policies before accepting them) are not adequate when it comes to protecting themselves and their personal information in a world that is alarmingly becoming more dependent on surveillance technologies, especially since being hit by the COVID-19 pandemic (Klein & Felten, 2020; Pantano, Pizzi, Scarpi, & Dennis, 2020).

(4) Tracking consumers' purchases

In retailance, there is a form of control that has shifted from the physical (Foucauldian “disciplinary societies”) to the digital (Deleuze’s “societies of control”); this digital control is best exemplified in the tracking of consumer purchases and the decoding of that information (Bogard, 2006; Deleuze, 1992). When asked whether they are bothered by the fact that their purchase history could be tracked, their consumption behaviour traits could be analyzed and predicted, and their personal information sold to third parties, interviewees’ answers ranged from (1) indifference, to (2) welcoming, to (3) mixed feelings, to (4) resignation (Figure 60).

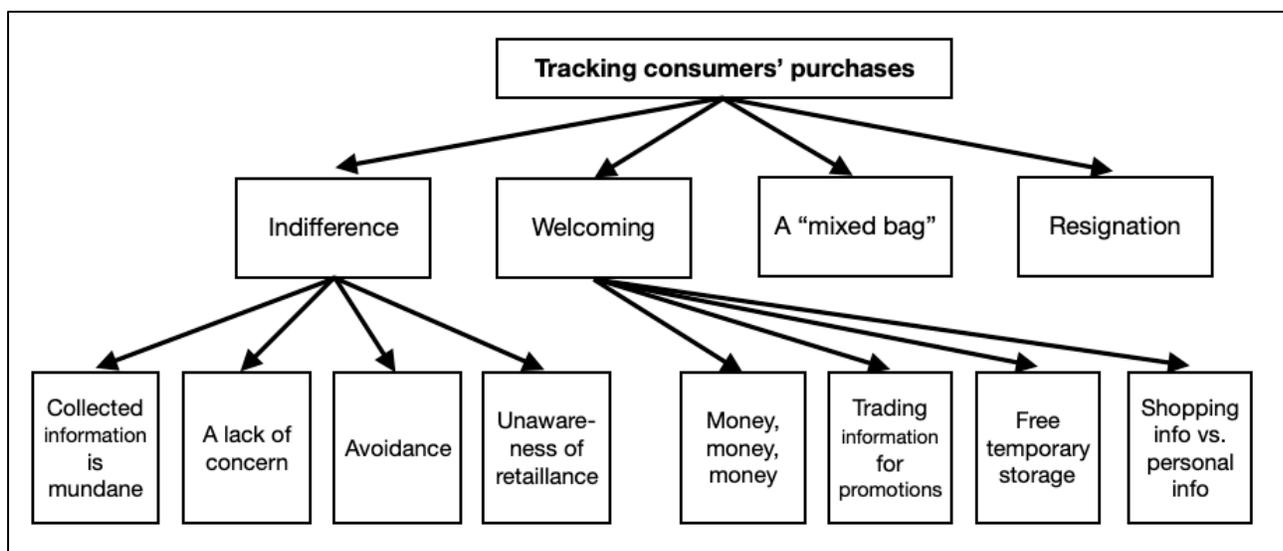


Figure 60 – Consumers’ reaction towards the tracking of their purchases

4.1 Indifference

Some interviewees simply did not mind their information being tracked for different reasons: (1) because they believed their information is mundane and not important enough; (2) they implied a lack of concern with any consequences; (3) they avoided both signing up for

loyalty programs and opening marketing emails; or (4) they were unaware that physical shopping could be tracked like online shopping.

4.1.1 Collected information is mundane

Mitig: Maybe I should be bothered, but I don't really seem to care that someone knows that I bought onions and peppers and milk this week and that sort of thing. But maybe that bothers some people, but I don't find it really more different than if a cashier kind of knowing what they're scanning for you.

4.1.2 A lack of concern

Olivia: I know it happens, like I will definitely get emails from like Sephora or even Shoppers being like, “Hey, like we noticed you bought this recently. Do you want to buy this?” But it's not like I don't really see it as an issue. I have an interest in the user experience design and like web and mobile. So, I'm very aware of the fact that everything I do online, or I do in store, is being tracked and collected. So, I don't really have an issue with it. I just tend to ignore it.

Hannah: You kind of have to be okay with it, if you're giving your info to like a loyalty program. Like you kind of have to know that your information is not totally private, it can be accessed like by somebody else. It is on the back of my mind, but is that a concern of mine? Not really.

4.1.3 Avoidance

In his 60s, James expressed how he neither uses his loyalty card enough to accumulate points nor does he open any advertisements sent to him; “If it happens, I never see it.” Thus, his indifference to the tracking of his shopping behaviour stems from his avoidance of both using the card and opening any marketing emails.

4.1.4 Unawareness of retailance

Jason—an American in his early fifties with a college degree—is indifferent to the tracking of consumer shopping history, saying that “It’s okay;” he believes most of the tracking is carried out when shopping online only.

4.2 Welcoming

While some consumers are indifferent to the fact that their retail information is collected in retail stores, others openly welcome such a practice because of the benefits they receive. To induce consumers to welcome retailance (in the form of having their purchases tracked), retailers employ what Boyne (2000) describes as “consumer seduction,” a post-panoptic paradigm in which the needs of consumers are targeted with the help of information and retailance technology, data gathering, and analytics. Retail consumers, therefore, are offered incentives and services tailored to them based on the results of the algorithms that continuously analyse their data and turn them (i.e., the consumers) into “data doubles,” an abstract, hybrid composition that is assembled by collected personal and shopping data (K. D. Haggerty & Ericson, 2000). There are four reasons behind consumers’ welcoming of this system of retailance: (1) to receive promotions; (2) to earn money rewards; (3) when they are asked to provide shopping information (deemed harmless when compared to personal information that might threaten their privacy); and (4) to get free temporary storage.

4.2.1 Trading information for promotions

Some consumers willingly trade their personal and shopping data and privacy for something in return (e.g., better services or special deals), hence, a commodification of the self. The 2019 Deloitte survey of consumer privacy in retail revealed that in the U.S., “nearly three in four consumers are willing to share personal data if they receive things like better pricing, special discounts, or exclusive offers” (Sides, Matt, Goldberg, & Mangold, 2019). In the MTurk survey, when asked if they feel it is acceptable for a business to use the information in their profile to inform them of products or services they think would be of interest to them, 40.14% somewhat or strongly agreed it is acceptable (Figure 61). Statistically significant associations were discovered between this question and both age ($X^2(24, N = 593) = 45.548, p = .005$) and

membership in a minority group ($X^2(8, N = 101) = 16.782, p = .032$). Looking at the association with age, it was revealed that the highest percentage of consumers who feel it is acceptable for their information to be used as a trade-off comes from those 55 years or older (55.56%), while young consumers aged 18-24 have the highest percentage (51.85%) of deeming this an unacceptable practice (Table 12). The second association, with membership in a minority group, showed that indigenous consumers are the minority group that had the highest acceptance percentage of trading-off their personal information (69.2% or 9 out of 13) compared to consumers identifying themselves as visible minorities (35.7% or 20 out of 56) and consumers with disabilities (25% or 8 out of 32) (Figure 62), although because of the low number of informants from minority groups, this interpretation should be treated with caution. No statistically significant associations were discovered with gender ($X^2(12, N = 593) = 015.966, p = .193$), education level ($X^2(24, N = 593) = 15.608, p = .902$), or income level ($X^2(24, N = 582) = 22.781, p = .533$).

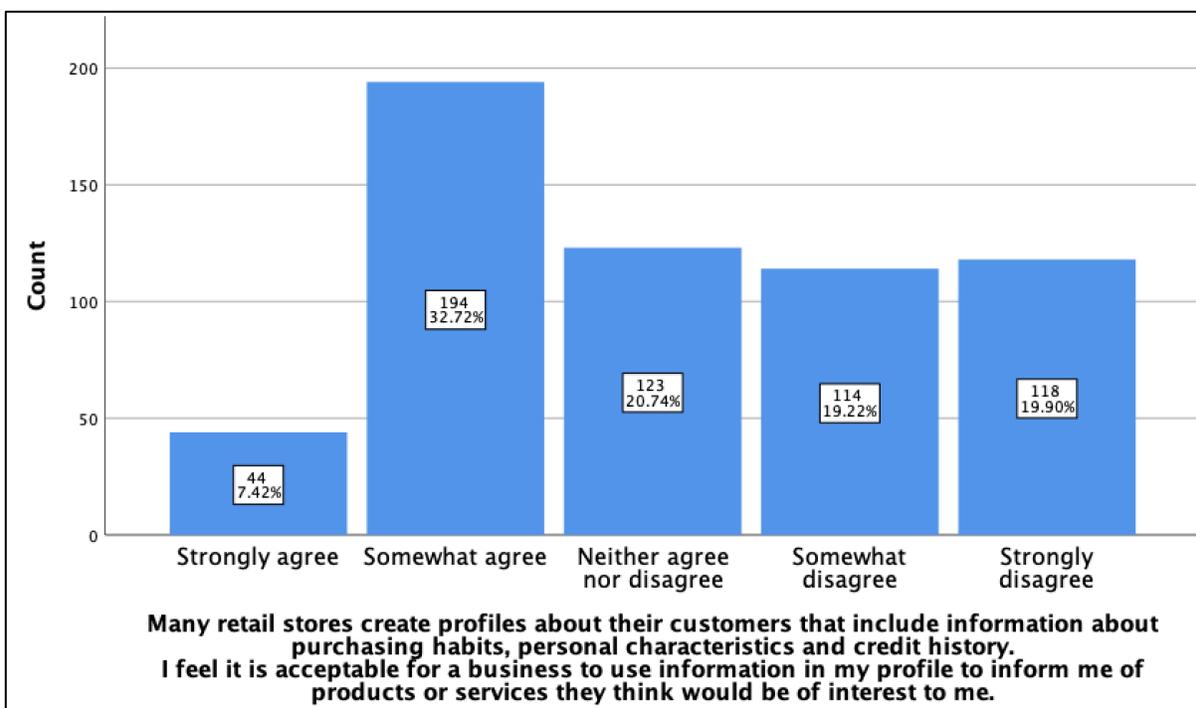


Figure 61 – Informants' acceptance of retailers' collecting consumers' information to inform them of products and/or services that might be of interest.

Age	Informants' feeling comfortable with sharing personal information for reward programs	
	Strongly or somewhat agree	Strongly or somewhat disagree
18 to 24 (n = 27)	25.93%	51.85%
25 to 34 (n = 181)	40.88%	38.67%
35 to 44 (n = 179)	36.11%	36.67%
45 to 54 (n = 104)	44.23%	37.5%
55 to 64 (n = 62)	38.71%	48.39%
65 or older (n = 36)	55.56%	33.33%

Table 12 – The correlation between age and accepting the use of personal information as trade-off, with the highest percentage under each category in red

		Do you consider yourself to belong to any of the following groups? – Selected Choice			Total
		A member of a visible minority, which is:	An indigenous/a boriginal person	A person with disability	
Many retail stores create profiles about their customers that include information about purchasing habits, personal characteristics and credit history. I feel it is acceptable for a business to use information in my profile to inform me of products or services they think would be of interest to me.	Strongly agree	4	4	0	8
	Somewhat agree	16	5	8	29
	Neither agree nor disagree	10	1	7	18
	Somewhat disagree	14	0	7	21
	Strongly disagree	12	3	10	25
Total		56	13	32	101

Figure 62 – The association between accepting the use of personal information as trade-off and belonging to a minority group

To some interviewees, providing their retailers with shopping and basic contact information is acceptable as long as they get something in return, whether it is a better service, personalized promotions, reward points, or coupons for future purchases.

Michael (late 40s, Black American): I don't have problems with it because I feel like there's a lot of potential for me to get promotions that [are] relevant. So, I don't have a problem with that in terms of being surveilled, in terms of the products that [I] buy. I think it helps me out.

Joshua (20 yrs, White Canadian): I look at it the same as the way that Google has ads that are geared toward me. If a store wants to use the information that they have on me, I don't think that I give them anything that they can use maliciously. So, I think if they really want to go throughout their day and go through my data and try to figure out what I want, I think that would be nothing but beneficial to me. I know some people may find that weird to have their life under a microscope from someone else but [at] the end of the day, it's just someone else doing their job.

Paulo (31 yrs, Brazilian in Canada): I don't believe [any] one with my name and my birth data [can] buy a house or buy a car. So, having my information and having my shopping behavior I think is beneficial to me. So, I will not get promotions about baby diapers. I'll get promotions about the things that I would like to purchase and maybe get, or products that [I] would never think about, but according to my shopping habits, they will see, "Okay though, this may be something that you'd like." And I like this. And I think it's good. So, I don't mind [them] following me. I think [it] is their job. I think they give a lot of things to us

for free. Everything has a cost. And the trade-off is giving information. And I've been watching all the documentaries about it. I know about Cambridge Analytica, you know. I know everything. But I get a lot of stuff for free. I think my payment is my information, and if they sell, I think they are very smart and they develop a great business model. And I think they deserve to have information. This is my mindset.

Robert (40 yrs, White American Canadian): Since I am a student, I like getting the discounts and getting the promotional email saying, "Okay, see in two-weeks' time, there's a promotion for Bath and Body Works, their hand sanitizers." I like getting those so that I know. Okay, I get paid in two weeks. I can go to Bath and Body and get some more hand sanitizer or a deal on lotions. For some of the other emails that I get are like for Victoria's Secret for my wife. [It] is like, "Oh, her birthday is coming up soon. I can go and go see what they have. And get their promotions and see." My wife said, "Oh yeah," she needs this. Okay, I can, you know, go into the store and get that item for her.

Li Na (30 yrs, Chinese Canadian): I'm fine with it only because I'm aware of it. If it benefits me with points or discounts, I'm more okay with it. At least I get a benefit this way.

To summarize, 40.14% of surveyed consumers agreed that trading off their personal information to get informed about products and services and receive rewards is acceptable, and this is more possible when those consumers are over the age of fifty-five and/or are indigenous. This statistical result is close to that of the 2006 GDP survey (Pridmore, 2010) in which 45% of respondents (in both Canada and the U.S.) saw that it is acceptable for a business to use information from their customer profile to inform them of products or services that they think would be of interest to them. We can, therefore, conclude that in the past fourteen years, and despite the rise in debates about consumer rights and privacy, there has not been much of a change in how consumers react towards trading off their information. In the survey of Canadians on privacy-related issues (Office of the Privacy Commissioner of Canada, 2019), around 30% of Canadians (especially those under 55 years of age, women, or have a post-secondary education) stated that they have willingly traded their personal information for discounts or incentives on a good or service. Comparing those three surveys, we can conclude that the number of consumers

who willingly trade their personal information (around 30%) is less than the number of consumers (between 40% and 45%) who accept that their personal information is being traded, which indicates a level of hesitancy when it comes to the acceptance of trading information for incentives.

4.2.2 Money, money, money

Although there was no statistically significant association between consumers' income level and their acceptance or non-acceptance of trading their personal information for information about products and services offered by the retailer (please see the above section), the interviews revealed that the impact of consumers' income level plays a more important role when consumers' information is traded for money. Thus, to some consumers, the promise of future promotions is not a sufficient reason to trade off their information, for they prefer on-the-spot discounts and/or money rewards. Working at The GAP, Rachel compares consumers' reactions when asked to give their email address while checking out:

Rachel (early 20s, white Canadian): A lot of people say "no." What I have found though is when the company [The Gap] offers [a] promotion, along with your email, almost everyone will say "yes." So, like, if I say, "You know, if you give me your email for promotions, I'll give you an extra 10% off today," nine out of ten people would say yes to that. Well, if I just asked at the end, like, "Can I get your email address for their promotions and coupons?" Most people say "no." [Give] some form of incentive, you get the email. [Personally,] if I'm not offered some kind of incentive for it, I'll usually say, "No." My email inbox is already flooded with flyers and promotions. I don't need another one, right?

The same reasoning is expressed by Matthew:

Matthew (30 yrs, white American): If they're ever asking me, "Do I want to sign up for some rewards card" or whatever and it is going to give me an immediate benefit, I want to take it every single time. No matter if I'm in a rush, or I'm sick, or I'm late. Or she [cashier] asked me 27 questions before I get my 5% off, I am always going to go through whatever whoops. It is to save whatever money I can.

As a promoter of products in different Walmart branches in the U.S., Matthew would sometimes organize a draw or competition for the customers; after collecting the name and email address, or phone number, from customers on a piece of paper, one customer is picked to receive a prize which could be cash money, gift card to the retailer, or a product sample. When asked about how willingly people would provide their information, he said if 60% of shoppers he asks agree to participate, this percentage would go up to 85-90% when the prize is money: “If it has to do with money, people will do it. Yes, cash is king. That's what we say.” However, this theory (“cash is king”) is dependent on the consumer’s income and the frequency of their visits to the store.

Thus, it is a different story when consumers are well-off:

Matthew (30 yrs, white American): And it seems like people that make more money don't care about, say, getting \$100. They may make 100 and \$200 in a day as a psychiatrist or whatever. And so, for them to take the time and write their email and put it in the box, they don't care. They just came to get eggs or whatever. You know what I mean? So, you kind of have to read the clients that are coming up to you.

In addition, approaching regular customers always helps in the collection of data:

Matthew (30 yrs, white American): If I approached the right customer, then it's always a yes. Especially, for example, regular customers. I'm there every day and they keep seeing me and seeing me, then I will always approach them.

The same theory (that well-off consumers are not interested in promotions) is described by Robert who talks about his interactions with Roots customers and their reaction when asked for their email addresses in order to receive Roots promotions. According to him, nearly 50% of the people he asks would agree to give their email addresses, while the other 50% are too well-off to bother with the hassle of receiving promotions:

Robert (40 yrs, white American Canadian): We [at Roots] also collect emails to send out promotions. On a normal basis, I would say it's 50:50, where I asked say 10 people and I would say five of them say, “Yes. Sign me up. Let me get the discounts. Let me get the notifications. Let me get the upcoming Christmas line or upcoming deals and stuff for Roots.” And the rest are like, “Oh no, I'm too busy

or this is, you know, not worth my time and everything.” [The] majority of the clientele that come to our store have, I would say, a large income. Where they're like well off and they don't have to worry about, you know, saving the pennies and getting all those discounts and getting the promotional emails from Roots.

Consumers, therefore, sometimes show the willingness to trade off their privacy rights for the promise of monetary compensation. This result is double-edged. On the one hand, it shows that low-income consumers are more vulnerable when it comes to agreeing to trade their privacy for on-the-spot monetary rewards in a retail setting. On the other hand, retailers can use this type of monetary reward to encourage this segment of consumers to provide the former with their personal data.

4.2.3 Shopping info vs. personal info

Other interviewees expressed that as long as their purchase history is accessed by the retail stores they frequent, they are fine with such tracking. In comparison, they are more fearful of the sharing of their health or credit card information.

Mary (60s, white American): Well! I mean we view it [tracing shopping info], that part of it, as kind of harmless, you know, who cares if they know that you like celery, for example. What they don't like is that it's attached to my financial information too. Because what they're doing is they keep points and they give you awards when you spend a certain amount of money. So, you know that your credit card or your debit card is tied to that information. And then when you're dealing with like a pharmacy, there's maybe medications that you take that you're not particularly interested in having other people know about. That's your medical information. It should be covered by HIPAA [the U.S. Health Insurance Portability and Accountability Act], but you know they have that information. You know they track it because they give you . . . rewards for using the pharmacy. So that's a concern to me and I actually don't belong to any pharmacy program.

Matthew (30 yrs, white American): Oh yeah, that's fine. I mean, I keep record of everything I buy anyway, and if they, for example, want to track that I buy a smoothie every Friday, and that I'm just a white male that likes smoothies or whatever, and that they put me in that demographic, and then somehow advertisement for a blender shows up on my phone, no, I'm not concerned about that in any way. This targeted advertisement definitely exists already.

Working at Lowe's, a retail store specializing in home improvement products and services, many consumers—especially contractors who have their own business and consumers—have no problem with giving out their information when shopping as long as it is not connected to their bank account via credit cards:

Wang Fang (30 yrs, Chinese and Permanent Resident in Canada): We have only one kind [of membership card] in our store and this for contractors. Contractors, they shop a lot in the construction store like our store. So, we give them this card and every time they make a purchase, they get 5% to 15% discount. I found them willing to give out information to use this kind of card, but they [are] less likely to give out information if this card is like a credit card [Lowe's Consumer Credit Card is available to all their consumers whether they are contractors or not], then they [are] less likely to give out information. I understand mainly because sometimes they don't want their purchase to get tracked, just in case. Some people, they prefer using cash. They don't like to have their product tracked, just in case one day they need to file tax. People like to take cash from people and use the cash to purchase. So, income or expense never get tracked by CRA [Canada Revenue Agency]. The credit card can easily be traced by the bank or CRA, but the discount card it's less likely to get traced.

The above quote, therefore, illustrates that both consumers and business customers (e.g., contractors) are more hesitant to provide their personal information (compared to their shopping information).

4.2.4 Free temporary storage

Sometimes, consumers would be more interested in temporary free storage when buying bulk items. According to Wang Fang, who works in Lowe's, consumers willingly give their contact information if it will help them with storing their purchases in the store temporarily:

Wang Fang (30 yrs, Chinese in Canada): Some people, they make a purchase, they make the payment, but they don't take the purchase. So, we will ask them for their phone number, first name, and last name. Because it's a bulky product, they don't have a big enough vehicle. They can't pick up today. So, they have to come back next week when their brother or uncle have the truck. They will come to pick up. And we will keep their first name, last name and phone number, so we can keep track. If they don't come to pick up, we can follow them.

4.3 A “mixed bag”

Maria expressed how she likes to receive recommendations based on her shopping preferences, but only if it is targeted towards her and not just an avalanche of sales advertisements.

Maria (early 40s, Argentinian-American): If it's the case like Sephora, where they have so many different products, I don't mind because at least I'm not going to sit here and search through a website 500 times just to find whatever I'm looking for. So, like I had skin cancer, so I'm always looking for any foundation or anything that has SPF 50 or more. So, if they track that and they send me recommendations for foundations with SPF 50 or more, great, I'm happy with it, that's one less thing I have to search for. I mean that's harmless, and if I don't find anything, I can just delete it . . . And just trash that email. Okay, well, nothing good there. But it doesn't hurt anything. I mean, is it annoying? Yes, but they're not so bad. They maybe two or three times a week send something. It's not as bad as other things. Like I used to, years and years ago, have one through Victoria's Secret and that was multiple times a day. And that was very irritating because it wasn't personalized at all. It was just sale sale sale sale and I just had to cut it off . . . And the niche shops, I don't mind because, I mean, if they're sending you something about sales, and it turns out something I can't afford, great. I mean, I love making different things so . . . If it's something I like, then I like it. If I don't, I don't. But I don't want my email going to 50 different companies . . . So, it's a mixed bag.

Similarly, Jennifer said:

Jennifer (50 yrs, white American): Sometimes I have mixed feelings. I mean, I don't feel strongly one way or the other . . . I think it's a little weird, like if I know I've looked at something and then all of a sudden, I'm getting information about it. But then on the other side, like now, when I'm ordering more things online, like I'll put my things in the cart and he'll be like, “Oh, well. Last time you ordered this, this and this. Do you want to add that?” So, then there are times I'm like, “Oh! yeah.” Like I do need that or whatever, I should add that. So, I feel like it's helpful also. But yeah, sometimes I'm kind of like, “Well, that's weird that they know that” but never to where I'd be like, “Oh, I have to figure out how they found that out,” or “I need to stop that.”

To consumers like Maria and Jennifer, therefore, having their shopping and personal data tracked might feel “weird,” but as long as this retailance is carried out by retailers they frequent and trust and if it caters to their future shopping needs, they accept it.

4.4 Resignation

Only a few consumers expressed their fear of the amount of tracked information related to their retail experiences. However, to them, the situation was like a “runaway train” that could no longer be contained. Zahra (an Iranian Canadian in her early forties), for example, does not mind because she sees that it is “something that it’s in our life” anyway.

David (mid-40s, white American): The negatives outweigh the benefits for me. I guess it [is] just the times we live in . . . it's just awkward, for lack of a better word, that companies would keep track of that. [It] just makes me a little uncomfortable. It's just like a runaway train, you know, we just don't even know where it goes after that. If I'm shopping . . . [I] do my research and I don't really need a company suggesting, you know, “if you like this,” or “get this,” [or] “you might like this.” I just prefer to have them leave me alone. Let me do my shopping.

Ashley (early 40s, white American): I'm not too crazy about that aspect of it at all. To me, that is part of your privacy.

Chan (20 yrs, Hongkonger Canadian): I find it unnecessary to collect like that much information. And I also find it unnecessary to track how many . . . like what's the item that I buy every time. Like, come on! You don't need to know how many bottles of pop that I buy every week, or like how much peanut butter I buy. Like why does it matter to you? To the store?

Ishita (early 20s, Indian Canadian): I find there's not a whole lot I could do about it. I feel at this time and age, everything's trackable. They're getting very clever with loopholes. But at the same time, I can't stop shopping, or I won't stop using the internet, or like doing certain things because of it. But I do wish that they would be more upfront about what information is being shared everywhere.

The same sentiment is expressed by Taiba (an Afghani Canadian in her early twenties): “How do they know that I would be interested in that kind of stuff? It doesn’t bother me to be honest. But I wanted to know.”

To conclude, when it comes to tracking their purchases and consumption behaviour, consumers' reactions ranged from (1) indifference (because their information is not important enough, they lacked concern, they avoided loyalty programs and their marketing emails, or they were unaware that physical shopping could be tracked), to (2) welcoming (for the sake of promotions or money rewards, or when retail workers empathize with the ones collecting their information when the former shop, or to get temporary free storage when shopping large items), to (3) mixed feelings, to (4) resignation. This array of different responses to retailance (specifically the collection of personal information) goes some way to explaining the differences between the results of the Pew Research Center survey (Rainie & Duggan, 2016) which found that up to half of Americans are willing to "share personal information or permit surveillance in return for getting something of perceived value" and Turow et al.'s (2015, p. 3) survey that stated that informants are actually resigned to give up their data and that they did not believe in the fairness of the "data for discounts." Marketers and retailers, therefore, need to be open about how they collect their consumers' data and to focus on sending relevant marketing material based on such data.

(5) Selling consumers' information to third parties

Poster's (1989, 1996) "super-panopticon" fittingly describes how retailers regard the data they collect about their consumers as their property, an asset they can sell to others (i.e., third parties). The same concept was described by Pridmore and Zwick (2011, 2013) as the "manufacturing of consumers," since the information about consumers, collected both physically and digitally, is in itself a commodity that could be sold to third parties. Another term for "third parties" is "data brokers" who are described by the Federal Trade Commission (FTC) as

“companies that collect consumers’ personal information and resell or share the information with others” (Federal Trade Commission, 2014, p. i; Kesan, Hayes, & Bashir, 2015).

When asked to rate the statement, “I think it is appropriate for a retail store to share customers’ personal information with (a) credit agencies and (b) marketing firms,” 23.4% of informants strongly and somewhat agreed to their information being sold by retailers to third parties such as credit agencies (Figure 63). There were no statistically significant associations with gender ($X^2(12, N = 593) = 15.994, p = .192$), age ($X^2(24, N = 593) = 14.092, p = .945$), education level ($X^2(24, N = 593) = 30.390, p = .172$), or income level ($X^2(24, N = 582) = 35.666, p = .059$). This percentage dropped to 8.8% when the third parties become marketing firms (Figure 64) which indicates that consumers do not want to receive any promotional material from marketing parties they are not familiar with. Again, no statistically significant associations were found with gender ($X^2(12, N = 593) = 9.540, p = .656$), age ($X^2(24, N = 593) = 25.857, p = .360$), education level ($X^2(24, N = 593) = 29.595, p = .199$), or income level ($X^2(24, N = 582) = 20.772, p = .652$). As per the chi-square test, the only statistically significant association was with membership in a minority group; in the case of credit agencies, it was ($X^2(8, N = 101) = 31.007, p < .001$); and in the case of marketing firms, it was ($X^2(8, N = 101) = 23.007, p = .003$). The results (Table 13) confirmed that even within minority groups, consumers are more apprehensive with marketing firms than with credit agencies. The assumption that consumers see credit agencies’ access to their information as more legitimate when compared to marketing agencies opens up avenues for future research that could explore how consumers view the legitimacy of marketing firms and whether they challenge or accept such legitimacy when it comes to the privacy of their personal and shopping information.

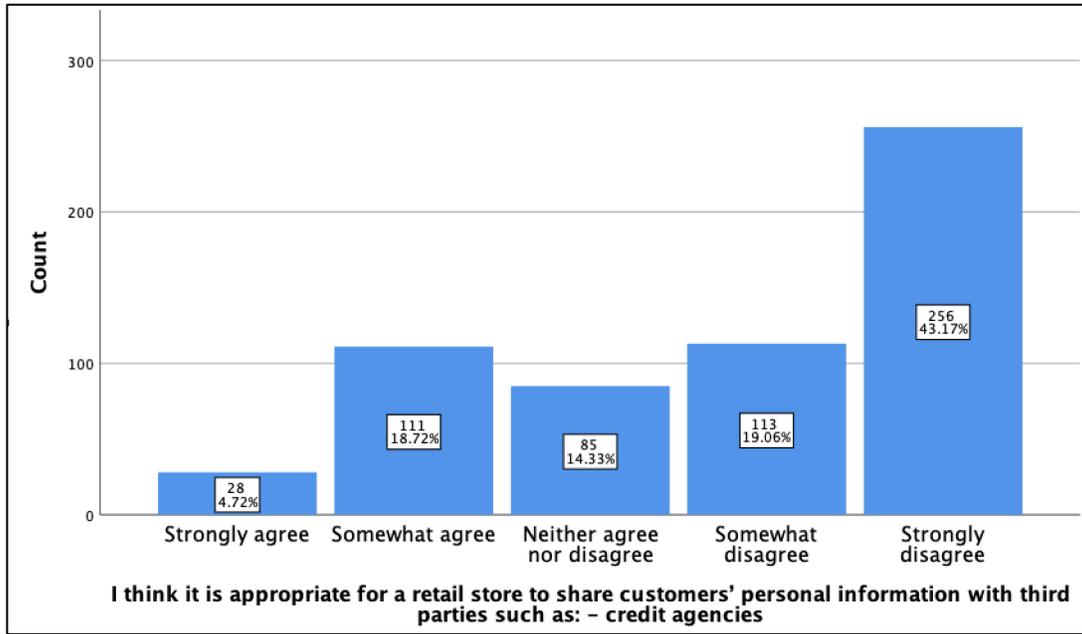


Figure 63 – Informants’ acceptance of selling their information to third parties like credit agencies

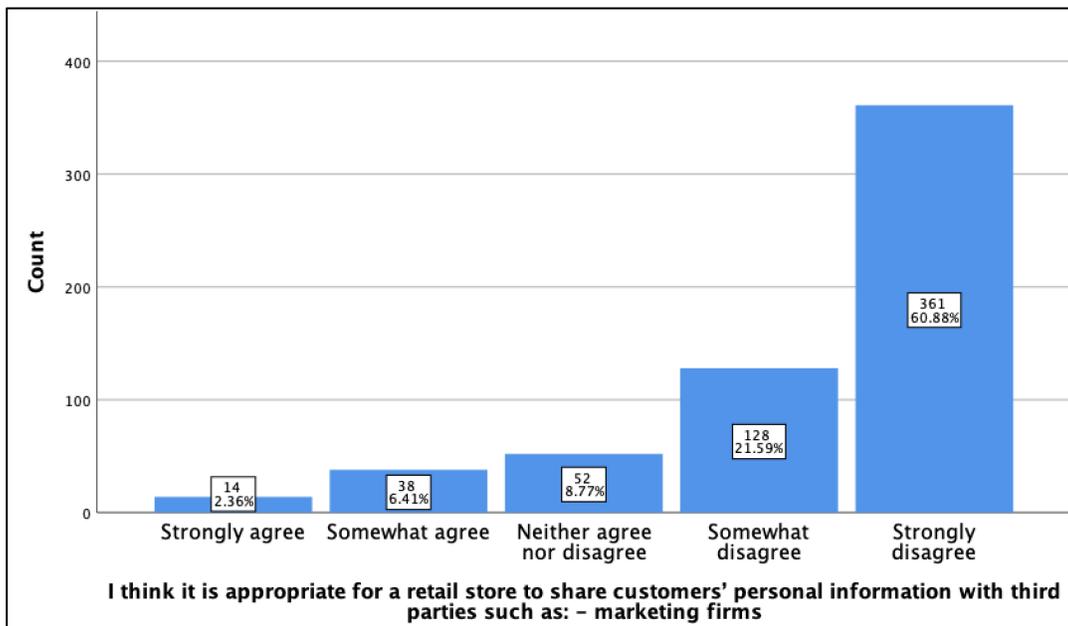


Figure 64 –Informants’ acceptance of selling their information to third parties like marketing firms

Membership in a minority group	Informants strongly or somewhat agree with retailers giving their personal information to third parties	
	Credit agencies	Marketing firms
Visible minority (n = 56)	17.86%	5.36%
Indigenous (n = 13)	76.92%	23.08%
With disability (n = 32)	25%	3.13%

Table 13 – The correlation between membership in a minority group and how comfortable informants are with retailers giving their personal information to third parties

To investigate consumers' type of acceptance and their reasons behind it, the interview informants were asked about whether it is appropriate for retail stores to share their personal information with third parties or not. Their answers varied from (1) outright acceptance, to (2) begrudging acceptance, to (3) conditional acceptance (on prior consumer approval, type of shared information and retailer's responsibility), to (4) refusal (Figure 65).

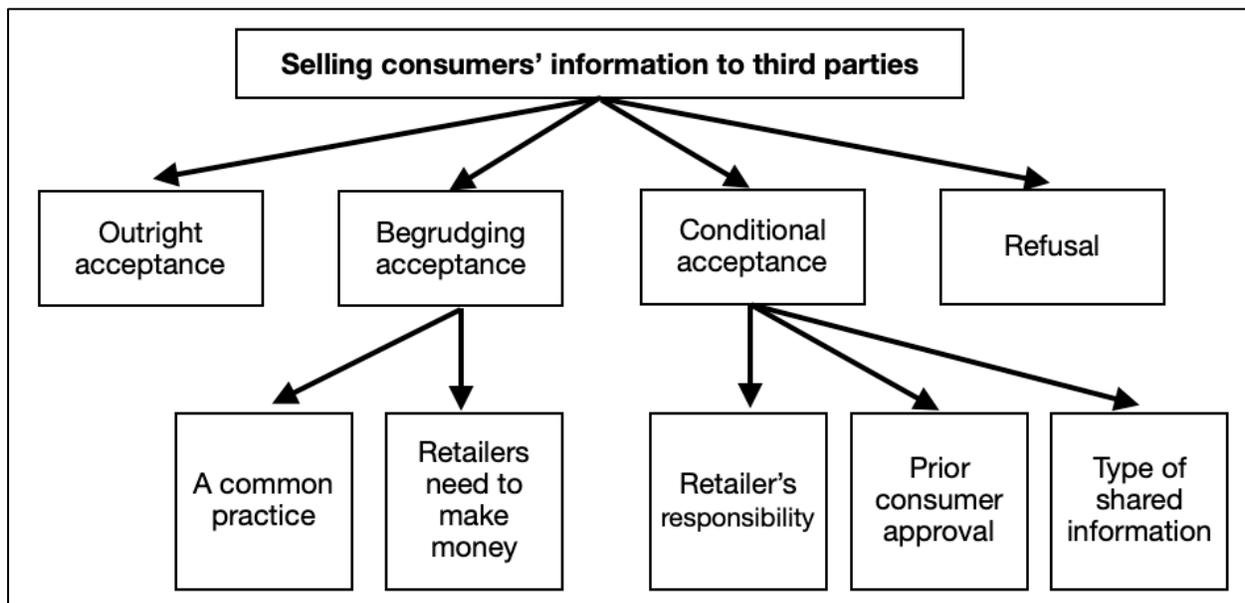


Figure 65 - Consumers' reactions towards their information being sold to third parties

5.1 Outright acceptance

Some informants simply accepted the fact that their information could be sold to third parties as long as the process is legal, even though there is always a risk of data hacks.

Myint (Burman Canadian): My husband [a data analyst] worked for those third parties too. He's working for like companies that work with Airbnb data, like that kind of thing. It's still generally the same principle. Of course, there's always a security risk. Of course, there's always data hacks that could happen. But for the most part, even in the third parties, no one really cares about you personally.

Megan (white Canadian): I'm okay with that [third parties buying my data] as long as everything is due diligence involved, everything is legal. I'm fine with that. I have nothing to hide. And again, if it's just going to help me and later, like, I don't mind at all . . . I'm fine with it.

5.2 Begrudging acceptance

Some consumers begrudgingly accept the selling of their information to third parties because (1) it is already a common practice, or (2) because they believe that retailers have the right to make money out of the collected information.

5.2.1 A common practice

To some consumers, it is already too late to turn back the clock when it comes to selling personal information to third parties; that genie is out of the bottle.

Michael (Black American): I just think that that genie [is] kind of out of the bottle in terms of the information . . . gathered and I think that it's going to be something as part of the new future in that, something that will probably be done, to be honest with you.

Li Na (Chinese Canadian): I'm okay with it only because I understand that this does happen. I am in the mindset knowing that any information I choose to share could be made public at any time and so I'm okay with retail stores doing it. Whether I necessarily think it's right or not? I'm on the fence about [it]. It's not illegal, but it's not also blatantly made obvious to consumers and that's not right either. At least I'm aware of it; most people aren't.

Olivia (white Canadian): I view it the same way I've used social media. So, like social media is the same concept, right? You get to use Facebook, and you get to use an Optimum card for free because your data is what people are paying for. And I don't like it but I know what's happening. And it, like I said, it's the same thing. Like I wouldn't use an Optimum card if I had to pay for it . . . So, I'm not particularly bothered by it. Like, I don't like it but it is what it is. Like, I know it was on and I think just being aware of it is what's important.

According to a 2019 Pew Research survey (Auxier et al., 2019b), 62% of American adults believe that it is not possible to go through daily life without companies collecting data about them. This result is exemplified by the above quotations that show that some consumers begrudgingly accept having their data sold to third parties because whether they like it or not, this practice will increasingly take place.

5.2.2 Retailers need to make money

To some consumers, at the end of the day, retailers need to “make money,” and it is enough to know that their data is being sold.

Michael (Black American): It is okay in the sense that in the grand scheme of things, they're in the business of making money. And I think that everything is moving in that direction. I think the future of business is customizing at a micro level with their customers. So, I think that is going to be necessary.

Joshua (white Canadian): I'm obviously not okay necessarily with that. Because when I signed up, I gave my information to that person who I was talking to then and there, but I think that either way, whether I like it or not, it's going to happen. Either it's going to happen legally and the company's going to do it, or there's going to be some data breach that it's going to happen. Anyways, I think it's just a part of the trade off and people's information is always being bought and sold. I think it's just something that comes with it.

This begrudging acceptance of having their personal, shopping and consumption information collected in brick-and-mortar stores sold and exchanged is similar to the results of a study exploring consumer knowledge about privacy and informed consent online (Hayes, Kesan, Bashir, Hoff, & Jeon, 2014, p. 3) which suggests that:

...there may be a sense of helplessness among consumers, with a majority of respondents indicating that on at least one occasion, they had felt compelled to submit information when they did not want to do so. This “information submission regret” may also contribute to a feeling that taking more time to learn about policies online would be a wasted effort, because the consumer would still not have any meaningful alternative.

To Hayes et al., informed consent should have five components: disclosure (providing accurate information to the consumer, for example, what information is being collected, who will have access to it, how long it will be kept, how it will be used, and how it will be protected), competence (the consumer has to be capable of giving informed consent), comprehension (the consumer has to have an accurate interpretation of the disclosure), voluntariness (the consumer’s actions should not be controlled or coerced), and agreement (the consumer accepts the terms of the agreement and has the ability to withdraw consent) (p. 4). Ultimately, informed consent would mean that consumers will have a sense of control and engagement³³ which will eventually increase the level of trust between consumers and retailers.

5.3 Conditional acceptance

Some consumers put conditions on their acceptance of their information being sold by retailers to third parties, and they are either (1) the retailer obtains the consumer’s prior approval or (2) that approval is dependent on the type of shopping and personal information being sold.

³³ Until the 1990s, marketing was focused on customer transactions and profitability. This evolved—between the late 1990s and the early 2000s—to a focus on ensuring customer satisfaction and loyalty via better products and services (i.e., a relationship built on trust and commitment). Pansari and Kumar (2017) suggest that when a relationship (between customer and firm) is satisfied and has emotional bonding, it progresses even further to a higher stage of customer engagement (CE) which ultimately ensures a sustainable competitive advantage.

5.3.1 Prior consumer approval

Some consumers, like Rahul (Indian Canadian), accept the tracking of their shopping history and the selling of that information as long as they approve beforehand. A similar reaction is conveyed by Ishita:

Ishita (Indian Canadian): I think as long as they make it [selling info to third parties] clear in the beginning, from where initially you're purchasing your items, that your information may be passed on. And I think the individual has the choice to decline . . . [to] be like, "I don't want to share anything about it" . . . I think that's okay. But if I'm not aware of it and then someone else is essentially looking at my trends, of how I shop, that I don't find I'm okay with.

Ashley (white American): I don't feel like it's all right. I think it should be "illegal." . . . Even though it's legal, it's still your private information and, I mean, if they're going to, in my opinion, going to share your information, they should at least let you know that they're going to do it or give you a choice whether they can do it or not.

Thus, to consumers like Ishita and Ashley, prior approval of having their data sold to third parties is essential.

5.3.2 The retailer's responsibility

To be able to give their consent, a consumer should first understand what is at stake. To Christopher, the responsibility, or "burden," of providing a clear explanation should fall on the retailer's shoulders and not the consumer's.

Christopher (white American): The burden should not have to be on the user, it should be on the company itself to be ethical and be transparent about how data is being collected, but unfortunately, it has just shifted . . . [to] the user, it becomes a responsibility to look through complicated privacy disclosures and determine what data is being collected and how it's being collected and if it's being sent to third parties and things like that . . . which is really unfortunate.

Survey informant: I do understand that at some point, businesses can/will get hacked or breached. I would like to believe that they do their best to protect against that, but at the same time, that could very likely be a corner that is cut in order to make themselves more profitable. As a consumer I just have to make a choice and accept that risk. I do believe though that if a store is collecting my data, they should take responsibility for protecting that data.

According to the above quotes, the retailer's responsibility is two-fold: (1) to be transparent and inform the consumer about the implications to privacy, and (2) to protect collected consumer data (e.g., against data breaches). According to the 2019 Deloitte survey on consumer privacy in U.S. retail (Sides et al., 2019), while most consumers do not believe that retailers ensure data privacy (only 5% of consumers place the retail industry at the top in ensuring data privacy), nearly two-thirds of consumers say retailers (and not the government or tech vendors) are responsible for data security. In the 2020 McKinsey & Company survey on consumer data and privacy (Anant, Donchak, Kaplan, & Soller, 2020), 18% of respondents chose the retail industry as most trusted in protecting their privacy and data, compared to healthcare (44%) and financial services (44%) businesses. Retailers, therefore, are in a difficult position, for they lack consumer trust when it comes to data protection and yet they are being held accountable.

5.3.3 Type of shared information

To Emma, it all depends on the type of information being sold, for example, shopping trends versus a personal photo or contact information.

Emma (white Canadian): It depends on how personal the information is. Like if it's just like what foods you buy and stuff like that. Like, I guess I'm okay with that. It's more like if my name or photo or like something like that was used, or my email was sold like that's more what I have an issue. It's more personal information stuff rather than what I bought.

5.4 Refusal

To some people, the whole process of selling their information to third parties is simply wrong, "unethical" and "immoral".

Mary (white American): I don't think it's ethical. I don't think it's right, and it's very annoying . . . all of a sudden, my email is full of offers and I believe it, that it was from my interaction with that particular store.

Maria (Argentinian American): And that's probably even scarier . . . being able to just sell your information to somebody else . . . That to me is really immoral. Because how do I know that corporation (A) has any idea how ethical corporation (B) is that they're selling my information to? And if they're allowed to, they're not going to suffer any liability if corporation (B) goes around stealing from people, [they] are within their rights to sell that information . . . and that's terrifying.

Maria then goes on to explain how American companies only care about making their shareholders happy, forgetting about their customers.

Maria (Argentinian American): What I think the problem is, at least in the States . . . is these companies that have over the years . . . forgotten about long-term growth and keeping the company growing long term steadily. Everything is about the next quarter, bam, bam, bam, bam, bam, bam, always. Up, up, up, up, up. And everyone's always looking to make quick money, quick money, quick money. And so that's what leads to these things like selling information. It's just they have to find new more better ways to make money. Since people can only buy so much product. You know? I mean, how many smartphones do you need a year, you know? You don't. And they're expensive. So, you have to . . . justify some kind of way to make money to make those shareholders happy, and information [is] an easy way to do it . . . They don't realize that they alienate more people, and they will lose customers long term over that . . . And that's what's causing them to cross red lines. It's just easy money, the money and then other people will [say], “Oh they did that. I can do that too.” And it just becomes this whole mess that just gets exponentially bigger and scarier and . . . it's greed. And it's not sustainable. But I could be wrong. I don't know. I'm not an economist.

To some consumers, their refusal to have their data sold to third parties is mainly because a lack of knowledge; they “don't know” with whom their data will end up with.

Robert (American Canadian): Well, for me personally, I don't like the idea because it's one of those things where I don't know where they're selling it to. I'm not sure what kind of companies are going to buy this information . . . Say, I go to Bath and Body and they sell it to somewhere else. It's like, well, I don't want their junk mail. I never went to their location . . . like the store that they sold it to, I don't know where they are, you know, what kind of store it is. So, I . . . am hesitant sometimes to give information because they say, “Oh, we're not going to do this.” But then, if you're reading their actual disclosures, “We do sell to the third parties.” And . . . I have [said no]. And of course, that's when the sales associate gets all rude and defensive and be like, “Well, we normally don't sell it,” but I'm like “Right here says you do sell it, you're sort of, you know, going against your policy.” And of course, the sales associate's not sure what to tell you. I'm like, “Well, I'm not going to sign anything.”

To sum up, the survey analysis showed that while a relatively small percentage of consumers are comfortable with retailers sharing their personal information with third parties, they are even more apprehensive when those third parties are marketing firms they are unfamiliar with compared to credit agencies (as discussed earlier, financial services businesses are more trusted by consumers). Consumers' reactions, moreover, could be categorized under (1) outright acceptance, (2) begrudging acceptance, (3) conditional acceptance depending on prior approval by the consumer and, the retailer taking responsibility of protecting the collected data, and the type of shared information (for example, shopping trends versus contact information), and (4) refusal.

(6) Loyalty programs

A major retail system that tracks consumers' shopping history and behaviour is retail loyalty programs. Out of all 593 informants, 84.99% of informants are members in at least one loyalty program, and around 32% have subscribed to more than 5 different loyalty programs (Figure 66). Compared to the 2006 GDP survey (Pridmore, 2010), in which 40% (two-fifths) of the Americans and 66.7% (two-thirds) of the Canadians surveyed said that they carry at least one loyalty card, it appears that there has been a rise in loyalty memberships in North America, which shows how successful those programs are and how purchasing convenience, discounts, and tailored offers related to them surpasses privacy concerns.

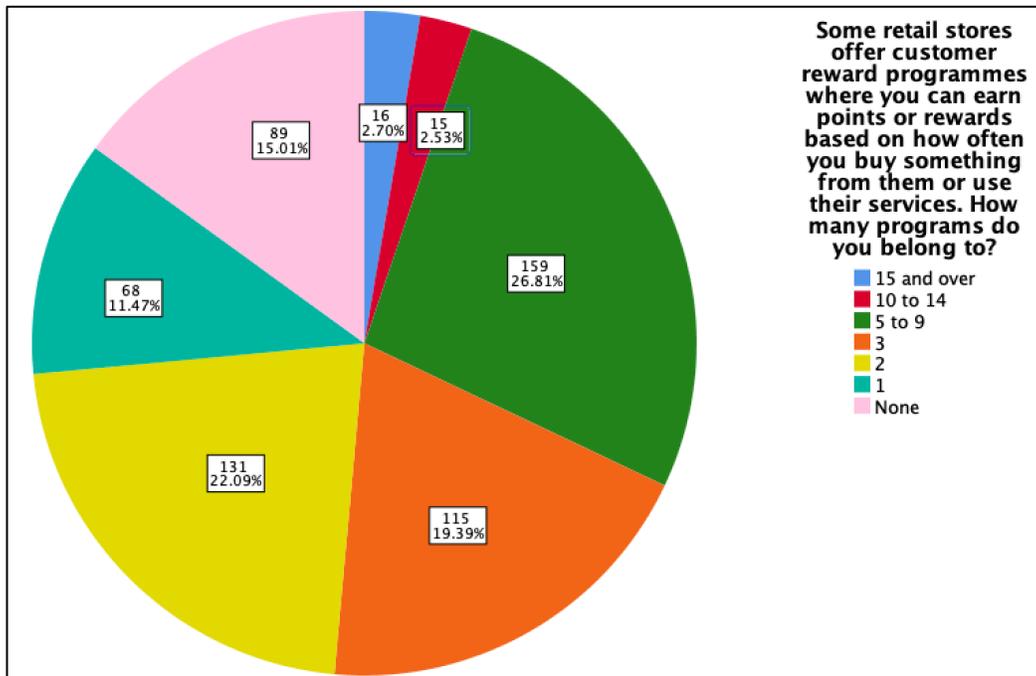


Figure 66 – Number of informants subscribing to loyalty programs

Looking at the data, there are statistically significant associations between the number of loyalty programs consumers subscribe to and age ($X^2(36, N = 593) = 70.198, p = .001$), gender ($X^2(18, N = 593) = 30.073, p = .037$), education ($X^2(36, N = 593) = 71.064, p < .001$), and income ($X^2(36, N = 582) = 62.211, p = .004$). There is not a statistically significant association with membership in a minority group ($X^2(12, N = 101) = 16.233, p = .181$). Looking specifically at consumers who have joined 5 or more loyalty programs, we can see that young and middle-aged (aged 18 to 54) (Figure 67 and Table 14), female (Figure 68 and Table 15), highly educated (enrolled in a bachelor's degree, have graduated from university, or have a graduate degree) (Figure 69 and Table 16), and high annual income (USD 77,000 and more) (Figure 70 and Table 17) consumers tend to make up this group. These statistically significant associations raise four interesting points: (1) It is not surprising that younger consumers (who are usually more technology savvy) join more loyalty programs. (2) In addition to females being more aware of

the presence of loyalty programs as a retailance system (the statistically significant association discussed earlier shows 91.1% female compared to 87.45% male), they are also more inclined to subscribe to a higher number of loyalty programs. It would be interesting to conduct a future study to see why female consumers are more likely to subscribe to a higher number of loyalty programs; is it because women shop more, are more interested in receiving discounts and deals, or for any other reason? (3) Post-secondary educated consumers are more likely to subscribe to more than five different loyalty programs. (4) Contrary to some of the interviewees who theorized that there is a negative correlation between a consumer's income and the number of loyalty programs they subscribe to (i.e., the higher the income, the less likely a consumer would join), the survey data showed that the correlation is positive, for consumers with higher annual income join more loyalty programs, which indicates that brand loyalty and receiving better services may be important elements when signing up for loyalty programs (i.e., it is not just about monetary benefits). This assumption corroborates the study published by Bond Brand Loyalty³⁴ (Bond Brand Loyalty, 2020b, 2020a; MACCORR, n.d.-a, n.d.-b) which stated that to 59% of Canadians, the biggest factors in their satisfaction with loyalty programs are program experience, brand alignment, digital experiences, and human touch, in contrast to 41% of Canadians and 39% of U.S. consumers who participate because of rewards, redemptions and how much they earn.

³⁴ It should be noticed that the Bond report includes different industry sectors and not just brick-and-mortar retail (e.g., airline, entertainment, online retail, gas and convenience, hotel, automotive, etc.).

