



# The International Review of Retail, Distribution and Consumer Research

ISSN: (Print) (Online) Journal homepage: <https://www.tandfonline.com/loi/rirr20>

## Retailance: a conceptual framework and review of surveillance in retail

Nada Elnahla & Leighann C. Neilson

**To cite this article:** Nada Elnahla & Leighann C. Neilson (2021) Retailance: a conceptual framework and review of surveillance in retail, *The International Review of Retail, Distribution and Consumer Research*, 31:3, 330-357, DOI: [10.1080/09593969.2021.1873817](https://doi.org/10.1080/09593969.2021.1873817)

**To link to this article:** <https://doi.org/10.1080/09593969.2021.1873817>



Published online: 01 Feb 2021.



Submit your article to this journal [↗](#)



Article views: 750



View related articles [↗](#)



View Crossmark data [↗](#)



Citing articles: 1 View citing articles [↗](#)



# Retailance: a conceptual framework and review of surveillance in retail

Nada Elnahla  and Leighann C. Neilson 

Sprott School of Business, Carleton University, Ottawa, Canada.

## ABSTRACT

Retailance is surveillance in a brick-and-mortar retail setting. In today's world, brick-and-mortar retailers are threatened by competition from online retailers and the need to compete with sellers not just in the same city or country, but from all over the world. Retailers have, therefore, moved beyond the routine surveillance of consumers for security reasons, and begun to compete for consumers' personal and shopping data, in an effort to gain competitive advantage. Surprisingly, published academic research relevant to surveillance in a retail setting is quite limited. To address this apparent gap, this interdisciplinary literature review will first provide both a new definition and conceptual model of what surveillance in physical retail entails, before reviewing how retailers view retailance, how retailance impacts consumers and their relationships with retailers, along with associated moral and ethical dilemmas. Most importantly, we utilize our review as an opportunity to highlight 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 retailing and marketing by opening new and unexplored areas of study.

## ARTICLE HISTORY

Received 15 May 2020  
Accepted 6 January 2021

## KEYWORDS

Retailance; retail; retailing; surveillance; marketing; consumer behaviour; COVID-19 pandemic

## Introduction

Surveillance is not new. The roots of modern surveillance can be traced back to as early as the 15<sup>th</sup> century; the practice and concept can be found in ancient civilizations when records were kept for purposes of taxation, military service, immigration, and apportioning land. What is new about surveillance is the way it has become an intrinsic part of daily life. Surveillance is pursued by governments, organizations, businesses and even individuals, and its practices can be found in nearly all aspects of our lives, such as consumption, administrative recording, protection, monitoring, tracking, controlling, and management. While not determinative, technological developments, especially computerization, have been profoundly important in the rise of new forms of surveillance (Haggerty and Ericson 2006, 4), turning societies into 'information societies' (Fuchs 2014; Lyon 1998) and 'surveillance societies' where every day, normal life is closely monitored (Lyon 2001b, 1; 2008) Clarke III and Flaherty 2008).

When it comes to the world of physical retail, retailers have moved beyond the routine scrutiny of consumers for security reasons, to competing for consumers'

personal and shopping data, even if this information is not voluntarily reported. When consumers are inside the store, retailers can: collect their shopping and personal information; capture their images; record their conversations; track, and even deny, their merchandise returns; biometrically surveil their bodies (for example, their faces and fingerprints); and/or track their location inside, and maybe even outside, the store. Such surveillance raises ethical and moral questions regarding the differences between the public and the private spheres. For their part, retail consumers have their own expectations of what their shopping experience should be like. They want, and expect, better service, discounts, attractive and personalized offers, to use the store's Wi-Fi for free, collect more points on their loyalty cards, fast checkout lines, aisles that are not crowded, well-stocked shelves, and, of course, a safe and secure environment in which to shop.

As a first step towards understanding the impact and outcome of contemporary surveillance in retail on both consumers and retailers we conducted a substantial literature review. Structured around a conceptual model, this review will cover: a new definition of retail surveillance (i.e., 'retailance'); understanding retailers' four main reasons behind their use of surveillance (controlling loss and enhancing security, creating a pleasant and personalized shopping experience, enhancing profitability, and ensuring safety during the COVID-19 pandemic); a review of retailance systems and channels; consumers' awareness of retailance on individual, societal and governmental levels; the impact and outcome of retailance; and the ethical and moral dilemmas of retailance. According to Paul and Criado (2020), by using a narrative versus bibliometric style, this systematic review could be classified as a 'hybrid domain-based' review in which a framework is presented to provide directions for future research.

This systematic interdisciplinary review makes several contributions. First, it brings together scholarly and practitioner literature from the fields of marketing, consumer behaviour, sociology, political science, communications, media studies, and law in order to provide an integrated assessment of our current understanding and offer definitional clarity. Second, it provides a conceptual model to organize and highlight gaps in previous research. Next, it offers a categorization of surveillance systems based on their attributes that is flexible enough to incorporate new systems that may emerge and, finally, in addition to critiquing existing understandings, we offer suggestions for future research.

## Conceptual model

To lay the groundwork for our model (Figure 1), we synthesized readings from marketing, consumer behaviour, sociology, political science, communications, media studies, and law (more details in the following sections). The model's components then served as the structure for the review. In this model, retailance (manifested in surveillance channels and systems) directly influences the relationship between retailers (i.e., the surveiller) and consumers (i.e., the surveilled). Consumers' reaction to retail surveillance channels is influenced by their awareness of both 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 affect the retailers, creating a never-ending circle.

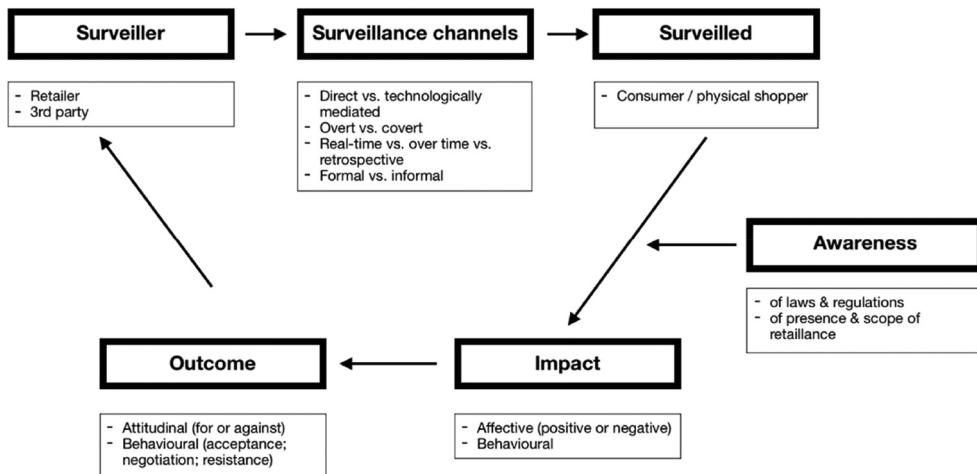


Figure 1. Retailance model.

## Research method

Despite the fact that surveillance is a hot topic nowadays, only twenty-five academic papers (published between 1993 and 2019) employing empirical research relevant to the field of retail have been published (one of them is more conceptual than empirical and another is a literature review). To retrieve these papers, 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. When fitted into the retailance model, this past research has been divided into three categories: from the surveillant/retailers' perspective (10 papers), from the surveilled/consumers' perspective (12 papers), conceptual research (1 paper), and literature review (1 paper). A chronological summary list of this research is provided in Table 1.

As a result of the availability of only a small number of academic business sources, our search to build a literature review was expanded to include sociological publications and practical sources, such as: reports issued by retail and surveillance businesses and associations, newspaper articles, magazine articles, law guides, forums, and websites (e.g., of market research and consulting firms, security firms, privacy groups, retail businesses, governments, etc.). Overall, the literature review highlights the following: first, scholarly marketing research related to the topic of retailance is very limited. Secondly, because of the rapidly changing nature of surveillance technology, there is a need for up-to-date research. Therefore, 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 new technology. Thirdly, published academic research based on an empirical model relevant to surveillance in a retail setting is surprisingly quite limited.

**Table 1.** A chronological summary of the 25 previous research studies.

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, and Martin (1994)	Retail	<i>International Journal of Retail &amp; 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 and 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, Stewart & Logan, (1995)	Retail	<i>International Journal of Retail &amp; Distribution Management</i>	Retailer	Empirical: survey	Scotland, U.K.	-	Surveying retail security methods employed by retailers
Lee, Hollinger & Danbey, (1999)	Criminology	<i>American Journal of Criminal Justice</i>	Retailer	Empirical: analysing data on crime incidents, private security measures & demographic measures	U.S.A.	-	Relationship between crime and private security at shopping centres
Smith & 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



Table 1. (Continued).

Paper	Discipline	Publication venue	Perspective	Research model	Research location	Theory employed	Research aim(s)
Hossain & 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 & US	–	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 and 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 &amp; 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 and Lindblom (2011)	Security	<i>Security Journal</i>	Retailer	Empirical: internet survey of retail entrepreneurs	Finland	CPTED	Retailers' approaches to preventing shoplifting
Lindblom and Kajalo (2011)	Retail	<i>International Review of Retail, Distribution &amp; 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 and 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 analysis of interviews	U.S.A.	Rational choice theory (RCT), situational crime prevention & CPTED	Identifying in-store situational (physical) cues for crime prevention planning

**Table 1. (Continued).**

Paper	Discipline	Publication venue	Perspective	Research model	Research location	Theory employed	Research aim(s)
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, and 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 and Lindblom (2016)	Retail	Facilities	Consumer	Empirical: survey of shopping mall visitors	Russia	-	The role of formal and informal surveillance in creating a safe & entertaining retail environment
Esmark, Noble, and Breazeale (2017)	Retail	Journal of Retailing	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, and Babcock (2017)	Security	Conference paper (Symposium on Usable Privacy & Security)	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, and Becker (2018)	Computing	Conference paper (Multikonferenz Wirtschaftsinformatik)	-	Literature review	-	-	Identifying digital capabilities of in-store technologies and relating them to the retailer's profit equation.



Table 1. (Continued).

Paper	Discipline	Publication venue	Perspective	Research model	Research location	Theory employed	Research aim(s)
Margulis, Boeck & Laroche, (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



## The definition of retailance

The origin of the word 'surveillance' is rooted in Latin – in which *vigilare* means 'to keep watch' and the prefix *sur* refers to 'below' (Marx 2016b, 46) – and the French verb *surveiller*, literally to 'watch over.' When it comes to the brick-and-mortar retail setting, the currently used definitions of surveillance (Dandeker 1990, p. 37; Grenville 2010, p. 81; Lyon 2007, pp. 13–14; Marx 2012, p. xxv, 2016, pp. 1–2) 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 that such data can be shared with third parties. Again, this definition is too broad for the physical retail sector.

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

Retailance, or surveillance in a brick-and-mortar retail setting, is the focused, systematic, and routine scrutiny of consumers, and 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 brings the following features of our review into focus: (1) a focus on consumption in a brick-and-mortar setting versus online consumption; (2) the routine, everyday nature of surveillance; (3) the Business to Consumer (B2C) rather than Business to Business (B2B) nature of the model; (4) that 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) the different reasons behind the collection of surveillance data; and (6) the existence of different retail surveillance systems.

## The surveiller: retailers' goals

To understand the role that retailers (i.e., surveiller) play in retailance, we should first understand what their goals are, how they align with or contradict the goals of consumers (i.e., the surveilled), and the outcome of such retailance in terms of how it affects consumers' attitudes and behaviour and the retailer-consumer relationship. 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, and Maris 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).

Amid a technological retail revolution, retailers have the potential to enhance both their operations and the experience they can provide their consumers (Grewal et al. 2020, 96). Thus to 21<sup>st</sup>-century merchants, retailance has become a strategic imperative (Turow, McGuigan, and Maris 2015). Physical stores now compete with sellers not just in the same city or country, but from all over the world. In addition, when shopping in a physical store, consumers can use their smart phones as a competitive weapon, browsing product ratings, price comparisons, comments and feedback on social media, as well as offers from competitors, becoming 'omnichannel shoppers' (Lazaris et al. 2014). Based on our review of academic sources, security/surveillance businesses' websites and reports, newspaper and magazine articles, and retailer guides, a more detailed discussion of why retailers employ retailance follows.