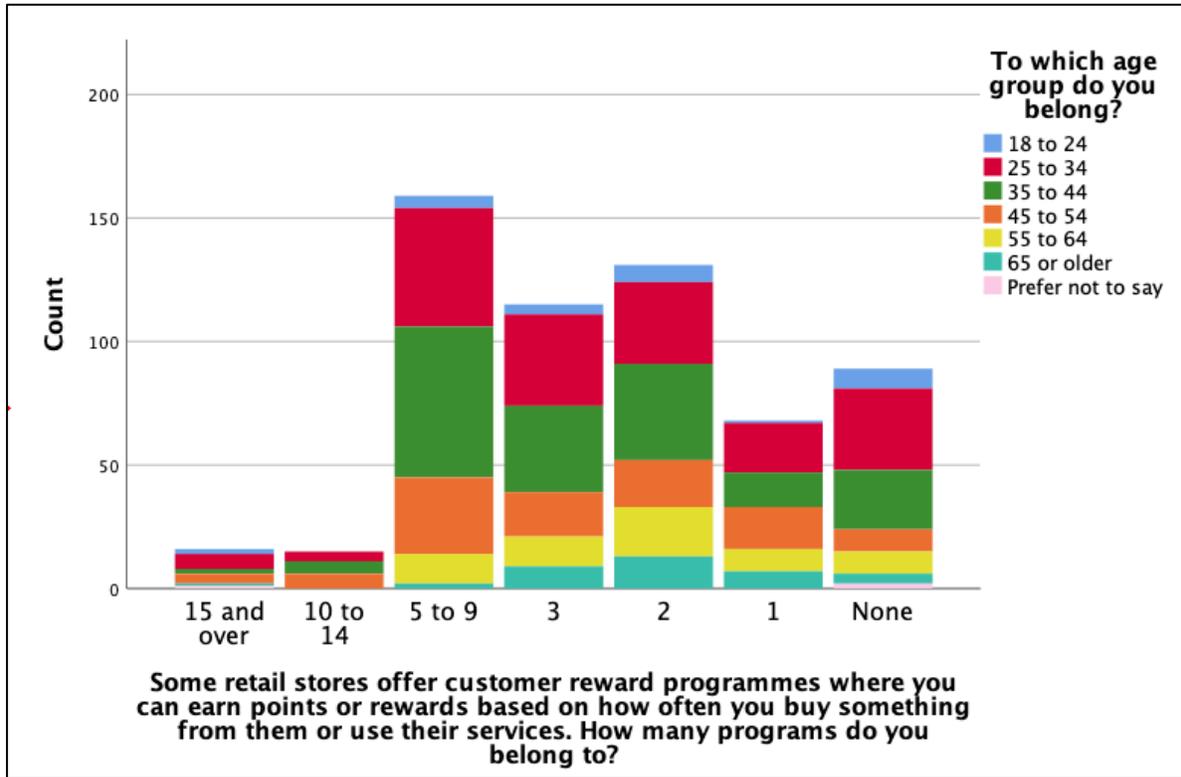


Figure 67 – Impact of age on the subscription to loyalty programs

Age	Percentage of informants subscribing to loyalty programs					
	15 loyalty programs and over	10 to 14 loyalty programs	5 to 9 loyalty programs	3 loyalty programs	2 loyalty programs	1 loyalty program
18 to 24 (n = 27)	7.4%	0%	18.51%	14.81%	25.93%	3.7%
25 to 34 (n = 181)	3.31%	2.2%	26.52%	20.44%	18.23%	11.04%
35 to 44 (n = 180)	1.11%	2.78%	33.89%	19.44%	21.67%	7.78%
45 to 54 (n = 104)	3.85%	5.77%	29.8%	17.3%	18.27%	16.35%
55 to 64 (n = 62)	0%	0%	19.35%	19.35%	32.26%	14.52%
65 or older (n = 36)	2.78%	0%	5.56%	25%	36.11%	19.44%

Table 14 – The correlation between age and the number of loyalty programs informants subscribe to, with the highest percentage under each category in red

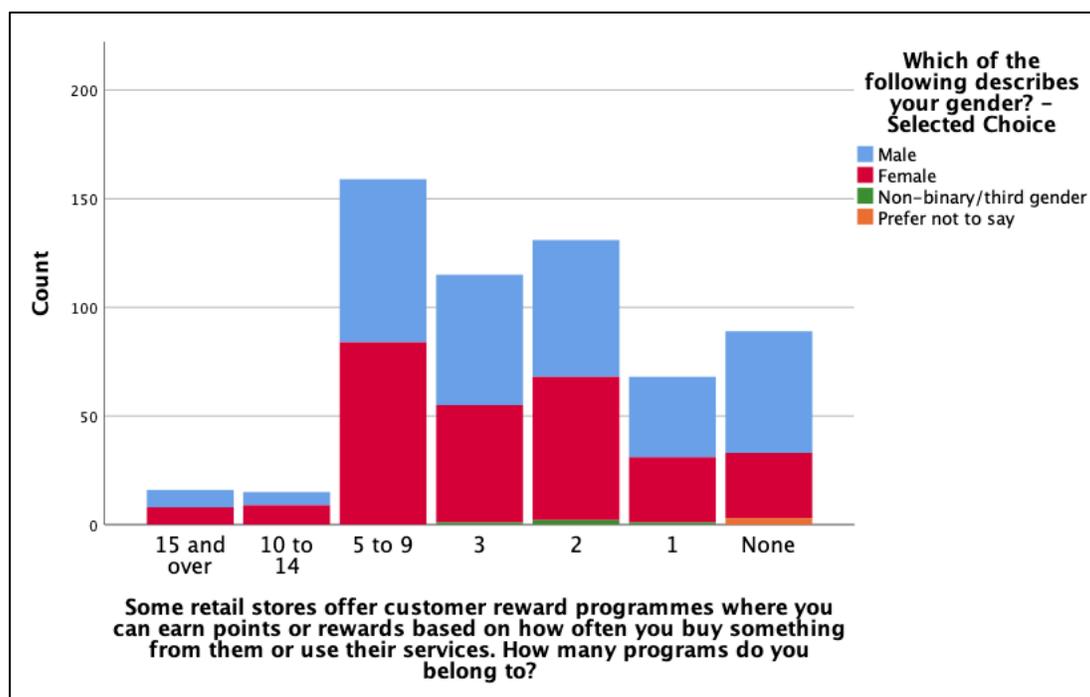


Figure 68 – Impact of gender on the subscription to loyalty programs

Gender	Percentage of informants subscribing to loyalty programs					
	15 loyalty programs and over	10 to 14 loyalty programs	5 to 9 loyalty programs	3 loyalty programs	2 loyalty programs	1 loyalty program
Male (n = 305)	2.62%	1.97%	24.59%	19.67%	20.66%	12.13%
Female (n = 281)	2.84%	3.2%	29.89%	19.22%	23.49%	10.68%

Table 15 – The correlation between gender and the number of loyalty programs informants subscribe to, with the highest percentage under each category in red

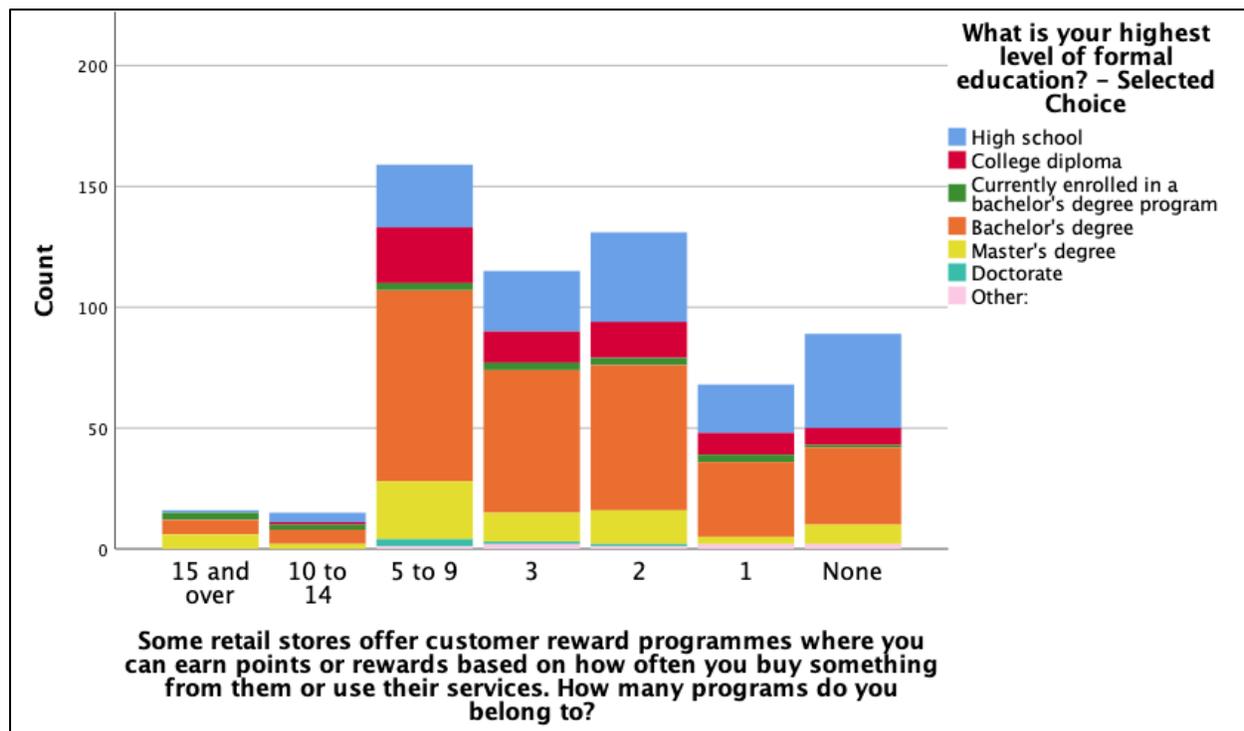


Figure 69 – Impact of educational level on the subscription to loyalty programs

Education	Percentage of informants subscribing to loyalty programs					
	15 loyalty programs and over	10 to 14 loyalty programs	5 to 9 loyalty programs	3 loyalty programs	2 loyalty programs	1 loyalty program
High school (n = 152)	0.66%	2.63%	17.11%	16.45%	24.34%	13.16%
College diploma (n = 68)	0%	1.47%	33.82%	19.12%	22.06%	13.24%
Enrolled in a bachelor's degree (n = 18)	16.67%	11.11%	16.67%	16.67%	16.67%	16.67%
Bachelor's (n = 273)	2.2%	2.2%	28.94%	21.61%	21.98%	11.36%
Graduate (Master's & Doctorate) (n = 74)	8.12%	27.03%	36.49%	17.57%	20.27%	45.95%

Table 16 – The correlation between education level and the number of loyalty programs informants subscribe to, with the highest percentage under each category in red

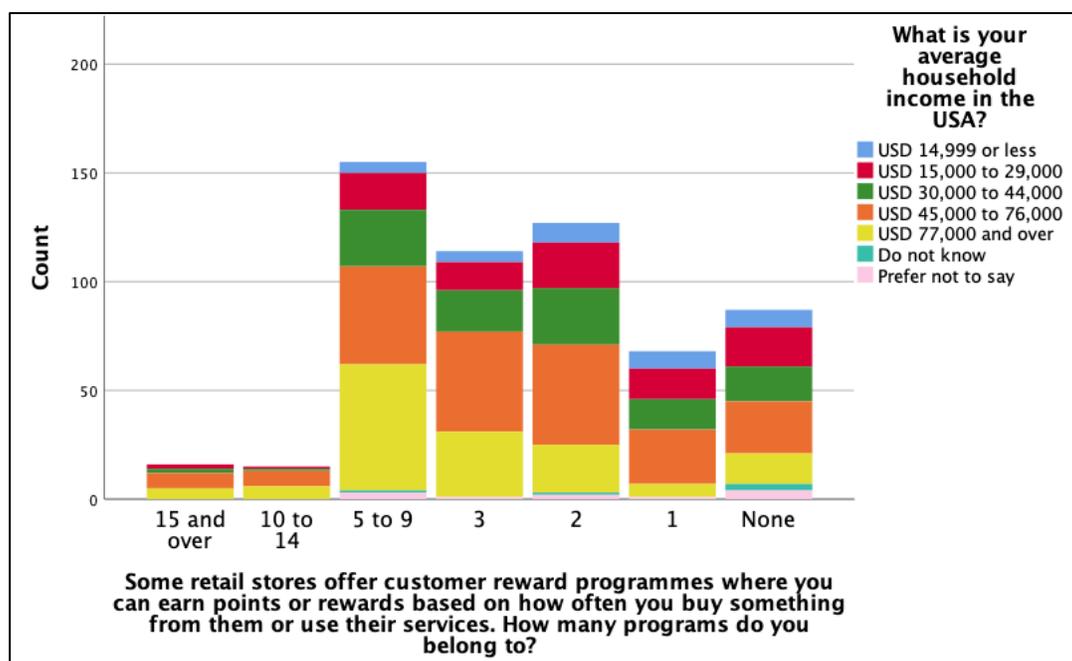


Figure 70 – Impact of U.S. household income on the subscription to loyalty programs

U.S. income	Percentage of informants subscribing to loyalty programs					
	15 loyalty programs and over	10 to 14 loyalty programs	5 to 9 loyalty programs	3 loyalty programs	2 loyalty programs	1 loyalty program
USD 14,999 or less (n = 35)	0%	0%	14.29%	14.29%	25.71%	22.86%
USD 15,000 to 29,000 (n = 86)	2.33%	1.16%	19.77%	15.12%	24.42%	16.28%
USD 30,000 to 44,000 (n = 104)	1.92%	0.96%	25%	18.27%	25%	13.46%
USD 45,000 to 76,000 (n = 200)	3.5%	3.5%	22.5%	23%	23%	12.5%
USD 77,000 and over (n = 141)	3.55%	4.26%	41.13%	21.28%	15.6%	4.26%

Table 17 – The correlation between U.S. income and the number of loyalty programs informants subscribe to, with the highest percentage under each category in red

When survey informants were asked to rate the statement, “I am comfortable with sharing personal information (such as my name, address, telephone number, email address, date of birth, or financial information) for reward programs (for example, at gas stations),” 46.8% strongly or somewhat agreed that they felt comfortable sharing their information and only 35.98% reported somewhat or strong disagreement with the statement (Figure 71). Although a higher percentage (46.8% compared to 35.98%) do not worry about sharing their privacy via loyalty programs, there is still a sizeable segment (17.23%) who could not yet decide whether they feel comfortable or not, an opportunity that marketers and retailers need to address. A chi-square test of independence showed that there was a statistically significant association between that statement and age ($X^2(24, N = 592) = 44.098, p = .007$). This significant association with age was discussed in a 2018 KMPG survey (Dragan, 2018) which showed that millennial consumers are more likely (21%) than their baby boomer counterparts (5%) to trade their data for better

customer experience and personalization. Likewise, a fifth (19%) of millennial consumers would trade their data for better products and services, versus just 8% of baby boomers. Comparing the MTurk results in Tables 14 (see above) and 18, I noted that although the younger consumers tend to subscribe to more loyalty programs, they are also more likely to feel uncomfortable with sharing their private information. This indicates that although young consumers desire purchasing convenience and tailored offers more than they care about privacy issues, they are not completely blind to them (see Nussbaum's (2007) discussion of young people forsaking their privacy on social media). There were no statistically significant associations between feeling comfortable and gender ($X^2(12, N = 592) = 18.138, p = .112$), education level ($X^2(24, N = 592) = 28.672, p = .0233$), income level ($X^2(24, N = 581) = 25.771, p = .365$), or membership in a minority group ($X^2(8, N = 101) = 6.520, p = .589$).

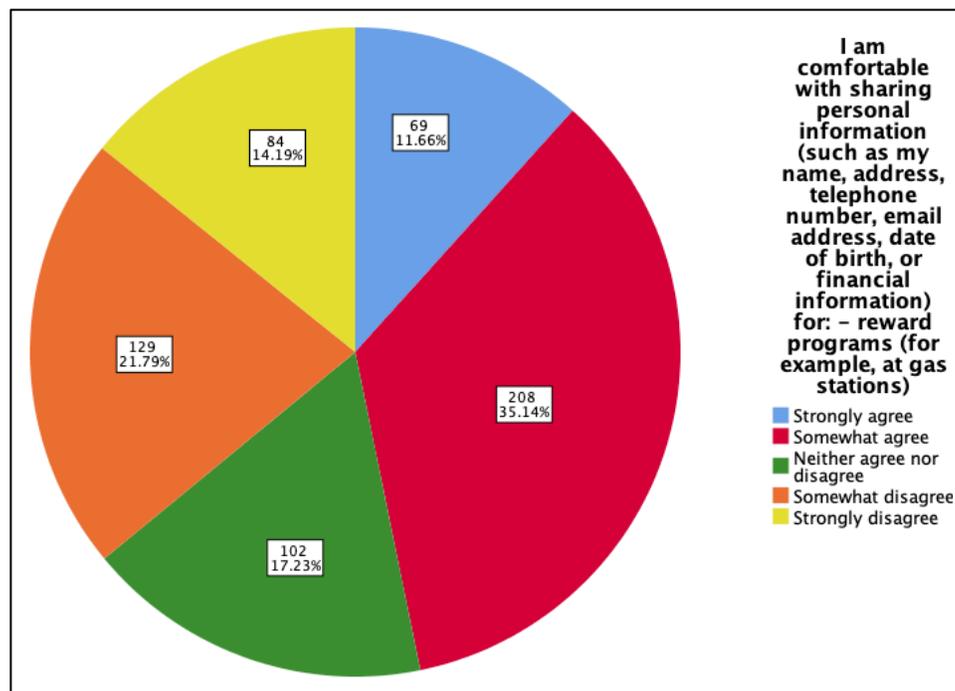


Figure 71 – Informants' feelings of comfort when sharing personal information via loyalty programs

Age	Informants feeling comfortable with sharing personal information for reward programs	
	Strongly or somewhat agree	Strongly or somewhat disagree
18 to 24 (n = 27)	33.33%	47.88%
25 to 34 (n = 181)	49.17%	40.88%
35 to 44 (n = 179)	48.04%	41.9%
45 to 54 (n = 104)	49.04%	39.42%
55 to 64 (n = 62)	46.77%	25.8%
65 or older (n = 36)	38.89%	25%

Table 18 – The correlation between age and how comfortable informants are with providing their personal information for reward programs, with the highest percentage under each category in red

The interview data complemented the survey findings. During the interviews, and whether participants kept a stack of loyalty cards in their wallets or uploaded them on mobile apps, most of them could not tell for sure how many loyalty programs they have signed up for. Though they could identify how many they actively and frequently use, when discussing the total number of programs, they have subscribed for, words like “I think; they don’t really come to mind; I guess; I know that’s bad, but . . .” were repeated. In general, consumers’ reaction towards signing up for new loyalty programs could be divided into two main categories: (1) embracing loyalty programs and (2) guarded and limited acceptance (Figure 72).

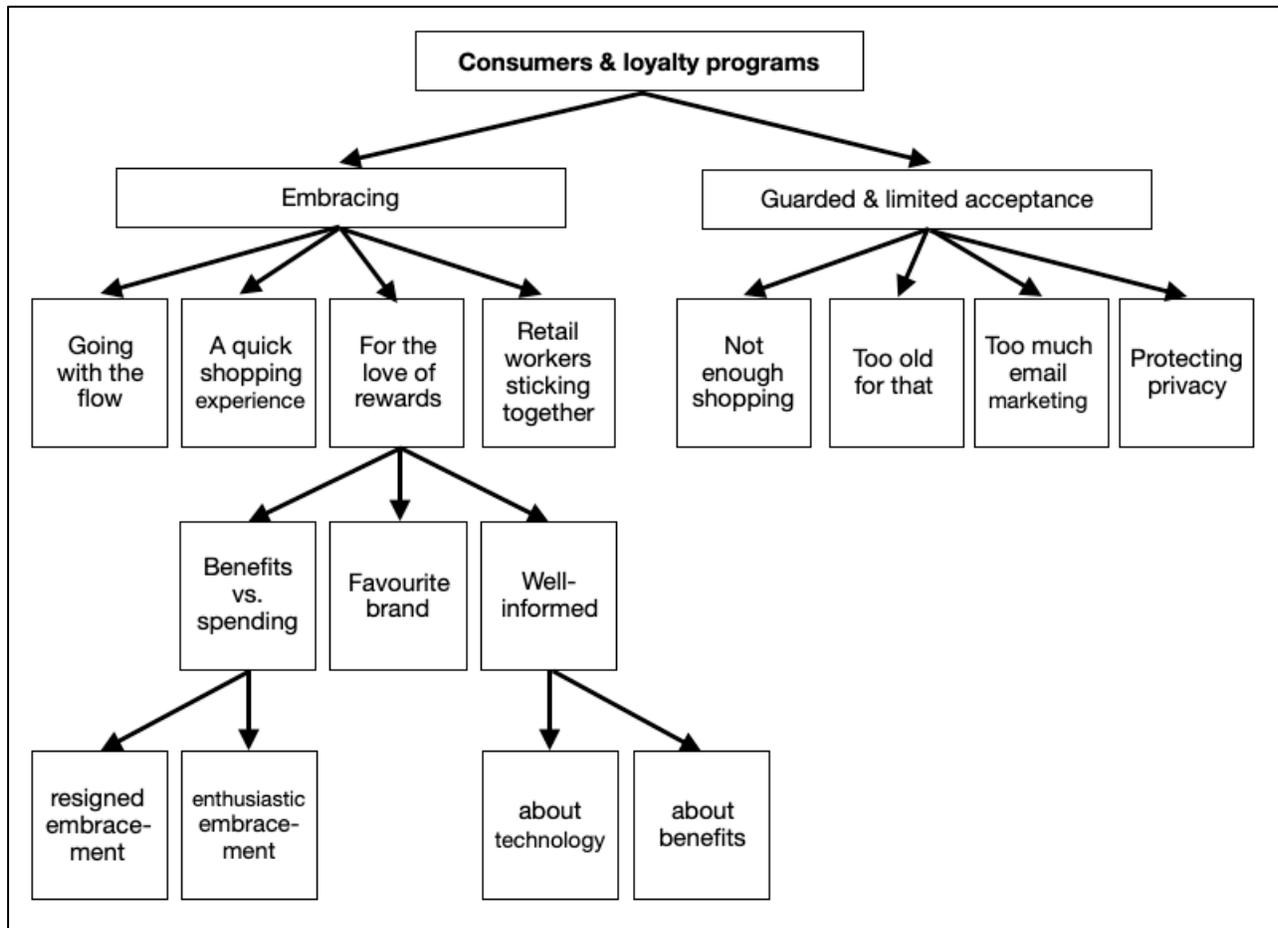


Figure 72 – Consumers’ reactions towards loyalty programs

6.1 Embracing loyalty programs

There are four reasons behind consumers’ embracement of loyalty programs: (1) going with the flow, (2) having a quick shopping experience, (3) loving the rewards, and (4) if they work in retail, empathising with fellow retail workers.

6.1.1 Going with the flow

To some consumers, being members in different loyalty programs is part of the shopping experience that they no longer think about.

Emma (F, 34 yrs, HS, CAD 60,000): It's a little weird but I don't usually think about it. I like that Loblaw's [through PC Optimum card] does collect the

information about you, because then they give you points based on what you buy and that's okay.

6.1.2 A quicker shopping experience

Christopher (a thirty-eight-year-old male) talked about how he keeps accepting new loyalty programs not only to access the store savings, but to access them quickly. To him, therefore, a loyalty card not only gives him access to savings and store offers, but they also allow him to access those offers quickly and seamlessly.

Christopher (M, 38 yrs, HS, USD 17,000): I just want to get the savings, real quick, and I may not even go back to that store again. But I'll be like, "Okay, fine, just sign me up real quick."

6.1.3 For the love of rewards

Some retail consumers embrace signing up for loyalty programs because of their love of the rewards they expect to earn. Yet their feelings behind this acceptance are slightly different. Some consumers want to earn something extra when spending money, whether they are resigned to joining those programs or feeling enthusiastic about them.

Ishita (F, early 20s, BA, CAD 15,000): The way I interpret it is like I'm gonna spend the money regardless. I might as well get some benefits out of it.

Talking about her experience working in Coach Outlet, Wang remarked that collecting consumers' information is not difficult and that signing up is "actually pretty good" for them:

Wang (F, 21 yrs, college, CAD 90,000): I'd find about like eight times out of ten, people do want it [our loyalty program] just because like our bags are so expensive. You get birthday rewards, you get like discounts. So, I think every little bit helps. And so people are more inclined to be like, "Oh, okay."

Rachel (F, early 20s, MSc, min. wage): Oh my God! So many. Oh my God! Like you think pretty much every store I regularly shop at, I've got their card, especially as a student. I mean, if it's free, it's just one more way to possibly save a bit of money or, you know, get some extra coupons or something. I think they're awesome.

Other consumers associate their love of rewards with their favourite brands, for example, Taiba—a female in her early twenties—expressed how she “love[s] taking points from Hudson’s Bay.”

Some consumers are not just attracted to the rewards, but they are also well-informed about the technology behind and/or benefits of loyalty programs. For example, because her husband works as a data analyst with some of the major loyalty programmes in Canada, Myint feels that she has a better understanding of the positive impact of surveillance, especially when it comes to loyalty programs’ data collection:

Myint (F, early 20s, BA, CAD 125,000): Pffffff! I don't want to say [I subscribe to] all of them because there's millions of them. But basically, at any point, if I encounter a loyalty program, I will sign up for it. And anytime I spend \$1, there's some sort of loyalty points being collected. Yeah, I have a different opinion on it than most people. I know that there is sometimes a lot of negative energy around Big Brother watching and collecting your data. And I feel like being married to someone who works with that data, I have a better understanding of the fact that yes, like data hacks could happen. Yes, someone could technically watch you, but [at] the end of the day, they don't care about you personally. No one cares what movies I saw. They're looking at trends. They're looking at demographics. No one cares what [I] did. And so, I care a lot less about having my information and 70,000 loyalty programs.

Mitig also talked positively about loyalty programs because she believed she was well-informed about their benefits.

Mitig (M, 20 yrs, university, CAD 20,000): One thing we had was if you had the [PC Optimum] card, then you got 2 or \$3 off of a whole cooked rotisserie chicken. So, like if someone had the chicken and they didn't have the card then, “Oh, you can sign up today and save two or \$3.” Some people like it. Some people didn't care. But I mean, sometimes the benefits are really nice. People probably don't want another card in their wallet. That's probably why I think. Or they don't understand how the benefits work, because you can get good benefits. I mean, I work there, but I still use the reward. Lots of the customers shop by the offers on my app, and I save up money, and I have enough points now that I can have pretty well a whole month of groceries for free, one month. So, you can really get good benefits. I don't think people realize how the benefits work well for them.

To summarize, embracing memberships in loyalty programs for the sake of rewards could be a result of consumers' need to earn benefits (whether they are resigned or enthusiastic about loyalty programs), being loyal to their favourite brands, or being well-informed about the technology behind loyalty programs and/or their benefits.

6.1.4 Retail workers sticking together

As for those who either have previously worked or are still working in retail, they join the loyalty programs because they empathize with their fellow workers. For example, Emily (a young female Canadian in her early thirties) works in one of the Target branches in the U.S. where cashiers are expected to get at least 4 new credit members per week, otherwise, the number of their working hours is threatened. Target cashiers are also expected to sign up consumers to the new Target Circle app, however, they resist the latter, for they are apprehensive of the app (which asks for too much information like a phone number) in comparison to the older system of a physical card with a barcode, and besides, consumers would only get 1% off for being a participant. Thus, although she does not like putting loyalty program apps on her cellphone (because she is not sure how they will invade her privacy, what they will do in the background of her phone, and what type of info they will collect), she always “feels bad” towards the workers. She ends up signing up for loyalty programs but not for credit cards. In another interview, Wang's first reaction to being asked about the number of programs she is a member of was “Oh, God! Shit.” Though she is aware of their tracking capabilities, she still signs up for new programs because in Coach Outlet where she works,

Wang (F, 21 yrs, college, CAD 90,000): Employees get judged on how many people sign up for those loyalty programs. And so, I just do it because if it were me, I'd want them to do it. So, I just give them [my information]. I have like a separate email for that. So, I was like, “Here, get your quota done.”

6.2 Guarded and limited acceptance of loyalty programs

Some of the interviewees conveyed their guarded and/or limited acceptance of being members in loyalty programs. Their reasons were: (1) they did not shop enough (whether in a particular store that offers a loyalty program or in general); (2) they were too old to embrace this technology; (3) they were weary of receiving email marketing; and (4) they wanted to protect their privacy.

6.2.1 Not enough shopping

Some interviewees talked about how their occasional refusal to sign up for new loyalty programs stems not from fear of surveillance, but because they either do not shop enough at particular stores or they simply do not have much money for shopping in general.

Zahra (F, early 40s, MA, CAD 160,000): If it's a store that I go once or twice, like Chapters, I usually say "No, thank you."

William (M, 65 yrs, college, CAD 75,000): I'm not a big shopper. So, it [not signing up] is just convenient for me. I don't want to have to keep track of multiple cards . . . I only use the one card, it's not really an issue. I don't do a lot of just random irrelevant shopping, like I buy necessities and that's it pretty much. And things for the girl, my granddaughter. But basically, that's it. So, not really. I don't think I have too much of a problem with that.

Wang (F, 21 yrs, college, CAD 90,000): [I] Tried to collect points, but I didn't shop too much. I'm not good at spending. I don't usually spend too much money [Laughs]. I don't get too much points. So slowly, slowly, I lost track of how many points I have on my card. And I don't really use those cards now.

Sarah (F, late 20s, MA, CAD 63,000): I guess I never actually really thought about them tracking what I purchased, but I also am like the stingiest person on the earth. So, I don't shop that much. So, there's like not a lot for them to track. I guess I'm okay with it.

To conclude, while some consumers embrace loyalty programs because of the expected trade-offs, others do not expect to receive enough financial benefits, because of the low volume of their purchases, to warrant signing up for loyalty programs. The latter, therefore, are an untapped

market segment beyond the reach of loyalty programs that retailers and marketers can target through other marketing programs.

6.2.2 Too old for that

Corroborating the statistical analysis that showed that age is significantly associated with signing up for more loyalty programs, the interview data shows that older consumers are more reluctant to join loyalty programs. Paulo (a thirty-one-year-old Brazilian male living in Ottawa) talked about his experience working at Value Village and how cashiers need to collect information (mainly phone number, email, postal code, first name and birth date) to sign consumers up in the Value Village loyalty program, the Super Savers Club. According to him, age plays a crucial part in consumers' acceptance of loyalty programs:

Paulo (M, 31 yrs, post-grad, CAD 60,000): The people that have [a] problem with giving their information is, I think, older people, like over 60, you know. That they think we'll steal when we use their information. I don't think they see all the benefits of being part of Clubs . . . don't look at emails, getting discounts, or having specific promotions to your shopping behaviours and stuff.

This is echoed by Ishita who sees this attitude of accepting loyalty programs as another difference between her generation (she is currently in her early twenties) and that of her parents who are “very skeptical.”

Ishita (F, early 20s, BA, CAD 15,000): They don't like to give their information out to everyone. But I know from my generation, we just give our phone numbers and emails out if we get to collect points. So everywhere I shop [I sign up]. If it's a free card or a membership where you get points off, I do tend to always be involved in it.

Her embrace of loyalty programs, however, does not extend to signing up for store credit cards.

This disregard of the importance of privacy by the young brick-and-mortar consumers compared to the much older generation is also reflected in online retail, where the younger generations care less about their online privacy than older generations (Bashir et al., 2014).

6.2.3 *Too much email marketing*

To some consumers, the problem with being members in loyalty programs is not the collection of their personal and shopping information, but the constant advertisements they receive by email.

Emma (F, 34 yrs, HS, CAD 60,000): But the only time I really have an issue [with collecting my information] is when you get mass emailed over and over again. So, I wouldn't say like have an issue with the data collecting itself, unless it's excessive. It's more just the constant emails.

In the earlier section (entitled “Going with the flow”), Emma expressed liking to collect points by her PC Optimum card. This highlights the fact that for some consumers, their hesitancy to sign up for loyalty programs is not about the expected benefits or their privacy concerns, but rather about the fear of receiving too much marketing correspondence. Retailers, therefore, could get better membership rates to their loyalty programs if they address this concern of how and how often they communicate with their card holders.

6.2.3 *Protecting privacy*

Yet there are consumers who try to limit the number of loyalty programs they sign up for in a *meek* attempt to protect their private information (I use the adjective “meek” since they still subscribe to some programs).

Hannah (F, 30 yrs, BSc, CAD 60,000): I personally don't like to give out like too much information. Like I'll give out information to the stores I like I [and] I really shop at like often. But if it's like a place I don't go to that often, and I don't . . . I don't know . . . I don't give my information for that.

Olga (F, 22 yrs, university, CAD 65,000): I don't want my information to be everywhere on the internet. But I only delete the account if I know I am not shopping there anymore. So, I tried to like minimize the amount of personal information that [I] give to the store.

It is worth noting that although for those two informants not frequenting a specific store is part of the reason why they do not sign up for loyalty programs, their main concern is protecting their

privacy (in contrast to the informants quoted under the above “Not enough shopping” section who had no privacy concerns).

To sum up, retailers can try targeting the market segments beyond the reach of their loyalty programs, for example, consumers with low annual incomes, infrequent shoppers, and older consumers. Retailers also need to address consumers’ concerns about receiving too much marketing correspondence and privacy (especially amongst young consumers). Looking at the survey and interview data, it is apparent that to the consumers signing up for loyalty schemes, privacy concerns are not a very powerful disincentive compared with perceived benefits, or alternatively that consumers are in denial. Moreover, while young consumers are inclined to sign up for more loyalty programs, they are also more prone to feeling uncomfortable when providing their personal information. It is worth remembering that unlike other means of consumer surveillance, in loyalty schemes, the consumer is a willing participant and is, therefore, complicit in the use of individual data and any compromise of privacy (Smith & Sparks, 2003). This makes loyalty programs a combination of overt and covert surveillance, for consumers have to accept being part of them even though they might not be aware of the full scope of the programs’ surveillance outreach.

(7) Tagging

This section looks at consumers’ behavioural and affective reactions when setting off tagging alarms (specifically false alarms). This part of the study is a continuation of the previous studies by Dawson (1993), Handford (1994) and Bonfanti (2014), and it also provides more in-depth discussion related to Margulis et al.’s (2019) model of consumer reactions to ubiquitous technology in general, and RFID in particular, which showed seven factors that can influence

consumer reactions, including privacy and security expectancies and previous experience with technology. At the end of his 2014 paper on how to make store surveillance secure and appealing to shoppers, Bonfanti called for future research that would complement his study on retailers' perspective by making a direct analysis of customers/shoppers since "it would be useful to determine the customers' point of view for purposes of comparison." This section on tagging, therefore, is built on how both consumers and retail workers think about tagging as a retailance system.

As mentioned earlier, 88.87% of informants indicated that they were aware of the presence of tagging as a retailance system in stores, an awareness that has significant statistical associations with both age (with consumers aged sixty-five or older the most aware) and income level (with consumers earning USD 77,000 and over the most aware). To find out consumers' behavioural reaction after triggering a false tagging alarm, informants were asked to rank the impact of and their (expected) reactions towards experiencing a false tagging alarm. A nonparametric Friedman test of differences among related measures was conducted and rendered a chi-square value of 1179.321 (4, $N = 577$) which was significant ($p < .001$). Informants' choices were (with 1 being the top choice): (1) "I would never shop at the store again" (mean rank 4.64); (2) "I would shop less at the store in the future" (mean rank of 3.58); (3) "I would expect an explanation and apology from the store manager" (mean rank of 2.75); (4) "I would expect an explanation and apology from the store employee" (mean rank 2.2); and (5) "I would not be bothered; I accept that stores need to prevent shoplifting" (mean rank 1.82). This shows that the majority of consumers tend to avoid the store where they experienced a false tagging alarm more than wanting to get an apology from the store employee or manager. For example, during the interviews, Ashley, an American in her early forties, hypothesized that "if it happened

at the same store more than once, then definitely, I wouldn't want to go back.” This result is opposite to Dawson’s (1993) who came to the conclusion that most consumers who set off the EAS alarm would expect an explanation and apology from store manager (74%) rather than shopping less at the store in the future (38%) and never shopping at the store again (16%). Retailers, therefore, should be aware that consumers nowadays are not very forgiving when they experience triggering a false tagging alarm which might jeopardize their future shopping habits (i.e., choosing another retailer).

During the interviews, informants (both retail workers and consumers) were asked about their affective and behavioural reactions after a false tagging alarm is set off. Figure 73 (based on the survey and interview data) shows informants’ different reactions.

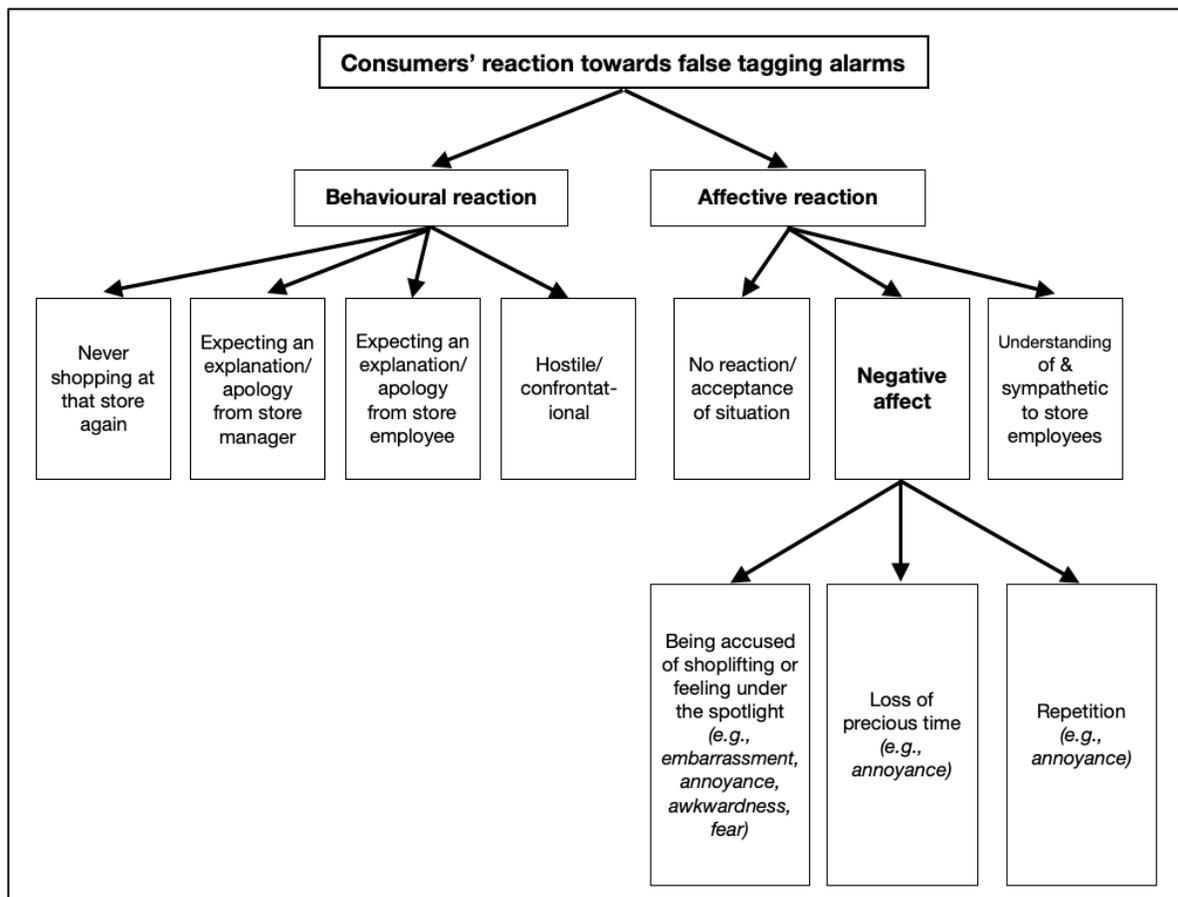


Figure 73 – Consumers’ reaction towards triggering a false tagging alarm

7.1 No reaction/acceptance of situation

Consumers conveyed a different range of emotions (both negative and positive) when describing real and hypothetical situations in which they triggered a false tagging alarm. Some consumers are not bothered since they know they have done nothing wrong (i.e., shoplifting or forgetting to pay for an item before leaving the store).

Wang Fang (30 yrs, CAD 6,000): I'm fine with it. I'm fine with it since I've never done anything wrong. I know nothing will happen on me, even though the alarm went off, nothing will happen on me.

7.2 Negative affect

The following quotes re-affirm previous research that many consumers experience negative affectivity when triggering a false tagging alarm. For example, Handford's research (1994) concluded that EAS is not perceived by the public as a threat although it might make them feel irate, upset, uncomfortable or embarrassed for being viewed as likely thieves when they are stopped because an alarm system has been triggered by non-deactivated security tags (due to technical failures or unprofessional staff). When describing their actual and hypothetical experiences, interviewees used words like "embarrassed; nuisance; moment of fear; worried; awkward" to describe their experience. I underlined the words describing negative affect for emphasis in the quotes below.

Jessica (late 30s, CAD 30,000): I might avoid the store for a little while. Probably for this a little bit because I'd still be embarrassed about the situation.

David (mid 40s, USD 35,000): There's no anxiety really there. It's just an annoyance really, I understand things like that happen once in a while. So, it's not really a problem.

Matthew (30 yrs, USD 25,000): Of course, it draws unwanted attention to me for a reason that, you know, people are having suspicions about me and my character

in that way. [If] it was just the alarm going off as I'm walking out and nothing happens, they just wave at me, or whatever, I'd be okay going back.

Janani (35 yrs, undisclosed income): I feel bad. But still, like as long as I know that I paid for it, I don't mind it much. I just go back. [But] everybody like turn around and look at you like in their head, "She's stealing something?" That matters to me. But as long as like camera wise they know "Okay, she paid and then she's going outside and it . . .," so I don't mind that. But I'm not happy [when] everyone like stare at you.

Olivia (20 yrs, CAD 200,000): It's always a little bit awkward, but I personally know that there's nothing on me. So, I'm always happy to stop and wait and see if someone wants to check my bag or purchases. It's awkward, but again, like I know I haven't done anything wrong. So, I'm not like scared or worried or anything.

Mitig (20 yrs, CAD 20,000): It was a little embarrassing at the start, but I felt reassured quite quickly that they would take care of it. And thankfully, there I wasn't treated like I stole. Like they immediately treated it like it was a mistake on their part. Which I was very glad about because it could have definitely gone the other way. Like they really had two options: to assume that it was a mistake on their part, or to assume that I stole it. And I was glad that it was the first option.

Some informants talked about how false tagging alarms are usually the result of an unintentional "human mistake."

Sarah (late 20s, CAD 63,000): Well, sometimes there's like a very relaxed feeling about it, like, "Oh, just go ahead. This thing beeps all the time." There's no check of my bag or anything. But there have also been instances where I go back to the cash, they take off the tag, or they asked to see my receipt or proof of payment. But most of the time, there's like little to no reaction. But yeah, [there's] like a moment of fear, even though I know I didn't do anything wrong. I would go again [to the same store]. Because, I mean, it's an honest mistake. It's a human mistake.

For some consumers, in addition to understanding that this is an unintentional mistake on the part of the retail employee (such as over-worked cashiers), the repetition of that experience actually lessens their sense of discomfort.

Maria (early 40s, USD 36,000): Oh yeah, it's happened and it's embarrassing, but most people just look for a second. They get over it because it's happened to them too. So, he [retail worker] just walked back and [I] show them the receipt. "Oh, I'm so sorry. And I'll just take it off." And that's it. The first time it happened was really embarrassing. I was just looking around, like, "Oh my god! I swear I didn't

steal anything.” I used to steal things in middle school. I don't anymore. I'm more responsible now. But I mean it's like buying tampons at the store, you know. At first, you're terrified of it and you're like, “Well, this isn't really for me.” But after a while, you realize this happens all the time, every day, nobody cares. I mean these are human beings that are working behind that register, especially if it's really busy and there's a line of people trying to check out. It's going to happen and it's okay. They don't make enough money for me to yell at them for it. It's just a human mistake, it happens.

Describing the experience from their side, retail workers have expressed that forgetting to remove a tag is common, especially during busy holiday seasons like Christmas.

Robert (40 yrs, CAD 40,000): For me, when I have the customer sales [at Roots], [customers] say, “You forgot to take this off.” I apologize and say, “I'm sorry.” I was rushing or trying to get other stuff done at the same time and I just forgot. And majority of the customers that I've forgotten to take off a tag, they were very sympathetic. They weren't angry. They weren't upset. They weren't rude in any way. They were just like, “Okay, stuff happens.”

Wang Fang (30 yrs, CAD 6,000): I've had customers come in, like, yell. Like it's never happened to me at Coach [Outlet store], but at Banana Republic, I worked as a cashier supervisor with a whole bunch of other people. And usually, they were all high school students. And so, like if someone forgot to take a tag out, the customer would come to me and like they complain, and I'd be like, “Okay, let me just take off the tag and you can be on your way.” Like I don't know what the big deal [is]. They'd be like, “How dare you? Like we didn't steal.” and I'm like, “Okay, like someone made a mistake. Like it happens. Like calm the fuck down. Like I'll just take it out.” But it's rare that people get angry about that. Usually, they're pretty understanding.

To Myint, working in the theatre industry has allowed her to have a different reaction, for she is used to being under the spotlight:

Myint (early 30s, CAD 125,000): I'm sort of in the minority there where I'm used to everyone looking at me when I'm at work. So, the alarm going off and everyone looking at me, that doesn't really bother me. Because if the alarm went off, I wouldn't try to leave the store. I'd go right back to the cashier that I was just chatting with and be like, “Ah, something went wrong here.”

To summarize, when confronted with a false tagging alarm, many consumers experience negative emotions (e.g., embarrassment, annoyance, unwanted attention, unhappiness, “bad” feelings, awkwardness, or moment of fear). Some consumers, however, are more understanding

and sympathetic, a “learned” response that is a result of either having a retail work experience or being repeatedly exposed to that situation (i.e., learning that there are no repercussions from false tagging alarms).

7.3 Loss of precious time

To many, the annoyance resulting from tagging alarms is not about being under the spotlight inside the store when the alarm goes off, rather, it is discovering that the tags were not removed after leaving the store (whether at home or when they set off an alarm at a different store), for that means scheduling another visit to the store to have the tag removed.

Mary (60s, USD 50,000): It happened at Ross Dress for Less [in the U.S.], both setting up an alarm and getting home and finding I still had this security thing attached to my item. And I had to take it back. That was very annoying, and it cost me time, but I have no problem getting them to remove it.

Jennifer (50 yrs, USD 99,000): It's no big deal. I think I've only had it once that I got all the way home. A dress had something on there, so I had to go back. Like that was it. I mean [it's] not the end of the world, but a little frustrating. Just because it's another trip back, but . . . accidents happen. So, I guess if I was stealing it, yes, it would be embarrassing. But since I know that I've done everything right, I don't have a problem with it.

Although Zahra has an insider's perspective (which means triggering a false tagging alarm is not embarrassing for her), when thinking about a hypothetical situation, she still expressed feelings of frustration when it comes to losing time just to go back and remove the tag.

Zahra (early 40s, CAD 160,000): It's annoying for the customer and for the store crew, both at the same time, you know, to check everything and figure it out. Check the receipt. Check the item. But it happens. I never felt embarrassed, maybe because I was in the situation of selling and I know that it's normal. I've never been embarrassed. But sometimes, if I'm in a big mall, and this store is at the very other end of the mall and I'm here, I feel like “Aghhh, I don't want to go the whole way” to like deactivate the tag. I was lucky. I never had a hard tag left. It was always a soft tag and I don't bother to go back for a soft tag. Yeah, I just cut it [soft tag] because most of the time it's in the washing instruction or just it's taped at the bottom of the box, so it's easy to remove it. I never had a hard tag left on it. But if it's a hard tag, definitely I have to go on, get it removed. But I never felt embarrassed.

Thus, while some consumers are not embarrassed about triggering a false tagging alarm, losing time by going back to the store to remove the tag becomes a source of frustration.

7.4 Repetition leading to negative affect

One of the reasons behind consumers feeling annoyed is when the alarm is repeatedly set off because of the same product or for any other reason.

Emma (34, yrs, CAD 60,000): There was one time in the past where I'm not sure why this was happening, but every store that I walked in or out of, the alarm would go off. And I feel like there was some kind of a magnet in my purse that I couldn't find at the time, and it was driving me crazy. And in that case, it was embarrassing because it was literally every single store I walked in or out of, and it was getting very annoying.

In the case of Ishita, making a distinction between whose mistake it is helps her to feel less embarrassed.

Ishita (early 20s, CAD 150,000): I used to have a jacket that would always beep no matter what, I would be very embarrassed because I was like, I know I didn't steal anything, but I don't want anyone to think that I did. But I would generally just walk away. No one would ever say anything. Maybe once or twice people have stopped to just be like, "Oh, we just want to make sure that you haven't taken anything." But in general, if it's an item that I have that constantly beeps, I'm more embarrassed. But if it's something that was a mistake, from the cashier or something, I don't mind. I just go back to [the store].

Zahra recalls that some of the "funniest stories" that happened when she was working as a salesperson in Winners and the Hudson's Bay were related to those alarms and how they annoyed consumers.

Zahra (early 40s, CAD 160,000): Most of the old people here in Canada they do hip replacement. And if the hip is made of metal, not composite, it will beep at the store. So, there was a old lady and a old man, they were shopping and every time they get close to the gate, it was beeping. As a person who is selling, I have to approach them and say, "Hey, can I see your bag. I can help you to remove the tag or deactivate the tag." Five times. And then at the end, the old lady was so miserable and annoyed. Like, "This is my hip that is beeping. I know. It happens in every store." That was my first time finding that. I have to go do some Google

search. So, what is this? And yeah, poor lady, she had this problem in many stores, which is really annoying. See, it was very unique situation and, you know, as a person when you deal with something like this. You want to laugh but it's rude. I like “Okay, I'm just sorry. Okay, I'm not getting close to you anymore, asking for your bag. I'm so sorry.” [Laughs].

While the tagging alarm does not personally bother him, Robert recounts how it is sometimes an extremely embarrassing experience for his wife:

Robert (40 yrs, CAD 40,000): But for my wife, it's happened, but of course they forgot to like de-magnetise the tags in her bras. Because I know like Victoria's Secret and some of The Bay and everything, they have a sewn in magnetic tags. And of course, she feels embarrassed because, you know, they forgot to do this at the store. So, on occasion, she would wear a bra or something, and it would go off. And she's not even like carrying anything and it would just go off because of the tag in the bra.

To sum up, some consumers feel annoyed and/or embarrassed not because the tagging alarm sets off, but because this happens repeatedly. To some consumers, the incident becomes more tolerable if it is a result of the retail employee's mistake.

7.5 Fighting back

To James, a retired white American lawyer in his 70s, he sees tagging alarms setting off as confrontational situations in which he refuses to be intimidated.

James (70s, USD 14,000): I just keep walking. I think once or twice, I've been asked [if they can] look at [my] receipt and I told them “no.” They're not pleased. They can't do anything to you. I don't worry about it. I don't let them intimidate me. Remember, one of my careers was law, so I certainly know my rights and I don't let people push me around.

Compared to other informants' responses, James' reaction to tagging is quite hostile and confrontational.

7.6 Racial discrimination

Although there were no statistically significant associations between membership in a minority group and the awareness of tagging as a retailance system (discussed earlier), a few interviewees spoke strongly about how they saw the impact of racial discrimination after false

tagging alarms in the store. This shows that while that problem is thankfully not a common occurrence in retail, it is not totally eradicated.

Michael, a Black American male engineer in his late 40s whose annual income is over US\$100,000, described how bad his experiences with tagging alarms were since he is usually a focus of retaillance as a result of racial discrimination, a situation that he is increasingly avoiding by relying more on online shopping.

Michael [Black American]: It has been a situation where it [tag] hasn't totally been deactivated. I generally don't like those situations because there's always the assumption that you stole it from a racial bias standpoint. But I just know that happens, it can happen because it's sometimes this thing is faulty. And I just kind of deal with it. I would look for other alternatives to some degree, it will make the experience to where if I had another alternative, I might go to somewhere else, and like I kind of told you before, if I could probably find it online, and I don't have to generally avoid that situation, and I think that I would do that.

Other non-minorities (i.e., white) interviewees reflected on the impact of racial discrimination when it comes to tagging alarms:

Mary [white American]: I would think that probably my reaction is based on being an older and somewhat affluent-looking white lady. So, I think if I was a younger person or if I was a minority person, that that might expose me to some pretty bad stuff, even though I could still prove I paid for it

Rachel [white Canadian]: Most people have been nice about it. I think part of that might be because I am a nice young white female which is awful. But it's the sad reality of it. People are normally pretty nice about it, even when it beeps when I leave a store. It's never a problem. It's always, "Oh, I just want to make sure we didn't do this." I've never felt the blame for it, but I can only imagine what some people go through. It's terrible.

The above interviews were conducted in the Summer and Fall following the murder of George Floyd and the subsequent Black Lives Matter worldwide protests³⁵. However, what informants

³⁵ On May 25, 2020, George Floyd, a 46-year-old black man, was murdered in Minneapolis, Minnesota, United States, while being arrested on suspicion of using a counterfeit \$20 bill. Floyd's murder led to worldwide protests against police brutality, police racism, and lack of police accountability. The protests also supported Black Lives Matter (McLaughlin, 2020).

talked about was systematic racial discrimination and not just an aftermath of an external environmental influence (i.e., Floyd's murder). Marketers and retailers, therefore, should be aware of the fact that that retailance has the capacity to discriminate among consumers with visible differences (e.g., racial), an impact that is also noticeable to non-minority (i.e., white) consumers; therefore, such discrimination could negatively affect how consumers view the retailer (i.e., brand image) and trust it.

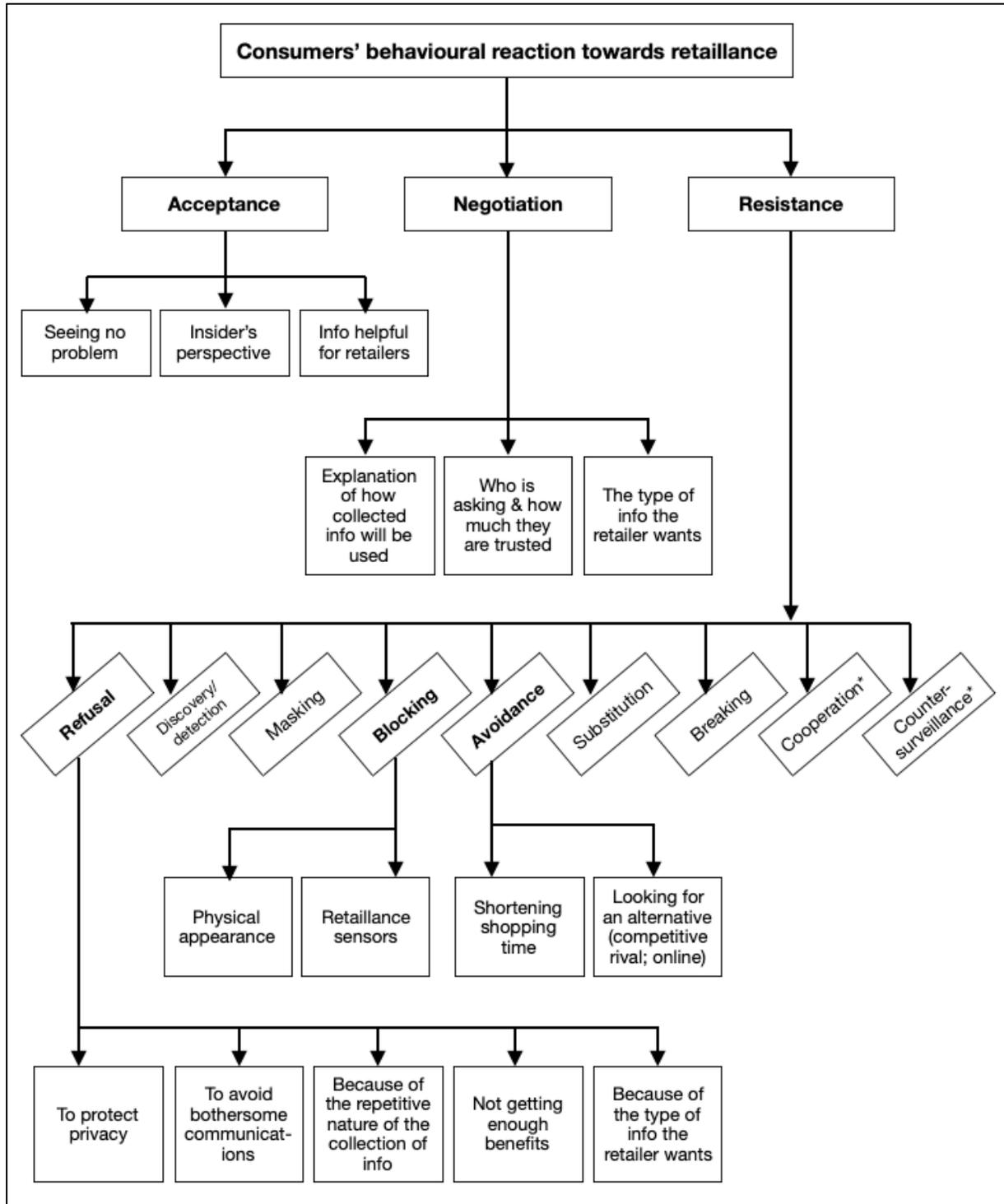
When it comes to the use of tagging as a retailance system, retailers should be aware that although EAS (Electronic Article Surveillance) represents a cost effective substitution of technology (i.e., a mediated technology channel) for people (i.e., a direct retailance channel) when it comes to shoplifting prevention and detection (Dawson, 1993), poor implementation (e.g., when store personnel causes false alarms, or when its usage is combined with racial discrimination) can negatively impact store customers. To avoid any negative repercussions to the retail store, retail personnel should be well trained in handling the tags and avoiding discrimination of all types, and when a tag is falsely set off, they need to apologize to the consumer and try to alleviate their feelings of embarrassment and annoyance.

To sum up the above section on consumers' awareness of the different retailance systems, consumers are generally aware of the presence of at least traditional overt retailance systems, however, many of them are not knowledgeable about the scope of such retailance or the new advances in this field. Consumers are less knowledgeable about the laws and regulations that are there to protect their privacy and many conveyed their doubts of the effectiveness of such protection. Feeling that the law is usually a step behind technological advances, many admitted that they do not bother to read the long and complex retail privacy policies before signing away their acceptance of the terms. The impact of such beliefs could be traced in

consumers' reactions towards the common retailance systems employed in brick-and-mortar stores: the tracking of their purchases, the selling of their personal and consumption information to third parties, loyalty programs, and tagging.

Second: Consumers' behavioural outcomes

Behaviour is described as “actions, consciously intended or not, that [individuals] engage in” (Hulland & Houston, 2021, p. 438). Once consumers are aware of retailance (which could be either covert or overt) or they are asked to provide their information, they show a behavioural reaction. Based on the literature review and the analysis of collected data, this behavioural reaction could be divided into: acceptance, negotiation, and resistance (Figure 74).



*Topics not covered in this research.

Figure 74 – Consumers' behavioural reaction towards retailance

(1) Acceptance

Some consumers willingly accept retailance. This willingness falls under what Gary T. Marx (2016) described as “behavioural compliance.” It is interesting that when talking about retailance, most interviewees focused on the collection of personal information and not on the physical retailance systems (maybe because they have no say in having those systems installed or removed). This “self-disclosure” of one’s information is defined by Aiello et al. (2020) as the “voluntary communication of personal information such as one’s name, preferences, and demographics to one or more recipients.”

1.1 Seeing no problem

Some informants declared that they accept retailance because they see no problem in the retailer collecting their information.

Michael: No, I haven't really done anything like that [resisting surveillance]. And I've never been against anything in terms of that because . . . I don't mind giving my numbers of as part of rewards program.

Jason: My cell number I give it all the time whenever they ask and that's not a problem.

Another informant who accepts retailance willingly is Matthew who considers himself “a very open person.”

1.2 Insider's perspective

Myint does not resist surveillance for two reasons: first, “because of living with a data analyst,” which gives her an insider’s perspective, and second, because of her work as a founder and member of a theatre company:

Myint: I know what generally what it's [collected data] being used for. I mean I run a business too. We get feedback from our audience members. That feedback and those demographic breakdowns, and where they came from, how the marketing worked, where they heard about it. Those things are . . . valuable. More precious than anything. So, I know how useful those things are to a business. And

I think if they take my information and tag it to my receipt, and they send me a personalized ad of things on sale that I want to buy based on past things I have bought, great. That's the benefit to me. And if they just use it to improve their business, great. That's also good.

1.3 Information helpful for retailers

Some interview informants revealed that they can self-disclose some of their personal information if it will help the retailer.

Zahra (MSc): I'm always okay to give the postal code because postal code is usually for their collecting information to see where their shoppers are coming from. It's usually helpful with opening new stores³⁶.

To summarize, when it comes to self-disclosing their personal information (an act that conveys consumers' acceptance of retailance), consumers do that because they see no problem in the retailer's collection of their information, they have an insider's perspective of how retailance (specifically data analysis) work, or they believe the collected information will be helpful to the retailers.

(2) Negotiation

Some consumers' willingness to self-disclose their personal information is contingent on different factors: (1) receiving an explanation of how their information would be used; (2) which retailer asks for the information; (3) how much they trust that retailer; and (4) what type of information they are asked to share.

To accept disclosing their personal information, what some consumers need is to simply receive as an explanation of how their collected information will be used.

³⁶ Retailers (such as IKEA, LCBO and Walmart) claim that they collect postal code information to fine-tune services, such as product selection, for flyer distribution accuracy, and deciding where to put new stores. However, retailers can also use postal code information to compile personalized mailing lists that can be sold or shared (Kopun, 2013).