### ***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, and Shaw 2005). To combat retail misbehaviour, retail security is concerned with products, consumers and staff (the last is not covered by this review) (March Networks 2019). For example, packaging design (Coles and Kirwan 2011) – in addition to its aesthetic function – 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 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, abduction of small children) has 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 inside the stores, 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 and Hayes 2012, p. 23).

### ***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* (Retail Council of Canada 2018) 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* (Grewal et al. 2020) as much as finding products and the best prices (both of which could be attained online). Retailers have always leveraged on the 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 (interpersonal interactions in the form of customer-to-customer and customer-to-staff interactions) (Baker 1986). 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 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’ (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 (e.g., locking products in cabinets), 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, and Martin 1994, p. 24). Since shoplifting is the main cause of shrinkage (Cardone and 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, Hastings, and Martin 1994)), locking and security systems, personnel training, and technological systems. Bonfanti’s (2014) conceptual framework 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).

### ***To enhance profitability***

In retail environments, 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 et al. 2020). Shoppers’ behaviour, moreover, can be observed within different store and shelf layouts to provide 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 assistance, 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 touch-points, and PoS data) from the collected information help retailers set the foundation for the individualization and cost optimization capabilities (Betzing, Hoang, and Becker 2018, p. 1675).

### ***To ensure safety during the COVID-19 pandemic***

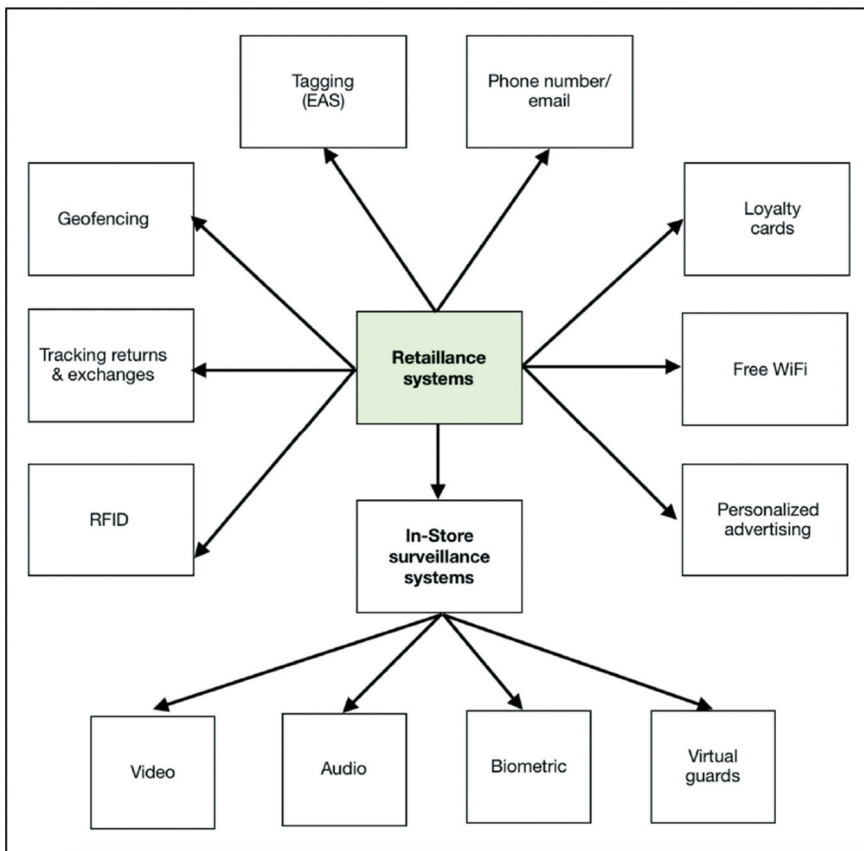
With the spread of the COVID-19 pandemic, the demand for retailance has increased, since retailers need to: secure their stores during temporary closures or reduced operating hours; ensure staff are in compliance with health and safety regulations to avoid government fines and reduce community transmission; 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 limits as part of their plan to safely reopen. 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 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). Another type of video/bio-surveillance, that is both covert and mediated in real-time, is thermal imaging camera systems that have the capability of detecting an elevated temperature in consumers or employees prior to entry (Ouellette 2020).

### **Retailance systems and channels**

In retail, different surveillance systems can be used (Figure 2), including: (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. Based on our reading of the literature, we group these systems into four different categories based on their attributes (Figure 3): direct vs. technologically mediated; overt vs. covert; real-time vs. over time vs. retrospective; and formal vs. informal.

#### ***Direct vs. technologically mediated***

Retailance can be conducted face-to-face (e.g., security guards and floor personnel) or through security systems (discussed in depth in the next section). Even though there is

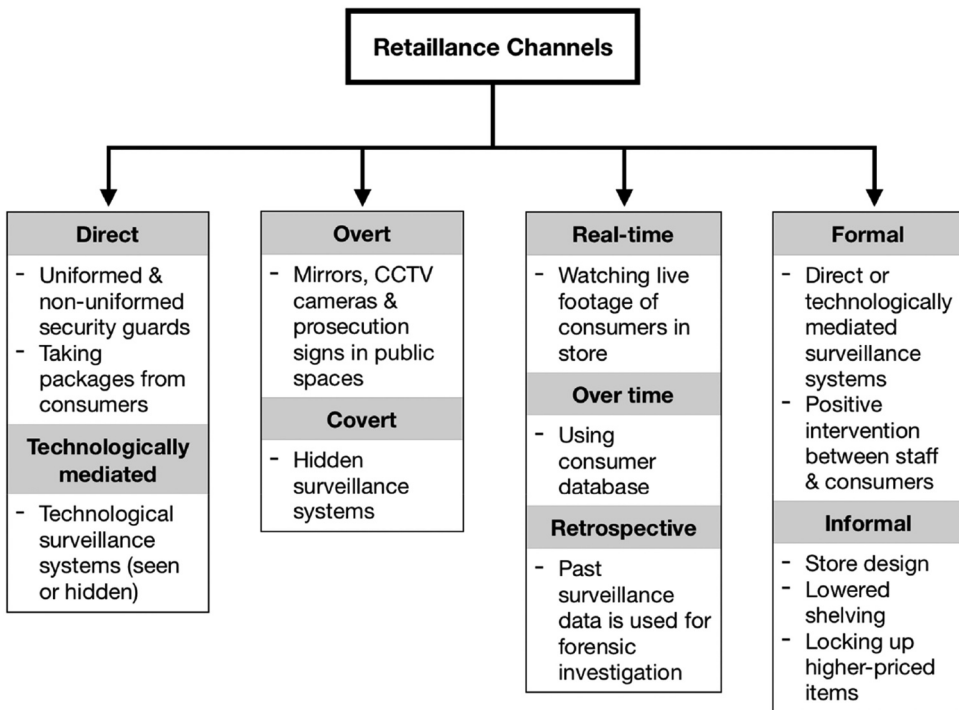


**Figure 2.** Retailance systems.

a human element behind all surveillance systems, we classify surveillance elements as '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, the tagging surveillance system is considered both direct and technologically 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).

### ***Overt vs. covert***

Installed retail surveillance can be overt or covert and it includes video, audio, biometric, and visual guards. 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,



**Figure 3.** Retailance channels.

and employees positioned within view (Kaitlyn 2018). On the other hand, some retailers opt to use concealed (i.e., covert) security applications, for example, 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).

### ***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 (Stores, 2019), retailers can now identify criminals more easily. Retailers can give high-resolution images of people who commit crimes in their stores to Rite Aid, a U.S. company that uses a criminal identification system known as 'Captis I-4' and on whose website (solvecrime.com) retailers can upload their photos and videos. Those photos/videos are then broadcast to a 50-mile radius around the area where the crime occurred, as well as to multiple surrounding cities, in effect crowdsourcing them. 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 (Schulz 2019).

### **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. 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 (Cardone and Hayes 2012, p. 29). For example, to enhance informal retail security, retailers can plan the arrangement of merchandise and employ protective design through lighting and mirrors (Phillips, Alexander, and Shaw 2005, 68).

Kajalo and Lindblom (2010) and Lindblom and Kajalo (2011) collected data from 161 grocery store retailers to create a comprehensive understanding of the ways in which retailers perceive the link between surveillance and customers' and employees' sense of security. Their study (2010, 2016) employs elements of Crime Prevention Through Environmental Design (CPTED); CPTED is a multi-disciplinary approach to crime prevention that offers a range of strategies to prevent crimes (e.g., access control, surveillance, territorial reinforcement, and maintenance of the facility), and asserts that the design and management of the physical environment can encourage or discourage opportunities for crimes (Kajalo and Lindblom 2010, p. 304). 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 (Lindblom and Kajalo 2011). In 2016, Kajalo and Lindblom used data gathered from a survey of 200 shopping mall visitors to reveal 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).

In an exploratory study to examine retail managers' attitudes towards shoplifting and identify how they deal with it, Lin, Hastings, and Martin (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); – can ward off shoplifters, they also make the shopping experience more unpleasant for honest customers.

While 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. 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, and Farrington 2009). 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.

To sum up, 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. A matrix that explains how these systems fall under the various retailance channels is provided in [Table 2](#).

## The surveilled: consumers' awareness

Consumer awareness of retailance is when the consumer knows of the presence of retailance (i.e., overt retailance) and when they are aware of the laws, policies and regulations governing retailance and their rights (note that this knowledge could be partial or complete). Consumer awareness, moreover, could be either individual (i.e., negative opinions about targeted ads) or societal (i.e., understanding the broader benefits and risks).

### Individual awareness

Direct surveillance (when an employee overtly watches consumers in real-time) can have negative outcomes, for example, leading to defensive merchandising. Defensive merchandising is when shoppers are simply too embarrassed to ask an employee for access to embarrassing products (e.g., condoms or foot fungal cream) and end up either abandoning their purchase (Redfeam 2006) or self-consciously shoplifting (Beck and 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

**Table 2.** A matrix of retailance channels and systems.

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



privacy, resulting in negative consequences for the retailer. Increasing options that allow a consumer to regain control will reduce the overall reactance to the threat to privacy and will improve retailer outcomes.

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). Targeted advertising is defined as 'the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests' (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 the 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?

### ***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 (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. 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.

Not only are consumers being watched, they sometimes voluntarily share their data. 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 and 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 (327–328).

### ***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 and Bies 2003). In the late 1990s, Canadians started to take seriously the privacy issues raised by the personal data-gathering activities of private corporations (Lyon 2003, 169). Currently, the Office of the Privacy Commissioner of Canada (OPC) 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.). Tabled in the Canadian Parliament on 17 November 2020, Bill C-11, the Digital Charter Implementation Act (DCIA), will include some significant new changes to Canada’s privacy framework (CMA 2020a, 2020b).

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). To varying degrees, privacy laws have been enacted in over eighty countries around the world (“What’s data privacy law in your country?,” 2019).

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 and Flaherty 2008; Taylor 2003), for example, there are currently 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).

### ***Impact and outcome: consumers’ perceptions of surveillance***

In today’s world, enhancements in the shopping experience come hand in hand with the technological advancement in surveillance. Many marketers justify their data-collection practices with the argument that there are trade-offs (Turow, Hennessy, and Draper 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 various statistical tests to analyse 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. According to the survey, 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 (76–78). Similar conclusions are stated in a 2009 report about Canadians and privacy (Ekos Research Associates, I 2009): the more transparent the rules are, the less concerned individuals are that their privacy will be violated. Another survey of American consumers (in general, and not just restricted to physical retail stores) found that they 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, and Draper 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, email 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 site visitors. The fact that such data was even collected and resold came as a surprise to many (Gruske 1999; Lyon 2001).

Marketers often claim that users give out information about themselves as a trade-off for benefits they receive (Romele et al. 2017). For example, 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. They argue, on the basis of a representative survey of 1,506 Americans aged 18 and older, that users are actually resigned 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;<sup>1</sup>

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, and Draper 2015)

The survey shows, moreover, that a large percentage of consumers 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) (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, and Draper 2015). Such a paradox only highlights the complicated nature of the relationship between consumers and retailance.