Taiba: For a long time, Walmart was moving into a different location and they always wanted our postal code. And they kept asking for postal code or zip code. And I asked them, “Why do you need it?” because every time we come in, they asked us where we live. So, the employee explained to me that because they want to move their location, they want to see where the customers come from. When this was explained, I always try to give my postal code. When it came to email, I also asked, “Why do you need my email?” . . . I probably would never give a false email address; I wouldn't be able to make it. Especially when you're right in the moment. But yes, I did ask question, “Why do you need my email?” Just because sometimes I do get emails that are going my spam or like, let's say, they're not something I want to look at.

Although Christopher does not like sharing all types of personal information, he believes that self-disclosure is “not a big deal” because of the “kind of world” we live in today.

Christopher: So, there is certain personal information I'm willing to share and certain information I'm not. Like I feel like at this point that if somebody really wanted to, they could probably get my email and phone number anyway, so I'm usually pretty likely to share those. I don't really like sharing my last name. If I don't need to. And then it just kind of escalates. From there, where it's like I am not going to give you anything related to my social security number. Unless it's like the last four digits. And it's like a banking thing with an institution that I have trust in and things like that. So, there's definitely a scale where it's like . . . What I'm willing to share is just because I understand that this is kind of the world we're in now and this information is probably being shared regardless, so it's not a big deal.

Christopher, therefore, is a representative of the consumers who accept retailance and share their information, not because he sees no problems with retailance or has an insider's perspective (i.e., unlike the consumers who “willingly” accept retailance), but because this is the “kind of the world we're in now” and his information will be end up being shared regardless of how he feels about retailance. However, Christopher's resigned acceptance is contingent on who is asking and how much he trusts them (e.g., a banking institution he trusts) and what type of information they want (e.g., his first versus last name). Looking at the 2019 Deloitte U.S. survey (Sides et al., 2019) which indicated that “only 5 percent of consumers place the retail industry at the top in ensuring data privacy, compared to 63 percent for banking,” it is evident that retailers

need to reassure their consumers that they are trustworthy of protecting the latter's data. Lyon (2007, pp. 165–166) reasons that when compliance is questioned, some sort of negotiation takes place, and surveillance becomes dynamic and amenable to modification, for example, leading to updated and/or new privacy laws.

(3) Resistance

From a critical marketing perspective, the conflict between understanding and distrust is a form of resistance, a power struggle between consumer and retailer. As discussed earlier, there are nine types of resistance that consumers can carry out inside a retail store, and they are: (1) refusal, (2) discovery/detection, (3) masking, (4) blocking, (5) avoidance, (6) substitution, (7) breaking, (8) cooperation, and (9) counter-surveillance. The first seven types are discussed in more detail below. Only the last two types of resistance were not included in the interview and survey questions: cooperation (which is resisting retailance by colluding with surveillants, or employees working in retail security providing insider information and/or access to restricted areas to consumers/violators) and counter-surveillance (when the consumer starts surveilling the retailer); to collect this data, different groups should be targeted (for example, prior offenders and activists) which is beyond the scope of this research.

3.1 Refusal

Refusal is when a consumer says “no” when asked to disclose their personal information or to participate in a survey run by the store. Informants were asked to answer four dichotomous yes/no questions: (1) The first question asked generally about providing their personal information, “I refuse to give information to a retail business because I think it is not needed.” (2) The second question (“When a cashier asks for my postal/zip code, I refuse to give it and still

make the purchase”) asked about a specific type of information requested by retailers; the “postal/zip code” was chosen as an example of personal information that does not threaten the consumer’s sense of privacy (since they apply to a group of households compared to “date of birth” which is specific to the individual). (3) The third question was concerned with what happens to the collected information; “I asked a retail business not to sell my name and address to another retailer.” (4) The fourth question (“I asked a retail business to remove me from the lists it uses for marketing”) looked at the possibility of consumers taking more action and asking to control where their information goes.

Looking at the data (Figure 75), 51.8% of informants said they refuse to self-disclose their personal information in the retail store when they think it is not needed. When compared to the survey of Canadians on privacy-related issues (Office of the Privacy Commissioner of Canada, 2019), in which 76% of Canadians (and more likely those 35-54 years of age and with a post-secondary education) admitted to refusing to provide an organization or business with personal information, we can deduce that a higher percentage of individuals agree to self-disclose their personal information to retailers compared to organizations or other types of business. This refusal number (51.8%) went down to 29.3% when it came to giving their postal code (indicating that to consumers, postal code information is considered not as privacy invasive as other personal information). Only 26.9% specifically ask retailers not to sell their information to third parties; this is a much lower percentage than that published in the 2006 GDP survey (Pridmore, 2010) which stated that 66% of respondents in Canada and 73% in the U.S. have requested that their name and address not be sold to another company. There could be two reasons for such a difference, first, the GDP survey was on privacy in general and not just focused on the retail sector (which could indicate that retailers’ sharing their customers’

information is not trusted when compared to other sectors and institutions); second, there is a time difference of fifteen years between the two surveys (which could indicate that consumers are more weary with the selling of their personal information compared to before). When asked whether they have asked a retailer (at least once) to be removed from the marketing lists, 48% said yes. In the 2006 GDP survey (Pridmore, 2010), 71% of Canadian participants and 77% of those in the U.S. indicated that they have asked to be removed from a company's marketing list. This difference in percentages (from 48% to 77%) may indicate that consumers are more accepting of marketing communications when it comes from retailers. There is no evidence that demographic differences influence consumers' resistance to retailance. A chi-square test (Table 19) showed that the only statistically significant associations were between the level of education and both the relinquishing of postal/zip code information ($X^2(6, N = 593) = 12.745, p = .047$) and asking to be removed from marketing lists ($X^2(6, N = 591) = 12.665, p = .049$); the level of education was found to be positively correlated with consumer refusal to provide their postal/zip code, for the higher the level of education is, the higher the percentage of refusal is (Table 20 and Figure 76).

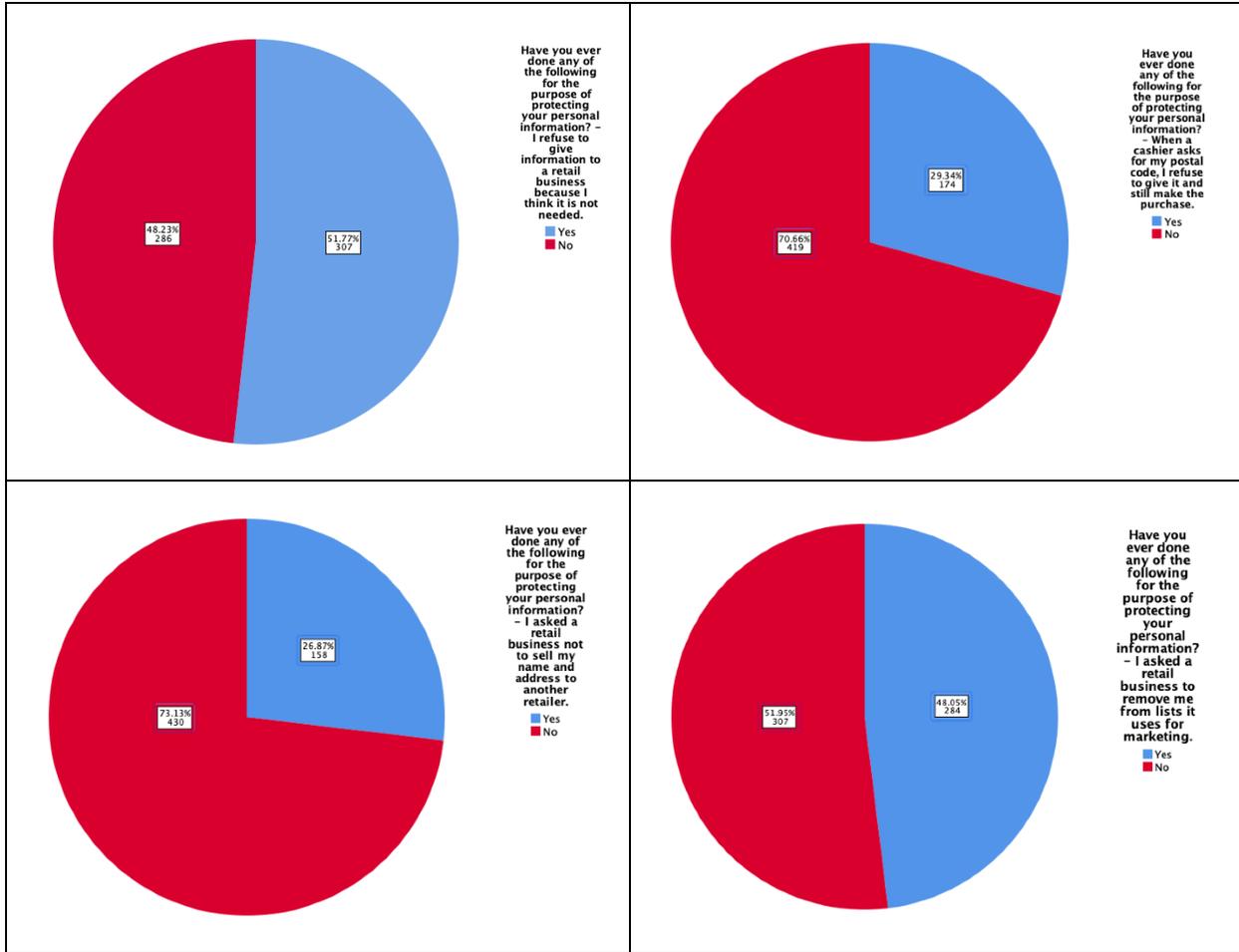


Figure 75 – Survey informants’ resistance to retailance

Refusal of retailance survey question	Chi-Square test																			
	Gender				Age				Education				Income (U.S.A.)				Minority			
	X^2	df	N	p	X^2	df	N	p	X^2	df	N	p	X^2	df	N	p	X^2	df	N	p
I refuse to give information to a retail business because I think it is not needed.	4.176	3	593	.243	8.772	6	593	.190	2.799	6	593	.834	2.514	6	582	.867	.303	2	101	.859
When a cashier asks for my postal/zip code, I refuse to give it and still make the purchase.	3.524	3	593	.318	6.480	6	593	.372	12.745	6	593	.047	2.699	6	582	.846	3.809	2	101	.149
I asked a retail business not to sell my name and address to another retailer.	2.893	3	588	.408	3.763	6	588	.695	9.261	6	588	.159	7.399	6	577	.286	.432	2	99	.806
I asked a retail business to remove me from lists it uses for marketing.	4.082	3	591	.253	11.237	6	591	.081	12.665	6	591	.049	5.565	6	580	.474	.317	2	100	.853

Table 19 – Chi-square test results of informants' refusal of retailance with the statistically significant associations in red

Education level	Refusal to give postal/zip code	Asking to be removed from marketing lists
High school (n = 152)	20.4%	44.7%
College diploma (n = 68)	25%	35.3%
Enrolled in a bachelor's degree (n = 18)	27.8%	44.4%
Bachelor's (n = 273)	32.6%	49.5%
Graduate (Master's & Doctorate) (n = 74)	39.19%	63.8%

Table 20 – The correlation between education and refusal of retailance, with the highest percentage under each category in red

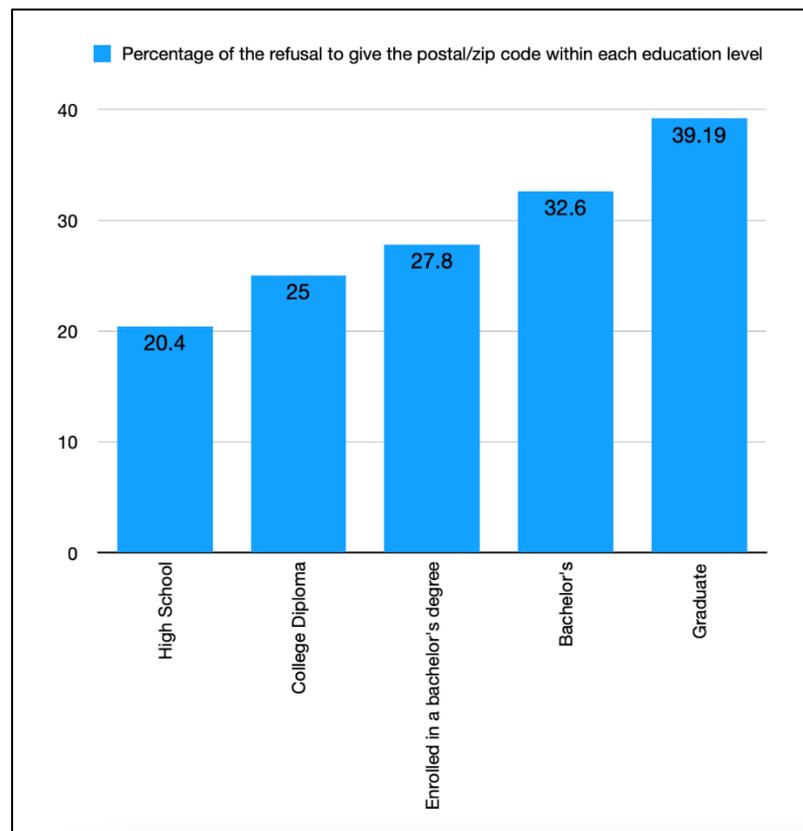


Figure 76 – The correlation between consumers' level of education and their refusal to give their postal/zip code

To learn more about the reasons behind consumers' refusal to give away their personal information, interview informants were asked whether they had ever resisted retailance and how. Analysing the interview data, five reasons for refusal emerged: (1) refusal of the concept of surveillance in general; (2) to avoid bothersome communications; (3) because of the repetitive

nature of the collection of information; (4) because they are not getting enough benefits: and (5) because of the type of information being collected.

3.1.1 Refusal of surveillance

Some consumers outright refuse to disclose their personal information out of principle (they want to protect their privacy).

For example, James (PhD) said, “Oh, I just tell them no. They don't need my phone number.” In some situations, this refusal can lead to frustrating emotions for both consumers and retail workers. For example, as a consumer, Emma understands how frustrating it can get when she is pressured to give away her personal information:

Emma (HS): In the past, when I've gone to Rexall or something like that, sometimes the cashiers can be really pushy about getting you to take their loyalty card if you don't have one. That's the only time where I've gotten kind of annoyed because it's like, “Take it,” I'm like, “Okay, but I don't need it. And I don't want to take it.” They're like, “No, yeah, we just need to give it to you and just take it.” . . . It's excessive. And I'm sure they're pressured to do that and pressured to get your email and your information for that. But it's just that is kind of over [the top]. I think that [a] customer should have the choice whether they want to be giving their information and not be pressured to do so.

At the same time, as a retail manager of a wireless provider, Emma needs to collect her customers' personal information so that it can be used as an authentication step when accessing their accounts, when they refuse, she can only provide them with basic service which further exasperates them:

Emma (HS): We do have some customers that get really upset when we do ask them because they don't understand why we need it for simple transactions and stuff like that. But most people are generally great with that. But we do get a few that don't understand it or they start picking arguments because of it . . . [Those who refuse] I can give them general information, nothing private about their accounts, but say like if they were coming to get a cell phone plan, I couldn't tell them anything about their account, but I could tell them, “Hey, this is what's in [the] market.” Other than that, I wouldn't be able to like do any transactions for them that day.

Retailers, therefore, need to tread carefully when trying to convince consumers to disclose their information, keeping in mind whether providing their full services is contingent on receiving that information or not.

3.1.2 To avoid bothersome communications

Other consumers refuse to disclose their information in an attempt to avoid what they consider bothersome communications (e.g., marketing emails) from the retailer. They, therefore, refuse the result of retailance and not the idea of it.

Sarah (MA): Yeah, I've definitely not given my personal information when they've asked or asked them what they need it for. And then they're like, "Oh, it's so you can subscribe to our newsletter." Like, I don't want your newsletter. I have enough things in my inbox.

Olga (undergraduate): So usually, when I leave the checkout, and the cashier asked me, like if I would like to receive emails from the store to know more about the sales and everything, I usually like just because they tried to be polite, I say "Thank you. I'm already subscribed." . . . sometimes I say that [even when I'm not subscribed].

While Zahra has no problem when it comes to retailance itself, she refuses to provide her email address so that she does not receive "marketing gimmicks" from retailers that she does not frequent.

Zahra (MSc): It happens a lot that I don't give my email, not because of the surveillance, just because they're not my frequent shopping spots and I don't want to receive their marketing gimmicks.

3.1.3 Because of the repetitive nature of the collection of information

Some consumers do not mind giving retail employees their personal information, but they are put off by the repetitive demand for such information.

Jennifer (BA): The only thing that comes to my mind like a Bath and Body Works. Every time I shop there, they asked for my email . . . You know, it's obviously associated with my credit card. I have a rewards thing box that really rewards . . . So there have been times like that. They asked me for an email, but I know that they already have it. So, I say no at that point only because I don't feel

like I need to give it to them every single time because I'm already getting the emails; I already have everything I need. So that's the only time really I probably resist.

Chan (undergraduate): One of the example[s] will be Bath and Body Works, they tend to ask for your postal code and an email all the time. The first time when I shop there, I don't care that I will just give them. And now I'm like, "No, thank you." It's like, you don't need to know where I live. Like I understand what they're doing behind. They are trying to have like a big picture of where their consumers are usually from, or like the age group, or something like that. I just don't find it necessary to ask me every time anymore . . . No, it is more like I get annoyed by that [repetition].

As a retail manager, Emma has noticed that the repetitive demand of customer information does annoy her consumers.

Emma (HS): It really depends on the person. And it really depends on your staff. So, when I first got to my store, I noticed a lot of customers were very weird about me asking for their information because they would say, "Oh, I have been asked this before." And at the time I had thought that it was just them saying that but I started to realize that maybe the staff before that was there weren't the greatest asking for the personal information.

To summarize, some consumers avoid disclosing their information not because they want to protect their privacy, but because they get annoyed by the repetitive nature of being asked to provide that information. Retailers and marketers, therefore, should be aware of the number of times they approach their consumers asking for the latter's personal information, for they do not want to frustrate and alienate them, which can ultimately lead to "avoidance" (another form of retailance resistance discussed later).

3.1.4 Not getting enough benefits

Some consumers refuse to disclose their personal information because they do not believe that giving their information would provide them with a benefit (e.g., they are not frequent shoppers in a particular store, or when they are in a hurry).

Jessica (HS): I haven't given my information, like when they've asked for email address or something like that. I wouldn't give it. Like that's the extent of it, I

suppose. Well, usually it's like a store I know I won't probably spend much in, or I won't go to that often. Or if I'm just in a hurry.

3.1.5 Refusal because of the type of information collected

Earlier, in the section titled “negotiation,” it was explained how some consumers agree to self-disclose their personal information if they deem that type of information acceptable for sharing. However, in other cases, the type of information requested by the retailer leads the consumer to refuse providing it. For example, while consumers were mainly accepting of giving away their postal code (which they do not view as sensitive information) or even their personal email address (since marketing emails can be easily deleted or blocked), many refuse to provide more sensitive personal information that can make marketing communications more difficult to avoid (e.g., their cell phone number), threaten their physical safety (e.g., home address), aid in identity theft (e.g., birthday date), or get monitored at work (e.g., work email address).

Aye (college): Sometimes, they asked me, “Will you like to give me your email address?” I did give them email address. But when they asked my phone number, I never did . . . Because I don't like any call coming through that I don't know. And because sometime, when the call come through, it's a silent number, so I don't know who [is] phoning me . . . Because with email, I look at it and if I don't know [the sender], I can delete it, but with the phone, it will be very annoying because they will come up any other time.

Rachel (MSc): Often, no [I don't give my cell number]. I think emails . . . like I said, I've already got so many of them, it doesn't feel like a big deal, right? It's just one more. I feel like I'm more hesitant to give out my cell phone number. I'm also not asked for that one as frequently.

Janani (MSc): I don't give like all my information, especially I'm not happy giving my birthday [date].

Joshua works at Pet Smart and he is sometimes responsible for signing up people for the store's reward program.

Joshua (undergraduate): If they've already said yes to making an account, typically they're fine with giving [me their] information. But I run into issues sometimes with people giving their email addresses because people work for, like,

government agencies and such. And they can't give it out . . . In that case, I usually just give them a random email, “blah blah blah@gmail.com” kind of thing . . . I'm not supposed to do that but like, I do.

To summarize, 26.9% to 48% of surveyed consumers indicated their refusal to go along with retailance in different situations. Amongst those who refuse, their level of education is positively correlated to their refusal. Looking at the interview data, five reasons behind their potential refusal emerged and they are: (1) to protect their privacy; (2) to avoid bothersome communications; (3) because of the repetitive nature of the collection of information; (4) when they do not get enough benefits; and (5) because of the type of information collected (note that if they accepted to self-disclose because of the type of information, their behavioural reaction becomes one of negotiation and not resistance/refusal).

3.2 Discovery/detection

Discovery, or detection, is when a consumer tries to find out if there is retailance, where the systems are located inside the store, or what type of information is being collected (note that this research focuses on that second theme). Based on the answers, a consumer can behave accordingly (for example, a consumer might decide not to shoplift because there are CCTV cameras). Survey informants were asked to answer three dichotomous yes/no questions. First, when given the statement “I asked a retail business I was shopping at about its policies on the collection of consumer information,” only 17% disclosed that they do ask the retail business they are shopping at about its policies on the collection of consumer information. Answering the statement “I read the online privacy policies at the retail store website when/before making a purchase,” 44% agreed that they read about the store’s privacy policy online when or before making a purchase (whether online before going to the store or during in-person purchases). Replying to the third statement, “I asked a retail business to see what personal info, besides

billing info, it had about me in its records,” 20% chose the “yes” answer. This percentage (20%) is close to the 2006 GDP survey results (Pridmore, 2010) which concluded that consumers (18% in Canada and 24% in the U.S.) rarely ask about what type of information a company has in its consumer records.

Running a chi-square test (Table 21), the only statistically significant associations were found between asking about the type of personal information that the store already has and both age ($X^2(6, N = 591) = 4.464, p = .025$) and belonging to a visible minority ($X^2(2, N = 101) = 10.142, p = .006$). It is not surprising that the older the consumer is, the higher the possibility that they would ask about the nature of the information the retailer has on their records (Table 22), a fact that supports the argument (Nussbaum, 2007) that the younger generations are more complacent when it comes to their privacy (i.e., a disregard of privacy rights that Vaidhyathan (2011) calls “cryptopoticon”). Looking at the answers provided by the 101 informants belonging to a visible minority, 25% of informants who identified as belonging to a visible minority (14 out of 56), 61.54% of indigenous informants (8 out of 13), and 15.63% of informants with a disability (5 out of 32) stated that they ask about their information held by retailers in their records, compared to 33.96% of non-minority (91 out of 268). Although those results should be considered with caution because of the low number of visible minority informants, it is interesting to notice that while 33.96% of non-minority/white (91 out of 268) ask about what personal information is held by retailers, only 25% of visible minority informants ask the same question. Whether this is because racialized minorities (compared to non-minority consumers) try to avoid confrontation or not is a question for future research.

Discovery/detection of retail survey questions	Chi-Square test																			
	Gender				Age				Education				Income (U.S.A.)				Minority			
	X ²	df	N	p	X ²	df	N	p	X ²	df	N	p	X ²	df	N	p	X ²	df	N	p
I asked a retail business I was shopping at about its policies on the collection of consumer information.	2.885	3	591	.410	1.623	6	591	.951	7.425	6	591	.283	9.352	6	580	.155	2.256	2	101	.324
I read the online privacy policies at the retail store website when/before making a purchase.	1.382	3	592	.710	2.472	6	592	.872	6.016	6	592	.421	10.007	6	581	.124	3.525	2	101	.172
I asked a retail business to see what personal info, besides billing info, it had about me in its records.	2.316	3	591	.509	14.464	6	591	.025	4.840	6	591	.565	10.121	6	580	.120	10.142	2	101	.006

Table 21 – Chi-square tests of the informants' discovery/detection of retail, with the statistically significant associations in red

Age	Informants asking to see what personal info the retail store has in its records
18 to 24 (n = 27)	20.4%
25 to 34 (n = 181)	25%
35 to 44 (n = 180)	27.8%
45 to 54 (n = 103)	32.6%
55 to 64 (n = 62)	37.7%
65 or older (n = 35)	60%

Table 22 – The positive correlation between age and discovery of retail

3.3 Masking

Masking is another form of resisting retailance when a consumer intentionally misleads the surveillance mechanism by providing useless information, such as a fake email address. To protect their privacy, consumers have been known to fabricate aliases and misrepresent identifying information (Horne et al., 2007, p. 90). More than one third (39.6%) of the informants confessed to purposefully giving wrong information about themselves to retail stores. As per the chi-square test, there was a statistically significant association between age and purposefully giving incorrect information to the retailer ($X^2(6, N = 593) = 15.152, p = .019$) (Table 23), with the highest category being consumers aged 18 to 24 (55.56%) and the lowest being consumers aged 65 or older (19.44%). There were no statistically significant associations with gender ($X^2(3, N = 593) = 4.275, p = .233$), education level ($X^2(6, N = 593) = 3.185, p = .702$), income level ($X^2(6, N = 582) = 7.027, p = .318$), or membership in a minority group ($X^2(2, N = 101) = 1.698, p = .428$).

Age	Informants asking to see what personal info the retail store has in its records
18 to 24 (n = 27)	55.56%
25 to 34 (n = 181)	40.88%
35 to 44 (n = 180)	43.33%
45 to 54 (n = 104)	41.35%
55 to 64 (n = 62)	29.03%
65 or older (n = 36)	19.44%

Table 23 – The correlation between age and masking, with the highest percentage in red and the lowest in bold black

When asked about masking during the interviews, some of the informants talked about using dummy email addresses.

Mary (60s yrs): I've given an email that I really don't use, I actually set up a dummy account that nobody can trace back to me. I'll give that out.

In general, Mitig does not feel the need to hide from any sort of security or surveillance and has no problem giving her postal code when asked for it. However, that does not extend to her email address; her solution is giving an “old” email address that she set aside for receiving advertisements:

Mitig (20 yrs): I've never been wary to give out my email either because I have . . . like my oldest email, you should give out because that one has more of like the advertisements that go to it.

This shows that when the consumer deems a specific type of information not acceptable for sharing (which is one of the reasons behind “refusal” discussed earlier), instead of bluntly refusing to give that information, they can resort to “masking” or purposefully giving wrong information. In the 2006 GDP survey (Pridmore, 2010), only 20% of respondents in Canada and 22% in the U.S. admitted using dissimulation as a means to protect their privacy. Comparing those numbers with this research survey (in which nearly 40% of informants confessed to purposefully giving wrong information about themselves to retail stores), it is evident that the number of consumers who lie about their information as a protective measure is rising.

Therefore, it is important for marketers and retailers to be aware of the type of information they ask their consumers to provide, for they run the risk of consumers not just withholding that information, but also of deliberately providing the wrong information.

3.4 Blocking

Blocking is when a consumer hides their physical appearance (for example, by wearing clothes that reveal little about their physical appearance) or when a shoplifter blocks the sensors on electronically tagged consumer goods (e.g., by using a metallic shield that prevents signal transmission). This research focused on the first type of blocking, for shoplifting offenders were

not part of the participant pool. Nearly a quarter of informants (22.6%) confessed to wearing clothes that reveal little about their physical appearance when going to the retail stores. No statistically significant associations were discovered with gender ($X^2(3, N = 593) = 3.020, p = .389$), age ($X^2(6, N = 593) = 2.551, p = .863$), education level ($X^2(6, N = 593) = 5.395, p = .494$), income level ($X^2(6, N = 582) = 4.364, p = .628$), or membership in a minority group ($X^2(2, N = 101) = 2.434, p = .296$).

In the interviews, some consumers talked about how concealing oneself is quite futile nowadays because of the level of technology employed in retail systems:

Mary: I never have [covered myself]. And I'll tell you why, I think that if you're obviously trying to conceal yourself, you attract more attention . . . Of course, now that everyone is routinely wearing masks, I think that's kind of interesting, but I know that, for example, iPhones that people use have the facial recognition feature. They modified that so now they can identify you even if you're wearing your protective face mask. So, I'm not quite sure how, you know, how effective covering yourself up is. I mean after all, back before they discovered fingerprints, they used to identify people by their ears because the ears are very unique. Everyone's ears are different.

Ishita: The only thing I can think of is I like to hold my hand over the pin. When you're entering your pin into the credit card because I don't like that. There might be a camera looking or the cashier looking so I cover my hand and then enter my pin. That's the only sort of thing I personally do. I usually do give my emails out, or I don't really dress in a way to hide myself.

After the COVID-19 pandemic hit, some retail workers complained that one of the drawbacks of wearing a mask is that it gives consumers a sense of invisibility, encouraging them to shoplift.

Olivia: So, one of our theories is that with masks on, people know that us figuring out who they are is like less likely . . . I think some of that as well is where our [store] is located. We have a very low-income neighborhood right next door to us and I think a lot of those people have been like really badly affected by loss of income as well. So, we see the people that come in and they steal the perfume because they know they can . . . for the cosmetics, I think it's just a crime of opportunity, like people know they're less likely to be detected when they have the mask.

To summarize, nearly quarter of the informants revealed that they sometimes hide their physical appearance in order to block retailance. Since the COVID-19 pandemic hit, some consumers have been encouraged to shoplift, aided by the partial anonymity the facial masks provide them.

3.5 Avoidance

When confronted with retailance, some consumers either shorten their shopping time (which means less time for browsing and buying products) or passively withdraw from the store and look for an alternative (going to a competitive rival or shopping online). When confronted with retailance (Figure 77 and Table 24), 12.5% of informants chose to shorten their shopping time to avoid retailance, and the chi-square analysis showed that the association between this choice and gender is statistically significant ($X^2(3, N = 592) = 8.206, p = .042$) with 14.43% male (44 out of 305) and 10% female (28 out of 280) reducing their shopping time. Choosing to go to another brick-and-mortar store (i.e., a competitor) are 12.9% of informants; there are statistically significant associations between this choice and both age and membership in a minority group. First, when it comes to age ($X^2(6, N = 591) = 18.538, p = .005$), the highest percentage (25.93%) was reported by the informants aged 18 to 24, and the lowest percentage (1.61%) was reported by the informants aged 55 to 64 (Table 25) which shows that when encountered with retailance, young consumers are more inclined to switch to shopping from a different retail store. Secondly, there is a statistically significant association with membership in a minority group ($X^2(2, N = 100) = 22.382, p < .001$), specifically 8.93% of visible minority informants (5 out of 56) and 58.33% of indigenous informants (7 out of 12), and 6.25% of informants with a disability (2 out of 32). Those results should be considered with caution because of the low number of informants. Compared to the 12.9% who would choose to go to another physical retail store, a much higher percentage, 34.8%, chose to turn to an alternative

shopping format (i.e., online), a choice that (once again) has statistical significance when associated with age ($X^2(6, N = 593) = 13.737, p = .032$) with the highest percentage (around 38%) belonging to informants aged 25 to 44, and the lowest percentage (1.61%) belonging to the informants aged 45 to 54. It is worth mentioning here that because of the COVID-19 pandemic, there has been a shift in consumers' choice of physical versus online shopping due to safety reasons and this may have impacted consumers' responses. The impact of the coronavirus on consumers' acceptance/refusal of retailance is discussed further in the following chapter.

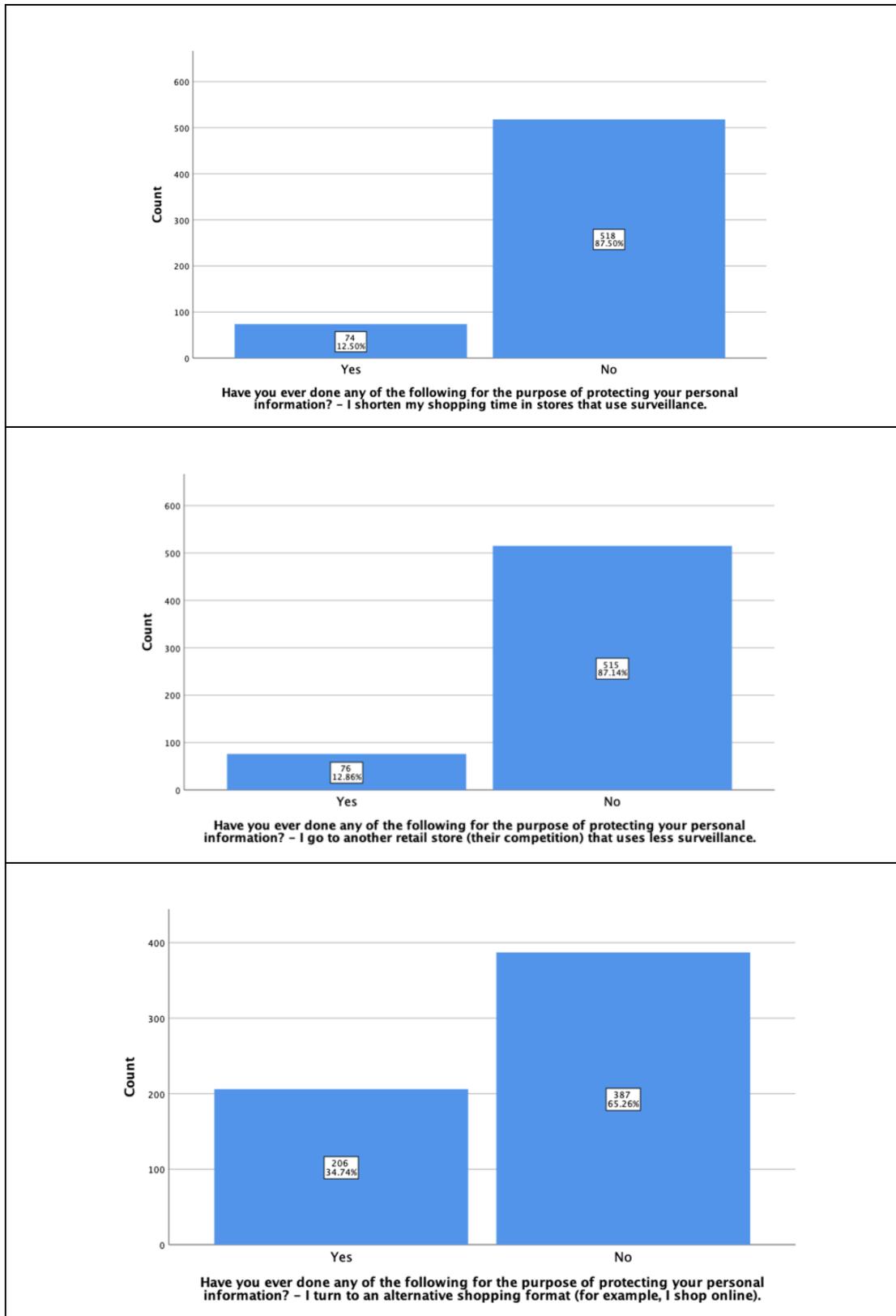


Figure 77 – Informants’ avoidance of retail stores employing retailance

Discovery/detection of retailance survey question	Chi-Square test																			
	Gender				Age				Education				Income (U.S.A.)				Minority			
	X ²	df	N	p	X ²	df	N	p	X ²	df	N	p	X ²	df	N	p	X ²	df	N	p
I shorten my shopping time in stores that use surveillance.	8.206	3	592	.042	6.389	6	592	.381	4.710	6	591	.582	7.252	6	581	.298	2.643	2	101	.267
I go to another retail store (their competition) that uses less surveillance.	5.883	3	591	.117	18.538	6	591	.005	7.936	6	591	.243	6.317	6	580	.389	22.382	2	100	<.001
I turn to an alternative shopping format (for example, I shop online).	3.413	3	593	.332	13.737	6	593	.032	4.093	6	593	.664	2.534	6	582	.865	1.730	2	101	.421

Table 24 – Chi-square tests of informants’ avoidance of retailance, with the statistically significant associations in red

Age	Informants avoiding retailance by going to another store	Age	Informants avoiding retailance by shopping online
18 to 24 (n = 27)	25.93%	18 to 24 (n = 27)	27%
25 to 34 (n = 181)	17.68%	25 to 34 (n = 181)	38.12%
35 to 44 (n = 178)	12.36%	35 to 44 (n = 180)	38.33%
45 to 54 (n = 104)	7.69%	45 to 54 (n = 104)	24.04%
55 to 64 (n = 62)	1.61%	55 to 64 (n = 62)	27.42%
65 or older (n = 36)	13.89%	65 or older (n = 36)	33.33%

Table 25 – The association between age and avoidance

3.6 Substitution

Instead of refusing to self-disclose, a few consumers resort to “substitution,” or “switching,” when they use another consumer’s credit or loyalty card or identity instead of their own. Only 12% of informants admitted they sometimes use someone’s else identity, for example, using a loyalty card that belongs to another consumer, a result that has statistical significance when associated with gender ($X^2(3) = 8.261, p = .041$), for 13.77% males (42 out of 305) and 9.64% females (27 out of 280) chose the “yes” answer. I, therefore, concluded that males are more inclined to substitute their identity to avoid retailance. No statistically significant associations were discovered with age ($X^2(6, N = 592) = 5.883, p = .436$), education level ($X^2(6, N = 592) = 9.906, p = .129$), income level ($X^2(6, N = 581) = 1.809, p = .936$), or membership in a minority group ($X^2(2, N = 101) = .365, p = .833$). While no interview informants admitted to personally using substitution, one recalled the following incident:

Sarah (F): My dad gave my mom's email while they were shopping the other day, so she made him go back to the store and find out how he can get her taken off whatever she was added into³⁷.

The above interview quotation shows us how the husband employs “substitution” as a form of resisting retailance (to avoid self-disclosing his own contact information) and how his wife’s reaction is another example of resistance (she wants to avoid bothersome communications by not being part of any marketing lists).

³⁷ In Bill C-11 being debated (to date) in the Canadian Parliament, section 55 of the Consumer Privacy Protection Act (CPPA) proposes to create a clear right for individuals to have their personal information (collected from them) disposed (i.e., permanently and irreversibly deleted) by an organization in control upon request (Office of the Privacy Commissioner of Canada, 2021).

3.7 Breaking

“Breaking” is the physical disabling of a retailance system. In the survey, 36 consumers (6%) admitted to intentionally breaking a surveillance system inside a store, a result that is significantly associated with membership in a minority group, with 5.36% of visible minority informants (3 out of 56) and 38.46% of indigenous informants (5 out of 13) and 3.13% of informants with a disability (1 out of 32), compared to 5.49% of non-minority/white informants (27 out of 492). Those results should be considered with caution because of the low number of informants. No statistically significant associations were discovered with gender ($X^2(3, N = 593) = 1.734, p = .629$), age ($X^2(6, N = 593) = 7.309, p = .293$), education level ($X^2(6, N = 593) = 3.502, p = .744$), income level ($X^2(6, N = 582) = 7.668, p = .263$).

However, all interviewees denied ever breaking a retailance system since it would only cause them trouble.

James (white American): [As for breaking surveillance equipment,] I would think if you broke it, you probably could get in trouble with them. That would not be a good idea.

To summarize, the above section provided a roadmap to understand consumers’ behavioural reactions to retailance. Consumers accept (either willingly or resigned), negotiate or resist retailance. Nine types of consumer resistance were identified and seven of them were discussed in more detail: refusal, discovery/detection, masking, blocking, avoidance, substitution, and breaking. While the gender, age, education level and membership in a minority group had some impact on informants’ choice to resist retailance (gender was associated with avoidance and substitution; age with discovery, masking and avoidance; education level with refusal; and membership in a minority group with discovery, avoidance and breaking), there was

no statistically significant association between any of form of resistance and consumers' income level.

Third: More factors affecting the consumer's behavioural reaction to retailance

As discussed earlier in this chapter, there are many factors that affect consumers' behavioural reaction to retailance, including their awareness of the laws and regulations related to privacy, their awareness of the presence and scope of used retailance systems and channels, what they gain in return for disclosing their information (e.g., future offers, money rewards, temporary storage space), whether they are regular store customers or not, the type of information they are requested to self-disclose, and their general trust in the retailer's ability to protect their personal information. There are, however, more factors that affect a consumer's behavioural reaction to retailance and they are: political affiliations (e.g., accepting surveillance during the COVID-19 pandemic) and the consumer's past experiences.

(1) Political affiliations during crises

Since the beginning of the COVID-19 pandemic, adhering to new store regulations (for example, properly wearing a mask, social distancing, sanitizing one's hands, etc.) has been resisted by some consumers, especially in the U.S. where the pandemic is a profoundly partisan issue (Gollwitzer et al., 2020).

Christopher: I think that's going to be very dependent on, let's just say, somebody's political beliefs. I don't necessarily know how it is in Canada, but it's very partisan here [in the U.S.] and it's very polarized. And if a person is already predisposed to believe that coronavirus is a hoax or that we do not need to wear masks and they don't want to be told, I think those people are going to be very heightened and defensive about being watched. But as someone who, like me, who is very much, you know, working from home and avoiding people and only going out when I need to, and always wearing a mask, I appreciate stores that are

going to enforce the rules. So, it's really going to be, at least here in the United States, dependent on a person's belief about coronavirus and whether or not its regulations are infringing on their freedom, I guess.

The above quote about the impact of political affiliations on consumers' behavioural reaction during crises corroborates the 2020 Pew Research Center survey (Kessel & Quinn, 2020) that stated that the COVID-19 outbreak has exposed growing divisions between supporters of the U.S. two major political parties, for Republicans and Republican-leaning independents were roughly twice as likely as Democrats and Democratic-leaning independents to mention "masks" in the context of negative effects from the outbreak (19% versus 10% respectively).

(2) Consumers' past experiences

In some cases, consumers' personal background and past experience, especially during their childhood, can have an impact on how they perceive and accept retailance. For example, being raised to be wary of store surveillance, growing up in a country where women are not safe shopping late at night, or growing up in a country where the importance of surveillance is drilled into the citizens.

Mary: I think it's very common here [Reno, Nevada] that people steal things frankly. And yeah, I think that if you do pick things up, you know, my concern is, okay, so I picked this up right, if the camera doesn't catch you putting it back down, you know, will they accuse you of stealing? I don't know. It was also something my father often would say when I was living at home. He would say, "Now when you go into stores, you know, you want to be careful. You want to keep your purse zipped up because you don't want somebody to slip something in there and then they're going to accuse you of having stolen it. You don't want to pick things up, you know, just look at them from afar. Keep your hands to yourself." . . . Well, when I was coming up there really wasn't this type of surveillance we have now. I think I told you my father was always very firm about, you know, "You need to be careful when you're in these stores," because in his day, as it was when I was a child, they had store detectives and I guess they had quotas to fill in his times . . . he indicated to me that it would be those store surveillance people who would slip something in your bag so . . . that they could

have a showing that they had made an arrest . . . So, I kind of got the impression they were like, maybe paid on a commission.

Maria: My sister and I would always make sure to go to the store, if we worked odd hours and went to school, so it only would be at night that we could go . . . Then we would be together, we would be safe. And this was before cameras everywhere. But now that there's cameras, I mean might somebody still try something? Yes, but at least if they can be identified in some way through the camera you have more of a chance of being able to get justice for it, and people are less likely to try to steal something from you or assault you. And maybe this is just because I grew up in Latin America, where . . . a lot of these assaults happen to women all the time, and nothing ever happens. And it was drilled into us from a very young age. "Don't go anywhere by yourself." So, the way I look at it is people here [in the U.S.] are kind of lucky in a way to have that [surveillance].

Wang Fang: I've never had any problem with surveillance, probably because of where I come from [China]. Where I come from, we have surveillance and parents always tell us "surveillance is helping us to keep our police safer and they're going to protect the good people and to catch the bad people." So, we never have problem with surveillance.

Amit: Yeah, we [in India] do have a lot more [surveillance] than what you have [in Canada] . . . The one example I could tell you is like while coming out of the store here, there is no person to check your bill and what you have taken by.

Olga: I have lived my entire life in Kazakhstan. So yes, I know that in grocery stores, . . . when I was growing up, you would walk into the store, and there would be cameras . . . As a child, I could identify this cameras in the store, like older years, like nine or ten year old. And on the way out of the stores, there was always like a security person who was like guarding the store in any case. So, there was always that one person and they would have like a screen with all the cameras, so they could like also see what is everywhere in the store, but that's from my childhood. I don't know how it is now. Probably the same . . . In stores, yes. Here [in Canada], I'm not really concerned about cameras.

Myint: [I] never had that experience [being targeted in a store] . . . I mean, maybe it's happened and I haven't noticed, but I was raised [by South-East Asian parents] in such a way that I was told that I was a human being who could do whatever I want, whatever other human beings did, and race and gender never came into the conversation that I was raised in. So, it never occurred to me that I was different than anyone else, or that I might be unequal because of circumstances I couldn't control.

It should be mentioned here that while some female informants talked about how their experiences of being a woman in their home countries impacted their acceptance of retailance,

according to the collected data, there is no evidence to support that gender plays a role in how consumers are targeted by retailers when it comes to retailance in North America (some interviewees only talked about stereotypical condescension when it came to customer service, for example, females are sometimes ignored in car dealerships and sports shops).

In summary, the above section discussed two more factors that can have an effect on consumers' behavioural reaction to retailance: (1) political partisanship affecting consumers' acceptance or refusal of retailance during the COVID-19 pandemic; and (2) consumers' childhood experience, for example, being raised to be wary of store surveillance, growing up in a country where women are not safe shopping late at night, or growing up in a country where the importance of surveillance is drilled into the citizens.

Fourth: Consumers' attitudinal outcomes

In the MTurk survey, when consumers were asked to choose one overall emotion that would describe how they feel when they encounter retailance (Figure 78), 69.9% chose positive emotions (security, transparency, or trust) while 30.1% chose negative emotions (distrust, intimidation, discomfort, embarrassment, frustration, or prohibition). This shows that a higher percentage of consumers accept retailance because of its positive connotations. This result was supported by another open-ended question (put at the end of the survey) that asked informants to describe what they think of and how they feel about surveilling customers in retail stores. Creating a word cloud of their answers (Figure 79), the top words reflected a positive reaction (e.g., protect, good, fine, helps) and were followed by words with more negative connotations (e.g., problem, bother).

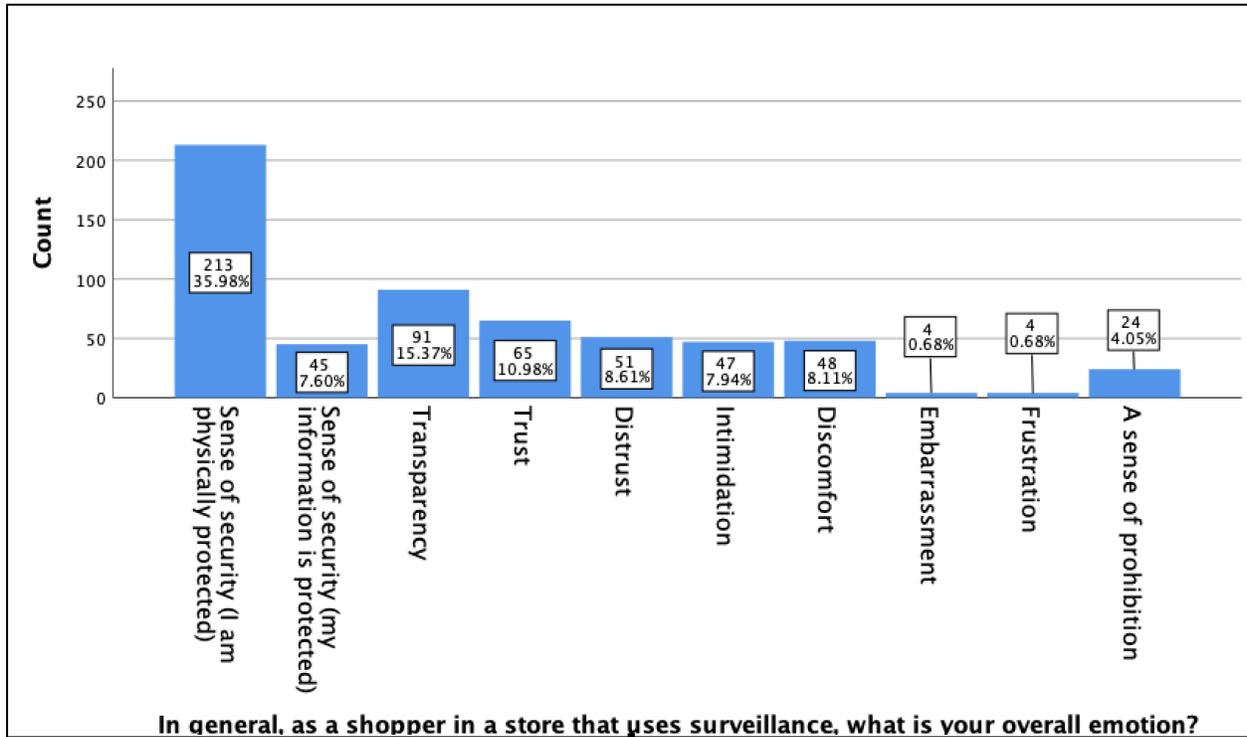


Figure 78 – Informants’ overall emotion when encountering retaillance

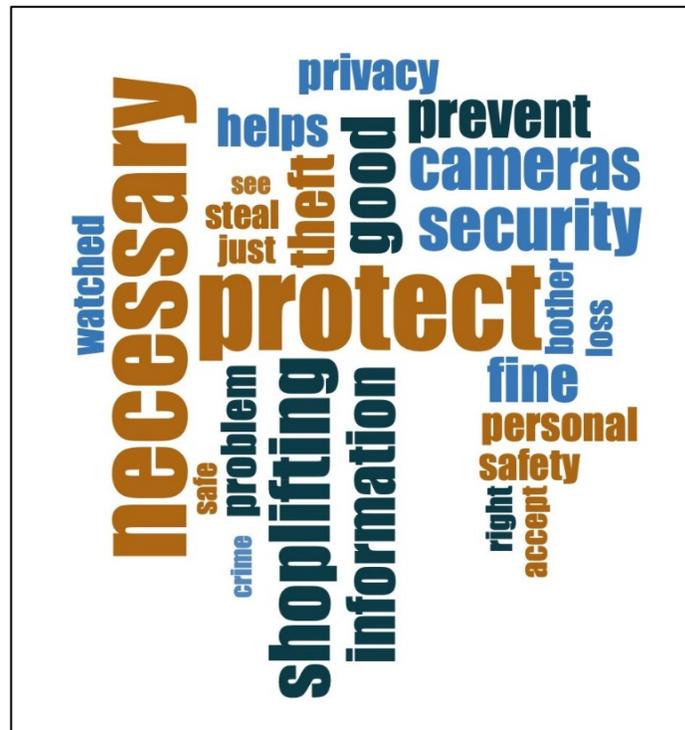


Figure 79 – Word cloud showing top twenty-five words used by survey informants describing what they think of and how they feel about retaillance

One of the informants, however, commented that because of the prevalence of retailance, it does not evoke any of his feelings.

Survey informant: Earlier in the survey you asked how I felt about surveillance and you forced me to choose an emotion. I chose trust. The truth is I don't feel anything. I've never lived in a world where there wasn't surveillance, so I don't feel anything. It's like seeing a telephone pole outside. Does it evoke feelings? No. Neither does a video camera in a store.

Thus, when confronted with retailance, around two-thirds of the consumers conveyed positive emotions. Based on the analysis of the survey and interview data, consumers' attitudinal outcomes are either being for or against retailance (Figure 80).

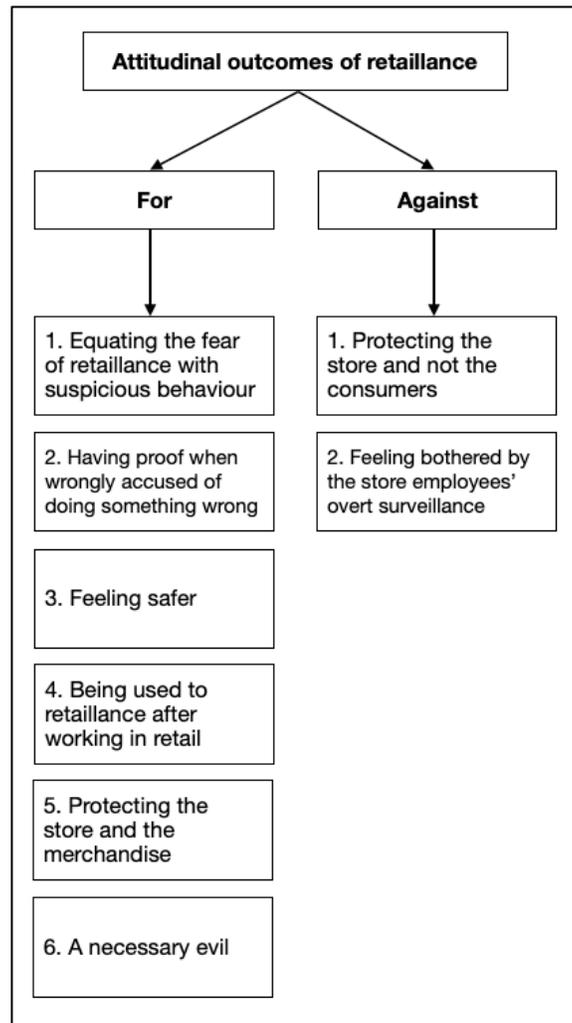


Figure 80 – The attitudinal outcomes of retailance

(1) Consumers for the use of retaillance

When it comes to consumers' attitudinal outcome (i.e., being for or against retaillance), despite the different reservations that may lead to various behavioural reactions against retaillance, 85.3% of total consumers surveyed admitted that in general, they are for the use of retaillance (Figure 81). No significant statistical associations were discovered with gender ($X^2(3, N = 593) = 6.583, p = .086$), age ($X^2(6, N = 593) = 8.653, p = .194$), education level ($X^2(6, N = 593) = 2.197, p = .819$), income level ($X^2(6, N = 582) = 8.711, p = .190$), or membership in a minority group ($X^2(2, N = 101) = 5.045, p = .080$).

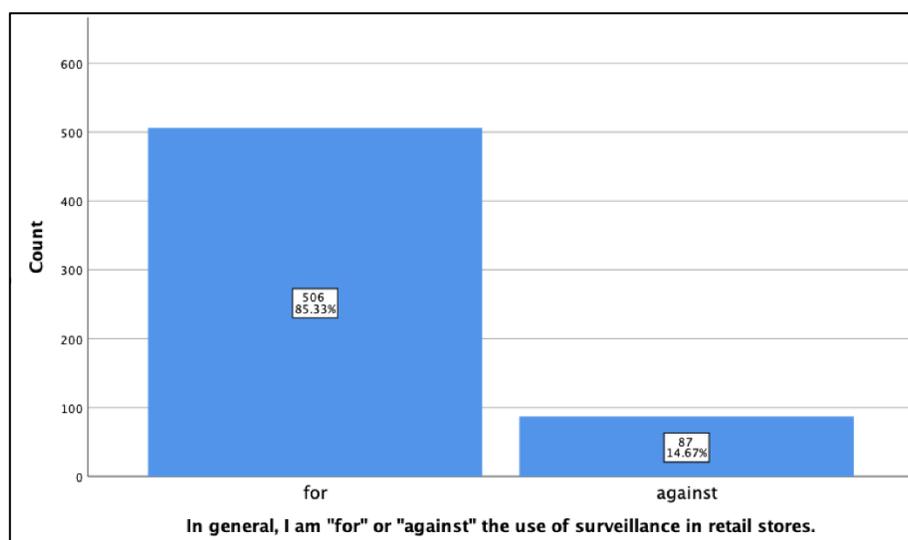


Figure 81 – Informants' for/against the use of retaillance in general

During the interviews, informants were asked to explain the reason behind their acceptance of retaillance. Their answers varied; they were divided into six different reasons: (1) equating the fear of retaillance with suspicious behaviour; (2) the need to have proof when wrongly accused of doing something wrong; (3) to feel safer; (4) being used to retaillance after working in the retail sectors; (5) understanding retailers' need to protect their stores and merchandise; and (6) believing retaillance is a necessary evil.

1.1 Equating the fear of retailance with suspicious behaviour

As discussed earlier, some consumers use the “nothing to hide argument” (Solove, 2011) to explain why they are not afraid of the presence and scope of retailance.

Chan: I'm aware that there's like surveillance everywhere. But I don't really care . . . because I'm not doing anything like suspicious or anything. So, I'm not too worried.

1.2 Having proof when wrongly accused of doing something wrong

Some consumers viewed retailance (such as CCTV cameras) as an “unbiased” source that can provide proof of their innocence if they are ever wrongly accused of doing something wrong/illegal.

Jessica: So, it's good to have some [surveillance] just like a backup to make sure that people know exactly what happened. So that one doesn't just rely on people's words that could be faulty.