To sum up, consumers' reactions towards retailance differ, ranging from willing or resigned acceptance, to objection, to resistance (i.e., behavioural outcomes). 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, more benefits, and a better customer experience.

## **The ethical & moral dilemmas of retailance**

With the proliferation of retailance, ethical (governed by professional and legal guidelines) and moral (individual principles with respect to what is right or wrong) dilemmas 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, 276). One of the pressing questions when it comes to the darker side of surveillance is how surveillance should be conceived in ethical and/or moral terms.

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, 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***

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. Marx (2003) identifies eleven general strategies of surveillance resistance, all of which could be applied to retailance: (1) switching (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 (when a consumer's behaviour varies depending on whether or not surveillance is detected); (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 pseudonymous email addresses); (9) breaking (physically disabling retailance systems); (10) cooperation (resisting retailance by colluding with surveillants, i.e., employees working in retail security), 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).

Since 2012 (Mann 1997), Steve Mann 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, and 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).

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. Although some countersurveillance activities are intended to be social and to raise social awareness, he cautions against activists' individualized countersurveillance measures that may unintentionally reinforce the systems of social control, 'leaving the institutions, policies and cultural assumptions that support public surveillance relatively insulated from attack' (p. 517). Monahan also voices concerns about focusing on individual agents of surveillance (such as store clerks or security guards) which 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.

### **Future research suggestions**

In a world that is increasingly dependent on technology, employing surveillance in the brick-and-mortar retail sector has become an expected norm. Such dependency has implications for consumers in terms of how they can protect their privacy rights and their personal and shopping data, while, at the same time, ensuring that they have a good customer experience. 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. For public policy makers, a better understanding of the impact of surveillance on consumer behaviour and its ethical implications is but the first step towards updating and implementing legislation. In terms of future research, we suggest the following research programmes:

#### ***Exploratory qualitative research focusing on the consumer***

When retail surveillance has been empirically studied, researchers have 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 consumers' awareness of retailance, the impact of its presence, and their reaction to it, and how such knowledge could impact their relationship with the retailer. Given the holistic nature of the consumer shopping experience, it seems likely that an inclusive approach would more closely parallel the actual shopping environment and produce actionable insights. Moreover, we call for research that integrates both retailer and consumer perspectives in order to make recommendations about the effects of retailance on customer relationship management efforts. In only one of the studies conducted to date were consumers (shoplifting offenders) interviewed in person, despite the fact that such narratives have the potential to open the door to new venues of consumption studies. Exploratory qualitative research, sensitive to the ways in which consumers experience retailance, has the potential to guide

further academic research as well as provide a richer understanding of the shopping experience to inform practice.

### ***Micro-research employing theory***

Most of the published research reviewed in this paper lack a theoretical foundation. Only ten papers utilized theoretical frameworks, six of which were conducted by the same researchers (Kajalo and Lindblom). Although conceptual papers help researchers to theorize 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. The door is therefore wide open for researchers to investigate retailance using new theories in order to provide a more solid theoretical foundation to the study of retailance. In addition, it would be of interest to develop and validate scales that could help in measuring consumers' reactions towards the various retailance systems and channels.

### ***The impact of the COVID-19 pandemic on retailance***

We hope that this review paper stimulates future work on the impact of the COVID-19 pandemic on retailers' use of and consumers' reaction to retailance. Retailers are now 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. Privacy advocates argue that such marked changes in privacy norms could threaten individual rights even after the pandemic has passed (Klein and 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 regulation might potentially lead consumers to lean 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)

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 and Martin 2020, p. 2).

To summarize, the field of retailance offers many opportunities for researchers, for there is a real need for more detailed, up-to-date empirical surveillance research that

focuses on the brick-and-mortar retail environment. Our recommendations for future research encompass the more general, or macro, suggestions of exploratory qualitative research and the more micro level which focuses on the use of and reaction to specific retailance channels and systems. We also recommend studying the ongoing impact of the COVID-19 pandemic on retailers' use of and consumers' reactions to retailance and what that means to the notion of privacy.

## Concluding remarks

Science advances by building on prior knowledge, consequently, review studies play a major role, not only by reconciling and synthesizing past findings (Marabelli and Newell 2014; Paul and Criado 2020), but by providing new conceptual frameworks that can offer specific guidance for future research which can 'extend past research in ways that help the field advance systematically in its knowledge' (Hulland and Houston 2020, p. 351). In the brick-and-mortar retail world, in-store technology has been a game changer, yet its impact surpasses enhancing the shopping experience and influencing sales. The central goal of this systematic review, therefore, is to provide a review of past research applicable to studying the impact of retailance (i.e., surveillance in a brick-and-mortar retail stores). Providing definitional clarity and using a framework that emphasizes six components (i.e., surveiller/retailer, surveillance channels, surveilled/consumer, awareness, impact and outcome), we have centred our discussion on how retailers view retailance, how retailance impacts consumers, and the impact of such retailance. Importantly, we identify opportunities for new research efforts that can contribute to the vitality of the fields of retailing and marketing by opening new and unexplored areas of study.

## Notes

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

## Disclosure statement

No potential conflict of interest was reported by the authors.

## Notes on contributor

*Nada Elnahla* has a Ph.D. in Comparative Literature and is presently a Ph.D. candidate at Sprott School of Business, Carleton University. Her current research interests include retail surveillance, the impact of the COVID-19 pandemic on retail, disposal, narratology, consumer behaviour, and marketing history.

*Leighann C. Neilson* is Associate Professor of Marketing at the Sprott School of Business, Carleton University. Her current research interests include marketing history, consumer culture theory and marketing in arts and culture organizations.

## ORCID

Nada Elnahla  <http://orcid.org/0000-0002-2721-3570>



Leighann C. Neilson  <http://orcid.org/0000-0001-9947-9899>

## References

- Baker, J. 1986. "The Role of the Environment in Marketing Services: The Consumer Perspective." In *The Services Challenge: Integrating for Competitive Advantage*, ed. J. A. Czepiel, C. A. Congram, and J. Shanahan, 79–84. Chicago: American Marketing Association Proceedings Series.
- Barnes, S. B. 2006. "A Privacy Paradox : Social Networking in the United States | Barnes." *First Monday* 11 (9). doi:10.5210/fm.v11i9.1394
- Beck, A., and W. Palmer. 2009. "Understanding Shrinkage." In *New Loss Prevention: Redefining Shrinkage Management*, edited by Adrian Beck and Walter Palmer, 60–83. UK: Palgrave Macmillan.
- Betzing, J. H., A. Q. M. Hoang, and J. Becker. 2018. "In-store Technologies in the Retail Servicescape." In *MKWI 2018 - Multikonferenz Wirtschaftsinformatik*, 1671–1682. Luneburg, Germany. March 2018. [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwierPG5iZfuAhXFZs0KHmKDiUQFjAAe-gQIBBAC&url=https%3A%2F%2Fmkiwi2018.leuphana.de%2Fwp-content%2Fuploads%2FMKWI\\_3.pdf&usg=AOvVaw0h1z\\_Txw2sLYtK-a6lr7i](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwierPG5iZfuAhXFZs0KHmKDiUQFjAAe-gQIBBAC&url=https%3A%2F%2Fmkiwi2018.leuphana.de%2Fwp-content%2Fuploads%2FMKWI_3.pdf&usg=AOvVaw0h1z_Txw2sLYtK-a6lr7i).
- Bonfanti, A. 2014. "A Dilemma for Retailers: How to Make Store Surveillance Secure and Appealing to Shoppers." In *Handbook of Research on Retailer–Consumer Relationship Development*, ed. F. Musso and E. Druica, 297–317. Hershey, PA: Business Science Reference (an imprint of IGI Global).
- Brough, A. R., and K. D. Martin. 2020. "Consumer Privacy during (And After) the COVID-19 Pandemic." *Journal of Public Policy and Marketing* 1–3. doi:10.1177/0743915620929999.
- Cardone, C., and R. Hayes. 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. doi:10.1080/19361610.2012.631178.
- Clarke III, I., and T. B. Flaherty. 2008. "RFID and Consumer Privacy." *Journal of Internet Commerce* 7 (4): 513–527. doi:10.1080/15332860802507370.
- Clarke, R. A. 1988. "Information Technology and Dataveillance." *Communications of the ACM* 31 (5): 498–518. doi:10.1145/42411.42413.
- CMA. (2020a, May 20). "Privacy Legislation Comparison Chart: PIPEDA, CASL, GDPR and CCPA." Retrieved 20 November 2020, from <https://www.the-cma.org/regulatory/resource-links>
- CMA. (2020b, November 17). "Canada Introduces New Privacy Legislation." Here is what marketers need to know. Retrieved 20 November 2020, from <https://www.the-cma.org/about/blog/canada-introduces-new-privacy-legislation>
- Coles, R., and M. J. Kirwan, Eds.. 2011. *Food and Beverage Packaging Technology*. 2nd ed. ed. Ames, Iowa: Wiley-Blackwell.
- Culnan, M. J., and R. J. Bies. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations." *Journal of Social Issues* 59 (2): 323–342. doi:10.1111/1540-4560.00067.
- Dandeker, C. 1990. *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*. Padstow, Cornwall: Polity Press.
- Dawson, S. 1993. "Consumer Responses to Electronic Article Surveillance Alarms." *Journal of Retailing* 69 (3): 353–62. doi:10.1016/0022-4359(93)90011-7
- Ekos Research Associates, I. 2009. *Canadians and Privacy: Final Report*. Ottawa, ON.
- Esmark, C. L., S. M. Noble, and M. J. Breazeale. 2017. "I'll Be Watching You: Shoppers' Reactions to Perceptions of Being Watched by Employees." *Journal of Retailing* 93 (3): 336–349. doi:10.1016/j.jretai.2017.04.005.
- Farrington, D., S. Bowen, A. Buckle, T. Burns-Howell, and John B. 1993. "An Experiment on the Prevention of Shoplifting." *Crime Prevention Studies* 1: 93–119.
- Ferracuti, N., C. Norscini, E. Frontoni, P. Gabellini, M. Paolanti, and V. Placidi. 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. doi:10.1016/j.jretconser.2018.11.005.