Maria: Honestly, like I said, at first it [store surveillance] was irritating and I would avoid places like that. But as it became more and more commonplace, it also made me feel better, like in parking lots and things like that. Because then if somebody hits your car in the parking lot, because I've had that happen, someone hit my car in the parking lot and just drove off. And there was nothing I could do about it and nobody caught their license plate number, nobody cared. So, I had a huge dent in the side door . . . And it's not just your word against their's, and it's a legitimate recording, right? It's . . . it's unbiased. It's from the store itself and it could be used against an employee if they were discriminating against you in some way. You can get that recording because they don't have any way of stopping that, right? That's being backed up somewhere else; the IT or whoever has that. So, you're actually more likely to be able to prove that you were mistreated in some way, if you have that, I mean a cell phone recording doesn't hurt but, in a way, I've come to where I'm okay with it because should anything happen, there is that, and it's like a deterrent also, if people know they're being watched.

Maria (quoted above) also references a previously discussed concept (i.e., retailance is a deterrent since people know they are being watched) which reminds us of the Foucauldian panopticon in which overt and covert surveillance leads to individuals' self-discipline.

1.3 Feeling safer

When asked if they agree with the statement, “I feel safer, personally and physically, when retail stores use surveillance,” 66.22% of consumers admitted that they somewhat agree or strongly agree. There were no statistically significant associations between that statement and gender ($X^2(18, N = 593) = 22.383, p = .215$), age ($X^2(36, N = 593) = 46.630, p = .110$), education level ($X^2(36, N = 593) = 33.248, p = .600$), income level ($X^2(36, N = 582) = 33.324, p = .501$), or membership in a minority group ($X^2(12, N = 101) = 16.203, p = .182$), which indicates the prevalence of that sentiment across different demographic groups. Interview informants talked about similar feelings:

Joshua: I'm personally okay with it because if I need to be recorded and monitored in order for other shoppers and myself to be safe and have the privilege to shop at these places, then I don't have an issue with it. If . . . I think it's just a part of going to the stores and using that service is that they want to monitor you to make sure you're doing what you're telling them you're doing.

Ashley: But I also feel that it's a good thing to have because, I don't know, I feels like it kind of protects us in some way.

Maria: It used to be a negative feeling when I first noticed it just because it was unusual. And it's just, it's like anything new. It kind of scares you at first, but now I'm glad because you see things like people trying to get in fights or whatever or you have, I mean, as a woman, when I see a man getting too close to me or I think they're following me. At least I know that there's a camera there and they're less likely to do something like that if they know they're being watched . . . Yes, I think it's less likely that you will be sexually harassed or harassed in some other kind of way, if there's cameras around . . . It's not like a cell phone that you can smack out of someone's hand, it's there. And it's catching everything.

Therefore, to some consumers, retail surveillance evokes positive feelings of physical safety and protection. The informants also touch on themes discussed earlier, such as the capacity of retail surveillance to provide proof of innocence when wrongly accused of doing something illegal and of deterring other shoppers from any wrongdoing (i.e., Foucauldian panopticon).

1.4 Being used to retailance after working in retail

To the consumers who have retail work experience, retailance is part of their work environment that has proven to ensure their safety (as both consumers and workers).

Mitig [currently works at Loblaw, Ottawa]: I think it [retailance] ends up being helpful because I think . . . even having a presence of a security guard, even if it's at the front door, puts you in a different mindset when you go shopping. And essentially, I think it's to make sure everyone stays safe. But there's definitely a . . . focus on ensuring worker safety.

Ashley [currently works in Publix, Florida]: I still feel that it's [surveillance] good. Because, God forbid, while you're at the store something happens, you know, they have the video to go back [to] . . . I don't know if it's because I've worked under surveillance, I guess you could say, for so long that I feel it's a good thing. I've never had like a bad experience with it.

Zahra [has work experience in Winners and Hudson's Bay, Ottawa]: Oh well, because I worked in retail . . . But it never bothered me.

Consumers with retail experience, therefore, appreciate the presence of retailance (whether direct or technologically mediated) and are, consequently, for its use for three reasons: (1) the presence of retailance ensures both workers and consumers' safety; (2) they got used to being around and monitored by retailance systems; and (3) they never had a "bad experience."

1.5 Protecting the store and the merchandise

Some consumers agree that the retailer has the right to protect their store and merchandise (e.g., from theft).

Janani: Um, I feel okay like as long as, like, we are in their property, so they have the right to look [after] it.

Jennifer: I think in general [it's] positive because . . . obviously, they have a right to protect their inventory or, you know, what they're trying to sell from people taking it. And I know myself. I'm not gonna do anything wrong.

Once again, the retailer's right to protect their space and merchandise is linked with the consumer's "nothing to hide argument" (Solove, 2011).

1.6 A necessary evil

Some consumers are not fans of retailance, however, they understand that it has become a sort of a necessary evil.

Joshua: If something ever did happen, big enough that I needed to get that [recording], I know I'd be able to get it . . . On the other side of the coin . . . I'd rather it be more difficult to get [it] just because I would rather not just anyone to be able to pull security camera footage . . . Like, I think it's kind of both sides . . . I think it's important that people are monitored and all that, because it sucks. But all the bad people in the world make the good people have to be watched and all that, but it's just the reality.

David: I guess if I'm in a store and I think about it, I see a camera, I feel a little creeped out like you wonder if someone's watching you at that exact moment. So that's negative. It makes the shopping experience a little less pleasant. Sure. But it's positive in terms of, you know, for the store because they need to protect themselves so yes, it's a mixed bag, I guess . . . I have to be for it [surveillance] because it just provides an additional layer of security and, you know, I don't have anything to worry about. So, I guess I have to be for it. It's just . . . it's such a part of our lives. Now that I don't really ever think about it, you know. Or at least before the pandemic I didn't [think about it]. So, I guess I'm for it . . . Yeah, the covert surveillance I find inappropriate and troubling even . . . the overt, I have no problem with, but people should know when they're being monitored, you know.

To sum up, when it comes to consumers' attitudinal outcomes of retailance, there are six different reasons for their being "for" the use of retailance. A common theme across some of those reasons is the argument that consumers have nothing to hide (opposite to those who exhibit suspicious behaviour). Moreover, consumers with or without prior retail experience touched on the importance of the Foucauldian panopticon, the need to have an overt and/or covert presence of retailance to deter consumers from hurting both retail employees and shoppers and from shoplifting or committing acts of violence and/or vandalism.

(2) Consumers against the use of retailance

As mentioned earlier, only 14.67% of surveyed informants were against the use of retailance. The two main reasons behind their refusal were that (1) retailance protects the store and not the consumers, and (2) because of feeling “bothered” by the store employees’ overt surveillance.

2.1 Protecting the store and not the consumers

In the above section, some consumers talked about how retailance is acceptable because it protects the retail store and its merchandise. However, to some consumers, that is not a good enough reason.

Sarah: I think [retailance] it's actually negative. I mean, what's it there for? Like, mostly it's just for the shop to protect itself and then punish people who are shoplifting. Sometimes it's helpful if there is some sort of crime committed in stores, but like in the grand scheme of things, how often is that? And how often are we using the footage in that way?

Sarah, therefore, equates the store protecting itself to punishing the consumers (who are allegedly accused of shoplifting). To her, stopping a few incidents of shoplifting is not a good reason for using retailance.

2.2 Feeling bothered by the store employees’ overt surveillance

Among informal surveillance techniques, the activity of personnel is the most important method to reduce crime at a shopping centre (Booth, 1981). However, while some consumers feel at ease with CCTV surveillance, they are deeply bothered by store employees keeping an eye on them.

Michael: Why would that make you feel safe? That makes you feel unsafe because people are watching you . . . I mean the downside of somebody watching you, they're going to misinterpret what you do, right? . . . Now somebody is watching you and they misinterpret what you do, you might have a problem as a result of it. Whereas if nobody's watching nothing, there's nothing to be misinterpreted.

Jessica: Cameras don't bother me as much . . . I wouldn't feel comfortable . . . shopping around with someone . . . looking at me the whole time . . . To me, I always feel like that's more for the store safety than my own.

Mary: It [store employees surveilling me] makes me feel uncomfortable . . . you have to say spied on. And particularly in the dressing room situations.

Mitig: I definitely feel a little more uneasy [if] there are extra security guard standing around or controlling in the store. Which is a little ironic because when I'm working [in Loblaw] and I see that, it makes me feel more at ease, but when I'm a customer, it makes me feel worse . . . I think it's because ultimately, when we have security when we're working is to make sure that we are more safe from customers. But then, if I'm a customer and then their security walking around watching me, making sure everything's okay, and then ultimately thinking that "I might be the one acting up that way.

To some consumers, even those with retail experience (i.e., they believe retailance protect them as retail employees), direct/overt retailance is unacceptable, for it is open to interpretation and makes them feel "uncomfortable" and "uneasy."

Fifth: Factors affecting the retailer's choice and scope of retailance channels and systems

In Chapter 2, the reasons behind retailers' use of retailance in general were discussed, and those goals are: (1) to control loss and enhance security; (2) to create a pleasant and personalized shopping experience; (3) to enhance profitability; and (4) to ensure safety during the COVID-19 pandemic. However, there are factors that affect the choice and scope of the specific retailance systems employed and, according to the interview data, they are: (1) profiling (based on race, age or physical appearance); (2) retail location; (3) size and type of retail; and (4) population size.

(1) Profiling

From a critical marketing perspective, profiling consumers can become a discriminatory practice that marginalizes some of them. The practice in which consumers are sorted according to their presumed value to the retailer, or filtered through a “triage,” was coined the “panoptic sort” by Gandy (1993), a form of disciplinary surveillance. Based on the data collected in the interviews (from retail managers, retail workers, and consumers), there are three types of consumer profiling that play a role in the retailer’s choice of retailance: race, age and physical appearance.

1.1 Racial profiling

Racial bias plays a major role in retailance in some areas (a recent example of racial profiling was during overt surveillance by an employee in a Walmart branch in Toronto, (Knope, 2021)). Since this research focused on North America, it was interesting to compare consumers’ reactions in both the U.S. and Canada. It should be noticed that this discussion is tentative considering the low number of Canadian informants recruited through the MTurk survey. According to the collected data, most of the consumers complaining about racial bias are from the U.S. Emily confessed that during a previous job (when she worked in Ulta, a low-end beauty store in the U.S.), she would be tasked with trailing any person of colour in the store to make sure they do not shoplift. Michael, a Black American, disclosed how strongly he feels about the way he is usually treated in retail stores, even though he is a well-off and educated middle-aged man (he is an engineer in his late forties with an MBA and an annual income of US\$105,000).

Michael: From an anecdotal standpoint and also from a statistical standpoint, it just that African Americans are more surveilled just from the buyer standpoint, just from the stories that I've experienced . . . I feel negative. Well, depends on the surveillance, but most of the time, if this is done by humans, in terms of

surveillance, more likely it's going to be the introduction of racial bias and it's a situation where there is never really equal. So, I've never seen a situation where [it] just been equally kind of distributed in terms of surveillance. And I would just have to see it now. It was more of the human or the computer where they're kind of doing it and it just like passive like a camera that's one thing but even I don't like that because it's still put up with the stigma of just being surveilled all the time . . .

Sometimes you get a lot of stares, and where people watch you all the time in certain places either covert where they had a uniform on, or where they're just watching you and that kind of thing. And it's just a little bit too much . . . I went to a store with my mom one time. We were going shopping at stores that are similar to Macy's, and we was just picking out some clothes because I was getting ready to go to work and I want us to wear clothes and it was very [uncomfortable] the way that the guy was following us around the store. He wanted to make [us] know that he was looking at us while we were shopping and we got to a point where we had to say something about it . . . We had to embarrass the guy to keep them from doing that.

While Michael has a general feeling of helplessness, he admits that the current retailance situation is better when compared to the past.

Michael: It depends on the situation. If it gets too much, I might call it out and then to embarrass the person, but most of times you get a feeling of helplessness like, why are you doing this? . . . Now things are kind of changing but back then it was so, like, there's nothing I can do about it. That's just a system of bias. They are here and I just got to deal with it because this word need to go . . . African Americans are getting more vocal with the ability to film kind of encounters that we're showing it more, we're calling it more out on social media. So, that's kind of . . . gives you . . . a bigger platform to kind of show it, which has made people kind of shun doing it, or get or stay away from, because they might find themselves being on the internet. So, I think we're more overtly dealing with it than we did before.

As for Michael's answer to that problem, it is to simply use the online platform for his purchases so that he does not have to "deal" with such racially biased retailance. Michael's behavioural reaction, therefore, is one of resistance, for he avoids retailance by choosing an alternative: defection to online shopping. His advice for retailers who need to use surveillance is to "make sure that there's controls in place, that everybody [is] equally being surveilled."

To Maria, an Argentinian American female living in Texas, Latinos are also racially targeted by retailance.

Maria: I don't look Hispanic in any way. But there have been times when I have been treated that way. Like most Latinos do when people find out that I'm not completely white or that my father was Hispanic in a way.

However, she agrees that at the end of the day, Black Americans will be always treated worse than Latinos.

Maria: But even then, a Latino is always going to be treated better than a black person. At least in the United States. Just because Latinos don't have a history of slavery. They don't have years and years and years of being demonized as criminals. A Latino is mostly seen as like a job stealer or somebody who refuses to adapt to the culture, so to speak, but black people . . . It doesn't matter what they do. It will never be good enough, just because they are black. So, I would never compare how any other minority gets treated compared to how African Americans get treated. Especially here in the States, because it's not comparable. Are there situations where other minorities get mistreated? Yes, but it's nowhere near on the same level. Never has been.

Other minorities, like Native Americans, are also sometimes racially targeted.

Mary: I know about the skin color difference. I had a friend who . . . was Japanese but she looked very Native American. And when she would go into stores in Arizona . . . she noticed they actually followed her physically.

As for Asians, they have been only brought to the centre of attention inside retail stores after the COVID-19 pandemic hit and its origin has been identified to come from Wuhan, the capital of central China's Hubei province. This mistreatment inside the stores, however, was more towards workers than consumers.

Chan: After COVID hit . . . there's one time a customer [in Loblaw] was like, "You guys bring the virus to Canada." . . . I just find it pretty hilarious . . . I'm like, "Okay, cool." But I only find it hilarious, but not like very offended. But indeed, that's something to be considered.

Matthew (who works in Walmart, Arkansas) talked about how hiring people of colour helps in preventing racial profiling of consumers walking into the store:

Matthew: I'm happy to say that at our store, our loss prevention, which are the people that are in plain clothes, looking for thieves, they are people of color. They are minorities. And so, you know what I mean? . . . I don't know if that was just the way it came down the pipe, those are the most qualified guys, or what? But I feel like that helps to have that sort of presence as minorities there in the store . . . The one near me [i.e., Walmart near my home] is ALL white people.

To summarize, racial profiling is one of the factors behind targeting specific groups of consumers with retail systems. Retailers, therefore, need to be careful when directing retail towards visible minorities, which could be achieved by (1) being fair by surveilling all consumers equally, and (2) hiring visible minorities to surveil retail consumers overtly and directly (e.g., as store security) and/or to operate technologically mediated retail systems (e.g., monitoring CCTV footage).

1.2 Age profiling

Some of the interviewed consumers felt that they are closely watched in the store because of their relatively young age. For example, Li Na recounted how when she was shopping for an expensive dress to attend a wedding, the store employees kept watching her closely, not paying much attention to her as a customer, and not allowing her to try many dresses at once. They thought that because she was young and not with an older adult, she was not serious in buying something expensive. Twenty-three-year-old Ishita talked about similar experiences in Ottawa:

Ishita: 100% yeah . . . I do definitely look like I'm a lot younger than I actually am . . . Specifically in stores . . . that are more expensive. Like if I'm walking by a jewelry store or something, like people will keep an eye on me . . . even when I go to LCBO [retail stores run by the Liquor Control Board of Ontario] . . . But I definitely find that more so in jewelry stores . . . [In Mississauga] I think I always would go with the parent to a store, so I never really paid attention/like no one really would pay attention to me either, because . . . I'm just a child with the parent. But here [in Ottawa], however, I'm just going by myself individually. And that's why [I] notice all the little things.

To summarize, some informants talked about being the focus of retail due to their apparent young age, especially when shopping in high-end stores, since store employees assume young

consumers cannot afford to purchase expensive merchandise when they enter the store without the presence of an older individual (e.g., a parent).

1.3 Physical appearance

The way consumers look when they set foot in a retail store (whether they act and behave suspiciously, look “poor,” or have too many tattoos) could also have an impact on the amount of retailance they are faced with.

David: I mean, there's times that I've gone shopping and I'm in my Saturday work clothes, you know, with paint on my shirt. You know, holes in my blue jeans, because that's my work clothes, and I imagine maybe they may have watched people who appear to have a lower income more closely.

Ashley: Maybe if they came in [to Publix, the store where I work] looking kind of dirty and stuff, you know, the radar might go up on them and they might watch them maybe a little bit closer than they would, you know, watch anyone else . . . It all depends on how they look. Or if they're acting suspicious . . . I think it comes from experience by the people's behavior because sometimes, you know, if they're gonna steal you can tell because they're acting almost paranoid and sketchy, I guess you would call it.

Sarah: I didn't look particularly wealthy or, like, well off, so . . . I justified [them watching me closely] as like they want to perform good customer service, but it doesn't feel that way . . . Do you really think I'm going to try to steal this \$13,000 dress? Like no, I just want to touch it . . . I don't think I like [to] dress in a way that suggests I could afford buying the goods. So then why am I even there really? Maybe [that's] what springs to mind for them. And so maybe I'm there to do harm.

In Sarah's quote, the word “touch” is mentioned, which is a reminder of a theme discussed earlier in the chapter, excessive retailance (from the consumer's point of view) can lead to consumers' fear of touching products (i.e., a haptic experience) which could eventually lead them to switch to another retailer (a physical store or online).

Robert admits that he looks different because of working in the U.S. marines for eight years as a second lieutenant and having visible tattoos, therefore, he feels to be always the focus of surveillance whenever he visits a store:

Robert: I do look different than everybody else. Because, of course, I was in the military, and I have that military ego, [a] sort of ego trip that military men has. So, I'm walking into a store, like everything showing off tattoos, that sort of thing. And of course, I do get watched by LP [Loss Prevention] or other, like actual sales associates, while I'm roaming around say the Walmart or another store . . . Of course, somebody wearing tattoos is like, "Oh, you're a bad guy . . . you have a criminal deviant side to you." And of course, that's typical stereotype of people with tattoos as like, "Oh, you have a tattoo, you are a bad guy." But, you know, if you actually look at them and asked me about them, I [would] tell you, and then you would actually understand; okay, yeah, I'm not a bad person.

To summarize, some consumers are profiled because of how they look (they are badly dressed and look poor or have visible body tattoos) which makes them feel defensive ("maybe I'm there to do harm"; "I'm not a bad person").

(2) Retail location

Store location (for example in the American South or a city known for its gambling casinos) sometimes plays a major role in the level of retailance used. This was highlighted by some of the U.S. interviewees.

Mary: I think that this town [Reno, Nevada] in particular is because it is like a gambling Mecca. And there's also a huge homeless population. I think they have, you know, just extreme surveillance.

Matthew: I do feel like that that [retailance] is something that happens. I live in the South [in the U.S]. You know what I mean? A lot of people are still racist. And there, for a long time . . . like the black hair products were locked up instead of the white hair products. Assuming that the black girl stole more shampoo than white girls, which is dumb.

Some retailers, therefore, make a choice to increase their retailance because of where their store is located, for example, because they are in an area with a large number of homeless people (i.e., fearing an increase in shoplifting) or in an area largely inhabited by visible minorities (which raises the question of racial discrimination).

(3) Size and type of retail

A retail store's choice of retail channels and systems is sometimes dictated by their size (small stores versus big-box stores) and/or type (low-end versus high-end).

Mary: I think that in particular, they're [retail] prevalent in very expensive stores . . . more upscale stores like Nordstrom. And maybe some of your lower more budget stores . . . because they have such a large volume.

Christopher: It's less sophisticated [in small stores] . . . We [in Campus Outlet, U.S.] have basically two simple cameras in the store one that tilts downwards over the checkout area and then we have one by the backdoor which can basically look out over the showroom . . . I mean it's basically just like closed circuit where we have a TV up behind the register where customers can actually see where the cameras are located and what it's showing and it's specifically used just for theft prevention. So, I'm almost certain in my case . . . [working] for a small company, that what we have is less sophisticated in nature and really just like for the purpose of, like I said, anti-theft measures.

Ashley: We [in Publix, U.S.] just have the cameras. Now other public chain [stores], the bigger, more busier ones, they do have security guards there also. But my store we don't. We just have the video.

Sarah: I think there's definitely way less surveillance in smaller shops. Although I will say in like in some of them, the more in the privately-owned ones, you are sort of starting to see an increase in cameras. Like, I went to a thrift store down the street and then I happened to be at the cash and I noticed there were like 12 screens around . . . like really? Like even in the thrift shop now we're being surveilled. Like, I don't want to steal this used t-shirt. I want to pay for it.

Rachel: I find working in like a smaller establishment, it's definitely a lot more laid back. Working in a bigger store, people are obviously more adamant about it [surveillance]. I've also noticed since being in Rideau street [GAP in downtown Ottawa], we do have a few repeat customers going to come back and tend to be a bit more problematic. So, I know like . . . the clientele that come in that are going to more likely to steal [and] that are going to, you know, be problematic or troublesome for the employees. I find that working in a big store you have more of those set people and you know who to look out for versus working in a smaller store where it's a little bit more, you know, calm, laid back, quiet.

Ishita: I worked in Dynamite [Group Dynamite Inc. which filed for creditor protection in September 2020 due to the pandemic]. I know there was no surveillance system there. It was mostly just employees making sure that everyone was good. And we contact each other through our headsets to make sure that if we thought someone was on alert or someone was in the case of doing that. But I find

in like big malls, like Bayshore mall or St. Laurent [shopping centres in Ottawa], I don't think there's much surveillance [in stores]. But in stores like Independent, Loblaw, Walmart, and things like that, I find there is surveillance.

The type of store (high- versus low-end) impacts not only the scope of used retailance, but also who is targeted by that retailance, for example, racially profiling Black Americans:

Michael: Generally, [retailance] is more of your high-end stores. For your high-end department stores to some degree, and even if your low stores like your convenience stores where they generally have frequent visitors of African Americans. They take a tone of being more vigilant, or however you want to be put in terms of watching African Americans. So, it's kind of those things that turn to that, high end stores and then also the low end and convenience stores.

To sum up, retailance is usually more prevalent in both high-end stores and budget stores (which usually carry a large volume of merchandise) though they are typically less sophisticated in the latter.

(4) Population size

In some cases, retailance is simply buffed up because of the expected number of consumers that would be visiting the store (i.e., population size in the area). The following quote is by Matthew, a retail employee who works at Walmart in the U.S.

Matthew: Like I said, I just I just moved back from Florida and [in Walmart there] . . . it felt like Big Brother or something . . . And there were people on both doors, multiple people on both doors. You couldn't get in without going through a turnstile . . . that's the right word, a "turnstile" . . . that made an alarm, whether you went in or out. And you were all on camera. Everything was on camera, whereas where I live now [Arkansas], where I shop, nothing's on camera . . . Because of like the population. There are a lot more people in Florida. I didn't even realize, but it's like there's about 300,000 people where I was living in Florida, whereas where I live now [Arkansas], there's about 60,000. So, they have a lot more people that keep track of.

To sum up, by talking to consumers and retail employees, we can infer that retailers' choice of the type and scope of retailance can be affected by one or more of following four factors: (1)

profiling based on race (e.g., in the U.S., Black Americans and Latinos are racially targeted by retailance), age (where younger consumers are usually surveilled in high-end stores) or physical appearance (especially when consumers look poor or have too many visible tattoos); (2) retail location (e.g., in poor neighborhoods or the American South known for its racial inclinations); (3) size (small stores versus big box stores) and type (low-end versus high-end) of the retail store; and (4) population size of the area where the store is located (the higher the population, the more retailance is used).

Sixth: Privacy

In retail, the current data collection paradigms make it difficult for consumers to be involved in the choices made about their data. According to the MTurk survey, when asked to answer the statement “I am concerned about the impact of new technologies used in stores on my privacy,” 68.8% of informants admitted that they were somewhat or strongly concerned about the impact of new technologies used in retail on their privacy (Figure 82). As per the Chi-square test, no statistically significant associations were discovered between being concerned about the impact of retailance technologies on consumers and gender ($X^2(12, N = 593) = 8.187, p = .770$), age ($X^2(24, N = 593) = 34.265, p = .080$), education level ($X^2(24, N = 593) = 25.597, p = .374$), income level ($X^2(24, N = 582) = 018.248, p = .791$), or membership in a minority group ($X^2(8, N = 101) = 11.757, p = .162$), leading me to conclude that the concern over privacy is wide-spread. In the survey of Canadians on privacy-related issues (Office of the Privacy Commissioner of Canada, 2019), nearly half (48% of informants) felt confident that they know enough information about how new technologies (in general) might affect their personal privacy (down from 52% in 2016). When comparing this result to the MTurk result (where 16.52% somewhat

or strongly admitted being unconcerned about retail technology), we can deduce that consumers do not view retail technologies as threatening to their privacy when compared to surveillance in other sectors (e.g., in the online platform).

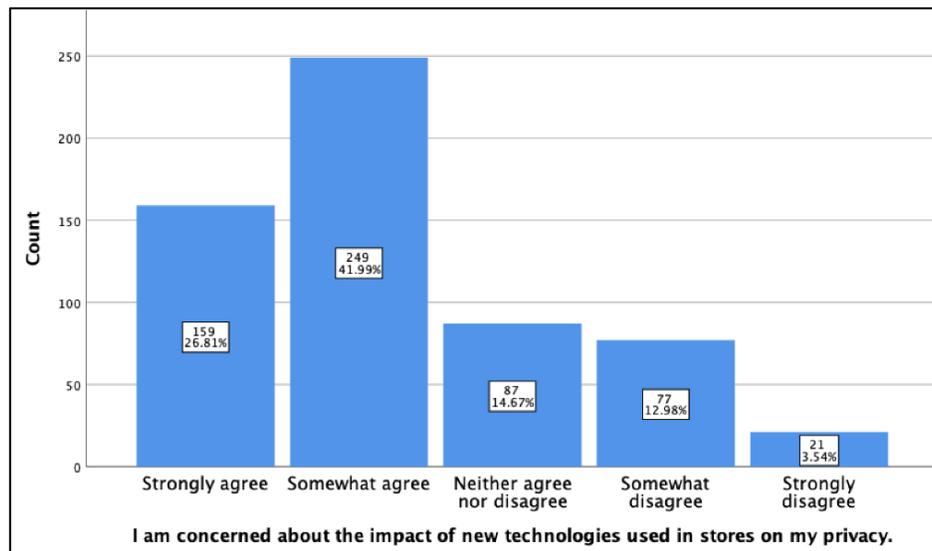


Figure 82 – Informants’ concern about the impact of new technologies used in retail on their privacy

When asked if they agree with the statement “My privacy is respected in retail stores,” 23% of informants indicated that their privacy is not respected in retail stores (Figure 83) and there were no statistically significant associations discovered between that question and gender ($X^2(12, N = 593) = 7.558, p = .819$), age ($X^2(24, N = 593) = 25.252, p = .392$), education level ($X^2(24, N = 593) = 27.533, p = .280$), income level ($X^2(24, N = 582) = 29.023, p = .219$), or membership in a minority group ($X^2(8, N = 101) = 7.074, p = .529$). The following (one of the answers, to the open-ended question about how to define privacy, in the survey) is an example of the opinions expressed:

Survey informant: I think the most important thing in a free society is privacy. Otherwise, it would be an Orwellian technocratic dictatorship where Big Brother is always watching your every move similar to places today like India's Aadhar

biometrics and China's social credit system where some negligible benefits are offered to the masses so that the elite can monitor and spy on everyone.

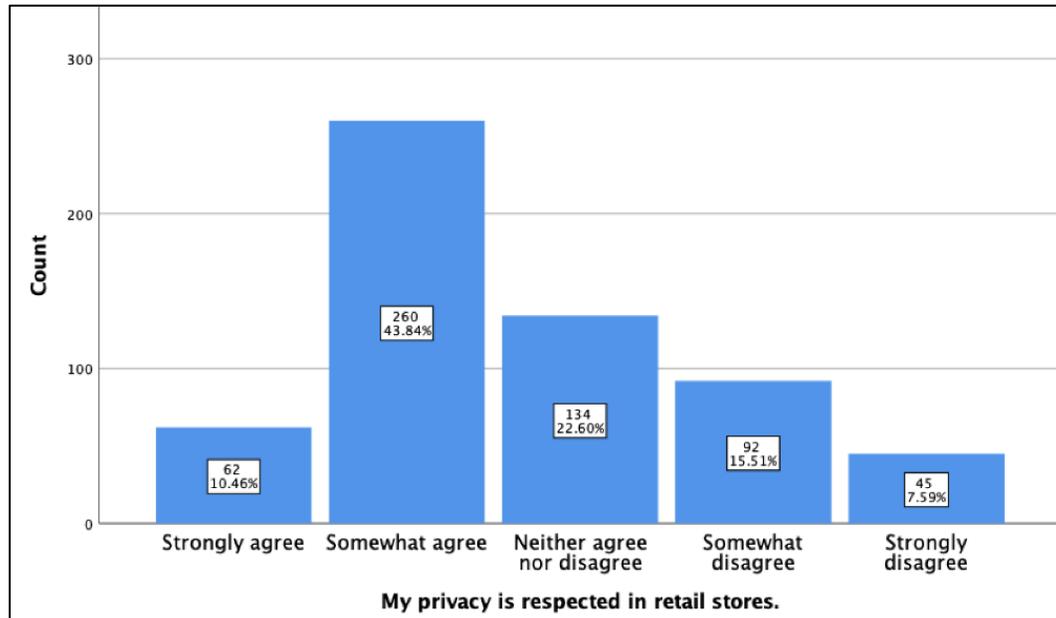


Figure 83 – Informants’ concern about how their privacy is respected in retail stores

In the MTurk survey, 43.2% of informants strongly or somewhat agreed to the statement, “I am confident that the stores that collect my personal and shopping information have adequate security safeguards to protect my information” (Figure 84). Running the chi-square test, a statistically significant association between this statement and membership in a minority group was discovered ($X^2(8, N = 101) = 16.166, p = .040$): 50% of informants who identified as belonging to a visible minority (28 out of 56), 53.85% of indigenous informants (7 out of 13), and 21.88% of informants with a disability (7 out of 32). This means that 43.5% of non-minority (i.e., white) informants (214 out of 268) admitted to never reviewing a privacy policy, which is the highest percentage. No statistically significant associations were found with gender ($X^2(12, N = 593) = 13.634, p = .325$), age ($X^2(24, N = 593) = 18.201, p = .793$), education level ($X^2(24, N = 593) = 17.412, p = .831$), or income level ($X^2(24, N = 582) = 21.572, p = .605$).

Consequently, we can tentatively conclude that indigenous consumers have the highest percentage of confidence that stores have the capability to protect their information.

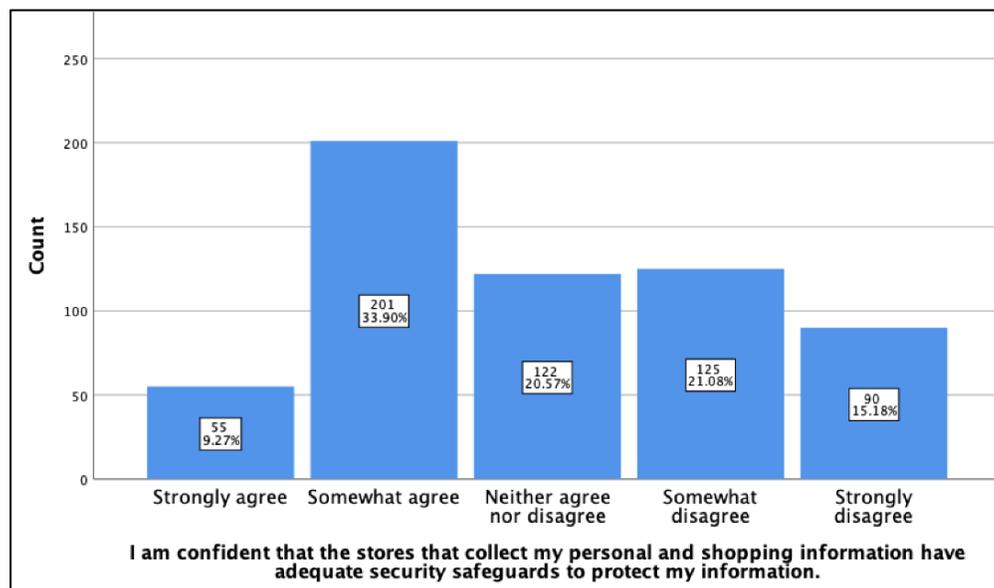


Figure 84 – How informants perceive retailers' protection of consumers' information

When asked if they agree that “Businesses take their responsibility to protect consumers’ personal and shopping information seriously,” 54.81% of informants strongly or somewhat agreed (Figure 85). This answer was statistically significantly associated with gender ($X^2(12, N = 593) = 23.366, p = .025$), specifically, 51.48% males (157 out of 305), 59.43% females (167 out of 281). This shows that female consumers have more confidence in retailers’ ability to protect consumers’ information. There were no statistically significant associations with age ($X^2(24, N = 593) = 17.290, p = .836$), education level ($X^2(24, N = 593) = 21.319, p = .620$), income level ($X^2(24, N = 582) = 30.690, p = .163$), or membership in a minority group ($X^2(8, N = 101) = 8.315, p = .403$).

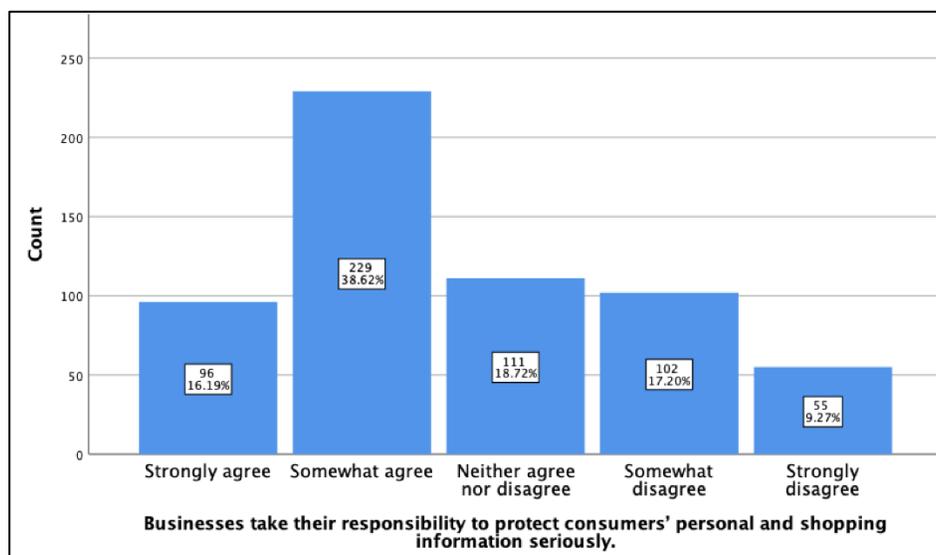


Figure 85 – How informants perceive retailers' protection of consumers' information

To discover what privacy means to consumers, informants were asked to answer, “In general, what does the word ‘privacy’ of your personal and shopping information mean to you?” by ranking four different definitions in order of importance. A nonparametric Friedman test of differences among related measures was conducted and rendered a chi-square value of 162.483 (3, $N = 584$) which was statistically significant ($p < .001$). Informants' top choice was “not being disturbed by marketers” (with a mean rank of 2.99), followed by “not being watched or overheard” (with a mean rank of 2.64), then “controlling what information is collected” (mean rank of 2.19) and lastly, “being in control of who has access to information” (mean rank of 2.18). This shows that the majority of consumers are concerned with the tangible aspect of privacy (for example, receiving marketing material or being physically surveilled inside the store) more than the privacy of their information. Analysing the interviewees' definitions of what privacy means to them, the following word cloud was created (Figure 86) in which the top twenty words include “information; phone; credit; name; address; control; hide; safe; access; damage; data; email.” This shows that to most consumers, privacy is mainly equated with them protecting their

personal information (such as their contact and credit card information). The discrepancy between the results of the MTurk survey and the interviews can be explained as following. In the MTurk survey, informants were asked to rank different definitions of privacy in the context of a retail setting, and their answers showed that they were more bothered by being openly surveilled and followed and receiving unwanted marketing communications than by having their personal information tracked. On the other hand, during the interviews, informants were asked to define privacy in general (and not just in a retail setting), consequently, their definitions focused on the intangible aspect of privacy: their personal information. We can, therefore, deduce that in a retail setting, consumers are more aware of physical, overt retailance.



Figure 86 – Word cloud showing top twenty words used by interviewees when defining privacy

According to the above discussion, consumers have their own definition of what constitutes their privacy. The question, therefore, becomes why they are complacent with their

privacy rights. To Kesan, Hayes and Bashir (2015), one reason behind consumers' complacency with their privacy rights is due to a lack of trust:

Consumers should be assured that their information will be shared only with their consent through an opt-in system, and they should also have the ability to view, challenge, and remove this information. This increase in transparency is likely to lead to an increase of trust, and thus move the consumer's relationship with data holders from complacency to consent. (p. 40)

Kesan et al. also argue that giving consumers the ability to view, challenge and remove data from their profile is an ethical decision. To them, having access to a centralized location for profile information would allow consumers to remove aspects of their profile that could trigger emotional distress, for example, a woman who had multiple miscarriages might choose to limit marketers' access to her sensitive medical information (p. 41). Researchers and public policy makers, therefore, need to call for baseline regulations that would emphasize protection for personally identifiable information to ensure that consumers are able to control their data both online and offline (i.e., in a brick-and-mortar setting). To Teresa Scassa, Canada Research Chair in Information Law and Policy at the University of Ottawa (Carleton History, 2020, Nov. 12), the law falls behind technology, a fact that calls for not just amending the current privacy laws, but for overhauling them.

Historically, privacy has been defined as a civil right (i.e., a right to protect personal information from others and a right to be left alone); it is also a social construct that shifts its meaning according to the norms of a given society and culture specific (Markos, Labrecque, & Milne, 2018). With rapidly evolving technologies (such as cloud services, biometric identification and satellite-based mobile data systems) that require an exchange of personal information in a global context, privacy has become an important quality of life issue. However, the notion of privacy is challenging, for it is quite impossible to find an all-encompassing

definition of privacy since it is always evolving, especially in this digital age. This ambiguity and the absence of a concrete definition impedes the development of privacy legislation and policies (Huang & Bashir, 2015).

Amidst growing concern about violations of privacy³⁸, marketers face the challenge of obtaining accurate personal information from consumers who are increasingly inclined to take measures to protect their privacy (for example, using unlisted telephone numbers or registering for the national “Do Not Call” list) or, when having their telephone numbers registered, not accepting marketing calls. According to Horne, Norberg and Ekin (2007), “there is a correlation between intimacy levels and a willingness to lie and it was shown that people are most likely to tell an untruth in contexts when the other party is unknown to them” (p. 98).

While some consumers are vigilant and seem to be concerned about their privacy being invaded, others will relax information privacy concerns when they feel the benefits for disclosure are significant (for example, receiving custom-designed promotional offerings) and that this trade-off of their information has value. Another segment of consumers simply pay less attention to any encroachments on their right to privacy, their “day-to-day concerns will inevitably erode the energy needed to preserve privacy” (Franzak, Pitta, & Fritsche, 2001, p. 640). Consumers, in general, surrender behavioural and consumption data, both knowingly and unknowingly, to “marketers, online advertisers, the government, and disparate social groups using apps, search engines, social media sites via mobile phones, tablets, wearable devices, and personal computers,” leading to an aggregation of data which increases the probability to identify and de-

³⁸ In Canada, despite feeling knowledgeable about their privacy rights, the vast majority (92%) expressed some level of concern about the protection of their privacy. Since 2012, the proportion of Canadians who rated their level of concern as extreme has increased 12% (from 25% to 37% in 2018) (Office of the Privacy Commissioner of Canada, 2019).

anonymize individuals (Markos et al., 2018, p. 48). Although privacy laws are consent-based, the context in which data collection is used has far exceeded the capacity of individuals to manage.

To summarize, this section on privacy has discussed the following topics: consumers' concern over their privacy; what they think about retail stores protecting their privacy; their definition of privacy in general and in a retail setting in particular; how their complacency with their privacy rights is mainly due to a lack of trust in the retailer and their inability to access their information; some of the challenges faced by marketers when consumers try to protect their privacy; and the repercussions of consumers surrendering their behavioural and consumption data.

An updated retailance model

As explained in Chapter 4, the last phase of this mixed methods research design was to interpret the collected data holistically, allowing new themes to emerge and others to consolidate. As a result, the retailance conceptual model introduced in Chapter 1 (Figure 87) was updated with the changes validated by the research results discussed earlier in this chapter (Figure 88).

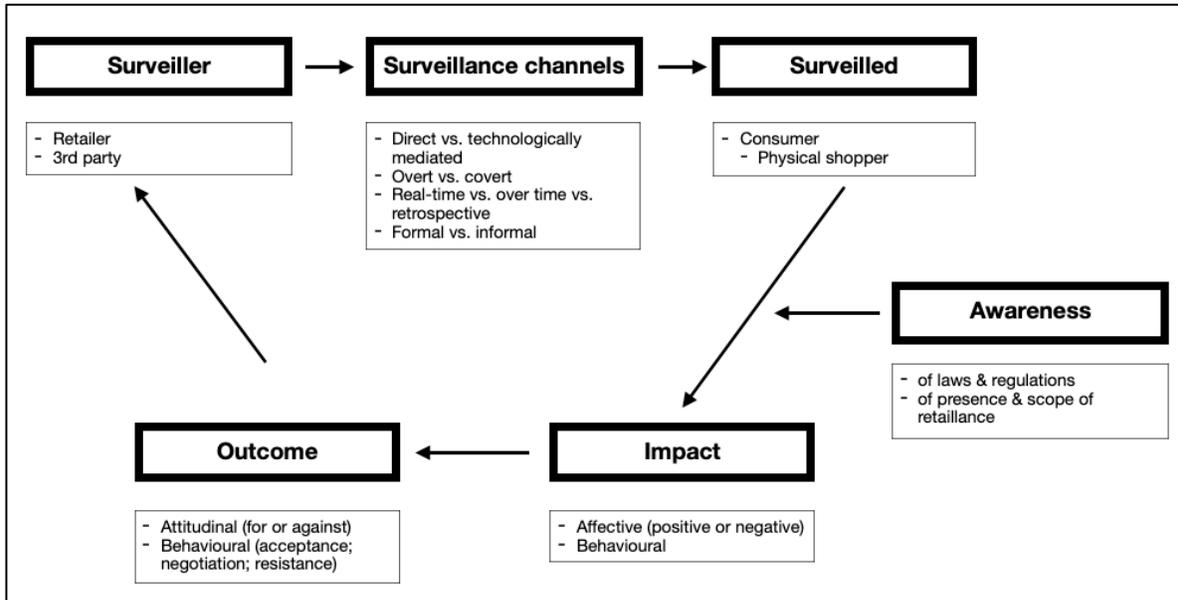


Figure 87 – The retailance model introduced in Chapter 1

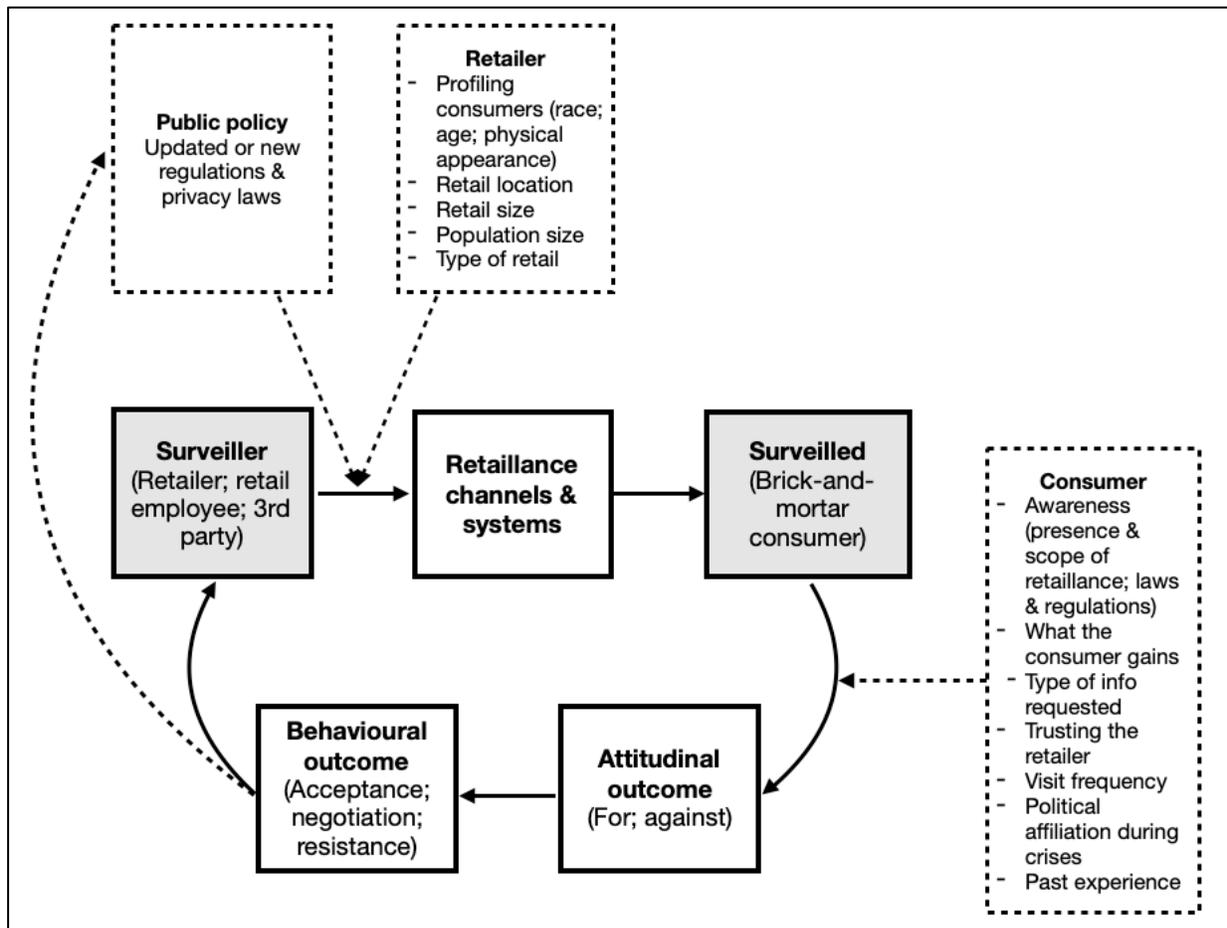


Figure 88 – The updated retailance model

Comparing the above two process models (Figures 86 and 87), the following changes could be seen: (1) The “surveiller” is represented by the retailer (i.e., the retail body in general), the retail employee (who is physically present inside the store) and/or a third party (e.g., security firms, other businesses having access to consumer data, etc.); (2) Both the surveiller and the surveilled are in shaded boxes to highlight the struggle of power (in critical marketing terms) between them when it comes to visibility and privacy; (3) A dotted box has been added that includes five factors that can impact the retailer’s choice of the type and scope of retailance employed. For example, a retailer may choose to increase the presence of retailance if: they are worried about the presence of a certain type of consumers (who are profiled based on belonging to a visible minority, looking too young to afford expensive merchandise, or having suspicious outer appearance), the store is located in an area with a high rate of homelessness; the store carries expensive, high-end merchandise, or a large volume of budget merchandise; or the store is located in an area with high population density (which means a larger number of consumers need to be surveilled inside the store); (4) In the preliminary model, the impact of retailance on the consumer is influenced by their awareness of laws and regulations and of the presence and scope of retailance. After analyzing the data, this list (in a dotted box) was expanded to include other influences: what consumers expect to gain from submitting to retailance (e.g., future offers, money rewards, loyalty points, temporary storage space, etc.); the type of information they are asked to submit (e.g., personal versus shopping data); their general trust in the retailer’s ability to protect their collected data; how frequently they visit the store; their past experiences with retailance; and their political affiliations during crises like the COVID-19 pandemic; (5) The box titled “impact” in the preliminary model has been removed from the final model.

Instead, the theme of consumers' affective and behavioural reactions to retailance was discussed under their awareness of "tagging," when they set off false tagging alarms; (6) The box titled "outcome" in the preliminary model has been transformed into two boxes: attitudinal outcome and behavioural outcome. "Attitudinal outcome" (being for or against retailance) precedes "behavioural outcome" (accepting, negotiating, or resisting retailance) since in social psychology, attitudes lead to and influence behaviour (Allport, 1935; Fishbein & Ajzen, 1975³⁹). Consumers' behavioural outcome would eventually impact the retailer's choice of retailance systems and channels, making this model a never-ending cycle; (7) A new dotted box was added to show how consumers' behavioural outcome can have an impact on public policy makers who can change or introduce new regulations and privacy laws to protect the consumer, which would ultimately have an impact on the retailer's choice of retailance channels and systems in order to comply with those laws and regulations. This section was added to the model to highlight the important role played by public policy makers in raising consumers' awareness of their rights and the impact they can have in the application of new retailance technologies. Moreover, this model was designed to be general enough to accommodate new emerging retailance systems and allow for the additions of new influences on both retailers and consumers (in the two dotted boxes). Future research can focus on testing the model.

³⁹ Fishbein's and Ajzen's Theory of Reasoned Action (TRA) explains the relationship between attitudes and behaviours (the A-B relationship) within human action and how individuals' behaviour is based on their pre-existing attitudes and behavioural intentions. According to the theory, the intention to perform a certain behaviour (i.e., behavioural intention) precedes the actual behaviour.

Chapter summary and conclusion

When the survey informants were asked to describe what retailance means to them (Figure 89), the fifteen top words show that being monitored by cameras and employing security to prevent shoplifting and guard the retail space is what retailance is mainly about from the consumer's perspective. The analyzed data revealed that the choices that consumers and retail workers make are sometimes structured by vulnerabilities, for example, poor neighborhoods, economic vulnerability, gender, and/or racial profiling. However, and as discussed above, retailance is much more complex, and consumers' lax approach to privacy cannot be only associated with lower awareness levels. Many consumers are willing to take risks associated with sharing their personal, shopping and consumption information as long as they receive benefits in exchange for their information. Although this exchange of personal and shopping information is beneficial to both consumers and retailers in many aspects, it does pose privacy challenges if the information is disseminated outside the originally intended contexts. While such consumer complacency is currently leading to favourable outcomes for businesses, marketers, privacy activists and policymakers need to recognize that many of those practices are unfair to consumers. Consumers need not just the ability to learn how to access their information, but to also control what information is in their consumer profile. This discussion is well-situated within critical marketing that adopts multidisciplinary insights. I second Zwick (discussed by Schroeder, 2007) that there is room for improving the workings of marketing practices, and this improvement is needed when employing retailance. Earlier (in Chapter 3), I discussed three of the main concerns of critical marketing that are relevant to retailance. Revisiting this discussion after analyzing the data only highlights their importance. (1) There is a need to challenge some of the present retailance practices in order to bring change that would be beneficial to both

retailers and consumers. (2) Retailers have an ethical responsibility to protect their consumers' privacy as well as their physical safety and financial well-being. (3) Policy could be influenced only when different stakeholders (i.e., consumers and retailers, marketers, and researchers) are involved.

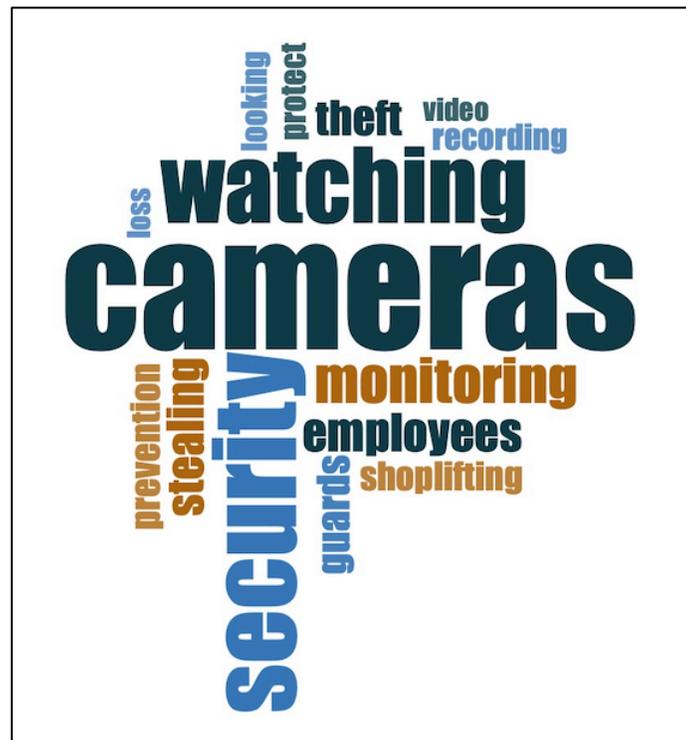


Figure 89 – Word cloud showing what retailance means to consumers

In Chapter 3, a theoretical model was created to show surveillance studies in the context of retailance. This model is revisited below (Figure 90) with examples added, integrating the literature review, the review of surveillance studies, the critical marketing perspective, and the analyzed data, hence, presenting a holistic view of retailance.

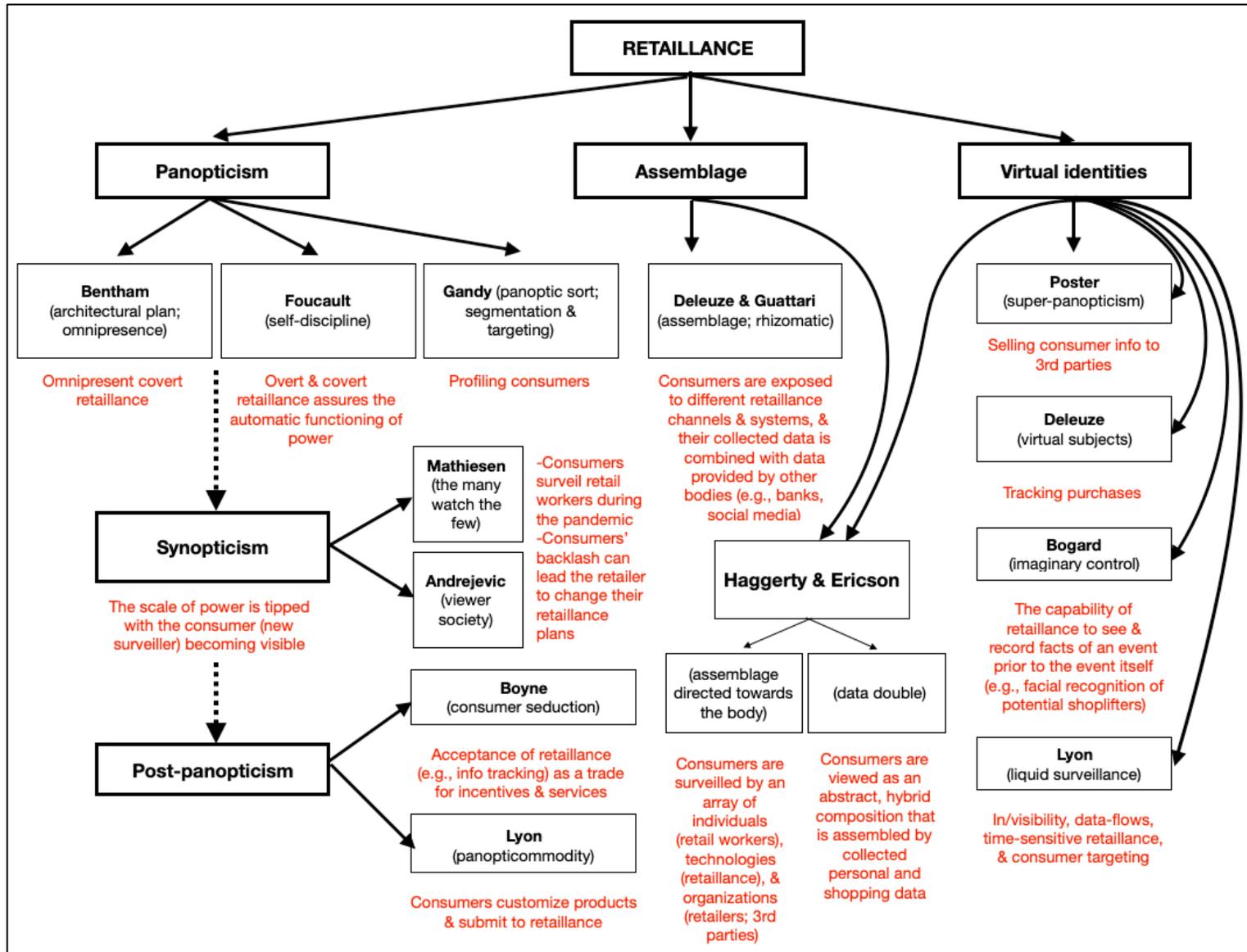


Figure 90 – Surveillance studies (in black) with examples (in red)

To summarize, this chapter opened with a brief introduction of the type of research data collected and its analysis. Afterwards, and structured around the preliminary retailance conceptual model, first introduced in Chapter 1, the findings were discussed. The chapter was divided into six main sections: consumers' awareness of the presence and scope of retailance and the impact of retailance systems on them, their behavioural reactions to retailance (from acceptance to negotiation to resistance), factors that can affect consumers' behavioural reaction, the attitudinal outcomes (being for or against retailance), factors affecting the retailer's choice of retailance, and a discussion of the notion of privacy in the context of retailance. Afterwards, an updated retailance process model was introduced and explained. The chapter concludes with re-introducing the theoretical model (this time linking it to the literature review, the critical marketing perspective and analyzed data) and a short summary.