- Fuchs, C. 2014. "Capitalism or Information Society?" In *Digital Labour and Karl Marx*, edited by Christian Fuchs, 135–152. New York, NY: Routledge.
- Gotlieb, C. C. 1996. "Privacy: A Concept Whose Time Has Come and Gone." In *Computers, Surveillance, and Privacy*, ed. D. Lyon and E. Zureik, 156–171. Minneapolis: University of Minnesota Press.
- Grenville, A. 2010. "Shunning Surveillance or Welcoming the Watcher? Exploring How People Traverse the Path of Resistance." In *Surveillance, Privacy, and the Globalization of Personal Information*, ed. E. Zureik, L. L. H. Stalker, E. Smith, D. Lyon, and Y. E. Chan, 70–83. Montreal, Ithaca: McGill-Queen's University Press.
- Grewal, D, S M. Noble, A L. Roggeveen, and J. Nordfalt. 2020. "The Future of In-Store Technology." *Journal of the Academy of Marketing Science* 48: 96–113. doi:10.1007/s11747-019-00697-z
- Gruske, C. (1999, February 11). "On-line Air Miles Files Left Accessible." Retrieved 8 July 2018, from <https://www.itworldcanada.com/article/on-line-air-miles-files-left-accessible/35719>
- Haggerty, K. D., and R. V. Ericson. 2006. "The New Politics of Surveillance and Visibility." In *The New Politics of Surveillance and Visibility*, ed. K. D. Haggerty and R. V. Ericson, 3–25. Toronto: University of Toronto Press.
- Handford, M. 1994. "Electronic Tagging in Action: A Case Study in Retailing." In *Crime at Work: Vol. 1: Studies in Security and Crime Prevention*, edited by Martin Gill, 173–85. Perpetuity Press Ltd
- Hossain, Muhammad Muazzem, and Victor R. Prybutok. 2008. "Consumer Acceptance of RFID Technology: An Exploratory Study." *IEEE Transactions on Engineering Management* 55 (2): 316–28
- Huey, L. 2009. "Subverting Surveillance Systems: Access to Information Mechanisms as Tools of Counter-surveillance." In *Surveillnace: Power, Problems, and Politics*, ed. S. P. Hier and J. Greenberg, 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 (2): 89–101. doi:10.1007/s10676-015-9363-z.
- Hulland, J., and M. B. Houston. 2020. "Why Systematic Review Papers and Meta-analyses Matter: An Introduction to the Special Issue on Generalizations in Marketing." *Journal of the Academy of Marketing Science* 48 (3): 351–359. doi:10.1007/s11747-020-00721-7.
- Kaitlyn, T. (2018). "Wouldn't It Be Better if Self-checkout Just Died?" Retrieved 19 July 2019, from <https://www.vox.com/the-goods/2018/10/2/17923050/self-checkout-amazon-walmart-automation-jobs-surveillance>
- Kajalo, S., and A. Lindblom. 2010. "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 (4): 300–305. doi:10.1016/j.jretconser.2010.03.001.
- Kajalo, S., and A. Lindblom. 2011. "An Empirical Analysis of Retail Entrepreneurs' Approaches to Prevent Shoplifting." *Security Journal* 24 (4): 269–282. doi:10.1057/sj.2010.3.
- Kajalo, S., and A. Lindblom. 2016. "The Role of Formal and Informal Surveillance in Creating a Safe and Entertaining Retail Environment." *Facilities* 34 (3/4): 219–232. doi:10.1108/F-06-2014-0055.
- Kerr, I., and J. Barrigar. 2012. "Privacy, Identity and Anonymity." In *Routledge Handbook of Surveillance Studies*, ed. K. Ball, K. Haggerty, and D. Lyon, 386–394. Oxon: Routledge.
- Klein, A., and E. Felten (2020, April 4). "The 9/11 Playbook for Protecting Privacy." Retrieved 22 July 2020, from <https://www.politico.com/news/agenda/2020/04/04/9-11-playbook-coronavirus-privacy-164510>
- Lace, S. 2005. "The New Personal Information Agenda." In *The Glass Consumer: Life in a Surveillance Society*, ed. S. Lace, 207–246. Bristol: Policy Press/National Consumer Council.
- Lazaris, C., A. Vrechopoulous, K. Fraidaki, and G. Doukidis (2014). "Exploring the "Omnichannel" Shopper Behaviour." In *AMA SERVICES 2014, International Service Research Conference*. Thessaloniki, Greece. doi:10.13140/2.1.1278.2089.
- Lee, G, R. C. Hollinger, and D A. Dabney. 1999. "The Relationship between Crime and Private Security at US Shopping Centers." *American Journal of Criminal Justice* 23 (2): 157–77. <https://doi.org/10.1007/bf02887270>

- Lin, B., D. A. Hastings, and C. Martin. 1994. "Shoplifting in Retail Clothing Outlets: An Exploratory Research." *International Journal of Retail & Distribution Management* 22 (7): 24–29. doi:10.1108/09590559410069909.
- Lindblom, A., and S. Kajalo. 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. doi:10.1080/09593969.2011.562677.
- Lyon, D. 1998. *The Information Society: Issues and Illusions*. Malden, MA: Polity Press.
- Lyon, D. 2001. *Surveillance Society*. Buckingham: Open University Press.
- Lyon, D. 2003. "Surveillance Technology and Surveillance Society." In *Modernity and Technology*, ed. T. J. Misa, P. Brey, and A. Feenberg, 161–184. Cambridge: Massachusetts Institute of Technology.
- Lyon, D. 2007. *Surveillance Studies: An Overview*. Cambridge, UK: Polity Press.
- Lyon, D. 2008. "Surveillance Society." In *Talk for Festival Del Diritto, Piacenza, Italia*. September 28, 2008. [http://www.festivaldeldiritto.it/2008/pdf/interventi/david\\_lyon.pdf](http://www.festivaldeldiritto.it/2008/pdf/interventi/david_lyon.pdf).
- Macdonnell, B. (2020, August 3). "Contact Tracing Information at Ontario Bars, Restaurants Raises Privacy Concerns." *CTV News*.
- Mann, S. 1997. "Smart Clothing : The Wearable Computer and wearCam." *Personal Technologies* 1 (1): 21–27. doi:10.1007/BF01317885.
- 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. doi:10.1145/1027527.1027673.
- Mann, S. 2009. *ShootingBack (Trailer)*. YouTube. <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., J. Nolan, and B. Wellman. 2003. "Sousveillance : Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments." *Surveillance & Society* 1 (3): 331–355. doi:10.24908/ss.v1i3.3344.
- Marabelli, M., and S. Newell. 2014. "Knowing, Power and Materiality: A Critical Review and Reconceptualization of Absorptive Capacity." *International Journal of Management Reviews* 16 (4): 479–499. doi:10.1111/ijmr.12031.
- Margulis, A, H. Boeck, and M. Laroche. 2019. "Connecting with Consumers Using Ubiquitous Technology: A New Model to Forecast Consumer Reaction." *Journal of Business Research* 121: 448–60. doi:10.1016/j.jbusres.2019.04.019
- Marx, G. T. 2003. "A Tack in the Shoe : Neutralizing and Resisting the New Surveillance." *Journal of Social Issues* 59 (2): 369–390. doi:10.1111/1540-4560.00069.
- Marx, G. T. 2012. "Preface: 'Your Papers Please': Personal and Professional Encounters with Surveillance." In *Routledge Handbook of Surveillance Studies*, ed. K. Ball, K. Haggerty, and D. Lyon, xx–xxxi. Oxon: Routledge.
- Marx, G. T. 2016. *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press.
- Moe, E. (2020, July 15). "Video Technologies Help Retailers Deliver a Safe In-store Shopping Experience in the Age of COVID-19." Retrieved 16 September 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. doi:10.1080/10350330601019769.
- Office of the Privacy Commissioner of Canada. (n.d.). Retrieved 23 July 2018, from <https://www.priv.gc.ca/en/for-individuals/>

- Ouellette, J. (2020, July 21). "How Thermal Imaging Cameras Will Help Facilities Reopen in a COVID-19 World." Retrieved 16 September 2020, from <https://www.securitymagazine.com/articles/92873-how-thermal-imaging-cameras-will-help-facilities-reopen-in-a-covid-19-world>
- Overstreet, J., and R. Clodfelter. 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.
- Pandolph, S. (2017, October 26). "Shoppers Expect More Personalization." *Business Insider*.
- Pantano, E., G. Pizzi, D. Scarpi, and C. Dennis. 2020. "Competing during a Pandemic? Retailers' Ups and Downs during the COVID-19 Outbreak." *Journal of Business Research* 116: 209–213. doi:10.1016/j.jbusres.2020.05.036.
- Paolanti, M., R. Pietrini, A. Mancini, E. Frontoni, and P. Zingaretti. 2020. "Deep Understanding of Shopper Behaviours and Interactions Using RGB-D Vision." *Machine Vision and Applications* 31 (66). doi:10.1007/s00138-020-01118-w.
- Paul, J., and A. R. Criado. 2020. "The Art of Writing Literature Review: What Do We Know and What Do We Need to Know?" *International Business Review* 29 (4): 101717. doi:10.1016/j.ibusrev.2020.101717.
- Peek-Asa, Corinne, Carri Casteel, Jess F. Kraus, and Paul Whitten. 2006. "Employee and Customer Injury during Violent Crimes in Retail and Service Businesses." *American Journal of Public Health* 96 (10): 1867–72. doi:10.2105/AJPH.2005.071365
- Phillips, S., A. Alexander, and G. Shaw. 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. doi:10.1177/0276146705275715.
- Pretious, M, R. Stewart, and D. Logan. 1995. "Retail Security: A Survey of Methods and Management in Dundee." *International Journal of Retail & Distribution Management* 23 (9): 28–35. doi: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 *Surveillance, Privacy, and the Globalization of Personal Information*, ed. E. Zureik, L. L. H. Stalker, E. Smith, D. Lyon, and Y. E. Chan, 295–309. Montreal, Ithaca: McGill-Queen's University Press.
- Rainie, L., and M. Duggan. 2016. *Privacy and Information Sharing*. Pew Research Center: Internet and Technology.. <http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/>.
- Redfeam, S. (2006, April 11). "Prophylactic Measures." *Washington Post*.
- Retailer's Guide*. Vol. 1.1. 2018. BDO (Binder Dijker Otte) and RCC (Retail Council of Canada). 2018. [https://www.google.com/url?sa=t&rcct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwigjPj mudnoAhVFHc0KHZp2C2IQfJA-AegQIARAB&url=https%3A%2F%2Fwww.retailcouncil.org%2Fwp-content%2Fuploads%2F2018%2F09%2FBDO\\_Retailers\\_Guide\\_0.pdf&usg=AOvVaw3pzeJamFndMWvqcNFR82A](https://www.google.com/url?sa=t&rcct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwigjPj mudnoAhVFHc0KHZp2C2IQfJA-AegQIARAB&url=https%3A%2F%2Fwww.retailcouncil.org%2Fwp-content%2Fuploads%2F2018%2F09%2FBDO_Retailers_Guide_0.pdf&usg=AOvVaw3pzeJamFndMWvqcNFR82A).
- Rhee, J. (1999). "Mirroring Medusa : Counterveillance in ShootingBack." In *IEEE International Conference on Information Visualization (Cat. No. PR00210)* (pp. 1–5). London, UK: IEEE. doi:10.1109/IV.1999.781589.
- Romele, A., F. Gallino, C. Emmenegger, and D. Gorgone. 2017. "Panopticism Is Not Enough: Social Media as Technologies of Voluntary Servitude." *Surveillance & Society* 15 (2): 204–221. doi:10.24908/ss.v15i2.6021.
- Rosenbloom, S. (2010, March). "In Bid to Sway Sales, Cameras Track Shoppers." *The New York Times*.
- Samat, S., A. Acquisti, and L. Babcock (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.
- Schulz, D. 2019. "Captured on Camera: The Use of Body Cameras to Protect Retail Staff, Properties and the General Public." *Stores (NRF's Magazine)*, April 22, 2019.
- SDM. (2020, June 15). "Security & Safety Things Offers COVID-19 Video Analytics Solutions for Retailers." Retrieved 16 September 2020, from <https://www.sdmmag.com/articles/98159-security-safety-things-offers-covid-19-video-analytics-solutions-for-retailers>
- Shim, R. (2003, April 7). "Benetton Takes Stock of Chip Plan." Retrieved 12 July 2019, from <https://www.cnet.com/news/benetton-takes-stock-of-chip-plan/>

- Singer, N. (2016). "Why a Push for Online Privacy Is Boggled down in Washington." *New York Times*.
- Smith, A, and L. Sparks. 2003. "Making Tracks: Loyalty Cards as Consumer Surveillance." *European Advances in Consumer Research* 6: 368–73
- Surveillance system uses crowdsourcing to identify retail criminals. (2019, June 11). "Stores (NRF's Magazine)."
- Taylor, H. 2003. *Most People are "Privacy Pragmatists" Who, while Concerned about Privacy, Will Sometimes Trade It off for Other Benefits*. Harris Poll. (The Harris Poll). ISSN 0895-7983.
- 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 (2): 705–713. doi:10.1016/j.chb.2010.08.014.
- Turow, J., L. McGuigan, and E. R. Maris. 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. doi:10.1177/1367549415577390.
- Turow, J., M. Hennessy, and N. Draper. 2015. *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them up to Exploitation*. Annenberg School for Communication, University of Pennsylvania. 2015. [https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy\\_1.pdf](https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf).
- Welsh, B. C., M. E. Mudge, and D. P. Farrington. 2009. "Reconceptualizing Public Area Surveillance and Crime Prevention: Security Guards, Place Managers and Defensible Space." *Security Journal* 23 (4): 299–319. doi:10.1057/sj.2008.22.
- What's data privacy law in your country? (2019, September 4). Retrieved 2 April 2020, from <https://www.privacypolicies.com/blog/privacy-law-by-country/>
- 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. doi:10.1177/1095796018819461.