CHAPTER 6: THE IMPACT OF THE COVID-19 PANDEMIC ON RETAILLANCE

Since the onslaught of the COVID-19 pandemic in early 2020, retailers have been scrambling to adapt to a situation that has been changing daily and that produced short-term shocks and is expected to have longer-term implications. Since this global pandemic started unraveling when I was at the beginning of the data collection phase in my research, I added a research question: what is the impact of the COVID-19 pandemic on retailers' use of and consumers' reaction towards retaillance? This chapter is my answer to that question. The pandemic could be viewed as an example of a disruption to the market caused by a previously unknown factor. The unprecedented setting of the pandemic, therefore, has proven to be an opportunity to explore consumers and retail workers' complex reactions to enhanced levels of retaillance in a real-life setting (versus in a laboratory or by introducing a hypothetical situation).

The chapter proceeds as following: first, I briefly introduce the changes in the retailing sector after the COVID-19 pandemic hit. Secondly, I focus on the use and impact of retaillance during the pandemic. Thirdly, the findings, gleaned from data collected via the MTurk survey and the interviews, are discussed. Lastly, the chapter closes with a summary and conclusion.

The world of retail after the COVID-19 pandemic hit

The health crisis and the unprecedented disruption caused by the COVID-19 pandemic have had profound impacts on economies, businesses and consumers worldwide, changing the way consumers live, work and shop. The global economy is forecast to enter its worst recession since the 1930s. As uncertainty remains high and fears of a pandemic or other destructive event remain palpable, a new normal is expected to emerge (Boumphrey, 2020).

Trapped in a pandemic spiral, retail has been one of the sectors hit hard and retailers are now faced with an unprecedented situation that is causing disruptions in the short- and mid-term to which their businesses have to adapt. Driven by the loss of everyday consumer spending, a “service recession” (i.e., a sudden and dramatic job loss in the service industries) has started (Chaganti et al., 2020). Fittingly, the situation has been described as a “retail apocalypse” (Dohmen, 2020). Amid an unprecedented spike in retail insolvencies in Canada (Toneguzzi, 2020b), some retailers were forced to close while others are faced with challenges such as those related to health and safety, disrupted supply chains, the workforce (e.g., reskilling workers; worker safety), cash flow, changing consumer demand (which can either spike or drop for some products), sales, and marketing (Donthu & Gustafsson, 2020). Statistics Canada reported that about forty percent of Canadian retailers had to literally close their doors after going bankrupt in March 2020 when government lockdowns and physical distancing requirements set in (Evans, 2020b). However, even when the lockdown was eased, retailers could not rebound easily. Among those hit hardest by the changes in the consumption habits that were brought about by the pandemic are luxury retailers (Pantano et al., 2020, p. 211). In Canada over the Summer of 2020, after their brands had been hit hard in the wake of the COVID-19 pandemic, many stores (independent, medium and larger chains) started filing for bankruptcy protection (such as footwear retailer ALDO (Evans, 2020a)) or simply shutting amid financial turmoil. Some of those stores were already struggling with debt prior to the pandemic, and the pandemic led to speeding up the process by creating further financial challenges, for example, Victoria’s Secret (Sandler, 2020). According to De Brabant (2020),

In business, especially in retail, leaders were already being seriously challenged before the coronavirus crisis hit. Retail was already going through a period of unparalleled change and transformation, putting even the most successful retailers in some form of “survival” mode.

Other local and international retailers, who are still open, are reconsidering their operations altogether, their plans include focusing on online sales (e.g., Microsoft), operating with fewer store locations, implementing layoffs (e.g., Nordstrom), and seeking creditor protection (Patterson, 2020; Toneguzzi, 2020a). In an attempt to support small businesses, the Canadian government started providing rent and extended wage support as well as loans (Department of Finance Canada, 2020; Trudeau, 2020). A similar situation can be traced in the U.S. retail market, which has been hit hard by the “coronavirus Tsunami” (Petro, 2020), with more than 6,000 store closures expected by the end of 2020, including Men's Wearhouse, PVH Corp, Microsoft, GNC, JCPenney, Victoria's Secret, Nordstrom, and Sears (Peterson, 2020). With the growing competition from online stores, some retailers will have to permanently close all, or a high proportion of, their physical stores (which ultimately means that consumers will have to change their shopping habits).

On the other hand, retailers like grocery stores and health and personal care stores have seen a surge in their operations (Evans, 2020b). Lululemon, an athletic apparel retailer, has seen a big uptick in sales as people switch to more comfortable attire while working from home during the pandemic (Canadian Marketing Association, 2020c). Online grocery has skyrocketed during the COVID-19 emergency since consumers, even the older and less digitally-savvy ones, have started welcoming the safety offered by technology (Pantano et al., 2020, p. 210). Consequently, some retailers are planning major future investments, for example, Walmart Canada has accelerated its \$3.5 billion dollar investment (to be spent over the next five years) to strengthen the business and enhance both their online and physical stores (Toneguzzi, 2020a). In August 2020, an upgraded Costco Wholesale opened its second-largest Canadian location at Shoppers City East, Ottawa (Ottawa Business Journal, 2020).

One of the unprecedented challenges facing retail management is the acceleration of trends such as the rise of online shopping, click and collect, frictionless retail and D2C (Direct-to-Consumer) (Boumphrey, 2020). Also changing is how consumers are shopping differently as a consequence of the “extraordinary containment measures” (Pantano et al., 2020, p. 210). For example, the “scarcity effect” (Hamilton et al., 2019; M. L. Scott, Martin, Wiener, Ellen, & Burton, 2020), or the limiting of the number of items to buy per consumer, has dramatically impacted consumers’ stockpiling habits (one form of which is “panic buying” (He & Harris, 2020, p. 176)), and waiting times and crowding are not as tolerated as before—although research shows that long waiting times in an emergency context are not expected to negatively affect customer satisfaction with the stores (Mowen, Licata, & McPhail, 1993). Retailers have implemented new types of online services (Tarry, 2021) and home deliveries, though how satisfactory those experiences are depends on each consumer. Such profound changes in retailing are expected to leave a mark on consumers’ perceptions and shopping behaviours when the crisis is over (Arora et al., 2020). The question is, how much change should we expect? For example, would consumers switch from the retailers they usually patronize to their competitors due to special proximity or the (un)availability of goods during the emergency? Or would they develop stronger attachments towards the stores they patronize during the pandemic? Will they switch to online purchases, home-deliveries, or curbside pick-ups?

For those retailers finding themselves selling non-essentials, the pandemic has been nothing short of a nightmare (Winder, 2020). In an open letter signed by a coalition of forty-seven Canadian retailers on December 1st, 2020 (Cision, 2020), Ontario Premier Doug Ford and Christine Elliott, Deputy Premier of Ontario and Minister of Health, were called on to immediately open all retail stores. The coalition emphasized that the lockdown of non-essential

stores in Toronto and nearby Peel Region at the time was ineffective and would put businesses at risk of failure. On the other hand, commenting on the future of brick-and-mortar retail, Michael Kehoe, a retail real estate specialist in Calgary and a member of the International Council of Shopping Centres, says:

The fact that one of the largest retailers in the country [Walmart Canada] is doubling down on their bricks and mortar stores is proof that a physical store is the blue-chip workhorse of any retail strategy. The business of retail is a dynamic and ever-changing industry and firms like Walmart are constantly reinventing themselves. (Toneguzzi, 2020a)

To Michael Medline, President and CEO of the Empire Company and Sobeys Inc.,

[In] the foreseeable future most grocery will be in bricks and mortar. Ecommerce will be sexy. It will be the highest growth but bricks and mortar will be what funds all this ecommerce growth and it will be the heart of how people shop for a long time. (Toneguzzi, 2020c)

Unfortunately, amid the increase of daily coronavirus cases in Canada during the pandemic's third wave, and while some big-box retailers in Canada have been flourishing, small, non-essential retail businesses are still facing the possibility of permanent closures (BNN Bloomberg, 2021).

Retail during the COVID-19 pandemic

The COVID-19 pandemic, resulting in different versions of lockdowns and social distancing mandates, has disrupted consumers' habits of buying as well as shopping. The new regulations—for example, imposing a two-metre physical distance between people, having a maximum number of people allowed in the store, wearing masks, allocating opening hours specifically for the elderly, and cancelling product sampling stations (Saltwire Network, 2020)—have a vast, and varied, impact on consumers who are asked to be “responsible citizens” by complying with those new regulations and retail practices. And while consumers may go back to

their old habits post pandemic, “it is likely that they will be modified by new regulations and procedures” (Sheth, 2020). Whether consumers will go back to or modify their pre-pandemic shopping habits, or even create new habits, is yet to be seen. When asked about retailance in a post-COVID world, Gabrielle Hargrove⁴⁰—the Associate Vice President of the Business Transformation Office at the Canadian grocery-driven retailer Giant Tiger—said,

[In Giant Tiger,] as any retail organization has since the pandemic, there's been a lot of focus on ensuring that we're monitoring and assessing our customers' needs and expectations and how they're shifting very quickly over the last few months. So, I think it's probably the same in every retailer, there has absolutely been an increased focus in that space over the last two years.

On the other hand, retailers are constantly urged to vigilantly monitor their staff and incoming guests to identify any sick person, in order to avoid further spread of the coronavirus, and to report to concerned health authorities if anyone’s symptoms match with those of COVID-19 (Shahbaz, Bilal, Moiz, Zubair, & Iqbal, 2020). This monitoring is a form of overt retailance, for it is a “direct supervision of the activities of some individuals [consumers] by others in positions of authority [retail workers] over them” (Giddens, 2002, p. 14)⁴¹. Pre-pandemic, stores primarily used traffic counting technologies for labour scheduling (to make sure they had the right number of workers to meet expected demand) and to calculate conversion rates (i.e., the percentage of shoppers who entered the store who actually bought something). However, with governments restricting indoor occupancy rates and with retailers adopting their own guidelines for occupancy, social distancing rules, and health screening (e.g., temperature monitoring), retailance technologies (e.g., traffic counting cameras and sensors, thermal imaging cameras,

⁴⁰ Hargrove consented to having her identifying information (name and position at work) published.

⁴¹ Although Giddens (2002) might have failed to envision how surveillance could be employed outside governmental control and in a peer-to-peer fashion, his description of surveillance as both an accumulation of information and direct supervision applies to the retail sector.

and the soon-to-come mobile apps connected to health/vaccine passes) have been turned into COVID-19 compliance tools (Verdon, 2020). According to the Retail Council of Canada (2021a),

COVID-19 has raised many privacy issues for retailers. These include questions like, what information can be collected from customers and employees during temperature checks, as retailers try to keep stores and staff safe? The pandemic has also raised data sharing issues, such as what can be disclosed for contact tracing reasons with health authorities.

Thus, the newly created culture of post-pandemic surveillance underscores the need for new and/or updated policies relating to surveillance and privacy.

Retail workers are now considered “essential frontline workers” (F. D. Blau, Koebe, & Meyerhofer, 2020). However, Voorhees, Fombelle and Bone (2020, p. 396) refer to frontline service workers in the retail sector as “the *forgotten front line*” since they have received relatively less attention in the popular press and elsewhere in comparison to first responders and healthcare personnel. Not only do they have to cope with health risks associated with this medical crisis, but they also have to completely modify their routine to ensure their safety and that of their customers (De Felice, 2020; Ottawa Public Health, 2020). Thus, they have to conform to and enforce corresponding regulations governing previously unstructured practices, for example, allowing a limited number of consumers into the stores (according to the allowed indoor capacity in their area), maintaining social distancing and ensuring consumers are wearing their masks (which have become a source of contention between retail workers and customers (CBC, 2021)), using personal protective equipment (PPE), screening employees and/or customers, and cleaning and sanitization. Thus, the overt surveillance role played by retail workers during the pandemic has expanded.

Findings and discussion

To explore the impact of the COVID-19 pandemic on retail, I looked at how both retail consumers and workers think about the increase in retail during the COVID-19 pandemic. Out of the 77 informants who currently work in retail, nearly 39% admitted that compared to pre-pandemic times, they now have to keep a closer eye on consumers (Figure 91). There were no statistically significant associations discovered with gender ($X^2(1, N = 77) = 2.009, p = .156$), age ($X^2(6, N = 77) = 5.648, p = .464$), education level ($X^2(4, N = 77) = 8.015, p = .091$), income level ($X^2(65, N = 75) = 10.107, p = .072$), or membership in a minority group ($X^2(2, N = 18) = 3.448, p = .178$). This is not surprising since the increase of retail is put in place by management and carried out by retail workers regardless of their gender, age, education level, or income level, and whether they are members in a minority group or not.

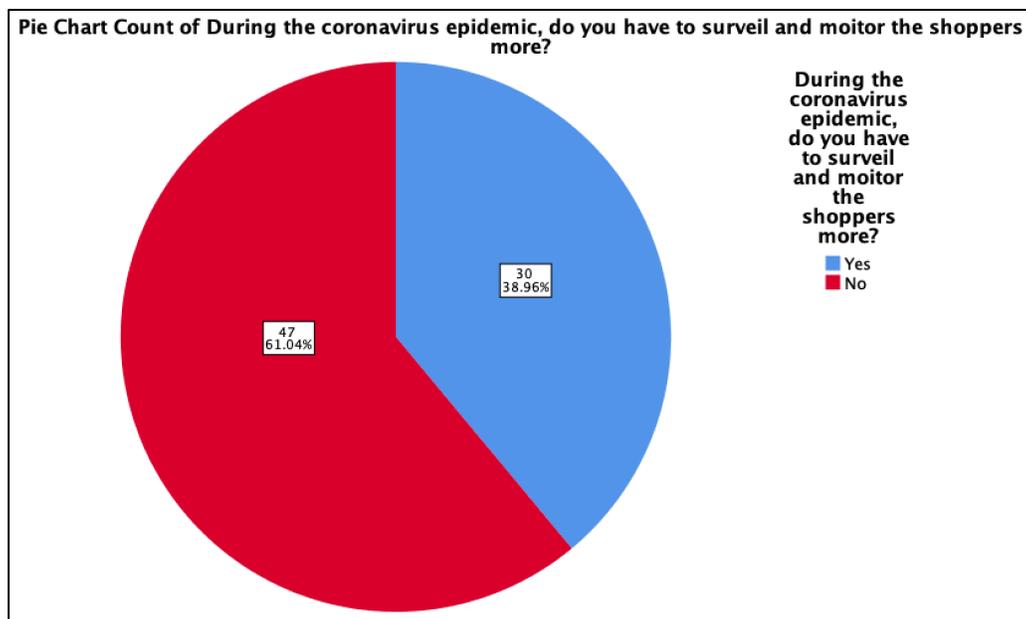


Figure 91 – Informants working as retail workers surveilling consumers during the pandemic

In the previous chapter, it was revealed that 85.3% of informants were “for” the use of retailance. However, when informants were asked to rate the statement, “When I go into a store during the COVID-19 pandemic, I accept that there are more employees surveilling the shoppers closely,” nearly 58% of informants consumers admitted that they either somewhat or strongly agree (Figure 92). This percentage shows that while a large percentage of the retail consumers (85.3%) accept retailance, not all of them (only 58%) believe that retailance should be increased (e.g., an increase in overt surveillance by being closely monitored by retail workers) because of the pandemic and the subsequent new store regulations. This statistical result was found to be significantly associated with belonging to a minority group ($X^2(8, N = 83) = 17.611, p = .024$). Compared to 56.8% of survey informants who belong to no minority groups (i.e., white, 246 out of 433) and who accept increased retailance, 79.2% of informants who identified themselves as belonging to a visible minority (38 out of 48), 14.3% of indigenous informants (1 out of 7), and 50% of informants with a disability (14 out of 28) somewhat or strongly agreed to having more retailance (Figure 93). This shows that North American visible minorities are more inclined to accept increased retailance because of the pandemic (this result should be considered with caution because of the low number of informants). No statistically significant associations were discovered with gender ($X^2(12, N = 516) = 10.919, p = .536$), age ($X^2(24, N = 516) = 29.804, p = .191$), education level ($X^2(24, N = 516) = 18.285, p = .789$), or income level ($X^2(24, N = 507) = 22.279, p = .563$). To better understand the reasoning behind consumers’ reaction towards the increase of retailance during the pandemic, an open-ended survey question asked why informants think retailers need more retailance during the pandemic. Out of 234 answers, the 25 most frequently used words were captured in the word cloud (Figure 94) and they

reflected the need to surveil consumers to ensure that new store regulations are followed, and to prevent shoplifting.

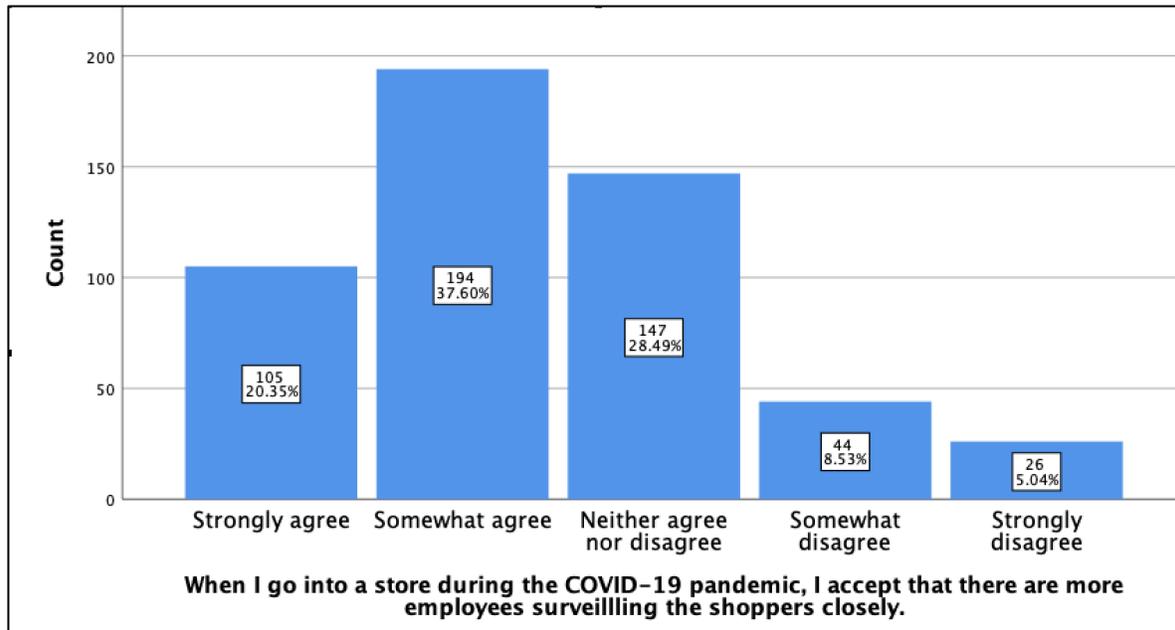


Figure 92 – Informants’ acceptance of more surveillance by retail employees during the pandemic

		Do you consider yourself to belong to any of the following groups? – Selected Choice			Total
		A member of a visible minority, which is:	An indigenous/a boriginal person	A person with disability	
When I go into a store during the COVID-19 pandemic, I accept that there are more employees surveilling the shoppers closely.	Strongly agree	15	1	4	20
	Somewhat agree	23	0	10	33
	Neither agree nor disagree	9	4	10	23
	Somewhat disagree	1	1	2	4
	Strongly disagree	0	1	2	3
Total		48	7	28	83

Figure 93 – The association between consumers’ acceptance of increased retailance because of the COVID-19 pandemic and membership in a minority group



Figure 94 – Word cloud of the 25 frequently used words by informants describing why retailers are using more retailance post the COVID-19 pandemic

Looking at the above discussion and findings from the perspective of surveillance studies, we can notice the following: (1) asking retail employees to keep a closer eye on the consumers during the pandemic turns the situation into an “Orwellian” one, in which the retail store/employee (instead of the state) uses surveillance as a means to maintain social order; (2) The situation where consumers are surveilling retail workers to ensure that the latter are following the new health regulations (e.g., using PPE) is an example of Mathiesen’s “synopticism,” where the many (i.e., consumers) watch the few (i.e., retail workers); (3) When consumers watch each other to ensure that the other shoppers are following the new public health regulations (e.g., wearing a mask), the situation can be described as “participatory panopticon” (a term introduced by Whitaker in 1999); (4) The future of post-pandemic retailance technologies will add to the “assemblage” of surveillance, for example, traffic counting cameras and sensors

will expose the shoppers to a more complex “rhizomatic” surveillance (Deleuze and Guattari), while using thermal imaging cameras and mobile apps connected to health/vaccine passes will enhance those assemblages directed towards the body of the consumer (Haggerty and Ericson); (5) An example of Bogard’s “imaginary control” over the consumer (who is considered a “virtual identity”) could be seen in the retailer’s capability to deny the consumer’s entrance to a retail store if the latter has a high temperature, which means that the retailer is recording a fact (i.e., high body temperature) and predicting that it would lead to an event (i.e., infecting the other shoppers).

To complement the survey data (discussed earlier) and to gain a better understanding of the impact of the COVID-19 pandemic on retailance, interviewees (consumers, managers and retailer workers) were asked if there is a real need for more retailance and how encountering/implementing retailance makes them feel. Figure 95 shows the three answers that emerged during the course of data collection: (1) acceptance, (2) refusal and (3) no clear standpoint.

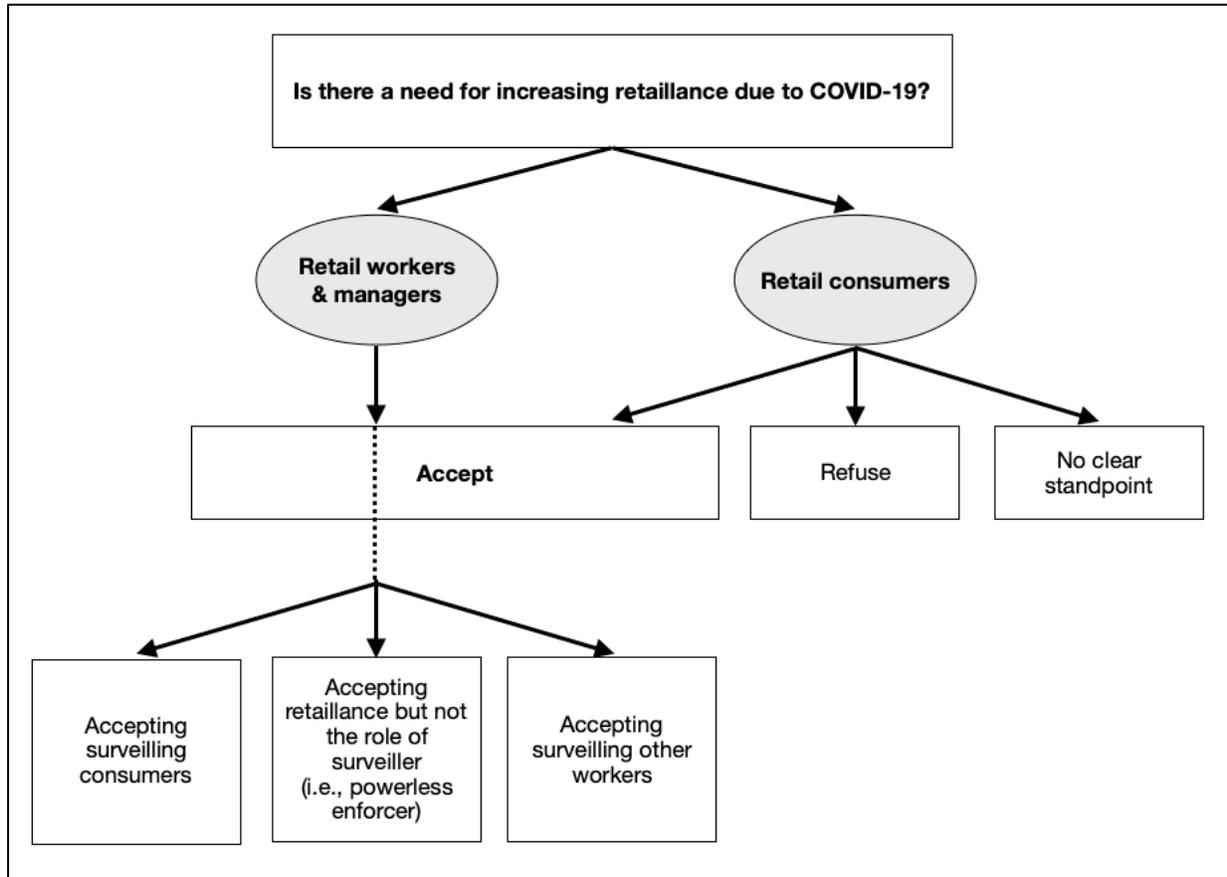


Figure 95 – The reaction of retail workers, managers and consumers towards the increase of retailance due to the COVID-19 pandemic

1. Acceptance of more retailance during the COVID-19 pandemic

This section discusses the reasons behind retail consumers', workers' and managers' acceptance of an increase in retailance because of the COVID-19 pandemic.

1.1 Acceptance by retail consumers

Many consumers agreed that stores should increase their retailance because of the pandemic.

Michael: Yes, in the sense that I think they need to kind of use their information to . . . understand that they're doing social distancing . . . [during the] corona [pandemic]. So, I think they should increase their surveillance in essence to kind of understand what better ways they can to protect people from the virus.

David accepts more retailance on the condition that it is "overt" and consumers are aware of it.

David: I guess they would [increase surveillance], but I do still think it should be overt and known. Well, I think it would help if people knew if it was overt. It would help people to focus on their social distancing and ideally, wearing a mask when they're supposed to. And it would help people to be on their best behavior in terms of the guidelines that will put forth in terms of being safe.

Myint: [It] would be kind of cool if they could afford it [more surveillance during COVID] . . . or if they could figure out a way to do it . . . And because one scenario that I can definitely see out there is someone being like, "Oh, I'm, you know, alone in this aisle. There's no one looking and I'm going to take off my mask. I'm going to like touch this product and then put it back on the shelf and then touch another one and put it back on the shelf," and like additional surveillance for COVID measures could help to keep things cleaner.

Ishita: I don't necessarily think they need to increase surveillance [during the COVID-19 pandemic] . . . The only thing that I thought would be maybe handy is like the body cams because I know that there's so many protests going on, especially people that don't wear face masks, and white supremacists. Like they are ridiculous. Things like that. And I think to protect the employees and workers, body cams are a good idea because it showcases if they get assaulted, if they're harassed for just simply doing their job. I think it's very important to do that kind of technology and like kind of surveillance is needed. But that's the only thing that I would say.

Some consumers added that they do not mind if the extra retailance is carried out by retail workers/employees who have to keep a closer eye on them,

Maria: So yeah, if you had an additional employee, it wouldn't bother me. As long as you're wearing a mask and they're wearing a mask.

Aye: I don't mind [being watched by workers] because, you know, they're doing their job. So, if I'm not doing anything wrong, I don't mind at all . . . now the COVID is there, now you have to obey that they put the rule for your safety as well as for the staff.

David: Thinking about it [workers surveilling shoppers] makes you feel safer, just to know that there is security. You know, especially these days, I think it definitely would. I went to a Walmart [in the U.S.] the other day, and that's a rarity, you know, with masks and gloves and the whole deals also distancing and . . . it's just had a bit of an apocalyptic feel there . . . I wouldn't want to be one of those employees [surveilling shoppers] . . . but, yeah, it's acceptable. I would even appreciate that, I guess.

Jennifer: I actually kind of prefer that [workers surveil shoppers in the U.S.] . . . we drove to the next county over [at the beginning of the pandemic] where there

was a mall and they had a sign like everybody had to have a mask on. And like every store that you went into there was somebody outside, making sure you have that on. And I mean, I was glad because I feel more comfortable when everybody has one on.

In general, therefore, many consumers accept an increase in retailance because of the pandemic whether it is technologically mediated (especially if it is overt) or carried out by retail workers.

1.2 Acceptance by retail workers

When interviewed, retailer workers accepted an increase in retailance to surveil consumers and/or fellow workers. However, some of them expressed that though they are not against an increase in retailance, they refuse being given the role of surveiller.

1.2.1 Surveilling consumers

Some retail workers and managers expressed a need to keep a closer eye on consumers to ensure that they are following the new store regulations:

Joshua: [Surveilling customers more at Pet Smart] Yeah, I find that especially the case with people bringing in their kids because I don't think kids necessarily understand this whole thing and what they have to do for their part to stay safe.

William: Oh, goodness, yes. Customers, you know . . . Many of them don't understand the concept of [a] personal bubble. So that's one thing that has to be monitored frequently. And proper wearing of their masks; they will come in with a mask on, but it may or may not cover their nose and their mouth type of thing. So, staff [at Independent Grocer supermarket] are put in a position where, you know, in order to protect their staff and the other customers, they didn't have to sort of monitor that kind of thing [before].

Mitig: I think [we have to surveil customers more at Loblaw] because at the start of things, like customers would get aggressive if they had to stand in the line. Some people were trying to skip the line and saying, "Oh, call the manager. I'm not waiting in the line." Or get aggressive with security teams or aggressive with workers if we were out of items. So, I think that increased security and surveillance of any kinds was necessary and still is necessary to try and make sure everything stays okay . . . We had a loss prevention team of two people . . . They have cameras in their office, but they would still rely on workers to call their extension and let them know as we saw anything suspicious. But since COVID started, they hired additional security for the store, which is very good, because

my location is right downtown. So, because of that you never really know who could be coming through the door.

Wang: I'd say that we have to surveil them [shoppers at Coach Outlet] more when it comes to like mask wearing properly . . . As for theft, we haven't really had a problem with theft. Ummm. So, it's always kind of just we're watching people to make sure they don't like take the mask off . . . that's the only reason we're paying more attention to the customers.

Taiba: Before Corona, everything was normal [in Farm Boy] and we didn't have to do this thing. Right now, what we have to watch the customers for is to if they take their masks off. For instance, when I was sanitizing at the front door, I was sanitizing carts that was also one of the things I did throughout the month, I had to watch customers not leaving their carts, to maintain the distance. I had to . . . not to force but convince them to get the cart with them.

An Assistant Buyer (i.e., a managerial position) at Giant Tiger, Hannah talked about how their stores have employees stationed at the door (to ensure that consumers are wearing masks and sanitizing their hands before entry) and others directing traffic at the cash registers during rush hour.

Hannah: I definitely think that surveillance increased just to make sure that people are following the social distancing guidelines. And making sure that people are being safe and being responsible . . . I don't think there has been an increase in surveillance like to prevent shoplifting. I think it's more surveillance to make sure that people are following the guidelines and to also like protect the other customers, but also to protect like the workers and to protect themselves.

Emma, a store manager of a wireless provider in Ottawa, differentiates between technologically mediated surveillance, like using cameras to detect fraud and shoplifting, and direct visual surveillance where employees keep watch of consumers during the pandemic.

Emma: We're definitely doing that [new regulations] in store. It just doesn't have much to do with the surveillance. So, us, like managers or salespeople, like we're told to make sure customers are wearing their masks unless they have an exemption, make sure that they're standing at side of the kiosk where there's plexi [plexiglass to protect workers]. If they're like abusive, we're not going to be tolerating it, but it doesn't really have much to do with the cameras. I would say when it comes to that, it's more for like fraud situations and stuff like that I would say.

Olivia talked about how shoplifting has increased since the pandemic started since some consumers, especially in low-income neighbourhoods, feel adequately concealed behind their masks to steal high-end perfumes and cosmetics.

Olivia: We [at Shoppers Drug Mart] have to have someone in the cosmetic sections at all time. So, from nine o'clock in the morning to 10 o'clock at night, there's no exceptions . . . So, one of our theories is that with masks on, people know that us figuring out who they are is like less likely. Ummm. I think some of that as well is where our Shoppers is located. We have a very low-income neighborhood right next door to us and I think a lot of those people have been like really badly affected by loss of income as well. So, we see the people that come in and they steal the perfume because they know they're not working, they're bored. It's just like they know they can get away with it. And then there's been a lot of people stealing groceries as well. That's been a really big problem. So, the people who literally like are struggling to make ends meet and come in and steal that. But for the cosmetics, I think it's just a crime of opportunity, like people know they're less likely to be detected when they have the mask on . . . We had a really big theft where about \$3,000 worth of perfume was stolen. And that's happened a few times and you know . . . they resell the perfume, because that makes them a lot of money as well . . . And it's been a really big source of tension in our store . . . the staff members will get blamed when these really big thefts happen. But they [management] refuse to hire a security guard. They refuse to hire for, like, just put extra people on shifts to do this, to keep an eye on customers.

To Taiba, who works in Farm Boy, announcements through the store speakers every 15 minutes to remind the consumers of the new safety measures are more than enough when it comes to extra security measures. Ashley, who works at Publix Super Markets in Deltona, Florida, echoes the same thought:

Ashley: At least at my store [Publix], if customers come in without a mask or if they're going the wrong direction, what my store does is they do announcements over the intercom to remind people that masks are required and the one-way directional arrows . . . So, I think they are watching them more to see who's abiding by the rules.

Those working in the retail sector, therefore, expressed a need to monitor consumers to ensure that the new store and health regulations are followed and to try and prevent a rise in shoplifting.

1.2.2 Accepting retailance and not the role of surveiller

Many retail workers expressed their frustrations regarding surveilling customers to ensure that they are following the new regulations. By asking them to implement those new store regulations that are not universally well-received by consumers, they have to endure the brunt force of the consumers' negative behaviours and emotions. Consequently, most of them agree that being forced into the role of "rule enforcer" is unwelcomed, for it not only adds to their emotional stress, but it also leads to direct confrontations with the consumers.

Stephanie: You get people yelling at you [in Costco] because, well, "That person over there is not wearing a mask." And it's like, "Okay, well what do you want me to do about it?" I'm not police. I'm not paid well enough to be able to go and police these people, to tell them that they have to put a mask on, you know. Like that's not what I get paid for. I get paid to make sure that you get your food and get your stuff in your shopping cart and get through the line as safe as possible. That's my job. But we can't tell people you have to put a mask on. We are told that we cannot enforce it. We can remind them that they should have a mask on, but we can't enforce it. So, you get the backlash from that.

Stephanie not only had to deal with irate consumers, but she increasingly found herself in situations where she had to referee interactions between consumers, which adds another layer to an already challenging job.

Stephanie: I could hear screaming in one of the back aisles. Of course, I looked and it was two grown men screaming at each other and throwing fists, because one individual got too close. [They were] passing each other and he got too close to the shopping cart. And I had to go and break up a physical altercation between two grown men. Just because people were freaking out . . . And that was the point where I was like, "No, this is not worth it. It's not worth the paycheck to come in here and have to deal with this." So, I took a two-week leave.

Surveilling consumers herself became a stressor, and Stephanie ended up going on a two-week leave and only returned to work when new protocols were put in place to help prevent such potentially abusive situations.

1.2.3 Surveilling other workers

Retail workers are at a significant risk of exposure to the virus simply because they interact with more people (UFCW, 2020) and there have been cases of coronavirus-related employee deaths (Bhattarai, 2020); consequently, they have to follow new practices to help prevent exposure (Centers for Disease Control and Prevention, 2020; National Retail Federation, 2020a). Retailers must have a COVID-19 health and safety plan to protect their employees (Centers for Disease Control and Prevention, 2020), including providing the latter with PPE in addition to notifying them when a colleague shows symptoms of the coronavirus (Burke, 2020).

Worried about their health and at the same time, needing the pay cheque, some retail workers talked about their feelings of confusion and worry about getting infected, not just from the consumers, but also from the other workers they interact with. To those workers, therefore, there is a need not just to surveil their colleagues, but to share any information regarding a worker getting infected with the coronavirus. Taiba, who works at Farm Boy, recounted how traumatic her work experience was during the first couple of weeks of the pandemic, between the end of March and early April 2020.

Taiba: We were very afraid. A lot of people quit jobs. There was a day where everybody at work was crying because we thought we would get it [coronavirus]. Someone at Shoppers in the same mall had [the virus], and they were taken to the hospital and Shoppers was closed for two weeks. A lot of our employees went there to the pharmacy or to just grab something like a snack or something [that] same day. And when they heard that Shoppers is closed right away, everybody started quitting for two weeks. They left for two weeks. A lot of my co-workers left but me, I was there and I was crying because I knew that I couldn't quit the job as it was a voluntary thing. And the government wouldn't fund me if I quit and, on the other hand side, I had my husband who didn't have a job. So, I was very traumatized and very afraid.

To summarize, many of the interviewed consumers said they accept more retailance (whether technologically mediated or in person by retail workers) although some hinged their

acceptance on the condition that it is overt and they are aware of it. On the other hand, retail workers and managers expressed the need to keep a closer eye on consumers to ensure they were following the new store regulations put into place because of the COVID-19 pandemic and to protect their stores against a rising rate of shoplifting.

2. Refusal of more retailance during the COVID-19 pandemic

Some interviewees were very clear about their refusal of more retailance systems, like James (a retired American lawyer in his 70s) whose immediate reaction was an “absolutely not.” In general, those consumers believe that retail stores have already installed enough retailance systems (like cameras) to monitor consumers.

Jessica: I don't think they would have to have more surveillance. I would think the regular cameras would be able to tell who was following the corona guidelines.

Sarah: Even if they see it on camera . . . then what? They're just going to like yell through the store speakers? Like “Hey, person in aisle two go[ing] in the wrong way,” like “please turn around,” . . . And if they're just going to have people on the ground, then doing that for them, then they may as well just have the people watching. It seems sort of like nonsensical to me to have more surveillance for COVID measures. And I mean, if they're screening people at the door to make sure they're healthy, then there's nothing really in that regard, no extra need for more cameras.

Some consumers were worried about the fact that store employees would be the ones who will end up surveilling the consumers more closely. For example, Michael, a Black American engineer in his 40s, who has repeatedly experienced biased surveillance due to his race.

Michael: Because what happens is that anytime that you have a system of enforcement, your bias comes into play. And you end up enforcing it with certain individuals and that certain individuals, and you're kind of never fails to where there be a situation where you have two people doing the same thing, but the person that you have a bias against will wind up being the one you try to enforce it with. There's just a lot of issues with that . . . But with all systems, when you have humans, they have their bias is going to appear in some way, and that would worry me.

The above quotes, therefore, show the point of view of some consumers who are against the “nonsensical” choice of implementing more retailance systems, especially if that retailance is direct and could lead to an abuse of consumer profiling.

3. No clear standpoint

Other interviewees were at a loss, not sure whether ensuring their safety during the pandemic is an enough reason to increase retailance.

Mary: I'm very torn about the issue with COVID because, of course, I would like to know if the particular little market, that I've been going to since the outbreak has started, . . . have had a customer in there who's tested positive. I would like to know that. But at the same time, it's really creepy to think that you could be tracked so closely and then people say, “Oh, if you're not doing something wrong, why do you care?” And it's kind of like, we don't know what people are doing with that information. If they can track you that closely and they know when you're gone, who's to say that someone who's going to come and break into your home. I mean . . . It's kind of a deep murky pool, when you get into that.

To conclude, because of the pandemic, an additional layer of surveillance has been required, whether it is direct (e.g., stationing employees at the store doors to ensure that consumers are wearing masks and sanitizing their hands before entry) or technologically mediated retailance (e.g., thermal imaging cameras and traffic counting sensors). Retailers have been tasked with ensuring that their consumers follow the new safety protocols and practices (e.g., wearing a mask properly, social distancing, etc.) and to protect their stores against a potential increase in shoplifting. This has led to more retailance, especially overt retailance carried out by retail workers. For retail workers, although they agree with the need to implement more retailance, making them act in the role of surveiller has put them into direct confrontation with irate, aggressive consumers. On the other hand, consumers' reactions to that increase in retailance varied from acceptance to refusal to having no clear standpoint. Moreover, while a

large percentage of consumers accept the presence and use of retailance in general, not all of them agree that there is a need to increase retailance in order to monitor them more closely during the COVID-19 pandemic.

Chapter summary and conclusion

This chapter has provided a review of how the retail sector is faring in North America since the outbreak of the COVID-19 pandemic and to date, and how both consumers and retail workers and managers are reacting towards the subsequent increase in retailance. Three consumer reactions were revealed: acceptance (especially amongst consumers belonging to visible minorities), refusal, and having no clear standpoint. On the other hand, retail workers and managers revealed the need to surveil both their consumers and fellow workers (specifically sharing medical information related to getting the coronavirus infection) although some talked about the extra stress they have to face when playing the role of surveiller.

In an attempt to combat the pandemic, governments worldwide have partnered with technology and health care providers in the private sector to institute tracking and surveillance systems that threaten individual privacy, for examples, in the United States, Apple and Google have provided the government with access to data from consumers' mobile phones for contact tracing (Brough & Martin, 2020, p. 1; Masoodi, 2021). Privacy advocates argue that such marked changes in privacy norms could threaten individual rights even after the pandemic has passed (Klein & Felten, 2020). Pantano et al. (2020, p. 210-211) raise the question of whether the countermeasures adopted by both retailers and governments to comply with public regulations might potentially lead consumers to lean more towards accepting more invasive surveillance measures (e.g., biometric surveillance such as face recognition, GPS tracking, body

scanning, etc.) which might further alter privacy perceptions over time. Brough and Martin (2020) argue that:

response to the outbreak has threatened privacy by reducing consumer control over the collection, sharing, and protection of some of the most sensitive types of personal information, including health and location data . . . new digital records that would not otherwise exist have been created as shelter-in-place orders have forced many consumers, including vulnerable populations [particularly those who tend to be late adopters of e-commerce, such as the elderly, disabled, immigrants, and lower-income households], to replace offline activities with online activities. (p.1)

Not surprisingly, retailers are now investing more in retailance, for example, some of Walmart Canada's key initiatives will include surveillance systems:

Accelerating digitization to create “smarter stores”, including: expanded electronic shelf labels, shelf scanners to monitor product volumes, robotics and computer vision cameras to simplify, minimize touches and maximize efficiency and accuracy. A new checkout experience to reduce touchpoints, including tap-to-pay, new bigger self-checkout and “Check Out With Me” mobile payment technology to allow associates to checkout customers anywhere in the store. (Toneguzzi, 2020a)

Optimistically, accelerated adoption of surveillance tools and online activates may lead to security enhancements that can ultimately improve privacy. In addition, post-COVID-19 consumers may become accustomed to the benefits of virtual shopping (e.g., greater convenience, reduced travel and wait times, free shipping offers), leading them to evaluate privacy cost-benefit trade-offs (Brough & Martin, 2020, p. 2).

CHAPTER 7: CONCLUSION

Old George Orwell got it backward.

Big Brother isn't watching. He's singing and dancing. He's pulling rabbits out of a hat. Big Brother's busy holding your attention every moment you're awake. He's making sure you're always distracted. He's making sure you're fully absorbed.

He's making sure your imagination withers. Until it's as useful as your appendix. He's making sure your attention is always filled.

And this being fed, it's worse than being watched. With the world always filling you, no one has to worry about what's in your mind. With everyone's imagination atrophied, no one will ever be a threat to the world (Palahnuik, 2012).

While this chapter concludes my dissertation research, it also opens up venues for future research. The chapter will proceed as following: after an introduction, the different research contributions (conceptual, theoretical, and practice-oriented for consumers, retailers, and public policy makers) are discussed. The chapter ends with a discussion of the research concerns and limitations and avenues for future research.

Nowadays, consumers are constantly seduced by the assorted abilities of the various new retailance technologies and by an array of promotions and rewards. Yet this research neither approaches retailance as inevitably dangerous nor as a hallmark of progress, for while there is a need for transparency and accountability, both consumers and retailers increasingly rely on retailance.

In Chapter 1, retailance has been defined as following:

Retailance, or surveillance in a brick-and-mortar retail setting, is the focused, systematic, and routine scrutiny of consumers and/or the collection of their personal and shopping data, which goes beyond what is voluntarily reported, for purposes of influence, management, protection, retail crime identification, shrinkage prevention, improving the consumer's shopping experience, and/or profit. Surveillance may be direct (face-to-face) or technologically mediated (overt or covert in-store security systems).

Yet what does the trend toward surveillance in retailing mean? Surveillance has even been commodified, where it (or the protection from it) is now a product to be purchased (Marx, 2012,

p. xxvi). Does surveillance imply a shift toward societies of dystopian social control and segmentation that transcend the omnipotent panopticon and the all-seeing Big Brother? Threats to privacy and liberty are not restricted to state power or the use of force. Dystopias like *Nineteen Eighty-Four* or *Brave New World* imagined an omnipotent, repressive state, yet today, the private sector, and its increasing surveillance of consumers, is proving to be as powerful, if not more powerful, as the state. Bogard (2006, p. 61) writes:

This is not Big Brother. In a world already scoured of problems, who needs an omnipresent watcher? And it is not Brave New World either. The new controls do not work on the level of pleasure or pain, but on the *plane of desire* [emphasis in original].

Graham (1999) argues that for retailers who interweave surveillance systems into their business, and within the context of a political economy dominated by a profit-driven ethos, surveillant-simulation systems have emerged as crucial techniques for bolstering profitability, flexibility, and responsiveness. One of the major challenges faced by retailers is getting shoppers to accept new data and surveillance practices, by implementing them in ways that do not alienate desirable customers worried about their privacy, and even make them happy to receive relevant offers and shopping deals (Turow, McGuigan, et al., 2015). One way to achieve this compliance is by investing in the consumer-retailer relationship, for trust is central to the customer experience (Isaeva, Gruenewald, & Saunders, 2020) since consumers need retailers to put their (i.e., consumers') needs first, respect them, and protect their privacy. Singh and Jain (2015, p. 971) define trust in a retail context as

...*emotional security in terms of fulfilment of tangible (retailer, employees, products etc.) and intangible (policies, communication, relationship quality etc.) expectations and a belief that dealings with the firm will be reliable, dependable and safe* [italics in original].

As discussed in Chapter 5, consumers' negative behavioural reaction towards retailance (one of its reasons being lost of trust) leads to resistance which can take several forms.

Then how can we (as consumers, retailers, marketers, and researchers) differentiate appropriate from inappropriate uses of surveillance? The answer to that question is grounded in the critical marketing approach employed in this research. Personal information defines our experience as consumers, however, though the personal information economy offers us many benefits, it has a broader impact and poses many risks, hence, the theme of understanding (the positive uses of retailance) versus mistrust (of the negative implications of retailance to privacy). To help consumers and interested stakeholders (note that involving multiple stakeholders is an element in critical marketing) better understand the benefits and risks of information use, there should be greater transparency about how organizations collect and potentially use data. This could involve allowing consumers to access their data, providing ongoing choices about information use, and making it easy for them to opt out of data collection (Lace, 2005, pp. 238–239). This challenging of the current retailance practices to bring beneficial change is a concern of critical marketing that would ultimately lead to a change in public and privacy policies. Thus, I recommend that privacy and data protection laws and policies be in a constant state of renewal and revision to be on par with the ongoing developments in technology and surveillance practices. A measure of democracy would be the extent of restrictions on and mandatory requirements for information flow across actors (i.e., different stakeholders) and sectors (e.g., retailing) (Marx, 2012, p. xxv). In the 1960s and 1970s, the first generation of consumer policy and advocacy focused on product safety (from cars to toys). The second generation advanced a wider agenda on services (from travel to pensions)

(Lace, 2005, p. 242). Today, we need to develop a new generation of consumer policy capable of addressing the current interests and fears of consumers in regards to protecting their privacy.

Surveillance, in general, always carries with it some plausible justification that makes most of us content to comply. To Lyon (2001b), the question of surveillance goes beyond the fear of data breaches and the concern with privacy, for its dark side is its “capacity to reinforce social and economic division, to channel choices and to direct desires, and even, at its sharp end, to constrain and control” (p. 4). According to the findings gleaned from the collected data, retailance can lead to direct and on the spot unequal treatment and further marginalisation of some consumers (such as Black Americans, consumers with visible tattoos, young consumers, and consumers who look too poor to afford the merchandise of the retail store they are visiting). Consumer information (whether personal or of consumption history) collected via retailance systems can be also used for segmentation, targeting and positioning, leading to possible discriminatory profiling of consumers by sorting them on their estimated value or worth to the retailer. From a critical marketing perspective, this discriminatory marginalization of consumers takes place when the scale of power (i.e., complete and unchecked control of the retailance process) is tipped with the retailer. By examining the origins of surveillance, both as theory and as practice in the field of retailing, this research attempts to further the understanding of the use of surveillance in the retailing sector, and its impact on both retailers and consumers.

Contributions

To generate the research questions for this research, I followed what Alvesson and Sandberg (2011) described as “gap spotting,”⁴² a process of identifying or constructing gaps in existing literature that need to be filled. Locke and Golden-Biddle (1997, p. 1030) described how a research gap is created by synthesizing coherence in which the researcher can “cite and draw connections between works and investigative streams not typically cited together . . . [which] suggests the existence of underdeveloped research areas.” The version of gap-spotting I followed was “neglect spotting” through which research questions are constructed to address spotting an overlooked area (i.e., surveillance in a brick-and-mortar setting), an under-researched area (i.e., the impact of surveillance in a brick-and-mortar setting is not as researched as that in an online setting), and a lack of empirical support (i.e., according to the conducted literature review, there is a scarcity of academic research based on a combination of theory and empirical findings) (Sandberg & Alvesson, 2011). In Chapter 1, a list of research questions was introduced: how much are consumers aware of the presence and scope of retailance? Are consumers aware of the laws and regulations that protect their personal information? What is the behavioural reaction to retailance (i.e., do consumers accept, negotiate or resist retailance)? What is the attitudinal outcome of retailance? What is the behavioural outcome of retailance? And finally, what is the impact of the COVID-19 pandemic on retailers’ use of and consumers’ reaction towards retailance? By answering those questions, this research enriches the prior literature concerning

⁴² Although gap-spotting plays a significant role in developing existing management literature, Alvesson and Sandberg (2011, 2013) call for the use of the “problematization” methodology that helps “to identify, articulate, and challenge different types of assumptions underlying existing literature and, based on that, to formulate research questions that my facilitate the development of more interesting and influential theories” (Alvesson & Sandberg, 2011, p. 267). However, in this research, retailance is a relatively untapped field of study and at this stage, it needs research gaps to be identified more than challenged.

retailing and surveillance, and its findings have various contributions that are conceptual, theoretical, practice-oriented (for both consumers and retailers) and relevant to public policy. A summary is provided in Table 26.

Contributions				
Conceptual	Theoretical	Marketing practice		Public policy
		Retail consumers	Retailers/ Practitioners	
<ul style="list-style-type: none"> • Bridging disciplines • Summarizing: literature review • Delineating: conceptual framework • Coining a new term (retailance) • Creating a retailance model • Updating past research • A macro perspective 	<ul style="list-style-type: none"> • Theory development • A multidisciplinary perspective through differentiating (classifying surveillance studies) and integrating past research • Opening up new areas of study • Creating a new model of theories through theory synthesis (summarizing and integrating) and typology (categorizing fragmented research) • Pragmatic importance • Reconciling contradictory reactions to retailance 	<ul style="list-style-type: none"> • Helping consumers understand their privacy rights & how retailance impacts them (both positively and negatively) 	<ul style="list-style-type: none"> • Helping retailers/ practitioners understand consumers' preferences in order to adjust their use of retailance 	<ul style="list-style-type: none"> • A better understanding of the ethical implications & impact of retailance on consumer behaviour

Table 26 – A summary of the contributions of this research

(1) Conceptual contributions

According to MacInnis (2011), conceptual academic work has five main contributions: (1) it plays a critical role in knowledge representation; (2) it helps in identifying, comparing, and distinguishing dimensions of our thinking and experience; (3) it helps academics and

practitioners categorize situations and decide what to do (i.e., action significance); (4) it reflects basic units of knowledge advancement; and (5) it forms the basis on which measures are derived and from which theories are tested (p. 141). Two possible conceptual contributions in the field of marketing are “relating” (i.e., “differentiating” and “integrating”) and “explicating” (i.e., “delineating” and “summarizing”) ideas, the other two being “envisioning” (i.e., “identifying” and “revising”) and “debating” (i.e., “advocating” and “refuting”). Janiszewski, Labroo and Rucker (2016) identify three strategies relevant to conceptual knowledge creation: bridging disciplines (i.e., “identifying pertinent theories that have been used to explain phenomena in another domain”), challenging assumptions (i.e., “identifying contexts where existing theory-based assumptions do not hold”), and introducing mediators and moderators (i.e., “providing evidence for an intervening process that explains the causal influence of one construct on another, as well as identifying conditions under which the causal relationship and/or process persists”).

The systematic literature review provided in this dissertation integrates published literature, synthesizes prior studies (Marabelli & Newell, 2014; Paul & Criado, 2020), identifies key knowledge gaps, and develops new theoretical frameworks, thus serving as a platform for future research. In the literature review, therefore, my contribution is twofold: first, I updated previous marketing research by including new retailance technologies not studied before; second, I provided a macro perspective by studying the impact of all retailance systems and channels at once instead of focusing on one system at a time (which has never been done to date). The creation of a retailance model is another conceptual contribution, for it brings together different disciplines, challenges how we look at the relationship between consumer and retailer in the context of retailance, and provides moderators (based on the research findings)

that explain the different influences. Moreover, since this research is exploratory, one of its aims was to create a model that (after testing and refining) would become the stepping-stone for future research. Thus, by coining a new word (i.e., *retailance*), providing definitional clarity, and creating a conceptual *retailance* model that works as a roadmap for this research and opens new avenues for future research, this research makes conceptual contributions to the fields of marketing, retailing and surveillance studies.

Huey (2009, p. 233) states that surveillance and counter-surveillance remain “largely contested, fluid terms in the academic literature” and therefore, in need of a significant amount of additional theoretical and research activity. This research has made conceptual contributions, primarily, understanding *retailance* by identifying the patterns, connections, and key underlying patterns. Conceptual advancements are relatable to theory and are critical to both academics and managers (MacInnis, 2011, p. 141). Conceptualization helps in: (1) clarifying the working of the world around us; (2) aiding managers to predict outcomes and marketers to better understand how to manipulate or arrange environments so that desired outcomes can be realized; (3) refining our understanding of the world by understanding the conditions under which actions will or will not produce desired outcomes; and (4) developing our knowledge.

To sum up, when applying MacInnis’s terminology to this research, the following conceptual contributions could be traced: (1) coming up with a conceptual framework of *retailance* that describes what it is, why it should be studied, how it works, and its roadmap for future research (i.e., delineating); and (2) providing a comprehensive literature review of published work that is clear, inclusive, accurate, has relevant conclusions, is simplified through reduction and helps in developing research priorities (i.e., summarizing). In conclusion, by advancing the conceptual framework of *retailance*, and creating a *retailance* model, this

research contributes to the vitality of the field of marketing by opening new and unexplored areas of study.

(2) Theoretical contributions

In general, this dissertation could be considered at the pre-theoretical stage in which the created heuristic model of theories identifies important analytical concepts. The research offers different theoretical contributions covering: (1) theory development; (2) a multidisciplinary perspective; (3) opening up new areas of study; (4) a new model of theories; (5) pragmatic importance; and (6) reconciling contradictory reactions to retailance.

2.1. Theory development

Although theories are needed to guide and inform consumer and marketing research, there is a scarcity of research aimed at theory development. One contribution of this research, therefore, is addressing the concern of “the decline of conceptual articles [aimed at theory building] and restoring their synergistic balance with other forms of scholarship” (Yadav, 2010, p. 1547).

2.2. A multidisciplinary perspective

This research makes another contribution to theory by embracing a multidisciplinary perspective on the development of surveillance studies (i.e., theories) and surveillance systems employed in retailing. This is achieved by bringing together past research by leading scholars from the fields of marketing, consumer behaviour, political science, communications, media studies, science studies, war studies, law, cultural studies, sociology, criminology, and literature. The process of borrowing theories from other disciplines (Murray et al., 1995) is achieved by (1) classifying the various surveillance theories, indicating how they are different and why that

matters, and showing what novel insights can be gleaned and/or what findings can be reconciled from such differentiation (i.e., differentiating); and (2) explaining extant knowledge and inconsistent findings in both the literature review and the theoretical foundations, and revealing novel insights (i.e., integrating). This research, therefore, follows in the footsteps of marketing researchers who have imported fundamental and interesting theories from other disciplines and introduced them to the marketing field (MacInnis, 2011, p. 115). The importance of conceptual advances pertaining to theories have been discussed by MacInnis (2011, p. 141) who identifies four reasons behind their importance: (1) they help “clarify the workings of the world around us;” (2) they enable “the development of process measures that have value in diagnosing whether a person is on course and what must be done to correct off-course deviations;” (3) they help “refine our understanding of the world by understanding the conditions under which actions will or will not produce desired outcomes;” and (4) they are “critical to knowledge development.” To conclude, by combining this multidisciplinary perspective with a critical marketing approach, novel insights when looking at retailance are revealed, for example, the power struggle between consumer and retailer, the impact of the assemblage of different retailance channels and systems on the consumer which leads to a need for updated public policies, how the use of retailance can lead to unequal treatment of marginalized groups, and how consumers are increasingly treated as virtual sources of data instead of visible individuals.

2.3. Opening up new areas of study

MacInnis (2011, p. 142) also discusses how conceptual advances at the domain level of the area/field of marketing (i.e., retailance in this research) “contribute to a field’s vitality by opening new and unexplored areas of study” and “foster spheres of competence and expertise.” Conceptual and theoretical work, therefore, provide the foundations for subsequent empirical

work (D. W. Stewart & Zinkhan, 2006). Moreover, with technological innovations transforming marketing practice and consumer behaviour, there is an urgent need for consumer research founded on theoretical and conceptual research that would push marketing scholarship out of its present confining boundaries (Moorman, van Heerde, Moreau, & Palmatier, 2019; Rifkin, 2011). A contribution of this dissertation, therefore, is opening up new venues of research by helping us understand the role played by current and emerging new surveillance technologies in brick-and-mortar retail and how to situate them within a larger frame of retailance studies, which is the first step towards studying their impact on both retailers and consumers.

2.4. A new model of theories

The chapter discussing surveillance studies is a conceptual work built on theory synthesis and typology (Cropanzano, 2009; Delbridge & Fiss, 2013; Jaakkola, 2020). (1) “Theory synthesis” is achieved by linking previously unconnected or incompatible surveillance studies that are fragmented across different literatures in a novel way through summarizing and integration; the chapter’s contributions, therefore, are pulling disparate elements into a more coherent whole, and helping to identify and underscore commonalities that build coherence and unveil a bigger picture pattern. (2) Chapter 3 can be also described as a “typology” work in which categorization is developed by organizing fragmented research, hence, a contribution through the differentiation of extant knowledge of a phenomenon or theories (i.e., retailance).

Stewart and Zinkhan (2006) define “good theory” as that which “identifies casual structures that provide the basis for forward prediction” and which “provides explanations of marketing phenomena” (p. 478). It is within this context that I introduced a new model of theories that can inform and inspire research which can broaden the current boundaries of studying surveillance in a brick-and-mortar retail setting. To synthesize the progress of

surveillance studies in the context of retailing, three groups of theory were identified and discussed in the model: panopticism/synopticism/post-panopticism; assemblage; and virtual identities. By developing a new theoretical framework, this research falls under what Yadav (2010) describes as the “strategy of interrelations” which initiates theory development that combines previously unconnected fields or bodies of knowledge (p. 1552).

[Using interrelations] spurs theory development by creatively integrating bodies of knowledge from one or more substantive areas to generate new insights and research opportunities . . . [which] can lead to important breakthroughs and create a new research stream. (p. 1552)

2.5. Pragmatic importance

Marketing theory is not just a tool to explain present and new phenomena, for it has a pragmatic importance for marketing practice. Rotfeld (2014) argues that practitioners need more than data analysis if they seek long-run business success, for “it also helps if the research generates a greater understanding of context, a theoretical explanation that could make predictions for the future” (p. 326). Even when research data is unavailable, Rotfeld stresses the fact that “theories provide an important tool for practitioners in guiding decisions by explaining and predicting consumer decision making when new specific research data might be unavailable,” for “an understanding of relevant theories provides a basis for new decisions, especially when new data are unavailable” (pp. 322-323).

2.6. Reconciling contradictory reactions to surveillance

By adopting a critical marketing perspective that allows the involvement of different stakeholders (i.e., the points of view of retailers/practitioners, consumers and researchers/theorists) and helps us in understanding the complex relationships between them (based on understanding versus mistrust and the shifting centre of power between them), this research reconciles two contradictory reactions to surveillance: (1) marketers’ reaction to

surveillance which tends to emphasize its positive aspects and outcomes to both retailers and consumers, and (2) surveillance theorists (many of whom are sociologists) who are inclined towards being critical of surveillance and its negative effect on both individuals and societies. This is achieved by understanding the perspective of both stakeholders (consumers and retailers), the importance of retailance to both of them, and the breaking point that when reached, consumers start resisting retailance (a reaction that negatively impacts the retailer). Thus, it is imperative to maintain a delicate balance between gaining benefits and protecting consumer privacy (examples are given in the next section).

To sum up, my research offers various theoretical contributions. (1) It fills a gap in marketing research by focusing on theory development. (2) It embraces a multidisciplinary perspective through the process of differentiating and integrating past research. (3) It contributes to the vitality of the fields of marketing, retailing, consumer behaviour, and surveillance by opening up new and unexplored areas of study. (4) It introduces a new model of theories which groups those theories based on how they explain retailance. (5) It has a pragmatic importance for marketing practice, for the model of theories provides explanation and can help guide practitioners' (i.e., retailers and marketers') future decisions. (6) It reconciles two contradictory reactions to surveillance by marketers (who tend to emphasize the positive aspects and outcomes of retailance) and surveillance theorists (who are inclined towards being critical of retailance and its negative impact). This reconciliation is further tested and explained through the analysis of data collection, showing the benefits of retailance (to both retailers and consumers) and at what point it starts alienating consumers.

(3) Marketing practice contributions

The implications of this research are important to both consumers and retailers.

3.1. Retail consumers:

To consumers, accepting the different retailance systems (discussed in Chapter 2) and trading off their personal, shopping and consumption information is the price they pay for receiving retailers' incentives and benefits, such as a better service, personalized promotions, reward points, better pricing, or coupons for future purchases. In addition, to some consumers, retailance evokes positive feelings of physical safety and protection. Thus, many are willing to take risks as long as they receive benefits in exchange for being under surveillance. Although this exchange of personal and shopping information is beneficial to both consumers and retailers in many aspects, it does pose privacy challenges if the information is disseminated outside the originally intended contexts. On the other hand, the excessive use of retailance can lead to consumers' feelings of distrust and intimidation for being under constant surveillance, ultimately becoming a risky choice for the retailers themselves. While there is a general sense of hopelessness when it comes to submitting their information, protecting their privacy, and resisting all those retailance systems, consumers can easily make the decision to change retailers, shop less frequently, or move to the online platform.

The research, therefore, is beneficial to retail consumers who, in addition to expecting increasingly higher levels of responsiveness and service quality, need to understand their privacy rights and how retailance impacts them (for example, by reading privacy policies before signing them off), and how to deal with such surveillance (i.e., should their behavioural outcome be one of acceptance, negotiation or resistance?) so that they can promote their own personal and financial well-being. Based on consumers' level of awareness of retailance, (mis)trust of

retailers, and having (or not having) a sense of control over their personal information, consumers can end up being content, concerned, or fearful that their privacy is being violated, and their reactions range from acceptance, to resignation, to objection, to resistance.

Consequently, when navigating their world of retailance and infringement of privacy, consumers need to find different ways of coping and protecting themselves. For example:

- (1) Consumers need to take retailance seriously and to be more sensitive to privacy matters; they need to be aware of how they are surveilled inside the store and how their data is used. While adhering to privacy laws and regulations should be a retailer's responsibility that is overseen by the government, in reality, even if privacy regulations are followed, the laws are not on par with the rapid technological development which results in various ethical dilemmas. It is, therefore, up to individual consumers, privacy activists, and organizations advocating for consumer protection (e.g., Consumers Council of Canada, Consumers' Association of Canada, Consumer Federation of America, and Consumers Union in the U.S.) to be vigilant.
- (2) Consumers should know that having "nothing to hide" is not an enough reason to forsake their privacy rights.
- (3) To understand their rights, consumers need to read privacy policy texts, instead of ignoring or skimming them, before signing off on them.
- (4) Negotiating with the retailer is a good behavioural reaction toward retailance. Consumers should be encouraged to ask for explanations pertaining to why the retailer needs a specific type of information (shopping and/or personal) and how the collected information will be used and safeguarded. They also need to only give out their shopping and personal data to retailers they trust.

One of the important implications of this research is bringing more awareness of the retailance technologies to consumers' attention. Based on my observations, the change in respondents' attitudes towards retailance (when comparing their answers at the beginning and at the end of the interview or survey) is worth future investigation. A swift impact of this research could be traced through the reactions of some the interviewed and surveyed consumers.

Christopher: I think it [interview] was very thought provoking. It really made me kind of like . . . had ideas about things about surveillance and when it's necessary, and when it is extraneous and too much. So, I feel like you ask the right questions because it really made me kind of, you know, I had some ideas, but it even helped me hone it a little further. So, I think it was very good.

Sarah: I found this [interview] super fun and also now, I'm going to like watch out for all this new security. I've never . . . My mind is blown! Maybe I will start also reading those notices [privacy policies].

Ishita: I think that was really well done. Like, I learned so much too and I think it was very informative, like I really enjoyed it.

The above quotes, therefore, show how increasing consumer awareness is the first step towards helping them weigh the benefits they receive for accepting retailance and the implications to their privacy. To get this research out to the public, I have started to present it in academic conferences and post-graduate contests, and to have it published in conference proceedings, academic journals, and online articles geared towards the public. To share the information more broadly, I intend to get some parts of the research published in Carleton University's E-Newsletter and *The Conversation* (a not-for-profit online media outlet).

3.2. Retailers/practitioners

As discussed in Chapter 2, retailers need retailance to (1) control loss and enhance security, (2) create a pleasant and personalized shopping experience, (3) enhance profitability, and (4) ensure safety during the pandemic. Therefore, from the retailer perspective, collecting

consumers' personal information is of paramount importance (Aiello et al., 2020). However, for them to grow and prosper, retailers have to navigate the thin line between using retailance to improve their profits and marketing effectiveness, being responsive to the consumers' increasing demand for technology, convenience, and better personalized deals, protecting consumers' health and safety during pandemics, and, on the other hand, alienating consumers weary of the implications of surveillance on their privacy.

Discussing what he describes as a "dilemma for retailers," Bonfanti (2014) argues that "It is not enough for retailers to rely on simple and functional store surveillance systems that are only designed to ensure a high level of security, they must also satisfy their customers in terms of their shopping experience." Thus, the retailance systems chosen by retailers can be positively or adversely perceived by consumers depending on how they emotionally affect their shopping experience. Consequently, retailers should invest in solutions that induce positive emotions in their customers and reinforce retailer/consumer relationships by means of an adequate level of security without interfering with CSE (Customer Shopping Experience). For example, during the interviews, some consumers were excited about using the digital fitting rooms while others were 'grossed out' by the EyeSee mannequin. Thus, while retailers have the right to protect their stores, employees and customers, to control their inventory shrinkage and to enhance their profitability, they still need to maintain a good relationship with their customers, not just by offering incentives, but also by building trust and being upfront about retailance and how data is secured.

Hulland and Houston (2021) call for examining "behavioral outcomes that both strengthen the theoretical contributions of . . . research as well as offer important managerial insights" (p. 440). By understanding consumers' attitudes and behaviours towards retailance

methods, retailers will be able to better understand their consumers' preferences, and, with this information, they can adjust their retailance methods. Thus, this research is relevant to practitioners because the results can provide insight to retailers using or exploring the use of different retailance systems and the impact of this use on consumer and societal well-being.

Based on the collected and analyzed research data, the following is a list of suggestions for retailers when employing different retailance channels and systems:

- (1) Retailers should be aware that excessive use of overt and formal retailance (e.g., having consumers followed by store security) can put consumers under pressure and prevent them from haptically experiencing the store merchandise (which influences purchasing and encourages consumers to shop in physical stores instead of online). To effectively employ retailance without alienating those consumers, retailers could employ a combination of formal/informal (an example of informal retailance is a store design that maximizes visibility and is well-lit) and overt/covert retailance. Thus, to stop honest consumers from feeling insecure, which turns the store environment into one of hostility, I agree with Kajalo and Lindblom (2016) that employing a mixture of formal and informal surveillance can help consumers feel secure and, at the same time, have a good shopping experience.
- (2) Retailers need to be cautious when experimenting with and introducing new technologically mediated retailance systems (e.g., facial recognition or emotional tracking), for they do not want to introduce the "creep factor" and make consumers feel uncomfortable when shopping. After weighing the benefits (e.g., more security and providing their customers with a memorable experience versus losing potential shoppers), retailers can choose to go ahead with introducing those new retailance

systems (preferably after ensuring that the consumer is aware of and understands the rationale and value of those systems) or forsaking them and looking for a more acceptable alternative.

- (3) While many consumers accept to trade their shopping information for better services and incentives, they are more hesitant to trade their personal information. For example, while many consumers feel that giving out their postal/zip code does not threaten their sense of privacy, since they apply to a group of households, they are more hesitant to provide retailers with their dates of birth or phone numbers which are more specific to them as individuals. Retailers, therefore, should prioritize the type of information they ask their consumers to trade, for they run the risk of consumers not just withholding that information, but also of deliberately providing the wrong information.
- (4) Some informants revealed that even though they are hesitant about having their information tracked, they accept this type of retailance if it is carried out by retailers they frequent and trust. Retailers, therefore, need to ensure having a good, solid relationship with their consumers that is built on trust and that caters to the latter's shopping needs.
- (5) To consumers hesitant about accepting retailance and sharing their information, retailers need to be transparent about how they collect and safeguard their consumers' data, and the implications to consumer privacy. This is important because while retailers generally lack consumer trust when it comes to data protection (e.g., against data breaches), they are held accountable for its protection. In other words, to build trust, retailers need to engage consumers on how their data is being used (for example, to increase efficiencies in operations, to improve product selection, and to enhance in-store

services or experiences (Sides et al., 2019, p. 6)). In addition, retailers need to have policies and procedures in place to assess privacy risks (e.g., data breaches that compromise their customers' privacy), to notify their customers when they are affected by a breach, and to enhance their security systems.

- (6) If consumer data is sold to third parties, it is essential that retailers get their consumers' prior approval of having their data sold.
- (7) This research shows that consumers are hesitant to sign up for retail loyalty programs (despite the expected benefits and their general lack of concern about their privacy) because of the fear of receiving too much marketing correspondence. Retailers, therefore, could get better membership rates to their loyalty programs if they address this concern of how (i.e., through which medium) and how often (i.e., frequency) they communicate with their card holders. This could be achieved by providing their consumers with the option of how often they would like to receive the retailer's communications and how they would like to receive that communication (e.g., via email or the post).
- (8) While some consumers embrace loyalty programs because of the expected trade-offs, others do not expect to receive enough financial benefits because of the low volume of their shopping to warrant signing up for loyalty programs. Those consumers, therefore, are an untapped market segment beyond the reach of loyalty programs that retailers and marketers can target through other marketing programs, such as using different sales promotions and price strategies.
- (9) Tagging is a cost-effective retailance system. However, some consumers are not very forgiving when they experience triggering a false tagging alarm (e.g., they feel

embarrassed for being signaled out or frustrated for having to go back to the store to remove/deactivate the tag), which might jeopardize their future shopping habits (i.e., choosing another retailer). To avoid any negative repercussions to the retail store, retail personnel should be well trained in handling the tags and avoiding discrimination of all types, and when a tag is falsely set off, they need to apologize to the consumer and quickly try to alleviate their feelings of embarrassment and annoyance.

(10) Retailers need to be transparent about the type and impact of their retailance systems.

This can be achieved by giving consumers the chance to give informed consent, which can only take place when the retailer provides accurate information to the consumer about the type of information collected via the different retailance systems, who will have access to it, how long will it be kept, how it will be used, and how it will be protected. Such information could be provided by the salespeople in the store, by printing and hanging it (e.g., next to the cashier, next to the store entrance, or in the changing rooms), or by sending it via email (if the consumer is a member in the stores' mailing list).

(11) Pressuring consumers to give away their information (e.g., by repeatedly asking for it) can lead to frustration. Retailers, therefore, need to tread carefully when trying to convince consumers to disclose their information, keeping in mind whether providing their full services is contingent on receiving that information or not.

(12) To convince consumers skeptical of retailance, retailers need to show how the use of retailance is beneficial to the consumer and not just the retailer.

(13) Retailers need to be careful when directing retailance towards consumers who are members in minority groups or who look different (e.g., have visible tattoos). One of the

interviewees suggested that such targeting could be avoided by (1) being fair by surveilling all consumers equally, and (2) hiring visible minorities to surveil retail consumers overtly and directly (e.g., as store security) and/or to operate technologically mediated retailance systems (e.g., monitoring CCTV footage). However, this puts an unfair burden on individual retail workers, for targeting minorities is a systemic problem that is engrained in the technology and its algorithms, for example, face recognition surveillance technology can be racially biased (Najibi, 2020). Retailers, therefore, are encouraged to ask about the algorithms behind the technologically mediated retailance systems they intend to purchase and implement.

- (14) During the pandemic, although many (consumers and retail workers) argue that there is a need to increase both overt and covert retailance (e.g., to monitor occupancy rates, social distancing rules, and health screening), when retail employees are tasked with implementing those changes, they are put in direct conflict with the consumers who are against the increase of retailance because of the pandemic. Retailers, therefore, should be careful when implementing more pandemic-related retailance in order not to antagonize their consumers and add to their employees' stress.

To sum up, retailers need to perform a delicate balancing act with retailance. On the one hand, they need to implement retailance and collect consumer data to drive growth, enhance consumer engagement, and reduce exposure to risk. On the other hand, they need to make their consumers feel valued (a protection against defection) and to be transparent with their consumers and build trust; this can be achieved by addressing consumers' fear of retailance and their need to have more control over their data. Retailers, moreover, need to be prepared for upcoming privacy regulations. Marketing associations (for example, the Canadian Marketing Association

(CMA) and the American Marketing Association (AMA)) can play a crucial role in educating their members and providing them with resources for a full understanding of compliance and legislation.

(4) Public policy contributions

By following a critical marketing perspective that acknowledges the rights of different stakeholders (i.e., consumers and retailers), I acknowledge that public policy can help with the topics of power (i.e., ensuring that the retailer does not have an unrestricted power of control and surveillance over the consumer) and trust (i.e., privacy laws and regulations can help retailers achieve a relationship built on trust with consumers) when it comes to retailance. In their 1986 paper, Gandy and Simmons outline the responsibility of scholars:

We must find ways to raise the level of political debate about what we see as threats to the basic moral and political principals of democracy. We must strive at every opportunity to make connections between actions and consequences, benefits and hidden costs. We must begin to articulate what the right of privacy means in concrete social and political terms. (p. 166)

Although technological advancement usually takes precedence over discussion of the potential detrimental effects to individuals and/or society at large, we, as scholars and researchers, need to be mindful of the potential socio-ethical and behavioural changes. Marketing academics, for example, need to study the interplay between retailance and privacy from the perspective of both stakeholders (retailers and academics) not just to build awareness (which is the first step towards change), but also to find solutions that would allow the different parties' goals to coexist. In a telephone survey of Canadians on privacy-related issues (Office of the Privacy Commissioner of Canada, 2019), two-thirds of Canadians said that government should be responsible for helping them protect their personal information. This underscores the important

role policy makers are expected to play. In this digital age, the ambiguity and absence of a concrete definition of privacy is challenging and it impedes the development and updating of privacy legislation and policies. While consumer complacency is currently leading to favourable outcomes for businesses, privacy activists and policymakers need to recognize that many of those practices are unfair to consumers. Consumers need not just the ability to learn how to access their information, but to also control what information is in their consumer profile.

Consumer privacy is a hotbed topic that has sparked considerable debate about consumers' rights and the role of policy makers in protecting them (Brough and Martin, 2020; Yun, Lee and Kim, 2019). However, the focus is often directed at protecting consumer privacy on the online platform (e.g., Lwin, Wirtz and Williams, 2007). Even when retail surveillance is studied, researchers tend to focus on only one aspect or method of surveillance; there is no previous research that provides a general and more comprehensive understanding of the consumers' awareness of retail surveillance, the impact of its presence and their reaction to it, and how such knowledge could impact the retailer. In the field of retail, comprehensive privacy legislation should set forth the initial guidelines needed to establish rules concerning the situations when a consumer's profile information can be shared with entities other than the consumer. Comprehensive data privacy legislation should also include amendments to existing laws not only pertaining to online data, but also to data collected offline inside the retail stores. Thus, for public policy makers, a better understanding of the impact of retail surveillance on consumer behaviour and its ethical implications is but the first step towards updating and implementing legislation. This study, therefore, will help policy makers gain a better understanding of the impact of traditional surveillance and smart retail technology on consumer behaviour and its ethical implications by providing empirical evidence as the basis for policy (re)formulation.

The following is a list of recommendations for public and privacy policy makers inspired by this research:

- (1) During data collection, it became clear that, unfortunately, the majority of informants were not only unaware of legislative protections of their privacy, but they also had doubts about the type of protection those regulations can offer. This lack of belief in the effectiveness of legislation leads to consumers not bothering to learn about legislative protections. Public policy makers, therefore, should focus on informing and educating consumers about their retail privacy rights.
- (2) To aid consumers in understanding privacy policy texts before signing them off, those policies need to be shorter, clearer, and to accommodate the different knowledge levels of diverse individuals (e.g., age and education level).

- (3) I second Sides et al. (2019) that:

Advanced privacy policies protect consumer data, but they do so much more. They create the ability to leverage more accurate information to create a more intimate and trusting relationship with the consumers. Privacy policies should be in line with, if not central to, the retailers' business strategy to build and maintain this consumer trust. (p. 2)

Up-to-date privacy policies, therefore, can help retailers become more trust-focused and consumer-centric in their policies regarding data privacy.

- (4) I agree with Culnan and Bies (2003, pp. 327–328) that offering benefits that consumers find attractive is not enough, for there is also a need to be transparent, open and honest about information practices so that consumers can perceive if disclosure is a low risk proposition and can make an informed choice about whether or not to disclose. Privacy policies should, therefore, ensure there is an “opt-out” where consumers' information will

be used for marketing unless they object. In addition, consumers should be allowed access to their data and ongoing choices about the use of their information.

- (5) There is a need for privacy laws on the federal level. In the U.S., there is a lack of a single, federal mandate and each state has its own privacy laws (Sides et al., 2019, p. 4), a situation that can potentially create a patchwork of legislation that could be confusing and complex to manage. This is a bit different from Canada where, to date, the federal Office of the Privacy Commissioner of Canada (OPC) administers the Personal Information Protection and Electronic Documents Act (PIPEDA) which governs consumer information held by retailers, although in many circumstances, the provincial law in British Columbia, Quebec and Alberta can be applied instead of the federal law (Retail Council of Canada, 2021).
- (6) This research has shown how quickly the advancements in new retail technologies are adopted in the retail sector. Therefore, privacy and data protection laws and policies need to be in a constant state of renewal and revision to be on par with the ongoing development in technology and retail practices.
- (7) Because of the pandemic, retailers have been using retail technologies as a COVID-19 pandemic tool (e.g., traffic counting cameras and sensors to restrict indoor occupancy rates and monitor social distancing rules, thermal imaging cameras for health screening, and the soon-to-be-introduced mobile apps that would be connected to health/vaccine passes). This newly created culture of post-pandemic retail technologies underscores the urgent need for new and/or updated policies that can protect retail consumers and help build a healthy relationship based on trust between consumer and retailer.

To conclude, this section documents the breadth of the contributions of this research and how they range from conceptual, to theoretical, to marketing practice, to a possible impact on public policy. As an academic researcher, I was able to connect my findings and compare them to (mostly) industry studies and government-commissioned surveys, for (and as previously discussed in Chapter 2), there is a limited amount of published academic research in that area of study, especially one that is both empirical and based on theory. This further underscores the urgent need for more scholarly research that could build on my findings.

Concerns, limitations, and avenues for future research

Research concerns

Some of the anticipated concerns at the beginning of this research did not surface. Since, in general, the majority of informants tends to be underemployed or unemployed, it was expected that their consumption experience would be limited when it comes to luxury products which would lead up to research results that cannot be generalizable to those product lines. To address this concern, a question asking for the household annual income was added to both the interviews and the surveys in an attempt to shed more light on this aspect. A wide range of household incomes (between less than CAD 20,000 and over CAD 100,000) was disclosed. Secondly, because of the nature of the recruiting pool (i.e., MTurk), it was expected that quite a number of informants would have worked in retail organizations or been employed by a manufacturer or seller of security or loss prevention products for the retail industry in the past 5 years, which might create bias. However, by including a question asking about their working in retail experience (if any), I ended up with be a rich source of information, for by identifying

which informants have had retail experience, a new perspective emerged that was worth studying.

As mentioned earlier (in Chapter 4), the COVID-19 pandemic impacted academic research and forced me to alter the design of this research to accommodate the new data collection restrictions and new procedures. However, despite such restrictions, studying the impact of the pandemic on retailance provided me with two opportunities. First, this part of the research complements a line of research that studies the impact of the COVID-19 pandemic, a time of distress and adaptation, on consumers (for example, research by Mehroliya, Alagarsamy and Solaikutty, 2021, and Sharma, Thomas and Paul, 2021). Second, the setting of the pandemic has proven to be an opportunity to explore consumers and retail workers' reactions to enhanced levels of retailance in a real-life setting (versus in a laboratory or by introducing a hypothetical situation). This could be an indication that even with the introduction of unprecedented situations (like a pandemic), consumer reaction is complex and is worth of studying.

Research limitations

This study is not without limitations. First, it focused on consumers in North America. It would be, therefore, fruitful to conduct comparative studies in different countries whose culture, privacy legislation, retail structure and consumer behaviour are different from that of the North American retail market. A second limitation is that the Amazon Mechanical Turk (MTurk) was used as a participant pool. Although previous researchers have shown that MTurk workers are more demographically diverse than the typical convenience samples of university students, and the results using MTurk samples are similar to more traditional population pools (Berinsky et al., 2012; Buhrmester, Kwang, & Gosling, 2011; Samat et al., 2017), this participant pool is likely to

be more savvy about computers, compared to the typical North American resident, and therefore, more accepting of surveillance technology. To resolve this limitation in future research, additional informants could be recruited for a live-intercept survey (for example, by contacting a local grocery store to coordinate times to ask customers who check out to complete a brief survey). This form of recruitment, however, can be only carried out post-pandemic.

Avenues for future research

The research findings open up a rich research agenda. (1) This research adopted an exploratory macro perspective of the impact of retailance in general (across the different channels and systems) on consumers and retailers. Follow-up studies could adopt a more micro perspective, for example, by using a quantitative research design while focusing on one retailance channel or system at a time, developing and validating scales that could help in measuring consumers' reactions towards specific retailance channels or systems, and making use of different variables, such as country of residence and demographic backgrounds. (2) While this research focuses on the brick-and-mortar (i.e., offline) retail context, a systematic in-depth analysis of the offline-online interplay could be valuable. There are few studies that focus on comparing online and offline self-disclosure, and there is also a notable lack of consistency in how self-disclosure is measured (Nguyen, Bin, & Campbell, 2012). One possible topic of comparison is how to alleviate consumers' privacy concerns. In an online retail setting, those concerns can be alleviated by choosing the time when personal information is disclosed. Aiello et al. (2020) studied consumers' willingness to disclose personal information throughout the customer online purchase journey (i.e., prepurchase, purchase, and postpurchase phases). Their findings show that asking for personal information at the end of the online customer purchase

journey (i.e., postpurchase phase) leads to a higher perception of warmth, which alleviates privacy concerns and, consequently, increases customers' willingness to disclose. This is because consumers perceive that the focus is on them instead of the potential benefits retailers can achieve by using their personal data. On the other hand, in a brick-and-mortar setting, consumers are usually asked to disclose their information during checkout (i.e., at the end of the purchase phase). Researchers, therefore, can investigate other factors that would help to alleviate consumers' privacy concerns when disclosing their personal and shopping information. (3)

Future research can focus on the two types of consumer resistance that were not covered in this research: cooperation (i.e., when consumers collude with retail employees who can provide the former with insider information and/or access to restricted areas) and counter-surveillance (i.e., when consumers start surveilling the retailer to oppose surveillance). To carry out this research that focuses on more extreme types of retailance resistance, prior offenders and privacy activists would be recruited as informants. (4) This research came out with interesting observations about the impact of the COVID-19 pandemic on retailers' use of and consumers' reaction to an increased level of retailance. Future research could build on those observations and include public health literature to form a new theoretical model. (5) For future research, researchers can distinguish between the different retail environments by type (e.g., groceries versus clothing) and/or size (e.g., small corner stores versus large department stores).

Concluding remarks

This research highlights the interdisciplinary nature of marketing, for it was built on theories found and studies conducted in other fields, such as sociology, political science, communications, media studies, science studies, war studies, law, cultural studies, criminology,

and literature. Employing a pragmatic approach, the research employed a mixed methods research design that comprised online self-administered surveys and semi-structured interviews. The research, moreover, addressed four main gaps: focusing on the brick-and-mortar retail environment, focusing on the consumer's perspective, providing a more comprehensive overview of retailance and its impact on consumer behaviour, and using interviews to gather detailed information from consumers. This research has practical implications for not only consumers (who need to understand the impact of retailance on their rights and weigh the benefits they receive for accepting retailance and the implications to their privacy) and retailers (who cannot afford to alienate consumers weary of the implications of surveillance on their privacy), but also for public policy makers who constantly need to implement new and updated legislative protections. A list of recommendations for each of the three stakeholders was included in Chapter 7. More importantly, this research highlighted a variety of directions for future research that can contribute to our understanding of the impact of retailance and add to the vitality of the fields of surveillance, retailing and marketing by opening new and unexplored areas of study.

REFERENCES

- Abbey, J. D., & Meloy, M. G. (2017). Attention by design: Using attention checks to detect inattentive respondents and improve data quality. *Journal of Operations Management*, 53–56, 63–70. <https://doi.org/10.1016/j.jom.2017.06.001>
- Abraham, M., Van Kerckhove, J.-F., Archacki, R., González, J. E., & Fanfarillo, S. (2019, June 4). The next level of personalization in retail. Retrieved June 16, 2019, from <https://www.bcg.com/en-ca/publications/2019/next-level-personalization-retail.aspx>
- Aiello, G., Donvito, R., Acuti, D., Grazzini, L., Mazzoli, V., Vannucci, V., & Viglia, G. (2020). Customers' willingness to disclose personal information throughout the customer purchase journey in retailing: The role of perceived warmth. *Journal of Retailing*, 96(4), 490–506. <https://doi.org/10.1016/j.jretai.2020.07.001>
- Alder, G. S. (1998). Ethical issues in electronic performance monitoring: A consideration of deontological and teleological perspectives. *Journal of Business Ethics*, 17, 729–743.
- Allen, H. D. (2006, December). Canadian Tire Scrip. Retrieved November 22, 2020, from <http://www.numismondo.net/pm/can/indexA1.htm>
- Allen, M. (1994). "See you in the city!" Perth's citiplace and the space of surveillance. In K. Gibson & S. Watson (Eds.), *Metropolis Now: Planning and the Urban in Contemporary Australia* (pp. 137–147). Sydney: Pluto.
- Allport, G. W. (1935). Attitudes. In C. Murchison (Ed.), *Handbook of Social Psychology*. Worcester: Clark University Press.
- Allvine, F. C. (1969). The future for trading stamps and games. *Journal of Marketing*. <https://doi.org/10.2307/1248745>
- Alvarez, R. M., Atkeson, L. R., Levin, I., & Li, Y. (2019). Paying attention to inattentive survey respondents. *Political Analysis*, 27, 145–162. <https://doi.org/10.1017/pan.2018.57>
- Alvesson, M. (1994). Critical theory and consumer marketing. *Scandinavian Journal of Management*, 10(3), 291–313. [https://doi.org/10.1016/0956-5221\(94\)90005-1](https://doi.org/10.1016/0956-5221(94)90005-1)
- Alvesson, M., & Sandberg, J. (2011). Generating research questions through problematization. *Academy of Management Review*, 36(2), 247–271. <https://doi.org/10.5465/AMR.2011.59330882>
- Alvesson, M., & Sandberg, J. (2013). Has Management Studies Lost Its Way? Ideas for More Imaginative and Innovative Research. *Journal of Management Studies*, 50(1), 128–152. <https://doi.org/10.1111/j.1467-6486.2012.01070.x>
- Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020, April 27). The consumer-data opportunity and the privacy imperative. Retrieved May 17, 2021, from <https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative#>
- Anderson, M., & Bolton, J. (2015). Integration of sensors to improve customer experience: Implementing device integration for the retail sector. In *e-Business Engineering (ICEBE) - 2015 IEEE 12th International Conference* (pp. 382–386).
- Andrejevic, M. (2004). *Reality TV: The Work of Being Watched*. Maryland: Rowman & Littlefield Publishers, Inc.
- Andrejevic, M. (2005). The work of watching one another : Lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4), 479–497.
- Andrejevic, M., & Gates, K. (2014). Editorial: Big data surveillance : Introduction. *Surveillance & Society*, 12(2), 185–196.

- Andrew, D. (2019). Programmatic trading: The future of audience economics. *Communication Research and Practice*, 1–15. <https://doi.org/10.1080/22041451.2019.1561398>
- Arora, N., Charm, T., Grimmelt, A., Ortega, M., Robinson, K., Sexauer, C., ... Yamakawa, N. (2020). *A global view of how consumer behavior is changing amid COVID-19*. McKinsey & Company.
- Arthur, R. (2017). Rebecca Minkoff launches “connected” bags that provide access to Fashion Week Show. *Forbes*.
- Arvidsson, A. (2003). On the ‘pre-history of the panoptic sort’: Mobility in market research. *Surveillance and Society*, 1(4), 456–474.
- Atkinson, R. (1998). *The Life Story Interview (Qualitative Research Methods, Volume 44)*. Thousand Oaks, CA: SAGE Publications.
- Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019a, November 15). Americans and privacy: Concerned, confused and feeling lack of control over their personal information. Retrieved March 22, 2021, from <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>
- Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019b, November 15). Americans and privacy: Concerned, confused and feeling lack of control over their personal information. Retrieved from <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>
- Azevedo, S. G., & Ferreira, J. (2009). RFID technology in retailing: An exploratory study on fashion apparels. *ICFAI Journal of Managerial Economics*, 7(1), 7–22.
- Babakus, E., & Mangold, W. G. (1992). Adapting the SERVQUAL scale to hospital services: An empirical investigation. *Health Services Research*, (February), 767–786.
- Baker, J. (1986). The role of the environment in marketing services: The consumer perspective. In J. A. Czepiel, C. A. Congram, & J. Shanahan (Eds.), *The Services Challenge: Integrating for Competitive Advantage* (pp. 79–84). Chicago: American Marketing Association Proceedings Series.
- Baker, S. E., & Edwards, R. (2012). *How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research*.
- Balasubramanian, S. K. (1994). Beyond advertising and publicity: Hybrid messages and public policy issues. *Journal of Advertising*, 23(4), 29–46.
- Barber, L. I. (1960). Retail Competition and TRADING STAMPS. *Business Quarterly*, 25(3), 153.
- Barnes, S. B. (2006). A privacy paradox : Social networking in the United States | Barnes. *First Monday*, 11(9). <https://doi.org/10.5210/fm.v11i9.1394>
- Bartlett, R. (1989). *Economics and Power: An Inquiry into Human Relations and Markets*. Cambridge, NY: Cambridge University Press.
- Bashir, M., Hoff, K., & Jeon, G. (2014). Poster : Factors associated with online privacy knowledge. In *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)* (pp. 1–2). Menlo Park, CA.
- Bauman, Z. (2000). *Liquid Modernity*. Cambridge, Malden, MA: Polity Press.
- Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, 8, 121–144. <https://doi.org/10.1111/ips.12048>

- Bauman, Z., & Lyon, D. (2013). *Liquid Surveillance: A Conversation*. Cambridge, UK: Polity Press.
- Beck, A., & Palmer, W. (2009). Understanding shrinkage. In A. Beck & W. Palmer (Eds.), *New Loss Prevention: Redefining Shrinkage Management* (pp. 60–83). UK: Palgrave Macmillan.
- Becker, L. (2018). Methodological proposals for the study of consumer experience. *Qualitative Market Research: An International Journal*, 21(4), 465–490. <https://doi.org/10.1108/QMR-01-2017-0036>
- Belisle, D. (2011). *Retail Nation: Department Stores and the Making of Modern Canada*. Vancouver, BC: UBC Press.
- Bentham, J. (1791). *Panopticon; or, The Inspection-House*. London: T. Payne at the Mews-Gate.
- Benton, R. (1985). Alternative approaches to consumer behavior. In N. Dholakia & J. Arndt (Eds.), *Changing the Course of Marketing: Alternative Paradigms for Widening Marketing Theory* (pp. 197–218). Greenwich: JAI Press.
- Berg, B. L. (2009). An Introduction to Content Analysis. In *Qualitative Research Methods for the Social Sciences* (7th editio, pp. 338–377). Boston: Pearson Higher Education.
- Berinsky, A. J., Huber, G. A., & Lenz, G. S. (2012). Evaluating online labor markets for experimental research: Amazon.com’s mechanical turk. *Political Analysis*, 20, 351–368. <https://doi.org/10.1093/pan/mpr057>
- Berinsky, A. J., Margolis, M. F., & Sances, M. W. (2014). Separating the shirkers from the workers? Making sure respondents pay attention on self-administered surveys. *American Journal of Political Science*, 58(3), 739–753. <https://doi.org/10.1111/ajps.12081>
- Berinsky, A. J., Margolis, M. F., & Sances, M. W. (2016). Can we turn shirkers into workers? *Journal of Experimental Social Psychology*, 66, 20–28. <https://doi.org/10.1016/j.jesp.2015.09.010>
- Bettany, S. (2007). Local accounts: Authoring the critical marketing thesis. In M. Saren, P. Maclaran, C. Goulding, R. Elliott, A. Shankar, & M. Catterall (Eds.), *Critical Marketing: Defining the Field* (pp. 69–81). Oxford, UK: Elsevier.
- Betzing, J. H., Hoang, A. Q. M., & Becker, J. (2018). In-store technologies in the retail servicescape. In *MKWI 2018 - Multikonferenz Wirtschaftsinformatik* (pp. 1671–1682). Lüneburg, Germany.
- Bhattacharai, A. (2020, April 6). Grocery workers are beginning to die of coronavirus. *The Washington Post*.
- Bigo, D. (2006). Security, exception, ban and surveillance. In D. Lyon (Ed.), *Theorizing Surveillance: The Panopticon and Beyond* (pp. 46–68). Abingdon, Oxon: Routledge.
- Blankenship, A. B., Chakrapani, C., & Poole, W. H. (1985). *A History of Marketing Research in Canada*. Toronto: Professional Marketing Research Society.
- Blau, F. D., Koebe, J., & Meyerhofer, P. (2020). *Who Are the Essential and Frontline Workers?* *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3686432>
- Blau, J. (2004, March 1). Metro store bows to pressure from anti-RFID activists.
- BNN Bloomberg. (2021, April 7). ‘Hunker down’: Business dealt a blow in Ontario stay-at-home order. Retrieved May 3, 2021, from <https://www.bnnbloomberg.ca/hunker-down-business-dealt-a-blow-in-ontario-stay-at-home-order-1.1587124>
- Bogard, W. (1996). *The Simulation of Surveillance: Hypercontrol in Telematic Societies*. Great Britain: Cambridge University Press.
- Bogard, W. (2006). Welcome to the society of control: The simulation of surveillance revisited. In K. Haggerty & R. V. Ericson (Eds.), *The New Politics of Surveillance and Visibility* (pp.

- 55–78). Toronto: University of Toronto Press.
- Boisvert, N. (2019, October 23). Sobeys unveils Canada’s 1st smart grocery cart, promising a “frictionless” shopping experience. *CBC News*.
- Bond Brand Loyalty. (2020a). The Loyalty Report: 2020 CAN Executive Summary. Retrieved May 7, 2021, from <https://info.bondbrandloyalty.com/tlr-2020>
- Bond Brand Loyalty. (2020b). The Loyalty Report: 2020 USA Executive Summary. Retrieved May 7, 2021, from <https://info.bondbrandloyalty.com/tlr-2020>
- Bonfanti, A. (2014). A dilemma for retailers: How to make store surveillance secure and appealing to shoppers. In F. Musso & E. Druica (Eds.), *Handbook of Research on Retailer-Consumer Relationship Development* (pp. 297–317). Hershey, PA: Business Science Reference (an imprint of IGI Global).
- Booth, A. (1981). The built environment as a crime deterrent: A Reexamination of defensible space. *Criminology*, 18(4), 557–570.
- Boumphrey, S. (2020). How will consumer markets evolve after coronavirus? Introductio to our COVID-19 themes. Retrieved September 29, 2020, from https://go.euromonitor.com/white-paper-2020-covid-19-themes.html?utm_campaign=SC_20_09_29_RELAUNCH_COVID_Themes&utm_medium=Email&utm_source=1_Outbound
- Boyne, R. (2000). Post-panopticism. *Economy and Society*, 29(2), 285–307.
- British Library. (n.d.). Your country needs you, a British advertisement. Retrieved January 23, 2020, from <https://www.bl.uk/collection-items/your-country-needs-you>
- Brough, A. R., & Martin, K. D. (2020). Consumer privacy during (and after) the COVID-19 pandemic. *Journal of Public Policy and Marketing*, 1–3. <https://doi.org/10.1177/0743915620929999>
- Brownlie, D. (2007). “Everything and nothing”: Habits of simulation in marketing. *Marketing Intelligence and Planning*, 25(7), 662–667. <https://doi.org/10.1108/02634500710834151>
- Brownlie, D., Saren, M., Wensley, R., & Whittington, R. (1999). Marketing disequilibrium: On redress and restoration. In D. Brownlie, M. Saren, R. Wensley, & R. Whittington (Eds.), *Rethinking Marketing: Towards Critical Marketing Accountings* (pp. 1–22). London: SAGE Publications Ltd.
- Bryman, A. (2007). Barriers to integrating quantitative and qualitative research. *Journal of Mixed Methods Research*, 1(1), 8–22. <https://doi.org/10.1177/2345678906290531>
- Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon’s Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science*, 6(1), 3–5. <https://doi.org/10.1177/1745691610393980>
- Burke, M. (2020, April 7). Walmart sued by family of worker killed by coronavirus. Retrieved May 2, 2020, from <https://www.nbcnews.com/news/us-news/least-4-grocery-store-workers-have-died-coronavirus-one-family-n1178371>
- Burns, D. J., & Rayman, D. M. (1995). Retailing in Canada and the United States: Historical comparisons. *The Service Industries Journal*, 15(4), 164–176. <https://doi.org/10.1080/02642069500000055>
- Burroughs, W. S. (1959). The Naked Lunch. Retrieved December 10, 2018, from <https://archive.org/details/nakedlunch00will>
- Buttle, F. A. (1996). SERVQUAL: Review, critique, research agenda. *European Journal of Marketing*, 30(1), 8–32. <https://doi.org/10.1108/03090569610105762>
- Caluya, G. (2010). The post-panoptic society? Reassessing Foucault in surveillance studies.

- Social Identities*, 16(5), 621–633. <https://doi.org/10.1080/13504630.2010.509565>
- Campbell, G. C. (1941). Merchandise returns- Retailer's viewpoint. *Quarterly Review of Commerce (Pre-1986)*, 8(2), 141–151.
- Canadian Marketing Association. (2020a, May 20). Privacy Legislation Comparison Chart: PIPEDA, CASL , GDPR and CCPA. Retrieved November 20, 2020, from <https://www.the-cma.org/regulatory/resource-links>
- Canadian Marketing Association. (2020b, November 17). Canada introduces new privacy legislation. Here is what marketers need to know. Retrieved November 20, 2020, from <https://www.the-cma.org/about/blog/canada-introduces-new-privacy-legislation>
- Canadian Marketing Association. (2020c, December 16). Cause sponsorship and COVID-19: From the what to the why. Retrieved December 18, 2020, from <https://www.the-cma.org/about/blog/Cause-sponsorship-and-COVID-19-From-the-what-to-the-why>
- Cardone, C., & Hayes, R. (2012). Shoplifter perceptions of store environments: An analysis of how physical cues in the retail interior shape shoplifter behavior. *Journal of Applied Security Research*, 7(1), 22–58. <https://doi.org/10.1080/19361610.2012.631178>
- Carleton History. (2020, November 12). The History of Privacy and the Future of AI with Dr. Teresa Scassa [Video]. Retrieved November 13, 2020, from <https://www.youtube.com/watch?v=MXGsRk8CL1o>
- Catterall, M., Maclaran, P., & Stevens, L. (2002). Critical reflection in the marketing curriculum. *Journal of Marketing Education*, 24(3), 184–192. <https://doi.org/10.1177/0273475302238041>
- CBC. (2021, May 14). Retail workers scared by number of unmasked customers allowed to walk in, says union. Retrieved May 17, 2021, from https://www.cbc.ca/news/canada/manitoba/masks-rules-grocery-stores-covid19-manitoba-ufcw-letter-1.6026674?fbclid=IwAR2GrTZDt4dSv8M-N9T5oXgboVz79uX81z1TH-YnFiZKfmbzbBPZF_-K9Ws
- Centers for Disease Control and Prevention. (2020, April 13). What Grocery and Food Retail Workers Need to Know about COVID-19. Retrieved May 2, 2020, from <https://www.cdc.gov/coronavirus/2019-ncov/community/organizations/grocery-food-retail-workers.html>
- Chaganti, S., Graves, E., Higgins, A., Mattingly, M., Savage, S., & Tonsberg, C. (2020, January). The effects of the novel coronavirus pandemic on Service Workers in New England.
- Chahal, M. (2016, March 4). Why marketers are failing to target consumers at key life events. Retrieved February 23, 2021, from <https://www.marketingweek.com/why-marketers-are-failing-to-target-consumers-at-key-life-events/>
- Charmaz, K. (2006). *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. London: SAGE Publications.
- Charmaz, K. (2008). Constructionism and the grounded theory method. In J. A. Holstein & J. F. Gubrium (Eds.), *Handbook of Constructionist Research* (pp. 397–412). New York: The Guilford Press.
- Charmaz, K., & Keller, R. (2016). A Personal Journey with Grounded Theory Methodology. Kathy Charmaz in Conversation With Reiner Keller [60 paragraphs]. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 17(1), Art. 16.
- Cision. (2020, December 1). Retailers Deliver An Open Letter To Premier Ford & Minister Elliott. Retrieved December 8, 2020, from <https://www.newswire.ca/news->

- releases/retailers-deliver-an-open-letter-to-premier-ford-amp-minister-elliott-872104684.html
- Claritas PRIZM. (n.d.). Retrieved July 23, 2018, from <https://segmentationsolutions.nielsen.com/mybestsegments/Default.jsp?ID=70>
- Clarke III, I., & Flaherty, T. B. (2008). RFID and consumer privacy. *Journal of Internet Commerce*, 7(4), 513–527. <https://doi.org/10.1080/15332860802507370>
- Clarke, R. A. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498–518.
- Clarke, S. (1996). Consumers, information, and marketing efficiency at GM, 1921-1940. *Business and Economic History*, 25(1), 186–195.
- Cliford, S., & Hardy, Q. (2013). Attention, shoppers: Store is tracking your cell. *New York Times*.
- Cloutier, C., & Ravasi, D. (2021). Using tables to enhance trustworthiness in qualitative research. *Strategic Organization*, 19(1), 113–133. <https://doi.org/10.1177/1476127020979329>
- Coleman, P. (2006). *Shopping Environments: Evolution, Planning and Design*. Oxford: Architectural Press, Elsevier.
- Coles, R., & Kirwan, M. J. (Eds.). (2011). *Food and Beverage Packaging Technology* (2nd ed.). Ames, Iowa: Wiley-Blackwell.
- Cozens, P. M., Saville, G., & Hillier, D. (2005). Crime prevention through environmental design (CPTED): A review and modern bibliography. *Property Management*, 23(5), 328–356. <https://doi.org/10.1108/02637470510631483>
- Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* (4th ed.). Los Angeles, CA: SAGE.
- Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and Conducting Mixed Methods Research* (3rd ed.). Thousand Oaks, CA: SAGE.
- Cropanzano, R. (2009). Writing nonempirical articles for Journal of Management: General thoughts and suggestions. *Journal of Management*, 35(6), 1304–1311.
- Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323–342.
- Cumming, D., & Johan, S. (2015). Cameras tracking shoppers: The economics of retail video surveillance. *Eurasian Business Review*, 5, 235–257. <https://doi.org/10.1007/s40821-015-0023-3>
- DailyMail. (2012). The bionic mannequins using hidden police surveillance technology to track shoppers' age, gender and race. Retrieved July 19, 2019, from <https://www.dailymail.co.uk/femail/article-2236540/The-bionic-mannequins-using-hidden-police-surveillance-technology-track-shoppers-age-gender-race.html>
- Dale, E. (1956). Contributions to administration by Alfred P. Sloan, Jr., and GM. *Administrative Science Quarterly*, 1(1), 30–62. <https://doi.org/10.2307/2390839>
- Dandeker, C. (1990). *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*. Padstow, Cornwall: Polity Press.
- Danna, A., & Gandy, O. H. (2002). All that glitters is not gold: Digging beneath the surface of data mining. *Journal of Business Anthropology*, 40, 373–386. <https://doi.org/10.1023/A>
- DataSparQ. (2019, August 1). Press release: Launching the world's first AI bar. Retrieved October 22, 2019, from <https://datasparq.ai/>
- Datoo, S. (2014). How tracking customers in-store will soon be the norm. *The Guardian*.

- Davis, B. (2014, August 12). Five retailers using NFC and RFID to enhance shopping: But do they work?
- Dawson, S. (1993). Consumer responses to electronic article surveillance alarms. *Journal of Retailing*, 69(3), 353–362.
- De Angelis, M. (2011). Global capital, abstract labour, and the fractal-panopticon, (October 2011).
- De Brabant, C. (2020, April 21). What can we learn from China as we prepare to open up the retail sector? Retrieved July 1, 2020, from <https://www.mcgill.ca/bensadoun-school/article/what-can-we-learn-china-we-prepare-open-retail-sector>
- De Felice, D. (2020, April 3). Life of a Retail Store Employee during the COVID-19 Pandemic. Retrieved May 2, 2020, from <https://www.westislandblog.com/life-of-a-retail-store-employee-during-the-covid-19-pandemic/>
- De Landa, M. (1991). *War in the Age of Intelligent Machines*. New York: Zone Books.
- Delbridge, R., & Fiss, P. C. (2013). No TitleEditors' comments: Styles of theorizing and the social organization of knowledge. *Academy of Management Review*, 38(3), 325–331.
- Deleuze, G. (1992). Postscript on the societies of control. *October*, 59, 3–7.
- Deleuze, G., & Guattari, F. (1987). *A Thousand Plateaus: Capitalism and Schizophrenia*. (B. Massumi, Trans.). Minneapolis: University of Minnesota Press.
- Denegri-Knott, J. (2019). Re-mapping power for critical marketing and consumer research. In M. Tadajewski, M. Higgins, J. Denegri-Knott, & R. Varman (Eds.), *The Routledge Companion to Critical Marketing* (pp. 287–305). London & New York: Routledge.
- Denzin, Norman, K. (2001). The seventh moment : Qualitative inquiry and the practices of a more radical consumer research. *Journal of Consumer Research*, 28(2), 324–330.
- Denzin, N. K. (1995). *The Cinematic Society: The Voyeur's Gaze*. London, Thousand Oaks, Calif.: SAGE Publications.
- DepartmentofFinanceCanada. (2020, October 9). Government announces new, targeted support to help businesses through pandemic. Retrieved November 17, 2020, from <https://www.canada.ca/en/departement-finance/news/2020/10/government-announces-new-targeted-support-to-help-businesses-through-pandemic.html>
- Deshpande, R. (1983). "Paradigms lost": On theory and method in research in marketing. *Journal of Marketing*, 47(4), 101–110.
- Devlin, S. J., Dong, H. K., & Brown, M. (2003). Selecting a scale for measuring quality. *Marketing Research*, 15(3), 13–16.
- DiLorenzo, R. L. (2018, September 11). Electronic Article Surveillance (EAS) Source Tagging: 20+ Years of Innovation.
- Dohmen, B. (2020, January 25). Is the retail apocalypse over? *Forbes*.
- Donthu, N., & Gustafsson, A. (2020). Effects of COVID-19 on Business and Research (Journal pre-proofs). *Journal of Business Research*. <https://doi.org/10.1016/j.jbusres.2020.06.008>
- Dragan, A. (2018, December 17). Study: Consumers are embracing new technologies, but are concerned by security.
- Drucker, P. F. (1950). *The New Society: The Anatomy of the Industrial Order*. New York: Harper.
- Drucker, P. F. (1954). *The Practice of Management*. New York: Harper.
- du Prel, J. B., Hommel, G., Röhrig, B., & Blettner, M. (2009). Confidence interval or p-value? Part 4 of a series on evaluation of scientific publications. *Deutsches Ärzteblatt International*, 106(19), 335–339. <https://doi.org/10.3238/arztebl.2009.0335>

- Duhigg, C. (2012). How companies learn your secrets. *The New York Times Magazine*.
- Duriau, V. J., Regeer, R. K., & Pfarrer, M. D. (2007). A content Analysis of the Content Analysis Literature in Organizations Studies: Research Themes, Data Sources, and Methodological Refinements. *Organizational Research Methods*, 10(1), 5–34. <https://doi.org/10.1177/1094428106289252>
- Eagleton, T. (1991). *Ideology: An Introduction*. London: Verso.
- Earley, A. (2015). Critical theory in consumer research: Advancing the conversation. In *Consumer Culture Theory (Research in Consumer Behavior)* (Vol. 17, pp. 77–87). Emerald Group Publishing Limited. <https://doi.org/10.1108/S0885-211120150000017020>
- ECAMSECURE. (2021, January 8). Virtual guard services. Retrieved April 10, 2019, from <https://www.ecamsecure.com/blog/retail-security/types-of-retail-theft-and-how-to-prevent-them/>
- Edmondson, A. C., & Mcmanus, S. E. (2007). Methodological fit in management fit research. *The Academy of Management Review*, 32(4), 1155–1179. <https://doi.org/10.5465/AMR.2007.26586086>
- Ekos Research Associates, I. (2009). *Canadians and privacy: Final report*. Ottawa, ON: Office of the Privacy Commissioner of Canada Communications.
- Ellul, J. (1964). *The Technological Society*. New York: Vintage.
- Elmer, G. (2004). *Profiling Machines: Mapping the Personal Information Economy*. Cambridge, MA: MIT Press.
- Elmer, G. (2012). Panoptican-discipline-control. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies* (pp. 21–29). Oxon: Routledge.
- Erevelles, S., Fukawa, N., & Swayne, L. (2016). Big Data consumer analytics and the transformation of marketing. *Journal of Business Research*, 69, 897–904. <https://doi.org/10.1016/j.jbusres.2015.07.001>
- Esmark, C. L., Noble, S. M., & Breazeale, M. J. (2017). I'll be watching you: Shoppers' reactions to perceptions of being watched by employees. *Journal of Retailing*, 93(3), 336–349. <https://doi.org/10.1016/j.jretai.2017.04.005>
- Evans, P. (2020a, May 7). Canadian shoe chain Aldo seeks creditor protection, citing pandemic pressure. Retrieved November 12, 2020, from <https://www.cbc.ca/news/business/aldo-bankruptcy-1.5559810>
- Evans, P. (2020b, May 22). COVID-19 pushed Canadian retail sales to their biggest ever plunge in March. *CBC Business*.
- Fairchild, A. L. (2006). Diabetes and disease surveillance [Image]. *Science*, 313(5874), 175–176. <https://doi.org/10.1126/science.1127610>
- Farjoun, M., Ansell, C., & Boin, A. (2015). Perspective-Pragmatism in organization studies: Meeting the challenges of a dynamic and complex world. *Organization Science*, 26(6), 1787–1804. <https://doi.org/10.1287/orsc.2015.1016>
- Farrington, D. P., Bowen, S., Buckle, A., Burns-Howell, T., & Burrows, J. (1993). An experiment on the prevention of shoplifting. *Crime Prevention Studies*, 1, 93–119.
- FederalTradeCommission. (n.d.). Protecting Consumer Privacy and Security. Retrieved February 12, 2019, from <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security>
- FederalTradeCommission. (2014). *Data brokers: A call for transparency and accountability*. Federal Trade Commission (FTC). Federal Trade Commission.
- Feilzer, M. Y. (2010). Doing mixed methods research pragmatically: Implications for the

- rediscovery of pragmatism as a research paradigm. *Journal of Mixed Methods Research*, 4(1), 6–16. <https://doi.org/10.1177/1558689809349691>
- Ferracuti, N., Norscini, C., Frontoni, E., Gabellini, P., Paolanti, M., & Placidi, V. (2019). A business application of RTLS technology in Intelligent Retail Environment: Defining the shopper's preferred path and its segmentation. *Journal of Retailing and Consumer Services*, 47, 184–194. <https://doi.org/10.1016/j.jretconser.2018.11.005>
- Filippone, R. (2019, October 13). Getting scanned for a pint: How facial recognition technology is being used in a London pub. *CBC News*.
- Fischer, B. (2015). *Bright and shiny objects*.
- Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Boston, Massachusetts: Addison-Wesley.
- Ford, J. B. (2017). Amazon's Mechanical Turk: A comment. *Journal of Advertising*, 46(1), 156–158. <https://doi.org/10.1080/00913367.2017.1281781>
- Foucault, M. (1978). *Discipline and Punish: The Birth of the Prison*. (A. Sheridan, Trans.). New York: Vintage Books. <https://doi.org/10.2307/2065008>
- Foucault, M. (1982). Afterword: On the genealogy of ethics: An overview of work in progress. In H. L. Dreyfus & P. Rabinow (Eds.), *Michel Foucault: Beyond Structuralism and Hermeneutics* (pp. 229–264). Brighton: Harvester.
- Franzak, F., Pitta, D., & Fritsche, S. (2001). Online relationships and the consumer's right to privacy. *Journal of Consumer Marketing*, 18(7), 631–641. <https://doi.org/10.1108/EUM0000000006256>
- Fuchs, C. (2011). New media, web 2.0 and surveillance. *Sociology Compass*, 2(2), 134–147. <https://doi.org/10.1111/j.1751-9020.2010.00354.x> New
- Fuchs, C. (2014). Capitalism or information society? In C. Fuchs (Ed.), *Digital Labour and Karl Marx* (pp. 135–152). New York, NY: Routledge.
- Fung, B. (2013). How stores use your phone's WiFi to track your shopping habits. *The Washington Post*.
- Gabriel, Y., & Lang, T. (2015). The consumer as worker. In *The Unmanageable Consumer* (3rd Editio, pp. 209–225). Sage.
- Galič, M., Timan, T., & Koops, B. J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the Panopticon to participation. *Philosophy and Technology*, 30, 9–37. <https://doi.org/10.1007/s13347-016-0219-1>
- Gandy, O. H. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview.
- Gandy, O. H., & Simmons, C. E. (1986). Technology, privacy and the democratic process. *Critical Studies in Mass Communication*, 3(June), 155–168.
- Garced, K. (2017). Rebecca Minkoff to unveil smart bags for spring.
- Giant Tiger. (2020a, February 28). TG VIP: Giant Tiger continues Loyalty program expansion. Retrieved October 27, 2020, from <https://www.newswire.ca/news-releases/tg-vip-giant-tiger-continues-loyalty-program-expansion-833502480.html>
- Giant Tiger. (2020b, September 11). GT VIP: Giant Tiger launches first-ever Loyalty program. Retrieved October 27, 2020, from <https://www.newswire.ca/news-releases/gt-vip-giant-tiger-launches-first-ever-loyalty-program-866527017.html>
- Gibbs, G. R. (2015). *A Discussion with Prof Kathy Charmaz on Grounded Theory [Video file]*. UK: YouTube.
- Giddens, A. (1981). *A Contemporary Critique of Historical Aterialism, Vol. 1: Power, Property*

- and the State*. London: Macmillan.
- Giddens, A. (2002). *The Nation-state and Violence: Volume Two of A Conetemporary Critique of Historical Materialism*. Cambridge: Polity Press.
- Gilchrist, K. (2017, September 4). Alibaba launches 'smile to pay' facial recognition system at KFC in China. *CNBC*.
- Gioia, D. a., Corley, K. G., & Hamilton, A. L. (2012). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods, 16*(1), 15–31. <https://doi.org/10.1177/1094428112452151>
- Gollwitzer, A., Martel, C., Brady, W. J., Pärnamets, P., Freedman, I. G., Knowles, E. D., & Van Bavel, J. J. (2020). Partisan differences in physical distancing are linked to health outcomes during the COVID-19 pandemic. *Nature Human Behaviour, 4*, 1186–1197. <https://doi.org/10.1038/s41562-020-00977-7>
- Gordon, D. R. (1987). The electronic Panopticon: A case study of the development of the national criminal records system. *Politics and Society, 15*(4), 483–511. <https://doi.org/10.1177/003232928701500404>
- Gotlieb, C. C. (1996). Privacy: A oncept whose time has come and gone. In D. Lyon & E. Zureik (Eds.), *Computers, Surveillance, and Privacy* (pp. 156–171). Minneapolis: University of Minnesota Press.
- Gould, S. J. (2008). Introspection as critical marketing thought, critical marketing thought as introspection. In M. Tadajewski & D. Brownlie (Eds.), *Critical Marketing: Issues in Contemporary Marketing* (pp. 311–327). West Sussx, UK: John Wiley & Sons, Ltd.
- Government of Canada. (2014). Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans. Retrieved May 5, 2021, from https://ethics.gc.ca/eng/policy-politique_tcps2-eptc2_2018.html
- Graham, S. (1999). Geographies of surveillant simulation. In M. Crang, P. Crang, & J. May (Eds.), *Virtual Geographies: Bodies, Space and Relations* (pp. 131–148). London, UK: Routledge.
- Greedy Rates. (2018). The top 15 Canadian loyalty rewards programs. Retrieved June 15, 2019, from <https://www.greedyrates.ca/blog/the-top-15-canadian-loyalty-rewards-programs/>
- Grenville, A. (2010). Shunning surveillance or welcoming the watcher? Exploring how people traverse the path of resistance. In E. Zureik, L. L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, Privacy, and the Globalization of Personal Information* (pp. 70–83). Montreal, Ithaca: McGill-Queen's University Press.
- Grewal, D., Noble, S. M., Roggeveen, A. L., & Nordfalt, J. (2020). The future of in-store technology. *Journal of the Academy of Marketing Science, 48*, 96–113. <https://doi.org/10.1007/s11747-019-00697-z>
- Grewal, D., Roggeveen, A. L., & Nordfält, J. (2017). The Future of retailing. *Journal of Retailing, 93*(1), 1–6. <https://doi.org/10.1016/j.jretai.2016.12.008>
- Groombridge, N. (2002). Crime control or crime culture TV? *Surveillance & Society, 1*(1), 30–46. <https://doi.org/10.24908/ss.v1i1.3392>
- Gruske, C. (1999, February 11). On-line Air Miles files left accessible. Retrieved July 8, 2018, from <https://www.itworldcanada.com/article/on-line-air-miles-files-left-accessible/35719>
- Haggerty, K. D. (2006). Tear down the walls: On demolishing the panopticon. In D. Lyon (Ed.), *Theorizing Surveillance: The Panopticon and Beyond* (pp. 23–45). Abingdon, Oxon: Routledge.
- Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of*

- Sociology*, 51(4), 605–622. <https://doi.org/10.1080/00071310020015280>
- Haggerty, K. D., & Ericson, R. V. (2006). The new politics of surveillance and visibility. In K. D. Haggerty & R. V. Ericson (Eds.), *The New Politics of Surveillance and Visibility* (pp. 3–25). Toronto: University of Toronto Press.
- Hamby, A., Brinberg, D., & Daniloski, K. (2017). Reflecting on the journey: Mechanisms in narrative persuasion. *Journal of Consumer Psychology*, 27(1), 11–22.
- Hamilton, R., Thompson, D., Bone, S., Chaplin, L. N., Griskevicius, V., Goldsmith, K., ... Zhu, M. (2019). The effects of scarcity on consumer decision journeys. *Journal of the Academy of Marketing Science*, 47(3), 532–550. <https://doi.org/10.1007/s11747-018-0604-7>
- Handford, M. (1994). Electronic tagging in action: A case study in retailing. In M. Gill (Ed.), *Crime at work: Vol. 1: Studies in security and crime prevention* (pp. 173–185). Perpetuity Press Ltd.
- Hardt, M., & Negri, A. (2001). *Empire*. Cambridge, Massachusetts: Harvard University Press.
- Harms, P. D., & Desimone, J. A. (2015). Caution ! MTurk workers ahead — Fines doubled. *Industrial and Organizational Psychology*, 8(2), 183–190.
- Harris, S. (2019, October 16). Loblaws wanted too much information for \$25 gift cards, privacy commissioner finds. *CBC Business*.
- Hayes, C. M., Kesan, J. P., Bashir, M., Hoff, K., & Jeon, G. (2014). Knowledge, behavior, and opinions regarding online privacy. In *Proceedings of the 42nd Research Conference on Communication, Information and Internet Policy (TPRC 2014)* (pp. 1–33). Arlington, VA. <https://doi.org/10.2139/ssrn.2418830>
- Hayward, S. (2018, July 14). Asda issues staff with personal CCTV devices to record abuse inside supermarkets. *Mirror*.
- He, H., & Harris, L. (2020). The impact of Covid-19 pandemic on corporate social responsibility and marketing philosophy. *Journal of Business Research*, 116, 176–182. <https://doi.org/10.1016/j.jbusres.2020.05.030>
- Herring, J. (2020, October 29). Cadillac Fairview covertly collected images of millions of shoppers: Privacy commissioner.
- Heydari, A. (2018, August 7). Cellphone tracking has been used in at least 1 Canadian mall, former employee says. Retrieved August 7, 2018, from <https://www.cbc.ca/news/canada/calgary/cadillac-fairview-mall-location-tracking-1.4775990?cmp=rss>
- Hill, K. (2012). How Target figured out a teen girl was pregnant before her father did. *Forbes*.
- Horne, D. R., Norberg, P. A., & Ekin, A. C. (2007). Exploring consumer lying in information-based exchanges. *Journal of Consumer Marketing*, 24(2), 90–99. <https://doi.org/10.1108/07363760710737094>
- Hossain, M. M., & Prybutok, V. R. (2008). Consumer acceptance of RFID technology: An exploratory study. *IEEE Transactions on Engineering Management*, 55(2), 316–328.
- Huang, H.-Y., & Bashir, M. (2015). Is privacy a human right? An empirical examination in a global context. In *Proceedings of 13th Annual Conference on Privacy, Security and Trust* (pp. 77–84). Izmir, Turkey.
- Hudson, A. (2013, July 30). Targeted real-life adverts “know who you are.” Retrieved April 10, 2019, from <https://www.bbc.com/news/technology-23425297>
- Hudson, L. A., & Ozanne, J. L. (1988). Alternative ways of seeking knowledge in consumer research. *Journal of Consumer Research*, 14(4), 508–521.
- Huey, L. (2009). Subverting surveillance systems: Access to information mechanisms as tools of

- counter-surveillance. In S. P. Hier & J. Greenberg (Eds.), *Surveillance: Power, Problems, and Politics* (pp. 219–235). Vancouver: UBC Press.
- Hull, G. (2015). Successful failure: What Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology*, *17*, 89–101. <https://doi.org/10.1007/s10676-015-9363-z>
- Hulland, J., & Houston, M. (2021). The importance of behavioral outcomes. *Journal of the Academy of Marketing Science*, 437–440. <https://doi.org/10.1007/s11747-020-00764-w>
- Internal data from FaceFirst. (n.d.). Retrieved July 2, 2018, from <https://www.facefirst.com/company-overview/>
- IpsosRetailPerformance. (2017, March 29). How to improve your store layout to attract more customers. Retrieved July 12, 2019, from <https://www.ipsos-retailperformance.com/resources/blog/is-your-store-layout-affecting-profit/>
- Isaeva, N., Gruenewald, K., & Saunders, M. N. K. (2020). Trust theory and customer services research: theoretical review and synthesis. *The Service Industries Journal*, *40*(15–16). <https://doi.org/10.1080/02642069.2020.1779225>
- Israel, S. (2013). How Walmart and Heineken will use Shopperception to put your in-store experience in context. *Forbes*.
- Ives, B., Cossick, K., & Adams, D. (2019). Amazon Go: Disrupting retail? *Journal of Information Technology Teaching Casenotes*, March 26, 1–11. <https://doi.org/10.1177/2043886918819092>
- Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, *10*(3), 18–26. <https://doi.org/10.1007/s13162-020-00161-0>
- Janghorban, R., Roudsari, R. L., & Taghipour, A. (2014). Skype interviewing: The new generation of online synchronous interview in qualitative research. *International Journal of Qualitative Studies on Health and Well-Being*, *9*(1). <https://doi.org/10.3402/qhw.v9.24152>
- Janiszewski, C., Labroo, A. A., & Rucker, D. D. (2016). A tutorial in consumer research: Knowledge creation and knowledge appreciation in deductive-conceptual consumer research. *Journal of Consumer Research*, *43*(2), 200–209. <https://doi.org/10.1093/jcr/ucw023>
- Jenkin, M. (2018, June 5). The steady decline of consumer protection in Canada. Retrieved June 9, 2021, from <https://policyoptions.irpp.org/magazines/june-2018/the-steady-decline-of-consumer-protection-in-canada/>
- Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, *33*(7), 14–26. <https://doi.org/10.3102/0013189X033007014>
- Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research*, *1*(2), 112–133. <https://doi.org/10.1017/9781316418376.015>
- Johnston, C. (2018). Amazon opens a supermarket with no checkouts. Retrieved April 7, 2019, from <https://www.bbc.com/news/business-42769096>
- Joinson, A. N. (2008). "Looking at", "Looking up" or "Keeping up with" people? Motives and uses of Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2008)* (pp. 1027–1036). Florence, Italy.
- Jolly, I. (Loeb & L. (2018). Data protection in the United States: Overview, Practical Law Country Q&A. Retrieved March 5, 2019, from <https://uk.practicallaw.thomsonreuters.com/6-502->

- 0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhc
p=1#co_anchor_a479701
- Jones, P., Clarke-Hill, C., Comfort, D., Hillier, D., & Shears, P. (2004). Radio frequency identification in retailing and privacy and public policy issues. *Management Research News*, 27(8/9), 45–56.
- Kafka, F. (1919). *In the Penal Colony*. (I. Johnston, Trans.).
- Kaitlyn, Ti. (2018). Wouldn't it be better if self-checkout just died? Retrieved July 19, 2019, from <https://www.vox.com/the-goods/2018/10/2/17923050/self-checkout-amazon-walmart-automation-jobs-surveillance>
- Kajalo, S., & Lindblom, A. (2010a). How retail entrepreneurs perceive the link between surveillance, feeling of security, and competitiveness of the retail store? A structural model approach. *Journal of Retailing and Consumer Services*, 17, 300–305. <https://doi.org/10.1016/j.jretconser.2010.03.001>
- Kajalo, S., & Lindblom, A. (2010b). Surveillance investments in store environment and sense of security. *Facilities*, 28(9/10), 465–474. <https://doi.org/10.1108/02632771011057198>
- Kajalo, S., & Lindblom, A. (2011a). An empirical analysis of retail entrepreneurs' approaches to prevent shoplifting. *Security Journal*, 24(4), 269–282.
- Kajalo, S., & Lindblom, A. (2011b). Effectiveness of formal and informal surveillance in reducing crime at grocery stores. *Journal of Small Business and Enterprise Development*, 18(1), 157–169. <https://doi.org/10.1108/14626001111106488>
- Kajalo, S., & Lindblom, A. (2016). The role of formal and informal surveillance in creating a safe and entertaining retail environment. *Facilities*, 34(3/4), 219–232. <https://doi.org/10.1108/F-06-2014-0055>
- Karrh, J. A. (1998). Brand placement: A review. *Journal of Current Issues and Research in Advertising*, 20(2), 31–49. <https://doi.org/10.1080/10641734.1998.10505081>
- Katwala, A. (2018). Here's how Nike, Alibaba and Walmart are reinventing retail. Retrieved April 10, 2019, from <https://www.wired.co.uk/article/future-of-retail>
- Kerr, I., & Barrigar, J. (2012). Privacy, identity and anonymity. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies* (pp. 386–394). Oxon: Routledge.
- Kesan, J. P., Hayes, C. M., & Bashir, M. (2015). Shaping privacy law and policy by examining the intersection of knowledge and opinions. In *Research Conference on Communication, Information and Internet Policy (TPRC 43)* (pp. 1–43). Arlington, Virginia.
- Kessel, P. Van, & Quinn, D. (2020, October 29). Both Republicans and Democrats cite masks as a negative effect of COVID-19, but for very different reasons. Retrieved May 17, 2021, from <https://www.pewresearch.org/fact-tank/2020/10/29/both-republicans-and-democrats-cite-masks-as-a-negative-effect-of-covid-19-but-for-very-different-reasons/>
- Klein, A., & Felten, E. (2020, April 4). The 9/11 playbook for protecting privacy. Retrieved July 22, 2020, from <https://www.politico.com/news/agenda/2020/04/04/9-11-playbook-coronavirus-privacy-164510>
- Knobe, J. (2021, March 5). Toronto woman says Walmart employees racially profiled her family, accused teen daughter of stealing. Retrieved March 8, 2021, from https://www.cbc.ca/news/canada/toronto/toronto-woman-walmart-employees-racially-profiled-family-daughter-stealing-1.5938533?fbclid=IwAR1HfyB2S18LOHQcA1NmE8hBWbeKC55U7KuKRxN311Kb4_mFkwNaHa53FS0
- Koh, R., Schuster, E. W., Lam, N.-S., & Dining, M. (2003). *White paper: Prediction, detection,*

- and proof: An integrated auto-ID solution to retail theft. Distribution.*
- Koistinen, K., & Peura-Kapanen, L. (2009). *Standing in the check-out line ranks high on the list of concerns - Consumers' views on the safety of running errands on grocery stores and shopping centres*. Helsinki: Publikationer 5/2009.
- Kopun, F. (2013, July 2). Canadian retailers using postal code information to target customers. Retrieved May 10, 2021, from https://www.thestar.com/business/2013/07/02/retailers_using_postal_code_information_to_target_customers.html
- Kotler, P. (1972). A generic concept of marketing. *Journal of Marketing*, 36, 46–54.
- Kozinets, R. V. (2020). *Netnography: The Essential Guide to Qualitative Social Media Research* (3rd ed.). London: Sage.
- Kupor, D., & Tormala, Z. (2015). Persuasion, interrupted: The effect of momentary interruptions on message and persuasion. *2015*, 42(August), 300–315.
- Kwan, C., Dai, X., & Wyer, R. S. J. (2017). Contextual influences on message persuasion: The effect of empty space. *Journal of Consumer Research*, 44(August), 300–315.
- Lace, S. (2005). The new personal information agenda. In S. Lace (Ed.), *The Glass Consumer: Life in a Surveillance Society* (pp. 207–246). Bristol: Policy Press/National Consumer Council.
- Ladd, B. (2018). The retail industry has A problem with returns: Return runners wants to be the solution. Retrieved June 17, 2019, from <https://www.forbes.com/sites/brittainladd/2018/12/19/retailers-are-about-to-get-hit-with-95b-of-holiday-returns-returnrunners-can-recover-those-losses/#7dfcb8426b66>
- Lamb, C. W., Hair, J. F., McDaniel, C., Kapoor, H., Shearer, J., Boivin, M., & Appleby, R. (2016). *MKTG: Principles of Marketing* (3rd Canadi). USA: Nelson Education Ltd.
- Lampe, C., Ellison, N., & Steinfield, C. (2006). A Face (book) in the crowd : Social searching vs. social browsing. In *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work (CSCW)* (pp. 167–170). Banff, Alberta.
- Larsen, M., & Piché, J. (2009). Public vigilance coampigns and participatory surveillance after 11 September 2001. In S. Hier & J. Greenberg (Eds.), *Surveillnace: Power, Problems, and Politics* (pp. 187–202). Vancouver: UBC Press.
- Lazaris, C., Vrechopoulous, A., Fraidaki, K., & Doukidis, G. (2014). Exploring the “Omnichannel” shopper behaviour. In *AMA SERV/SIG 2014, International Service Research Conference*. Thessaloniki, Greece. <https://doi.org/10.13140/2.1.1278.2089>
- Lazzaro, S. (2017, January 25). Sales of George Orwell’s “1984” have skyrocketed in wake of “alternative facts.”
- Leach, W. (1994). *Land of Desire: Merchants, Power, and the Rise of a New American Culture*. New York: Vintage Books.
- Lee, A. (2012). How luxury retailers are spying on shoppers with surveillance mannequins. Retrieved July 19, 2019, from <https://www.technobuffalo.com/how-luxury-retailers-are-spying-on-shoppers-with-surveillance-mannequins>
- Lee, G., Hollinger, R. C., & Dabney, D. A. (1999). The relationship between crime and private security at US shopping centers. *American Journal of Criminal Justice*, 23(2), 157–177. <https://doi.org/10.1007/bf02887270>
- Leedy, P. D., & Ormrod, J. E. (2010). *Practical research: Planning and design* (9th ed.). New Jersey: Merrill.
- Légis Québec. (2019, January 15). P-39.1 - Act respecting the protection of personal information

- in the private sector. Retrieved April 15, 2019, from <http://legisquebec.gouv.qc.ca/en/ShowDoc/cs/P-39.1>
- Leman-Langlois, S. (2002). The myopic panopticon : The social consequences of policing through the lens. *Policing & Society*, 13(1), 43–58. <https://doi.org/10.1080/1043946022000005617>
- Lennihan, M. (2015, March 16). Hello Barbie’s listening ability “creepy”, privacy group says. *CBC News*.
- Levy, S. J. (1959). Symbols for Sale. *Harvard Business Review*, 37(July-August), 117–124.
- Lim, W. M. (2018). Dialectic antidotes to critics of the technology acceptance model: Conceptual, methodological, and replication treatments for behavioural modelling in technology-mediated environments. *Australasian Journal of Information Systems*, 22.
- Lin, B., Hastings, D. A., & Martin, C. (1994). Shoplifting in retail clothing outlets: An exploratory research. *International Journal of Retail & Distribution Management*, 22(7), 24–29.
- Lindblom, A., & Kajalo, S. (2011). The use and effectiveness of formal and informal surveillance in reducing shoplifting: A survey in Sweden, Norway and Finland. *The International Review of Retail, Distribution and Consumer Research*, 21(2), 111–128. <https://doi.org/10.1080/09593969.2011.562677>
- Liptak, A. (2017, June 30). Minority Report holds up because it’s about surveillance, not gadgets.
- Locke, K., & Golden-Biddle, K. (1997). Constructing opportunities for contribution: Structuring intertextual coherence and “problematizing” in organizational studies. *Academy of Management Journal*, 40, 1023–1026.
- Lockley, L. C. (1950). Notes on the history of marketing research. *Journal of Marketing*, 14(5), 733–736.
- Lubin, D. M. (2016, April 30). Big Brother from “1984” is based on this infamous historical figure. *Business Insider*.
- Lupton, D. (Ed.). (2020). *Doing fieldwork in a pandemic (crowd sourced document)*.
- Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, 35(4), 572–585.
- Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.
- Lyon, D. (1998). *The Information Society: Issues and Illusions*. Malden, MA: Polity Press.
- Lyon, D. (2001a). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.
- Lyon, D. (2001b). *Surveillance Society*. Buckingham: Open University Press.
- Lyon, D. (2003a). Introduction. In D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (pp. 1–9). London: Routledge. <https://doi.org/10.1177/1440783306061355>
- Lyon, D. (2003b). Surveillance technology and surveillance society. In T. J. Misa, P. Brey, & A. Feenberg (Eds.), *Modernity and Technology* (pp. 161–184). Cambridge, Massachusetts: Massachusetts Institute of Technology.
- Lyon, D. (2006a). 9/11, synopticon, and scopophilia: Watching and being watched. In K. Haggerty & R. V. Ericson (Eds.), *The New Politics of Surveillance and Visibility* (pp. 35–54). Toronto: University of Toronto Press.

- Lyon, D. (2006b). The search for surveillance theories. In D. Lyon (Ed.), *Theorizing Surveillance: The Panopticon and Beyond* (pp. 3–20). Abingdon, Oxon: Routledge.
- Lyon, D. (Ed.). (2006c). *Theorizing Surveillance: The Panopticon and Beyond*. Abingdon, Oxon: Routledge.
- Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge, UK: Polity Press.
- Lyon, D. (2008, September 28). Surveillance Society. Retrieved from http://www.festivaldeldiritto.it/2008/pdf/interventi/david_lyon.pdf
- Lyon, D. (2009). *Identifying Citizens: ID Cards as Surveillance*. Cambridge, Malden, MA: Polity Press.
- Lyon, D. (2010a). Liquid surveillance : The contribution of Zygmunt Bauman to surveillance. *International Political Sociology*, 4, 325–338. <https://doi.org/10.1111/j.1749-5687.2010.00109.x>
- Lyon, D. (2010b). National ID card systems and social sorting: International public opinion. In E. Zureik, L. L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, Privacy, and the Globalization of Personal Information* (pp. 236–256). Montreal, Ithaca: McGill-Queen's University Press.
- Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, (July-December), 1–13. <https://doi.org/10.1177/2053951714541861>
- Lyon, D., Marmura, S., & Peroff, P. (2005). *Location technologies: mobility, surveillance and privacy: A report to the Office of the Privacy Commissioner of Canada under the Contributions Program*. Kingston, Ontario.
- Lyon, D., & Zureik, E. (1996). Surveillance, privacy, and the new technology. In D. Lyon & E. Zureik (Eds.), *Computers, Surveillance, and Privacy* (pp. 1–18). Minneapolis: University of Minnesota Press.
- MACCORR. (n.d.-a). Customer loyalty programs in Canada: Stats and facts. Retrieved May 7, 2021, from <https://www.macorr.com/blog/?p=342>
- MACCORR. (n.d.-b). Customer loyalty programs in the US: Stats and facts. Retrieved May 7, 2021, from <https://www.macorr.com/blog/?p=347>
- Macdonell, B. (2020, August 3). Contact tracing information at Ontario bars, restaurants raises privacy concerns. *CTV News*.
- MacInnis, D. J. (2011). A framework for conceptual contributions in marketing. *Journal of Marketing*, 75(July), 136–154.
- MacInnis, D. J., & Folkes, V. S. (2010). The disciplinary status of consumer behavior : A sociology of science perspective on key controversies. *Journal of Consumer Research*, 36(6), 899–914. <https://doi.org/10.1086/644610>
- Maclaran, P., & Kravets, O. (2019). Feminist perspectives in marketing: Past, present, and future. In M. Tadajewski, M. Higgins, J. Denergi-Knott, & R. Varman (Eds.), *The Routledge Companion to Critical Marketing* (pp. 64–82). London & New York: Routledge.
- Magnarelli, M. (2018). The next marketing skill you need to master: Touch. Retrieved May 16, 2021, from <https://www.forbes.com/sites/margaretmagnarelli/2018/09/14/haptic-marketing/?sh=5c3266a87a3f>
- Magnet, S. (2009). Bio-benefits: Technologies of criminalization, biometrics, and the welfare system. In S. Hier & J. Greenberg (Eds.), *Surveillance: Power, Problems, and Politics* (pp. 169–183). Vancouver: UBC Press.
- Mann, S. (1997). Smart clothing : The wearable computer and wearCam. *Personal Technologies*, 1, 21–27.

- Mann, S. (1998). WEARABLE COMPUTING as means for PERSONAL EMPOWERMENT. In *Keynote Address for The First International Conference on Wearable Computing, ICWC-98, May 12-13, Fairfax VA* (pp. 1–8).
- Mann, S. (2004). “Sousveillance”: Inverse surveillance in multimedia imaging. In *Proceedings of the 12th ACM International Conference on Multimedia* (pp. 620–627). New York, USA. <https://doi.org/10.1145/1027527.1027673>
- Mann, S. (2009). Shooting Back (Trailer) [Video file]. Retrieved July 8, 2018, from <https://www.youtube.com/watch?v=7QD5YDJ2NYU>
- Mann, S. (2012). How McDonaldized surveillance creates a monopoly on sight that chills AR and smartphone development. Retrieved from <https://www.webcitation.org/6Cb7y7KRb?url=http://wearcam.org/mcveillance.pdf>
- Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance : Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, 1(3), 331–355.
- Marabelli, M., & Newell, S. (2014). Knowing, power and materiality: A critical review and reconceptualization of absorptive capacity. *International Journal of Management Reviews*, 16(4), 479–499. <https://doi.org/10.1111/ijmr.12031>
- MarchNetworks. (2019). IP video solutions for retail. Retrieved November 21, 2019, from <https://www.marchnetworks.com/solutions/retail/>
- Margulis, A., Boeck, H., & Laroche, M. (2019). Connecting with consumers using ubiquitous technology: A new model to forecast consumer reaction. *Journal of Business Research*, 121, 448–460. <https://doi.org/10.1016/j.jbusres.2019.04.019>
- Markos, E., Labrecque, L. I., & Milne, G. R. (2018). A new information lens: The self-concept and exchange context as a means to understand information sensitivity of anonymous and personal identifying information. *Journal of Interactive Marketing*, 42, 46–62. <https://doi.org/10.1016/j.intmar.2018.01.004>
- Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and research. *Management Science*, 34(5), 583–598.
- Marton-Williams. (1978). Questionnaire design. In R. M. Worcester & J. Downham (Eds.), *Consumer Market Research Handbook* (2nd ed.). New York; Toronto: Van Nostrand Reinhold.
- Marx, G. T. (1996). Electric eye in the sky: Some reflections on the new surveillance and popular culture. In D. Lyon & E. Zureik (Eds.), *Computers, Surveillance, and Privacy* (pp. 193–233). Minneapolis: University of Minnesota Press.
- Marx, G. T. (2003). A Tack in the shoe : Neutralizing and resisting the new surveillance. *Journal of Social Issues*, 59(2), 369–390. <https://doi.org/10.1111/1540-4560.00069>
- Marx, G. T. (2008). Surveys and surveillance. In F. G. Conrad & M. F. Schober (Eds.), *Envisioning the Survey Interview of the Future* (pp. 254–266). New Jersey: John Wiley & Sons. <https://doi.org/10.1002/9780470183373.ch13>
- Marx, G. T. (2012). Preface: “Your Papers please”: personal and professional encounters with surveillance. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies* (pp. xx–xxx). Oxon: Routledge.
- Marx, G. T. (2016). *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: The University of Chicago Press.
- Marx, K. (1977). *Capital, volume I*. Moscow: Progress Publishers.
- Masoodi, J. (2021, March 3). Ontario’s plans for COVID-19 contact tracing wearable devices

- threaten freedom and privacy. Retrieved March 5, 2021, from <https://theconversation.com/ontarios-plans-for-covid-19-contact-tracing-wearable-devices-threaten-freedom-and-privacy-156028>
- Mathiesen, T. (1997). The viewer society: Michel Foucault's "Panopticon" revisited. *Theoretical Criminology*, 1(2), 215–234.
- Matsakis, L. (2019, October 19). At an Outback Steakhouse franchise, surveillance blooms.
- McCracken, G. (1988). *The Long Interview*. California: SAGE Publications.
- McGourty, C. J. (2015). *Common types of organized retail crimes*.
- Mchugh, M. L. (2013). The Chi-square test of independence. *Biochemia Medica*, 23(2), 143–149.
- McLaughlin, E. C. (2020, August 9). How George Floyd's death ignited a racial reckoning that shows no signs of slowing down. Retrieved May 11, 2021, from <https://www.cnn.com/2020/08/09/us/george-floyd-protests-different-why/index.html>
- Mehroliya, S., Alagarsamy, S., & Solaikutty, V. M. (2021). Customers response to online food delivery services during COVID-19 outbreak using binary logistic regression. *International Journal of Consumer Studies*, 45, 396–408. <https://doi.org/10.1111/ijcs.12630>
- Metz, C. (1982). *The Imaginary Signifier: Psychoanalysis and the Cinema*. (C. Britton, A. Williams, B. Brewster, & A. Guzzetti, Trans.). Bloomington: Indiana University Press.
- Meyers, L. S., Gamst, G., & Guarino, A. J. (2006). *Applied Multivariate Research: Design and Interpretation*. Thousand Oaks, CA: Sage Publications.
- Meyrowitz, J. (1985). *No Sense of Place: The Impact of Electronic Media on Social Behaviour*. New York: Oxford University Press.
- Michael, M. G. G., Fusco, S. J., & Michael, K. (2008). A research note on ethics in the emerging age of überveillance. *Computer Communications*, 31, 1192–1199. <https://doi.org/10.1016/j.comcom.2008.01.023>
- Mitchell, K. K. (2007). Journeying beyond marketing's collective consciousness. In M. Saren, P. Maclaran, C. Goulding, R. Elliott, A. Shankar, & M. Catterall (Eds.), *Critical Marketing: Defining the Field* (pp. 211–232). Oxford, UK: Elsevier.
- Moe, E. (2020, July 15). Video technologies help retailers deliver a safe in-store shopping experience in the age of COVID-19. Retrieved September 16, 2020, from <https://www.securitymagazine.com/articles/92836-video-technologies-help-retailers-deliver-a-safe-in-store-shopping-experience-in-the-age-of-covid-19>
- Monahan, T. (2006). Counter-surveillance as political intervention? *Social Semiotics*, 16(4), 515–534. <https://doi.org/10.1080/10350330601019769>
- Monieson, D. D. (1988). Intellectualization in marketing: A world disenchanted. *Journal of Macromarketing*, 8(2), 4–10.
- Moorman, C., van Heerde, H. J., Moreau, C. P., & Palmatier, R. W. (2019). Challenging the boundaries of marketing. *Journal of Marketing*, 83(5), 1–4. <https://doi.org/10.1177/0022242919867086>
- Mordini, E., & Green, M. (2009). Identity, security and democracy: The wider social and ethical implications of automated systems for human identification. In *Proceedings of the NATO Advanced Research Workshop on Identity, Security and Democracy: The Wider Social and Ethical Implications of Automated Systems for Human Identification*. Jerusalem, Israel: IOS Press.
- Morgan, D. L. (2007). Paradigms lost and pragmatism regained: Methodological implications of combining qualitative and quantitative methods. *Journal of Mixed Methods Research*, 1(1),

- 48–76. <https://doi.org/10.1177/2345678906292462>
- Mowen, J. C., Licata, J. W., & McPhail, J. (1993). Waiting in the emergency room: How to improve patient satisfaction. *Journal of Health Care Marketing*, 13(2), 26–33.
- Murray, J. B., Evers, D. J., & Janda, S. (1995). Marketing, Theory Borrowing, and Critical Reflection. *Journal of Macromarketing*. <https://doi.org/10.1177/027614679501500207>
- Myers, M. D. (2013). *Qualitative research in business management* (2nd editio). Los Angeles: Sage.
- Nagar, K. (2016). Consumer response to brand placement in movies: Investigating the brand-event fit. *Vikalpa: The Journal for Decision Makers*, 41(2), 149–167. <https://doi.org/10.1177/0256090916642678>
- Nagle, J. J. (1971, December 26). Trading stamps: A long history. *The New York Times*.
- Najibi, A. (2020, October 24). Racial discrimination in face recognition technology. Retrieved August 19, 2021, from <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>
- National Association for Shoplifting Prevention. (2014). Shoplifting Statistics. Retrieved July 2, 2018, from <http://www.shopliftingprevention.org/what-we-do/learning-resource-center/statistics/>
- National Retail Federation. (2020a). Prevent worker exposure to coronavirus (COVID-19). Retrieved July 26, 2020, from <https://nrf.com/resources/retail-safety-and-security-tools/coronavirus-resources-retailers>
- National Retail Federation. (2020b, July 13). NRSS 2020 National Retail Security Survey. Retrieved May 3, 2021, from <https://nrf.com/research/national-retail-security-survey-2020>
- National Retail Federation. (2020c, December 15). NRF 2020 Organized Retail Crime Survey. Retrieved May 3, 2021, from <https://nrf.com/research/2020-organized-retail-crime-survey>
- Nelkin, D., & Andrews, L. (2003). Surveillance creep in the genetic age. In D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (pp. 94–110). London: Routledge.
- Neslin, S. A. (2014). Customer relationship management (CRM). In R. S. Winer & S. A. Neslin (Eds.), *The History of Marketing Science* (Vol. 3, pp. 289–317). Hanover, MA, USA: World Scientific Publishing Co.
- Newport, H. (2020). Holiday shopping 2020 predictions from 7 customer experience experts. Retrieved October 9, 2020, from [https://www.medallia.com/blog/predictions-holiday-shopping-experience/?source=Marketing - Media&utm_campaign=FY21Q3_NA_CAN_Brand_Awareness_Campaign&utm_source=cma&utm_medium=paid-email&utm_content=retail-holiday-blog&utm_term=top5picks](https://www.medallia.com/blog/predictions-holiday-shopping-experience/?source=Marketing-Media&utm_campaign=FY21Q3_NA_CAN_Brand_Awareness_Campaign&utm_source=cma&utm_medium=paid-email&utm_content=retail-holiday-blog&utm_term=top5picks)
- Nguyen, M., Bin, Y. S., & Campbell, A. (2012). Comparing online and offline self-disclosure: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, 15(2), 103–111. <https://doi.org/10.1089/cyber.2011.0277>
- Norddeutscher Rundfunk. (2014, January 26). Snowden-Interview: Transcript.
- Norris, C. (2003). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (pp. 249–281). London: Routledge.
- Nussbaum, E. (2007, February). Say Everything: Kids, the Internet, and the End of Privacy: The Greatest Generation Gap Since Rock and Roll. Retrieved March 7, 2019, from <http://nymag.com/news/features/27341/>
- O’Neil, L. (2020, October 30). Toronto Eaton Centre owner found guilty of hiding facial

recognition cameras in kiosks.

- Office of Research Ethics. (2020). CUREB [Carleton University Research Ethics Board] Mandatory Requirements for Research during COVID-19 Outbreak. Retrieved May 9, 2020, from <https://carleton.ca/researchethics/>
- Office of the Privacy Commissioner of Canada. (2016, September). Business and your personal information. Retrieved February 12, 2019, from <https://www.priv.gc.ca/en/privacy-topics/your-privacy-rights/businesses-and-your-personal-information/>
- Office of the Privacy Commissioner of Canada. (2018). Guidelines for obtaining meaningful consent. Retrieved November 20, 2020, from https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/
- Office of the Privacy Commissioner of Canada. (2021, May). Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/
- Office of the Privacy Commissioner of Canada. (n.d.). Retrieved July 23, 2018, from <https://www.priv.gc.ca/en/for-individuals/>
- Office of the Privacy Commissioner of Canada. (2019, May 9). 2018-19 Survey of Canadians on privacy. Retrieved May 10, 2021, from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/
- Olson, K. E., O'Brien, M. A., Rogers, W. A., & Charness, N. (2011). Diffusion of technology: Frequency of use for younger and older adults. *Ageing International*, 36(1), 1230145. <https://doi.org/10.1007/s12126-010-9077-9>
- Orwell, G. (1989). *Nineteen Eighty-four*. London: Penguin.
- Ottawa Business Journal. (2020, August 27). Big move: Costco opens second-largest Canadian location at Shoppers City East. Retrieved August 29, 2020, from <https://obj.ca/article/local/retail/big-move-costco-opens-second-largest-canadian-location-shoppers-city-east>
- Ottawa Public Health. (2020). *COVID-19 guidance for retail workers - Including grocery stores and pharmacies*. *Ottawa Public Health*. <https://doi.org/10.1017/CBO9781107415324.004>
- Ouellette, J. (2020, July 21). How thermal imaging cameras will help facilities reopen in a COVID-19 world. Retrieved September 16, 2020, from <https://www.securitymagazine.com/articles/92873-how-thermal-imaging-cameras-will-help-facilities-reopen-in-a-covid-19-world>
- Overstreet, J., & Clodfelter, R. (1995). Safety and security concerns of shopping center customers and the effect of these concerns on shopping behavior. *Journal of Shopping Center Research*, 2, 91–109.
- Palahnuik, C. (2012). *Lullaby*. New York: Anchor Books.
- Palos-Sanchez, P., Saura, J. R., & Martin-Velicia, F. (2019). A study of the effects of programmatic advertising on users' concerns about privacy overtime. *Journal of Business Research*, 96, 61–72. <https://doi.org/10.1016/j.jbusres.2018.10.059>
- Pandolph, S. (2017, October 26). Shoppers expect more personalization. *Business Insider*.
- Pansari, A., & Kumar, V. (2017). Customer engagement: The construct, antecedents, and consequences. *Journal of the Academy of Marketing Science*, 45, 294–311. <https://doi.org/10.1007/s11747-016-0485-6>
- Pantano, E., Pizzi, G., Scarpi, D., & Dennis, C. (2020). Competing during a pandemic? Retailers' ups and downs during the COVID-19 outbreak. *Journal of Business Research*,

- 116, 209–213. <https://doi.org/10.1016/j.jbusres.2020.05.036>
- Paolanti, M., Pietrini, R., Mancini, A., Frontoni, E., & Zingaretti, P. (2020). Deep understanding of shopper behaviours and interactions using RGB-D vision. *Machine Vision and Applications*, 31(66). <https://doi.org/10.1007/s00138-020-01118-w>
- Patterson, C. (2020, July 8). Wave of store closures to hit Canada in the Summer of 2020. Retrieved July 15, 2020, from <https://www.retail-insider.com/retail-insider/2020/7/wave-of-store-closures-to-hit-canada-in-the-summer-of-2020>
- Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know? *International Business Review*, 29(4). <https://doi.org/10.1016/j.ibusrev.2020.101717>
- Pecora, V. P. (2002). The culture of surveillance. *Qualitative Sociology*, 25(3), 345–358. <https://doi.org/10.1023/A:1016081929646>
- Peek-Asa, C., Casteel, C., Kraus, J. F., & Whitten, P. (2006). Employee and customer injury during violent crimes in retail and service businesses. *American Journal of Public Health*, 96(10), 1867–1872. <https://doi.org/10.2105/AJPH.2005.071365>
- Peslak, A. R. (2005). An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics*, 59, 327–345. <https://doi.org/10.1007/s10551-005-2928-8>
- Petersen, C. (2013, July 18). How do retail shoppers feel about surveillance. Retrieved July 19, 2019, from <https://www.retailcustomerexperience.com/articles/how-do-retail-shoppers-feel-about-surveillance/>
- Peterson, H. (2018, May 22). Amazon isn't alone in punishing shoppers for too many returns—These are all the companies that track your returns. Retrieved April 10, 2019, from <https://www.businessinsider.com/stores-that-track-returns-list-2018-3>
- Peterson, H. (2020, July 21). More than 6,000 stores are closing in 2020 as the retail apocalypse drags on. Here's the full list. *Business Insider*.
- Petro, G. (2020, March 20). The Coronavirus Tsunami: What's To Come For U.S. Retail. *Forbes*.
- Phillips, D., & Curry, M. (2003). Privacy and the phenetic urge. In D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (pp. 137–152). London: Routledge.
- Phillips, S., Alexander, A., & Shaw, G. (2005). Consumer misbehavior: The rise of self-service grocery retailing and shoplifting in the United Kingdom c. 1950-1970. *Journal of Macromarketing*, 25(1), 66–75. <https://doi.org/10.1177/0276146705275715>
- Pisani, J. (2019, April 24). Cameras that guess your age and sex are coming to store shelves. Retrieved April 26, 2019, from <https://www.ctvnews.ca/sci-tech/coming-to-store-shelves-cameras-that-guess-your-age-and-sex-1.4392358>
- Polacco, A. (2018). The Amazon Go concept: Implications, applications, and sustainability. *Journal of Business Management*, 24(1), 79–92. <https://doi.org/10.6347/JBM.201803>
- Pole, A. (2010). Presentation: How Target gets the most out of its guest data improve marketing ROI. In *Predictive Analytics World conference*.
- Poster, M. (1989). *Critical Theory and Poststructuralism: In Search of a Context*. Ithaca, NY: Cornell University Press.
- Poster, M. (1990). *The Mode of Information: Poststructuralism and Social Context*. Oxford, UK: Polity Press.
- Poster, M. (1996). Databases as discourse, or electronic interpellations. In P. Heelas, S. Lash, & P. Morris (Eds.), *Detraditionlaization: Critical reflections on authority and identity* (pp.

- 277–293). Oxford: Blackwell.
- Poster, M. (2005). Hardt and Negri's Information Empire: A Critical Response. *Cultural Politics: An International Journal*, 1(1), 101–117. <https://doi.org/10.2752/174321905778054917>
- Powers, T. L., & Steward, J. L. (2010). Alfred P. Sloan's 1921 repositioning strategy. *Journal of Historical Research in Marketing*, 2(4), 426–442. <https://doi.org/10.1108/17557501011092475>
- Pretious, M., Stewart, R., & Logan, D. (1995). Retail security: A survey of methods and management in Dundee. *International Journal of Retail & Distribution Management*, 23(9), 28–35. <https://doi.org/10.1108/09590559510098681>
- Pridmore, J. (2010). Loyalty ambivalence in the United States and Canada: The GDP survey, the focus groups, and the context of those wonderfully intrusive loyalty cards. In E. Zureik, L. L. H. Stalker, E. Smith, D. Lyon, & Y. E. Chan (Eds.), *Surveillance, Privacy, and the Globalization of Personal Information* (pp. 295–309). Montreal, Ithaca: McGill-Queen's University Press.
- Pridmore, J., & Zwick, D. (2011). Editorial: Marketing and the rise of commercial consumer surveillance. *Surveillance & Society*, 8(3), 269–277.
- Pridmore, J., & Zwick, D. (2013). The rise of the customer database: From commercial surveillance to customer production. In R. W. Belk & R. Llamas (Eds.), *The Routledge Companion to Digital Consumption* (pp. 102–112). New York, NY: Routledge.
- PRIZM. (n.d.). Retrieved April 9, 2019, from <https://www.environicsanalytics.com/en-ca/data/segmentation/prizm>
- Rae, M. (2020). The challenge of measuring the economic impact of coronavirus. *SAGE Business Cases*. <https://doi.org/http://dx.doi.org/10.4135/9781529741377>
- Raffel, S. (2004). Baudrillard on simulations : An exegesis and a critique. *Sociological Research Online*, 9(2). <https://doi.org/10.5153/sro.908>
- Raghubir, P., Morwitz, V. G., & Santana, S. (2012). Europoly money: How do tourists convert foreign currencies to make spending decisions? *Journal of Retailing*, 88(1), 7–19. <https://doi.org/10.1016/j.jretai.2011.11.001>
- Rainie, L., & Duggan, M. (2016). Privacy and information sharing. Retrieved January 25, 2018, from <http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/>
- Redfeam, S. (2006, April 11). Prophylactic measures. Retrieved June 18, 2019, from <http://www.washingtonpost.com/wp-dyn/content/article/2006/04/10/AR2006041001312.html?noredirect=on>
- Redman, R. (2019, April 8). Loblaw pilots more personalized advertising. Retrieved April 10, 2019, from <https://www.supermarketnews.com/marketing/loblaw-pilots-more-personalized-advertising>
- Retail Council of Canada. (2017). Myth-Busting: Study shows Canadian consumers still prefer bricks-and-mortar stores but Retrieved August 5, 2019, from <https://www.retailcouncil.org/press-releases/myth-busting-study-shows-canadian-consumers-still-prefer-bricks-and-mortar-stores-but/>
- Retail Council of Canada. (2018). Avoid new \$100,000 penalties in force as of November 1, 2018 – New federal requirements on data breach record-keeping and reporting. Retrieved August 5, 2019, from <https://www.retailcouncil.org/advocacy/operations/avoid-new-100000-penalties-coming-into-force-on-november-1-2018-new-federal-requirements-on-data-breach-record-keeping-and-reporting/>

- Retail Council of Canada. (2021a). COVID-19 implications on privacy for retailers. Retrieved May 19, 2021, from <https://www.retailcouncil.org/coronavirus-info-for-retailers/covid-19-implications-on-privacy-for-retailers/>
- Retail Council of Canada. (2021b). Retail privacy and data. Retrieved May 19, 2021, from <https://www.retailcouncil.org/retail-privacy-and-data/>
- Retail Council of Canada. (2021c, February 24). Privacy Commissioners release findings on facial recognition in Clearview AI. Retrieved May 19, 2021, from <https://www.retailcouncil.org/privacy/privacy-commissioners-release-findings-on-facial-recognition-in-clearview-ai/>
- Retail Council of Canada. (2021d, March 25). Facial recognition and federal government developments. Retrieved May 19, 2021, from <https://www.retailcouncil.org/community/store-operations/facial-recognition-and-what-retailers-need-to-know/>
- Retailer's Guide - Vol 1.1. (2018). Retrieved August 5, 2019, from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwigjPjmudnoAhVFHc0KHZp2C2IQFjAAegQIARAB&url=https%3A%2F%2Fwww.retailcouncil.org%2Fwp-content%2Fuploads%2F2018%2F09%2FBDO_-_Retailers_Guide_0.pdf&usq=AOvVaw3pzeJamFIndMWvqcNFR82A
- RFID Journal. (2002, June 24). Learning from Prada. *RFID Journal*.
- Rhee, J. (1999). Mirroring Medusa : Counterveillance in ShootingBack. In *IEEE International Conference on Information Visualization (Cat. No. PR00210)* (pp. 1–5). London, UK: IEEE. <https://doi.org/10.1109/IV.1999.781589>
- Rhodes, L. A. (1998). Panoptical Intimacies. *Public Culture*, 10(2), 285–311. <https://doi.org/10.1215/08992363-10-2-285>
- Rhodes, L. A. (2004). *Total Confinement: Madness and Reason in the Maximum Security Prison*. Berkeley, CA: University of California Press.
- Rick, D. (2013, August 14). From Edison to internet: A history of video surveillance.
- Rieger, S. (2018, July 26). At least two malls are using facial recognition technology to track shoppers' ages and genders without telling. Retrieved July 28, 2018, from <https://www.cbc.ca/news/canada/calgary/calgary-malls-1.4760964>
- Rifkin, J. (2011). *The Third Industrial Revolution: How Lateral Power is Transforming Energy, the Economy, and the World*. New York: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-04423-1_2
- Rogers, E. W. (2003). *Diffusion of Innovations* (5th Ed.). New York, NY: Free Press.
- Romele, A., Gallino, F., Emmenegger, C., & Gorgone, D. (2017). Panopticism is not enough: Social media as technologies of voluntary servitude. *Surveillance & Society*, 15(2), 204–221. <https://doi.org/https://doi.org/10.24908/ss.v15i2.6021>
- Rorty, R. (1999). *Philosophy and Social Hope*. Harmondsworth: Penguin.
- Rosenbloom, S. (2010, March). In bid to sway sales, cameras track shoppers. *The New York Times*.
- Rosenthal, R., & Gaito, J. (1963). The interpretation of levels of significance by psychological researchers. *The Journal of Psychology: Interdisciplinary and Applied*, 55(1), 33–38.
- Rossi, P. E., McCulloch, R. E., & Allenby, G. M. (1996). The value of purchase history data in target marketing. *Marketing Science*, 15(4), 321–340.
- Rotfeld, H. J. (2014). The pragmatic importance of theory for marketing practice. *Journal of Consumer Marketing*, 31(4), 322–327. <https://doi.org/10.1108/JCM-02-2014-0854>

- Roy, S. K., Balaji, M. S., Sadeque, S., Nguyen, B., & Melewar, T. C. (2017). Constituents and consequences of smart customer experience in retailing. *Technological Forecasting and Social Change*, 124, 257–270. <https://doi.org/10.1016/j.techfore.2016.09.022>
- Safdar, K. (2018). The stores that track your returns; J.C. Penney, CVS, Sephora among retailers using Retail Equation to generate customers' "risk score." *The Wall Street Journal*, April 4.
- Salmons, J. (2011). *Cases in Online Interview Research*. London: Sage.
- Saltwire Network. (2020, March 10). EDITORIAL: Business world bracing for COVID-19. Retrieved July 26, 2020, from <https://www.theguardian.pe.ca/opinion/regional-perspectives/editorial-business-world-bracing-for-covid-19-421361/>
- Samat, S., Acquisti, A., & Babcock, L. (2017). Raise the curtains : The effect of awareness about targeting on consumer attitudes and purchase intentions. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* (pp. 299–318). Santa Clara, CA.
- Sandberg, J., & Alvesson, M. (2011). Ways of constructing research questions: Gap-spotting or problematization? *Organization*, 18(1), 23–44. <https://doi.org/10.1177/1350508410372151>
- Sandler, R. (2020, May 20). Victoria's Secret to close 250 U.S. and Canadian stores as sales plummet due to the Coronavirus. Retrieved May 3, 2021, from <https://www.forbes.com/sites/rachelsandler/2020/05/20/victorias-secret-to-close-250-us-and-canadian-stores-as-sales-plummet-due-to-the-coronavirus/?sh=59c977902d08>
- Saren, M., MacLaran, P., Goulding, C., Elliott, R., Shankar, A., & Catterall, M. (2007). Introduction: Defining the field of critical marketing. In M. Saren, P. MacLaran, C. Goulding, R. Elliott, A. Shankar, & M. Catterall (Eds.), *Critical Marketing: Defining the Field* (pp. xvii–xxiii). Oxford, UK: Elsevier.
- Saul, H. (2013, August 3). "Your country needs you": The myth of the most iconic World War I emblem. *Independent*.
- Schroeder, J. E. (2007). Critical marketing: Insights for informed research and teaching. In M. Saren, P. MacLaran, C. Goulding, R. Elliott, A. Shankar, & M. Catterall (Eds.), *Critical Marketing: Defining the Field* (pp. 18–29). Oxford, UK: Elsevier.
- Schulz, D. (2019, April 22). Captured on Camera: The use of body cameras to protect retail staff, properties and the general public. *Stores (NRF's Magazine)*.
- Schwab, K. (2019). It's not just Google or Facebook: The freezer aisle is ad targeting you now. Retrieved June 16, 2019, from <https://www.fastcompany.com/90302382/its-not-just-google-or-facebook-the-freezer-aisle-is-ad-targeting-you-too>
- Schwarzkopf, S. (2016). Too many compromises: Survey research and the spectre of communism. *Journal of Historical Research in Marketing*, 8(1), 197–214. <https://doi.org/10.1108/JHRM-11-2015-0046>
- Scott, L. M. (2007). Critical research in marketing: An armchair report. In M. Saren, P. MacLaran, C. Goulding, R. Elliott, A. Shankar, & M. Catterall (Eds.), *Critical Marketing: Defining the Field* (pp. 4–17). Oxford, UK: Elsevier.
- Scott, M. L., Martin, K. D., Wiener, J. L., Ellen, P. S., & Burton, S. (2020). The COVID-19 pandemic at the intersection of marketing and public policy. *Journal of Public Policy and Marketing*, 39(3), 257–265. <https://doi.org/10.1177/0743915620932151>
- Scranton, P., Berghoff, H., & Spiekermann, U. (2012). *The Rise of Marketing and Market Research*. New York: Palgrave Macmillan.
- SDM Magazine. (2020, June 15). Security & Safety Things offers COVID-19 video analytics solutions for retailers. Retrieved September 16, 2020, from <https://www.sdmmag.com/articles/98159-security-safety-things-offers-covid-19-video->

analytics-solutions-for-retailers

- Semple, J. (1993). *Bentham's Prison: A Study of the Panopticon Penitentiary*. New York: Oxford University Press.
- Shahbaz, M., Bilal, M., Moiz, A., Zubair, S., & Iqbal, H. M. N. (2020). Food safety and COVID-19: Precautionary measures to limit the spread of coronavirus at food service and retail sector. *Journal of Pure and Applied Microbiology*, 14(Special Edition), 1–8.
- Sharma, G. D., Thomas, A., & Paul, J. (2021). Reviving tourism industry post-COVID-19: A resilience-based framework. *Tourism Management Perspectives*, 37, 100786. <https://doi.org/10.1016/j.tmp.2020.100786>
- Shaw, H. (2018, February 2). “Why the hell are they at \$1.88?”: Inside the damning allegations of Canada’s bread price fixing scandal. Retrieved May 2, 2021, from <https://financialpost.com/news/retail-marketing/why-the-hell-are-they-at-1-88-inside-the-damning-allegations-of-collusion-between-grocers-producers-to-fix-bread-prices>
- Sheth, J. (2020). Impact of Covid-19 on consumer behavior: Will the old habits return or die? (Journal pre-proofs). *Journal of Business Research*, (January). <https://doi.org/https://doi.org/10.1016/j.jbusres.2020.05.059> JBR
- Shim, R. (2003, April 7). Benetton takes stock of chip plan. Retrieved July 12, 2019, from <https://www.cnet.com/news/benetton-takes-stock-of-chip-plan/>
- Sides, R., Matt, M., Goldberg, R., & Mangold, M. (2019). Consumer privacy in retail: The next regulatory and competitive frontier. Retrieved May 17, 2021, from <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/us-retail-privacy-survey-2019.pdf>
- Siegel, E. (2013). *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die*. Hoboken, New Jersey: John Wiley & Sons, Inc.
- Silverman, J. (2021, March 3). Vaccines are free at CVS and walgreens. You’re what’s for sale. Retrieved March 8, 2021, from https://newrepublic.com/article/161544/vaccines-free-cvs-walgreens-youre-whats-sale?utm_source=social&utm_medium=facebook&utm_campaign=sharebtn&fbclid=IwAR3l8E5tgoOIPSjL1oOpkqXyg4_wLSQgnvogn0wQ10gpspj_AgLDPVq6lS0
- Silverstein, J. (2018, July 13). Walmart patents audio surveillance technology to record customers and employees. Retrieved April 30, 2021, from <https://www.cbsnews.com/news/walmart-patents-audio-surveillance-technology-to-record-customers-and-employees/>
- Singer, N. (2016). Why a push for online privacy is bogged down in Washington. *New York Times*.
- Singh, A. S. (2011). Retailing in the twenty-first century: Current and future trends. *Journal of Consumer Mar*, 28(7), 551–553. <https://doi.org/10.5040/9781501304118>
- Singh, S., & Lyon, D. (2013). Surveilling consumers: The social consequences of data processing on Amazon.com. In R. W. Belk & R. Llamas (Eds.), *The Routledge Companion to Digital Consumption* (pp. 319–332). New York, NY: Routledge.
- Singh, V., & Jain, A. (2015). Consumer trust in retail: Development of a multiple item scale. *Journal of Economics, Business and Management*, 3(10), 971–976. <https://doi.org/10.7763/joebm.2015.v3.318>
- Singleton, R., & Straits, B. C. (2005). *Approaches to Social Research* (5th ed.). New York: Oxford University Press.
- Skrovan, S. (2017, April 26). Why many shoppers go to stores before buying online. Retrieved

- May 16, 2021, from <https://www.retaildive.com/news/why-many-shoppers-go-to-stores-before-buying-online/441112/>
- Smith, A., & Sparks, L. (2003). Making tracks: Loyalty cards as consumer surveillance. *European Advances in Consumer Research*, 6, 368–373.
- Smith, D. (2019, October 8). Amazon Echo Frames -- Here's what you didn't know about Amazon's new smart glasses. *Cnet*.
- Sobeys. (2021). Sobeys smart cart. Retrieved May 7, 2021, from <https://www.sobeys.com/en/smart-cart/>
- Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven & London: Yale University Press.
- Solutions for retailers. (n.d.). Retrieved July 19, 2019, from <https://www.shopperception.com/retailers.html>
- soundintelligence. (2021). Audio analytics for professionals. Retrieved April 30, 2021, from <https://www.soundintel.com/>
- Spiggle, S. (1994). Analysis and interpretation of qualitative data in consumer research. *Journal of Consumer Research*, 21(3), 491–503.
- Stewart, B. (2020, December 3). Online exam monitoring can invade privacy and erode trust at universities. Retrieved December 4, 2020, from https://theconversation.com/online-exam-monitoring-can-invade-privacy-and-erode-trust-at-universities-149335?utm_source=dlvr.it&utm_medium=facebook&fbclid=IwAR2ZN_xmVVJTXVQGPT9SikRu1mzU1pLmsJnjiC1E7Y0QxnEMOOvIC3hnTFQ
- Stewart, D. W. (2010). The evolution of market research. In P. Maclaran, M. Saren, B. Stern, & M. Tadajewski (Eds.), *The SAGE Handbook of Marketing Theory* (pp. 77–84). London: SAGE Publications Ltd.
- Stewart, D. W., & Zinkhan, G. M. (2006). Enhancing marketing theory in academic research. *Journal of the Academy of Marketing Science*, 34(4), 477–480. <https://doi.org/10.1177/0092070306291975>
- Stores. (2019a, June 11). Surveillance system uses crowdsourcing to identify retail criminals. *Stores (NRF's Magazine)*.
- Stores. (2019b, July 23). Retailers stem returns with new rules and oversized tags. *Stores (NRF's Magazine)*.
- Strum, B. J. (1962). Notes and comments: Trading stamps. *N.Y.U. Law Review*, 37, 1090–1127. <https://doi.org/10.3868/s050-004-015-0003-8>
- Svensson, P. (2019). Critical studies of marketing work. In M. Tadajewski, M. Higgins, J. Denergi-Knott, & R. Varman (Eds.), *The Routledge Companion to Critical Marketing* (pp. 155–171). London & New York: Routledge.
- Swedberg, C. (2016, March 18). Retailer Uses RFID, Social Media and Cameras to Track Shopper Behavior. Retrieved April 12, 2019, from <https://rfid.grandcentr.al/articles/retailer-uses-rfid-social-media-and-cameras-to-track-shopper-behavior>
- Sweeny, R. W. (2009). The pedagogicon : Other eyes in the 21st century classroom. *Journal of Social Theory in Art Education*, 28(1), 30–41.
- Tadajewski, M. (2010a). Critical marketing studies: Logical empiricism, “critical performativity” and marketing practice. *Marketing Theory*, 10(2), 210–222. <https://doi.org/10.1177/1470593110366671>
- Tadajewski, M. (2010b). Towards a history of critical marketing studies. *Journal of Marketing Management*, 26(9–10), 773–824. <https://doi.org/10.1080/02672571003668954>

- Tadajewski, M. (2011). Critical marketing studies. In M. Tadajewski, P. Maclaran, E. Parsons, & M. Parker (Eds.), *Key Concepts in Critical Management Studies* (pp. 83–87). London: Sage.
- Tadajewski, M. (2012). History and critical marketing studies. *Journal of Historical Research in Marketing*, 4(3), 440–452. <https://doi.org/10.1108/17557501211252970>
- Tadajewski, M. (2014). What is Critical Marketing studies? Reading macro, social, and Critical Marketing studies. In Ri. J. Varey & M. Pirson (Eds.), *Humanistic Marketing* (pp. 39–52). Hampshire: Palgrave Macmillan.
- Tadajewski, M., & Brownlie, D. (2008). Critical marketing: A limit attitude. In M. Tadajewski & D. Brownlie (Eds.), *Critical Marketing: Issues in Contemporary Marketing* (pp. 1–28). West Sussex, UK: John Wiley & Sons, Ltd.
- Tadajewski, M., Higgins, M., Denergi-Knott, J., & Varman, R. (2019). Introducing and advancing critical marketing studies. In M. Tadajewski, M. Higgins, J. Denergi-Knott, & R. Varman (Eds.), *The Routledge Companion to Critical Marketing* (pp. 1–34). New York, NY: Routledge.
- Tadajewski, M., & Jones, D. G. B. (2014). Historical research in marketing theory and practice: A review essay. *Journal of Marketing Management*, 30(11–12), 1239–1291. <https://doi.org/10.1080/0267257X.2014.929166>
- Takeuchi, C. (2020, October 29). Cadillac Fairview's use of facial-recognition tech at malls, including in Metro Vancouver, violated privacy laws: report. Retrieved October 31, 2020, from <https://www.straight.com/tech/cadillac-fairviews-use-of-facial-recognition-tech-at-malls-including-in-metro-vancouver>
- Tamilia, R. D. (2011, July). The wonderful world of the department store in historical perspective: A comprehensive international bibliography, partially annotated. Retrieved May 5, 2021, from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKewiK6N_s8bLwAhUDRK0KHV0CBrwQFjACegQICBAD&url=https%3A%2F%2Fcharmassociation.org%2Fwp-content%2Fuploads%2F2019%2F10%2Fdepartment-store-bibliography.pdf&usq=AOvVaw3_c4pYc7dTTDf0lhI-aDok
- Tamilia, R. D., & Reid, S. E. (2007). Technological innovation and the rise of the department store in the 19th century. *International Journal of Technology Marketing*, 2(2), 119–139.
- Tarry, S. (2021, February 24). Brick-and-Mortar Will Continue to Be Critical for Retail in Canada Post-Pandemic: Claude Sirois. Retrieved February 28, 2021, from <https://retail-insider.com/retail-insider/2021/02/brick-and-mortar-will-continue-to-be-critical-for-retail-in-canada-post-pandemic-claude-sirois/>
- Taylor, H. (2003). *Most people are "privacy pragmatists" who, while concerned about privacy, will sometimes trade it off for other benefits*. Rochester, New York: Harris Interactive (The Harris Poll). <https://doi.org/ISSN 0895-7983>
- Terlep, S. (2021, March 2). CVS, Walgreens look for Big Data reward from Covid-19 vaccinations. Retrieved March 8, 2021, from <https://www.wsj.com/articles/cvs-walgreens-look-for-big-data-reward-from-covid-19-vaccinations-11614681180>
- TheGuardian. (2019, September 4). Smile-to-pay: Chinese shoppers turn to facial payment technology. *The Guardian*.
- Tickell, S. (2010). The prevention of shoplifting in eighteenth-century London. *Journal of Historical Research in Marketing*, 2(3), 300–313. <https://doi.org/10.1108/17557501011067833>
- Tickell, S. (2015). *Shoplifting in eighteenth-century England*. *Shoplifting in Eighteenth-Century*

- England. University of Hertfordshire. <https://doi.org/10.1017/9781787443549>
- Tokunaga, R. S. (2011). Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships. *Computers in Human Behavior*, 27, 705–713. <https://doi.org/10.1016/j.chb.2010.08.014>
- Toneguzzi, M. (2020a, July 21). Walmart announces massive multi-billion dollar investment in Canadian operations. Retrieved July 21, 2020, from <https://www.retail-insider.com/retail-insider/2020/7/walmart-announces-massive-multi-billion-dollar-investment-in-canadian-operations>
- Toneguzzi, M. (2020b, August 20). Unprecedented spike in retail insolvencies in Canada due to COVID-19: Expert.
- Toneguzzi, M. (2020c, November 3). Empire's Michael Medline discusses the future of grocery retail amid second wave [Interview].
- Torpey, J. (2007). Through thick and thin : Surveillance after 9/11. *Contemporary Sociology*, 36(2), 116–119.
- Trottier, D. (2016). *Social Media as Surveillance: Rethinking Visibility in a Converging World*. New York, NY: Routledge.
- Trudeau, J. (2020, November 28). Over the past several months, we've introduced a number of benefits and supports to help you, your family, and your business get through this pandemic. [Facebook update]. Retrieved November 28, 2020, from <https://www.facebook.com/21751825648/posts/10159605072730649/>
- Turow, J. (1997). *Breaking Up America: Advertisers and the New Media World*. Chicago: The University of Chicago Press.
- Turow, J. (2006). Cracking the consumer code: Advertisers, anxiety, and surveillance in the digital age. In K. D. Haggerty & R. V. Ericson (Eds.), *The New Politics of Surveillance and Visibility* (pp. 269–307). Toronto: University of Toronto Press.
- Turow, J. (2017). *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power*. New Haven, Conn.: Yale University Press.
- Turow, J., Hennessy, M., & Draper, N. (2015). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to Exploitation. Retrieved February 15, 2019, from https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf
- Turow, J., McGuigan, L., & Maris, E. R. (2015). Making data mining a natural part of life : Physical retailing , customer surveillance and the 21st century social imaginary. *European Journal of Cultural Studies*, 18(4–5), 464–478. <https://doi.org/10.1177/1367549415577390>
- UFCW. (2020). Protecting Our Grocery Workers. Retrieved May 6, 2020, from <https://www.ufcw1518.com/protecting-our-grocery-workers/>
- Vaidhyanathan, S. (2011). *The Googlization of Everything (and Why We Should Worry)*. Berkeley, CA: University of California Press.
- Van De Ven, A. H., & Poole, M. S. (2005). Alternative approaches for studying organizational change. *Organization Studies*, 26(9), 1377–1404.
- Varman, R. (2019). Postcolonialism, subalternity, and critical marketing. In M. Tadajewski, M. Higgins, J. Denergi-Knott, & R. Varman (Eds.), *The Routledge Companion to Critical Marketing* (pp. 49–63). London & New York: Routledge.
- Verdon, J. (2020, June 28). The new science of counting shoppers: The tech tracking customers in the age of coronavirus. Retrieved May 18, 2021, from <https://www.forbes.com/sites/joanverdon/2020/06/28/the-new-science-of-counting->

- shoppers-tracking-customers-in-the-age-of-coronavirus/?sh=256288081de9
- Violino, B. (2004, April 18). Metro Future Store. Retrieved October 21, 2019, from <https://www.rfidjournal.com/articles/view?889>
- Voorhees, C. M., Fombelle, P. W., & Bone, S. A. (2020). Don't forget about the frontline employee during the COVID-19 pandemic: Preliminary insights and a research agenda on market shocks. *Journal of Service Research*, 23(4), 396–400. <https://doi.org/10.1177/1094670520944606>
- Warr, M. (2000, January). Fear of Crime in the United States: Avenues for Research and Policy Measurement and Analysis of Crime and Justice (Vol. 4). Retrieved May 6, 2021, from <https://nij.ojp.gov/library/publications/fear-crime-united-states-avenues-research-and-policy>
- Wax, M. L. (1967). On misunderstanding verstehen: A reply to Abel. *Sociology and Social Research*, 51(April), 323–333.
- Webster, F., & Robins, K. (1986). *Information Technology: A Luddite Analysis*. Norwood, New Jersey: Alex Publishing Corporation.
- Wehler, J. (2003, October 21). Prada pulls RFID because of privacy concerns. Retrieved October 21, 2019, from <https://www.secureidnews.com/news-item/prada-pulls-rfid-because-of-privacy-concerns/>
- Welsh, B. C., Mudge, M. E., & Farrington, D. P. (2009). Reconceptualizing public area surveillance and crime prevention: security guards, place managers and defensible space. *Security Journal*, 23(4), 299–319.
- Wensley, R. (2007). Relevance of critique: Can and should critical marketing influence practice and policy? In M. Saren, P. MacLaran, C. Goulding, R. Elliott, A. Shankar, & M. Catterall (Eds.), *Critical Marketing: Defining the Field* (pp. 233–243). Oxford, UK: Elsevier.
- West, J. D. (2018). New survey finds American favor face recognition to combat rising retail theft and violence. Retrieved July 2, 2018, from <https://www.facefirst.com/blog/new-survey-finds-americans-favor-face-recognition-combat-rising-retail-theft-violence/>
- Whitaker, R. (1999). *The End of Privacy: How Total Surveillance is Becoming a Reality*. New York: The New Press.
- Winder, B. (2020). *Retail Before, During & After COVID-19*. Bruce Edward Winder Consulting Ltd.
- Withiam, Gl. (2000). Carlson's "24K" consumer-centric. *Cornell Hotel and Restaurant Administration Quarterly*, 41(3), 13.
- Yadav, M. S. (2010). The decline of conceptual articles and implications for knowledge development. *Journal of Marketing*, 74(January), 1–19. <https://doi.org/10.1509/jmkg.74.1.1>
- Zuboff, S. (1988). *In the Age of the Smart Machine: The Future of Work and Power*. Oxford: Heinemann Professional Publishing Ltd.
- Zuboff, S. (2018). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London, UK: Profile Books Ltd.
- Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. *New Labour Forum*, 1–20. <https://doi.org/10.1177/1095796018819461>
- Zureik, E., Stalker, L. L. H., Smith, E., Lyon, D., & Chan, Y. E. (Eds.). (2010). *Surveillance, Privacy, and the Globalization of Personal Information*. Montreal, Ithaca: McGill-Queen's University Press.

APPENDICES

APPENDIX 1: SURVEY QUESTIONS

Survey topic	Question heading	Question(s)	Answer type
Consent	<i>Consent</i>	<i>(Online MTurk survey consent)</i>	---
	ConsentQ	I voluntarily agree to participate in this study.	Yes/No
	WorkerID	Please provide your worker ID (You can find it on your Dashboard or in the upper left corner of the Worker Website)	---
General, introductory questions	GeneralQ1*	What does surveillance in a brick-and-mortar retail store mean to you? Use as many words as you want.	[text]
	(GeneralQ2) GeneralQ2_1* GeneralQ2_2* GeneralQ2_3* GeneralQ2_4*	In general, what does the word “privacy” of your personal and shopping information mean to you? Please rank the following in order of importance (by dragging the sentences up or down), with 1 being the most important to you.	(1) Not being watched or overheard (2) Being in control of who has access to information (3) Controlling what information is collected (4) Not being disturbed by marketers
	GeneralQ3*	Some retail stores offer customer reward programmes where you can earn points or rewards based on how often you buy something from them or use their services. How many programs do you belong to?	(1) 15 and over (2) 10 to 14 (3) 5 to 9 (4) 3 (5) 2 (6) 1 (7) None
	GeneralQ4*	I am confident that the stores that collect my personal and shopping information have adequate	Likert 1-5*

		security safeguards to protect my information.	
GeneralQ5		I feel confident that I have enough information to know how new technologies used in stores might affect my personal privacy.	Likert 1-5
GeneralQ6*		Businesses take their responsibility to protect consumers' personal and shopping information seriously.	Likert 1-5
GeneralQ7*		I am concerned that in a time of economic uncertainty, businesses may choose to spend less to protect consumers' personal information.	Likert 1-5
GeneralQ8*		I am concerned about the impact of new technologies used in stores on my privacy.	Likert 1-5
(GeneralQ9) GeneralQ9_1 GeneralQ9_2* GeneralQ9_3		I am comfortable with sharing personal information (such as my name, address, telephone number, email address, date of birth, or financial information) for: <ul style="list-style-type: none"> • loyalty programs (such as Air Miles) • reward programs (for example, at gas stations) • credit cards which allow me to collect points. 	Likert 1-5
GeneralQ10		Sometimes, personal information that is held by a company or retailer about their customers might be compromised, either due to criminal activity or due to a flaw in the company's security	(1) Notify individuals who are affected (2) Notify government agencies who oversee privacy laws

		system. If a company were to experience a breach involving your personal information, what best describes your views? (Choose one)	(3) Notify both individuals and government agencies (4) There is no need to notify either individuals or government agencies (5) I do not know
	GeneralQ11	Have you ever experienced a serious incident where your personal information (such as credit card information) was used inappropriately or released without your consent?	Yes/No
	GeneralQ12	Can you tell us more about that incident?	[text]
Awareness	AwarenessQ1*	I am aware of Canadian or American federal institutions that help deal with privacy and the protection of personal information from inappropriate collection, use and disclosure.	Likert 1-5
	AwarenessQ2*	I am knowledgeable about the laws in Canada or the USA that deal with the protection of personal information.	Likert 1-5
	AwarenessQ3	I have sought out information about my privacy rights, for example, by contacting an organization, visiting a web site, or reviewing a publication for guidance.	Yes/No
	AwarenessQ4*	Have you ever reviewed a store/retailer's privacy policy?	Yes/No

Impact	(ImpactQ1) ImpactQ1_10* ImpactQ1_11* ImpactQ1_12* ImpactQ1_13* ImpactQ1_14*	Stores fix special tags onto merchandise to prevent shoplifting, and when they are not deactivated, an alarm is set off when the consumer is trying to leave the store. What would your reaction be if you accidentally set off the alarm because the store employees did not deactivate the tag? Please rank the following in order of importance (by dragging the sentences up or down), with 1 being the most important to you.	(1) I would not be bothered; I accept that stores need to prevent shoplifting. (2) I would expect an explanation and apology from the store manager. (3) I would expect an explanation and apology from the store employee. (4) I would shop less at the store in the future. (5) I would never shop at the store again.
	(ImpactQ2) ImpactQ2-1 ImpactQ2-2 ImpactQ2-3 ImpactQ2-4 ImpactQ2-5 ImpactQ2-6 ImpactQ2-7 ImpactQ2-8 ImpactQ2-9 ImpactQ2-10 ImpactQ2-11 ImpactQ2-12 ImpactQ2-13 ImpactQ2-14 ImpactQ2-15 ImpactQ2-16 ImpactQ2-17 ImpactQ2-18 ImpactQ2-19	Indicate to what extent you feel each of the following emotions after encountering surveillance in a retail store (e.g., video cameras, tags fixed on clothes): (1) enthusiastic (2) interested (3) determined (4) excited (5) inspired (6) alert (7) active (8) strong (9) proud (10) attentive (11) afraid (12) upset (13) distressed (14) nervous (15) ashamed/embarassed (16) guilty (17) hostile (18) annoyed	Likert 1-5 (1) Extremely (2) Quite a lot (3) Moderately (4) A little (5) Very slightly or not at all

		(19) uncomfortable during future shopping trips	
	ImpactQ3*	In general, as a shopper in a store that uses surveillance, what is your overall emotion?	Choose one: (1) Sense of security (I am physically protected) (2) Sense of security (my information is protected) (3) Transparency (4) Trust (5) Distrust (6) Intimidation (7) Discomfort (8) Embarrassment (9) Frustration (10) A sense of prohibition
Outcome	OutcomeAttQ1*	I feel safer, personally and physically, when retail stores use surveillance.	Likert 1-5
	OutcomeAttQ2	I have a say in what happens to my personal and shopping information held by retailers.	Likert 1-5
	OutcomeAttQ3*	I believe that laws are effective at protecting my personal information that is held by retail stores.	Likert 1-5
	OutcomeAttQ4	I trust that the places where I shop (i.e. retail stores) will protect my personal and shopping information (e.g., information I provide them with like name, email, and credit card, and my shopping history).	Likert 1-5
	OutcomeAttQ5*	In general, I am . . . the use of surveillance in retail stores. Complete the sentence using one of the following words: for or against.	(1) For (2) Against

	<p>(OutcomeBehQ1)</p> <p>OutcomeBehQ1_1*</p> <p>OutcomeBehQ1_2*</p>	<p>I think it is appropriate for a retail store to share customers' personal information with third parties such as:</p> <ul style="list-style-type: none"> • credit agencies • marketing firms 	Likert 1-5
	OutcomeBehQ2	Some retail stores use surveillance to monitor their space in order to deter shoplifting and protect customers. In my opinion, this surveillance is effective in ensuring my personal safety.	Likert 1-5
	OutcomeBehQ3*	My privacy is respected in retail stores.	Likert 1-5
	OutcomeBehQ4*	Many retail stores create profiles about their customers that include information about purchasing habits, personal characteristics and credit history. I feel it is acceptable for a business to use information in my profile to inform me of products or services they think would be of interest to me.	Likert 1-5
	<p>OutcomeBehQ5_1*</p> <p>OutcomeBehQ5_2*</p>	<p>RESISTANCE</p> <p>Have you ever done any of the following for the purpose of protecting your personal information? Choose from a list of behavioural outcomes:</p> <p>REFUSAL:</p> <ul style="list-style-type: none"> ○ When a cashier asks for my postal/zip code, I refuse to give it and still make the purchase. ○ I refuse to give information to a retail business 	Yes/No

	<p>OutcomeBehQ5_3*</p> <p>OutcomeBehQ5_4*</p> <p>OutcomeBehQ5_5*</p> <p>OutcomeBehQ5_6*</p> <p>OutcomeBehQ5_7*</p> <p>OutcomeBehQ5_8*</p> <p>OutcomeBehQ5_9*</p> <p>OutcomeBehQ5_10*</p> <p>OutcomeBehQ5_11*</p>	<p>because I think it is not needed.</p> <ul style="list-style-type: none"> ○ I asked a retail business not to sell my name and address to another retailer. ○ I asked a retail business to remove me from lists it uses for marketing. <p>DISCOVERY:</p> <ul style="list-style-type: none"> ○ I asked a retail business I was shopping at about its policies on the collection of consumer information. ○ I read the online privacy policies at the retail store website when/before making a purchase. ○ I asked a retail business to see what personal info, besides billing info, it had about me in its records. <p>MASKING:</p> <ul style="list-style-type: none"> ○ I purposefully gave incorrect information about myself to a retail business. <p>BLOCKING:</p> <ul style="list-style-type: none"> ○ I wear clothes that reveal little about my physical appearance. <p>AVOIDANCE:</p> <ul style="list-style-type: none"> ○ I shorten my shopping time in stores that use surveillance. ○ I go to another retail store (their 	
--	--	---	--

	<p>OutcomeBehQ5_12*</p> <p>OutcomeBehQ5_13*</p> <p>OutcomeBehQ5_14*</p>	<p>competition) that uses less surveillance.</p> <ul style="list-style-type: none"> ○ I turn to an alternative shopping format (for example, I shop online) <p>SWITCHING:</p> <ul style="list-style-type: none"> ○ I use the identity of another consumer (for example, I use someone else's loyalty card) <p>BREAKING:</p> <ul style="list-style-type: none"> ○ I physically and intentionally broke a surveillance system inside a store. 	
Ethics	EthicsQ	In general, why do you think people adhere to the retailer's regulations (e.g., no shoplifting or committing acts of violence in the store)?	<p>(1) They know the store is under surveillance</p> <p>(2) They know what is right and wrong (moral reason)</p> <p>(3) They know what the society deems acceptable behaviour (ethical reason)</p>
How Aware	<p>(HowAwareQ)</p> <p>HowAwareQ_1*</p> <p>HowAwareQ_2*</p> <p>HowAwareQ_3*</p> <p>HowAwareQ_4*</p> <p>HowAwareQ_5*</p> <p>HowAwareQ_6*</p> <p>HowAwareQ_7*</p> <p>HowAwareQ_8*</p>	<p>Which of the following surveillance systems have you come across in retail stores?</p> <ul style="list-style-type: none"> ○ Video surveillance ○ Audio surveillance ○ biometric surveillance ○ virtual guards ○ Tagging ○ Collecting phone numbers and emails ○ Customer Loyalty Card ○ Free Wi-Fi and/or 	Yes/No

	HowAwareQ_9* HowAwareQ_10* HowAwareQ_11* HowAwareQ_12*	Bluetooth <ul style="list-style-type: none"> ○ Personalized advertising ○ Return rewards ○ Radio frequency identification ○ Geo-fencing 	
Retail Work Experience	RetailWorkQ1	Do you currently work, or have you worked in the previous five years, in a retail store?	Yes/No
	RetailWorkQ2 RetailWorkQ2_1_TEXT RetailWorkQ2_2_TEXT	<i>[if yes]</i> Do you still work in retail now?	(1) Yes and my employer is . . . (2) No, I worked in retail in the past five years but not now. My employer was . . .
COVID-19 impact on current retail workers	CovidWorkerQ1*	During the coronavirus epidemic, do you have to surveil and monitor the shoppers more?	Yes/No
	CovidWorkerQ2*	Do consumers treat you badly because of their frustration with the newly implemented shopping regulations during the coronavirus?	Likert 1-5
	(CovidWorkerQ3) CovidWorkerQ3_1* CovidWorkerQ3_2*	While working in the store during the coronavirus, do you feel safe: <ul style="list-style-type: none"> ● from the virus? ● from angry consumers? 	Likert 1-5
	CovidWorkerQ4 CovidWorkerQ4_23_TEXT	Has your employer provided you with personal protective equipment (PPE)?	<ul style="list-style-type: none"> ● Yes, and they are: . . . ● No
	CovidWorkerQ5 CovidWorkerQ5_23_TEXT	Do you think your employer should have done more to protect you while working in the store	<ul style="list-style-type: none"> ● Yes, For example: . . . ● No

		during the COVID-19 epidemic?	
	CovidWorkerQ6 CovidWorkerQ6_24_TE XT	Do you receive any government-funded financial support due to the coronavirus pandemic?	<ul style="list-style-type: none"> • Yes • No. Why not?
	CovidWorkerQ7	Once the pandemic is over, do you still want to work in retail?	<ul style="list-style-type: none"> • Yes • No Why?
	CovidWorkerQ8	Do you live with vulnerable people who are more at risk of getting an infection and developing severe complications due to the coronavirus, like those with health problems, children or elderly people?	Yes/No
COVID-19 impact on consumers	CovidConsumerQ1*	Do you think that with the spreading of the coronavirus, retailers will need to increase their surveillance inside their stores?	Yes/No
	CovidConsumerQ2*	Why?	[text]
	CovidConsumerQ3*	When I go into a store during the COVID-19 pandemic, I accept that there are more employees surveilling the shoppers closely.	Likert 1-5
	(CovidConsumerQ4) CovidConsumerQ4_1 CovidConsumerQ4_2 CovidConsumerQ4_3 CovidConsumerQ4_4	Because of COVID-19, how do you prefer to shop? Please rank the following in order of importance (by dragging the sentences up or down), with 1 being the most important to you.	(1) In person in retail stores (2) Online and use curb pick-up (3) Online and use home delivery (4) Ask someone else (a family member, a friend, or a neighbour) to shop for me
	CovidConsumerQ5	Before COVID-19, I preferred to go shopping	Yes/No

		in the stores instead of online.	
	CovidConsumerQ6	In the future, and after COVID-19, I will prefer to shop . . . (Choose one answer)	<ul style="list-style-type: none"> • In person • online
<i>Intro</i>	<i>Intro</i>	<i>We would like to learn a little more about you to assist us with our analysis of the data you provide. You have the right to decline to answer of any of the following questions.</i>	---
Demographic	Age	Age	(1) Less than 18 (2) 18 to 24 (3) 25 to 34 (4) 35 to 44 (5) 45 to 54 (6) 55 to 64 (7) 65 or older
	Gender Gender_4_TEXT	Gender	(1) Female (2) Male (3) Non-binary/third gender (4) Prefer to self-describe (5) Prefer not to say
	Country	Country of residence	(1) Canada (2) USA
	Status Status_6_TEXT	Status in USA or Canada	(1) Citizen, by birth (2) Citizen, by naturalization (3) Permanent resident/landed immigrant (4) International student (5) Refugee claimant (6) Other: [explain] (7) Prefer not to say
	Country2	What other country are you a resident of?	[text]
	Education	What is your highest level of formal education?	(1) High school (2) College diploma (3) Currently enrolled

			<p>in a bachelor's degree program</p> <p>(4) Bachelor's degree</p> <p>(5) Master's degree</p> <p>(6) Doctorate</p> <p>(7) Other</p>
Education 7 TEXT			
Marital_status	How would you describe your marital status?		<p>(1) Single</p> <p>(2) Divorced/separated</p> <p>(3) Common-law/committed relationship</p> <p>(4) Married and living together</p> <p>(5) Married and living apart</p> <p>(6) Other: [explain]</p> <p>(7) Prefer not to say</p>
Marital_status_6_TEXT			
Employment	What best describes your employment situation?		<p>(1) Student</p> <p>(2) Student & working part-time</p> <p>(3) Not employed</p> <p>(4) Working full time</p> <p>(5) Working part time</p> <p>(6) Homemaker</p> <p>(7) Retired</p> <p>(8) Self-employed</p>
IncomeUSA	What is your average household income in the USA?		<p>(1) USD 14,999 or less</p> <p>(2) USD 15,000 to 29,999</p> <p>(3) USD 30,000 to 44,999</p> <p>(4) USD 45,000 to 76,999</p> <p>(5) USD 77,000 and over</p> <p>(6) Do not know</p> <p>(7) Prefer not to say</p>
IncomeCANADA	What is your average household income in Canada?		<p>(1) CAD 19,999 or less</p> <p>(2) CAD 20,000 to 39,999</p> <p>(3) CAD 40,000 to 59,999</p> <p>(4) CAD 60,000 to</p>

			99,999 (5) CAD 100,000 and over (6) Do not know (7) Prefer not to say
	Minority Minotiry_1_TEXT	Do you consider yourself to belong to any of the following groups?	(1) A member of a visible minority (2) An indigenous/aboriginal person (3) A person with a disability (4) None of the above
	Eng_lang	Is English your first or second language?	(1) First language (2) 2 nd language (3) Neither nor
Final questions	FinalQ1*	Thank you for providing that information. Before the survey ends, we would like you to describe what you think of and how you feel about surveilling customers in retail stores. Use as many words as you want.	[text]
	FinalQ2	Were any of the survey questions unclear to you?	Yes/No
	FinalQ3	Which survey question(s) was unclear to you?	[text]
	FinalQ4*	Is there anything else you would like to add?	[text]
Interview question	InterviewQ InterviewQ_1_TEXT	Do you agree to participate in a follow-up online interview? You will be compensated with a US\$5 Amazon gift card. If you agree, please write your email below and we will contact you.	<ul style="list-style-type: none"> • Yes, and my email is: • No
Thanks	RandomID	Thank you for taking part in this survey.	---

		<p>Here is your survey code ID: <code>{e://Field/Random%20ID}</code> When you have copied this survey code ID, please paste it into the box on your MTurk page (on which you accessed the survey link) to receive credit for taking this survey. Please click the next button to submit your survey.</p>	
Attention questions	AttentionQ1	I would rather eat a piece of fruit than a piece of paper.	Likert 1-5
	AttentionQ2	When you want to buy some milk . . . Select “none of the above”.	(1) Supermarket (2) Drug store (3) Discount store (4) None of the above

*Data from this survey question was analyzed and included in the dissertation.

APPENDIX 2: SEMI-STRUCTURED INTERVIEW QUESTIONS

Demographic information:

- Please introduce yourself. *The following prompts could be used:*
 - *Age group*
 - *Nationality*
 - *Highest level of formal education*
 - *Marital status (single; divorced; separated; common-law/committed relationship; married and living apart)*
 - *Employment situation*
 - *Annual household income*
 - *Belonging to a minority (visible minority; indigenous/aboriginal; with a disability)*

- In the past five years, have you been employed by either a retail organization or a manufacturer or seller of security or loss prevention products for the retail industry? If yes, which one(s)?

General introductory questions:

- Have you ever thought about the presence of surveillance in retail stores? If yes, what does it mean to you?
- Can you give examples of the type of surveillance systems that you have come across in retail stores?
- Why does surveillance in retail stores exist? What is its purpose?
- What type of personal information do various programs collect?

- Are you a participant in a loyalty/reward program? If yes, how many? (*at this point, the interviewee can get their wallet out or check their cellphone to count how many loyalty cards they actually have*). And why have you participated?
- Have you ever experienced an incident where your personal information was used inappropriately or released without your consent (e.g., credit card information)?
- How should retail stores behave if their security is breached and their collected personal information is compromised?
- Have you ever reviewed a retailer's privacy policy?
- How would you define privacy?
- Are you aware that there are laws and regulations that protect your personal information?
A hand-out that covers the consumer privacy rights in Canada will be given out at the end of the interview (see Appendix 2).
- *This question depends on the interviewee's gender and whether they belong to an ethnic minority* → Have you ever felt that you are a surveillance target because of your gender, ethnic background, or religious affiliation?

Impact on consumer:

- How do you feel after encountering surveillance in a retail store? Describe the positive and/or negative affect (i.e., feeling or emotion).
- If the retail store employs surveillance, does that make you feel more secure? Why or why not?
- Does anything bother you in terms of stores being able to track everything that you buy? Are there any issues there? Do you see any benefits to this practice?

- Stores fix special tags onto merchandise to prevent shoplifting, and when they are not deactivated, an alarm is set off when the consumer is trying to leave the store.

Have you ever accidentally set off the alarm because the store employees did not deactivate the tag? If yes, tell me about that experience. If no, how would you imagine what your reaction to be?

Prompts: Affective reaction (positive or negative) and behavioural reaction (e.g., not bothered since stores need to prevent shoplifting; expect an explanation and apology from store manager or employee, future less shopping in the store, or never shopping at that store)?

Outcome:

- In general, what do you feel towards the use of surveillance in retail stores? Are you for or against it?
- Do you do anything to protect your privacy of your personal information?
If yes, what? If no, why not?
- Do you feel that laws are effective at protecting your personal information held by retail stores?
- Do you trust the retail store to protect your personal information? Do you feel the same way about all stores, e.g., major chain stores versus locally owned boutiques?
- Is it appropriate for retail stores to share your personal information with third parties?

(Note: Third-party data is defined as any data collected from variety of sources by a company with no direct connection to the consumer whose data is collected. Third party

data sources may include credit agencies, marketing firms, websites, social media networks, surveys, and subscriptions.)

- Is retail surveillance effective in preventing shoplifting and protecting the customers?
- Is your privacy respected in retail stores?
- Is it acceptable that retail stores use your personal information to inform you of products or services that might be of interest to you? If yes, can you give any examples of when this has occurred? And what was your reaction then?
- Have you ever resisted store surveillance?

After hearing the interviewee's answer, a detailed explanation of examples of resistance is to be given, followed by asking the same question again (i.e., have you ever resisted store surveillance?)

REFUSAL:

- *When a cashier asks for my postal/zip code, I refuse to give it and still make the purchase.*
- *I refuse to give information to a retail business because I think it is not needed.*
- *I asked a retail business not to sell my name and address to another retailer.*
- *I asked a retail business to remove me from lists it uses for marketing.*

DISCOVERY:

- *I asked a retail business I was shopping at about its policies on the collection of consumer information.*
- *I read the online privacy policies at the retail store website when/before making a purchase.*
- *I asked a retail business to see what personal info, besides billing info, it had about*

me in its records.

MASKING:

- *I purposefully gave incorrect information about myself to a retail business.*

BLOCKING:

- *I wear clothes that reveal little about my physical appearance.*

AVOIDANCE:

- *I shorten my shopping time in stores that use surveillance.*
- *I go to another retail store (their competition) that uses less surveillance.*
- *I turn to an alternative shopping format (for example, I shop online)*

SWITCHING:

- *I use the identity of another consumer (for example, I use someone else's loyalty card)*

BREAKING:

- *I physically and intentionally broke a surveillance system inside a store.*

Ethics question:

- What do you think is the main reason other people adhere to the retailer's regulations (for example, no shoplifting or committing acts of violence in the store)?

Is it because (1) they know that the store is under surveillance; (2) for moral reasons (i.e., what they personally believe to be right or wrong); (3) for reasons ethical (i.e., adhering with societal or institutional codes of conducts)?

- What about you?

How aware question:

- *Using photos of retail surveillance, the interviewer can mention the different surveillance systems, including:*
 - *Video surveillance (known as CCTV, or Closed Circuit Television)*
 - *Internet Protocol (IP) surveillance*
 - *Audio surveillance (listening and sometimes recording your conversations in the store)*
 - *Biometric surveillance (e.g., using facial recognition software)*
 - *Virtual guards (i.e., guards keeping an eye on the store through monitors, and when a problem is detected, they use pre-recorded messages as warnings or send guards and/or police to the store)*
 - *Tagging (tags which when not deactivated at checkout counter result in the setting off of the alarms when the customer attempts to leave the store)*
 - *Collecting phone numbers and emails*
 - *Customer Loyalty Card (earning points, which translate into some type of reward)*
 - *Free Wi-Fi and/or Bluetooth*
 - *Personalized advertising (i.e., targeted video ads)*
 - *Return rewards (i.e., providing discounts for future purchases)*
 - *Radio frequency identification (i.e., RFID is a tracking technology that uses small tags or chips to transmit a signal to remote scanners)*
 - *Geo-fencing (i.e., stores using Wi-Fi and/or Bluetooth to automatically be alerted to the customer's presence when they approach, enter, and browse the store)*

Which of those surveillance systems have you come across in retail stores?

Impact of COVID-19 on retail CONSUMERS:

- Do you think that with the spreading of the coronavirus, retailers will need to increase their surveillance inside their stores? Why or why not?
- Now (i.e., during the COVID-19 pandemic) when you go to a store, do you accept that there are more employees surveilling the shoppers closely?
- Do you think store workers are treated differently because of the coronavirus? If yes, then how?
- Before the coronavirus pandemic, how did you prefer to shop? Online or in person?
- Now, and after COVID-19, how do you prefer to shop? In person; online and using curb pick-up; online and using home delivery; ask someone else to shop for you (e.g., a family member, a friend, or a neighbour).
- In the future, and after COVID-19, would you prefer to shop in person or online?

Impact of COVID-19 on retail WORKERS:

- During the coronavirus pandemic, do you have to surveil and monitor the shoppers more?
- Do consumers treat you badly because of their frustration with the newly implemented shopping regulations during the coronavirus?
- While working in the store during the coronavirus, do you feel safe: (1) from the virus? (2) from angry consumers?
- Has your employer provided you with personal protective equipment (PPE)?
- Do you think your employer should have done more to protect you while working in the store during the COVID-19 pandemic?

- Do you receive any government-funded financial support due to the coronavirus pandemic?
- Once the pandemic is over, do you still want to work in retail?
- Do you live with vulnerable people who are more at risk of getting an infection and developing severe complications due to the coronavirus, like those with health problems, children or elderly people?

Final questions:

- Before we end the interview, can you describe what you think of and how you feel about surveilling customers in retail stores?
- Is there anything else you would like to add?
- If we need to conduct a follow-up interview in the future, can we get in touch with you?

Thank you.

APPENDIX 3: CONSUMER PRIVACY RIGHTS

Privacy rights in Canada (Office of the Privacy Commissioner of Canada, 2016):

Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), sets the ground rules for handling of personal information in course of commercial activities. It applies equally to small and big businesses, whether they operate out of an actual building or only online. PIPEDA applies to private enterprises across Canada, except in provinces that have adopted substantially similar privacy legislation, namely Québec, British Columbia, and Alberta. PIPEDA also applies to all personal data that flows across provincial or national borders, in the course of commercial transactions involving organizations subject to the Act or to substantially similar legislation. PIPEDA protects information about an identifiable individual. Personal information includes your:

- Name, race, ethnic origin, religion, marital status, educational level;
- E-mail address and messages, IP (Internet protocol) address;
- Age, height, weight, medical records, blood type, DNA code, fingerprints, voiceprint;
- Income, purchases, spending habits, banking information, credit/debit card data, loan or credit reports, tax returns; and
- Social Insurance Number (SIN) or other identification numbers.

PIPEDA sets out 10 “fair information principles” which collectively form the underpinnings of PIPEDA. They are:

1. *Accountability* - Organizations should appoint someone to be responsible for privacy issues. They should make information about their privacy policies and procedures to available to customers.

2. *Identifying purposes* - Organization must identify the reasons for collecting your personal information before or at the time of collection.
3. *Consent* - Organizations should clearly inform you of the purposes for the collection, use or disclosure of personal information.
4. *Limiting collection* - Organizations should limit the amount and type of the information gathered to what is necessary.
5. *Limiting use, disclosure and retention* - In general, organizations should use or disclose your personal information only for the purpose for which it was collected, unless you consent. They should keep your personal information only as long as necessary.
6. *Accuracy* - Organizations should keep your personal information as accurate, complete and up to date as necessary.
7. *Safeguards* - Organizations need to protect your personal information against loss or theft by using appropriate security safeguards.
8. *Openness* - An organization's privacy policies and practices must be understandable and easily available.
9. *Individual access* - Generally speaking, you have a right to access the personal information that an organization holds about you.
10. *Recourse* (Challenging compliance) - Organizations must develop simple and easily accessible complaint procedures. When you contact an organization about a privacy concern, you should be informed about avenues of recourse.

As of November 1, 2018, retailers must notify the federal Office of the Privacy Commissioner (OPC) if they experience a data breach that creates a “real risk of significant harm” (considering

the sensitivity and probability of the information involved) with personal information that the organization controls. The retailer must also notify other organizations (e.g., law enforcement, banks, credit card companies, etc.) if they may be able to mitigate or reduce the risk of harm to the individuals affected (Retail Council of Canada, 2018).

Tabled in the Canadian Parliament on November 17, 2020, Bill C-11, the Digital Charter Implementation Act (DCIA), will include some significant new changes to Canada's privacy framework (Canadian Marketing Association, 2020a, 2020b), such as:

- enhanced enforcement (giving more powers to the OPC) and major financial penalties;
- more control for consumers (e.g., request for deletion and withdrawal of consent and requests for data mobility);
- upgrades to consent requirements;
- new transparency requirements;
- enhanced role for privacy codes and certifications;
- de-identification of personal information; and
- clarity on the obligations of service providers.

When it comes to consent, there are two forms: *implicit consent* (i.e., opt-out) if collected information is innocuous and the purpose is straightforward; & *expressed/explicit consent* (i.e., opt-in) for collections outside the reasonable expectations of the individual. According to the Office of the Privacy Commissioner of Canada (OPC), meaningful consent is “an essential element of Canadian private sector privacy legislation . . . However, advances in technology and the use of lengthy, legalistic privacy policies have too often served to make the control—and personal autonomy—that should be enabled by consent nothing more than illusory.” (Office of the Privacy Commissioner of Canada, 2018). The OPC outlines seven guidelines for obtaining

meaningful consent: (1) emphasizing key elements of the consent; (2) allowing individuals to control the level of detail they get and when; (3) providing individuals with clear options to say “yes” or “no”; (4) be creative and innovative when it comes to notices; (5) consider the consumer’s perspective by getting feedback and involving user experts; (6) making consent a dynamic and ongoing process by notifying individuals before implementing significant changes and periodically reminding them of privacy and consent options; and (7) standing ready to demonstrate compliance in the case of an individual’s complaint or a privacy regulator’s query.

Privacy rights in the U.S.A. (Federal Trade Commission, n.d.; Jolly, 2018):

In the U.S., there is no single, comprehensive federal law regulating the collection and use of personal data, and each Congressional term brings proposals to standardise laws at a federal level. Instead, the US has a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another. In addition, there are many guidelines, developed by governmental agencies and industry groups that do not have the force of law, but are part of self-regulatory guidelines and frameworks that are considered “best practices.” These self-regulatory frameworks have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators.

The Federal Trade Commission (FTC) has been the chief federal agency on privacy policy and enforcement since the 1970s, when it began enforcing one of the first federal privacy laws – the Fair Credit Reporting Act. Since then, rapid changes in technology have raised new privacy challenges, but the FTC’s overall approach has been consistent: the agency uses law enforcement, policy initiatives, and consumer and business education to protect consumers’

personal information and ensure that they have the confidence to take advantage of the many benefits of the ever-changing marketplace. Some of the most prominent federal privacy laws are:

- The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act) is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies. The FTC has brought many enforcement actions against companies failing to comply with posted privacy policies and for the unauthorised disclosure of personal data. The FTC is also the primary enforcer of the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§6501-6506), which applies to the online collection of information from children, and the Self-Regulatory Principles for Behavioural Advertising.
- As of March 28, 2018, all 50 states, as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted laws requiring notification of security breaches involving personal information.
- In July 2018, California passed the most sweeping of all privacy laws in the U.S., the *California Consumer Privacy Act of 2018* (effective from 1 January, 2020). The law provides consumers with several new rights, including the right to:
 1. Require the deletion of their data.
 2. Request disclosures of information about how information is collected and shared.
 3. Instruct a company not to sell their data.

There is also a private right of action for individuals to pursue violators, which will likely lead to significant class action lawsuits in California. This is a complicated law that remains subject to potential revisions before the 2020 implementation date.

APPENDIX 4: SUPPORT RESOURCES

The following is the contact information that was available to interviewees in case they felt stressed out when discussing the COVID-19 pandemic during the interviews and needed support.

(1) For Canadian interview participants:

The Canadian Mental Health Association (<https://cmha.ca/news/covid-19-and-mental-health>) offers some credible resources of recommended information including:

- A list of provincial/territorial public health authorities (<https://www.canada.ca/en/public-health/services/publications/diseases-conditions/2019-novel-coronavirus-information-sheet.html#pha>)
- The Government of Canada's COVID-19 webpage (<https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19.html>)
- The WHO webpage dedicated to COVID-19 (<https://www.who.int/emergencies/diseases/novel-coronavirus-2019>)

(2) For American interview participants:

- The CDC (Centers for Disease Control and Prevention) has a webpage dedicated to COVID-19, how individuals can cope with stress and who to call when help is needed (<https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/managing-stress-anxiety.html>).
- MHA (Mental Health America) has a webpage dedicated to COVID-19, providing information and resources (<https://mhanational.org/covid19>).

APPENDIX 5: EXAMPLES OF FACEBOOK ONLINE INVITATIONS



Facebook Online Invitation

Participants needed for a research on shopping in retail stores

We are looking for participants for an online research study. The study aims to better understand retail consumers' awareness of the presence and scope of surveillance in retail stores and its effect on them. You will be asked about your shopping experience in retail stores.

To be eligible, you must be:

- ✓ At least 18 years old
- ✓ Comfortable in the English language

The interview will be conducted online on ZOOM and should take approximately 60 minutes to complete. Your privacy will be protected.

Participants will be compensated with a **CAD 10 Interac e-transfer**.

If you are interested, please email Nada Elnahla @ nada.elnahla@carleton.ca for more details on participating.

This research has been cleared by Carleton University Research Ethics Board-A Clearance # 112372. Should you have any **ethical concerns** with the study, please contact the REB Chair, Carleton University Research Ethics Board-A (by phone: 613-520-2600 ext. 2517 or by email: ethics@carleton.ca). For all other questions about the study, please contact the researcher.



Facebook Online Invitation

Participants needed for a research on the effects of COVID-19 on retail workers

We are looking for participants for an online research study. The study aims to better understand the experience of retail workers during the COVID-19 epidemic.

To be eligible, you must be:

- ✓ At least 18 years old
- ✓ Comfortable in the English language
- ✓ Currently working in a retail store (part-time or full-time)

The interview will be conducted online on ZOOM and should take approximately 40-60 minutes to complete. Your privacy will be protected.

Participants will be compensated with a **CAD 10 Interac e-transfer**.

If you are interested, please email Nada Elnahla @ nada.elnahla@carleton.ca for more details on participating.

This research has been cleared by Carleton University Research Ethics Board-A Clearance # 112372. Should you have any **ethical concerns** with the study, please contact the REB Chair, Carleton University Research Ethics Board-A (by phone: 613-520-2600 ext. 2517 or by email: ethics@carleton.ca). For all other questions about the study, please contact the researcher.

APPENDIX 6: SHORT BIOGRAPHIES OF INTERVIEWEES**Retail consumers:**

- Michael is a Black American engineer in his late forties with an MBA and an annual income of US\$105,000.
- Jessica is a white, American stay-at-home mom in her late 30s with a high school diploma and household income of nearly US\$ 30,000.
- Jason is a white American male in his early 50s who has an associate degree and an annual income of US\$124,000, lives in Florida and whose wife works in Walmart.
- Mary is a single white American woman in her 60s who has a BA and an annual income of about US\$ 50,000, and who lives in the "gambling Mecca" Reno, Nevada.
- Maria is a single Argentinian American female in her early 40s who lives in Austin, Texas, who has a high school diploma, looks white and whose annual income is about US\$36,000.
- James is a retired, socialist, white American lawyer in his 70s who has two PhDs and whose current annual income is around US\$14,000.
- David is a white American male in his mid-40s from North Carolina with a high school degree. He works in IT and has an annual income of US\$35,000.
- Jennifer is a 50-year-old white American female and a mother of three. She has a BA and her family income is around US\$99,000.
- Aye is a 69-year-old retired Canadian Burman woman who has moved to Canada from Australia in 2012. She has a college degree and her annual income is CAD 35,000.
- Li Na is a 30-year-old Canadian university student of Chinese descent who lives with her family and whose average annual household income is CAD 13,000.

- Sarah is a single Canadian female consumer in her late twenties. She works as a legislative clerk in the Senate, has an MA and an annual income of \$63,000 before taxes.
- Myint is a young woman in her early thirties who runs a theater company. She is half-South-Asian (her father is a white Canadian and her mother is from Burma). She has a BA and her annual household income is CAD 125,000. Her husband is a data analyst who worked with some major loyalty programmes in Canada.

Retail consumers with retail work experience:

- Emily is a white female in her early thirties. With a BA and an annual income of US\$13,000, her latest job was working as a cashier in Target at Deptford, New Jersey until mid-March 2020.
- Zahra is a Canadian Iranian female in her early forties with a Master's degree and an annual household income of \$160,000. After immigrating to Canada, she worked in retail (in Winners and Hudson's Bay) for four years until April 2015. She lived briefly in Montreal before moving to Ottawa.
- Rahul is a 23-year-old Canadian male university student of Indian descent. In Summer 2019, he worked as a cashier in Shoppers.
- Ishita, a Canadian of Indian descent, is a female Carleton graduate in her early twenties with a BA and an average annual income of \$15,000. She lived in Mississauga before moving to Ottawa. She has retail experience; until 2017, she worked part-time for Dynamite and Lush Cosmetics, and after graduation, she started working full-time for Enterprise Rent a Car until she was let go early April 2020.

Retail workers:

- Ashley is a white American female in her early 40s with a high school degree and a US\$66,000 annual household income. She has a long experience working in retail, and for the past seven years, she has been working full-time in the bakery and as a cashier in Publix Super Markets in Deltona, Florida.
- Christopher is a thirty-eight, single American male who has a high school diploma and 20 years of retail experience. For the last 6 years, he has been working in Campus Outlet, an independently owned furniture store in Columbus, Ohio, doing all the sales and online interactions. Because of the pandemic, since March 2020, he has been working remotely from Florida. He has done one year of college and has an annual income of about US\$17,000.
- Matthew is a thirty-year old white American male with a college degree and a US\$25,000 annual income. For two years, and through "Advantage Solutions," he has been working in multiple retail stores (in Arkansas, Texas and Florida), promoting events and products. When the COVID-19 started, he was working in Walmart, Florida, then he moved to Walmart Arkansas.
- Robert is a tattooed American Canadian fourth-year law student at Carleton University who is forty years old and has an annual household income of \$ 40,000. After leaving the US marines, he moved to Canada where he has been working as a sales associate at Roots for the last three years, before which he worked in different places including Walmart for three years and the Carleton University Bookstore.

- Wang Fang is a 30-year-old female Chinese citizen who is a Permanent Resident in Canada since 2011. She has been working in Lowe's, the hardware store in Ottawa, since July 2019 as a recruiter, before that she worked for three years in their store in Saskatoon. In addition to working in an office, she spends most of her day walking around the store, helping with administration work, connecting with the manager and the other employees, working at the cashier, and helping the customers. She has a BSc and a personal annual gross income of CAD 6,000.
- Rachel is an MSc female student in her early twenties who is studying neuroscience at Carleton University. For the last two years, she has been working in Gap in Ottawa, between 15-40 hours a week; prior to that, she worked as a cashier in grocery stores and in the Carleton University Bookstore. She earns minimum wage.
- Taiba is a female Afghani-Canadian in her early twenties who has a high school degree and her annual household income is \$24,000. She immigrated to Canada more than eight years ago and her husband only joined her a few weeks before COVID-19 hit. Since 2015, she has worked with various retailers (including Hudson's Bay and Laura Secord) before going to Farm Boy full-time in January 2019. Before COVID, she was a chef in the hot buffet department but now, she has to be trained in every department.
- Joshua is a twenty-year old male who studies computer programming in Durham College in Oshawa, Ontario. Since early 2019, he has been working on and off as a part-timer at Pet Smart. After COVID-19 hit, and at the end of March 2020, he was let go from the Oshawa branch and he went back to working in the Ottawa branch at the end of August. He has an annual income of less than CAD 15,000.

- Janani is a thirty-five-year-old female Canadian Sri Lankan with a Master's degree. She has been working as a part-time sales associate at Home Sense for three years. She was temporarily laid off in March when the stores were shut down but only went back to work when schools reopened in early September because she did not want to send her kid to childcare during the pandemic.
- Olga is a 22-year-old political science female student at Carleton University with an annual household income of CAD 65,000. Originally from Kazakhstan, she has been a permanent resident in Canada since 2018. At the end of August 2020, and because of the COVID-19 pandemic, she was able to get a part-time job at Farm Boy where she sanitizes the shopping carts and counts how many people get in and out of the store.
- William is a sixty-five-year-old semi-retired male with a college degree and an average household income of CAD 75,000. In late 2019, he started working part-time in the deli department in one of the Independent grocery stores (which are independently owned and overseen by the parent company, Loblaw).
- Mitig is an aboriginal twenty-year-old male student at University of Ottawa who has an annual income of less than CAD 20,000. He works as a clerk in the meat department at Loblaw in downtown Ottawa (part-time in Winter and full-time in Summer).
- Amit is a 27-year-old Indian male who is an international student studying in Ottawa University and who works part-time in Walmart. He stopped working during March 2020 when the number of COVID-19 positive cases were significantly rising but had to go back to work in April to cover his expenses. His work is divided between unloading merchandise in the backroom and stocking the store shelves.

- Olivia is a twenty-year old female student at Carleton University with an annual household income of a little over CAD 200,000. She worked in Bulk Barn for over a year and left in February 2020 for what she believes is poor management, and in April, she moved to Shoppers Drug Mart where she is currently a supervisor. She mainly works part-time.
- Wang is a twenty-one-year-old college student of Chinese descent who has an annual household income of CAD 90,000. For two years and up till mid-October 2020, she worked as a part-time Sales Associate at Coach Outlet. Before that, she worked at Fossil, ALDO and Banana Republic.
- Paulo is a thirty-one-year-old Brazilian male who lives in Ottawa with his wife and has applied for his permanent residence. He has a post-graduate degree and an annual income of nearly CAD 60,000. He is a full-time front-end supervisor at a Value Village branch in Ottawa and his responsibilities include dealing with customers, supervising exchanges and authorizing price enquiries.
- Chan is a twenty- year-old male whose parents originally come from Hong Kong. He is a fourth-year student at Carleton University and his annual income is less than CAD 45,000. For two and a half years and until the end of September 2020, he worked as a part-time E-commerce Department Lead in Loblaw where he was responsible of picking up the grocery for online orders and loading them into customers' car trunks. In October 2020, he became a full-time Cash Manager at Shoppers.
- Stephanie is a 42-year-old female retail clerk at Costco. She has a high school diploma, an average household income of CAD 120,000, and four kids. She has been working at Costco for sixteen years and her shift is between 5:00 am to 1:30 pm. At the beginning of

the pandemic, she took two weeks off because of the chaos and the verbal and physical abuse she had to deal with at the workplace.

Retail managers:

- Emma is a thirty-four-year-old female who has a high school diploma and an annual income of CAD 60,000. She works as a store manager for a wireless provider in Ottawa, overseeing 5-10 workers.
- Megan is a 30-year-old Planning Manager in TJX Canada (representing Home Sense, Winners and Marshalls) who has been working remotely since March 2018.
- Hannah is a thirty-year old female with a BSc degree whose personal annual income is around CAD 60,000. Since July 2020, she has been working as an Assistant Buyer in menswear at Giant Tiger's Buying Office in Laval, Quebec, and her job includes checking out merchandise and having an open line of communication with store owners/managers and customers. Prior to that, she worked for nearly two years as an Assistant Account Manager for Product Services (APS) in the ALDO Group head office in Montreal but she was laid off in May due to the COVID pandemic.
- Gabrielle Hargrove is the Associate Vice President of Business Transformation, Giant Tiger Stores Limited. She oversees the process improvement, division change management, and strategic program management office. She is a 34-year-old Canadian of Asian origin who has a post-secondary degree and an annual household income of CAD 200,000.