From the Panopticon to Amazon Go: An Overview of Surveillance in Retailing

Nada Elnahla

Sprott School of Business,
Carleton University, Ottawa, Canada

Purpose - This overview attempts to build a broader understanding of the history of surveillance and its integration in the field of retailing in order to gain a better understanding of the impact of smart retail technologies on consumer behaviour.

Design/methodology/approach - This paper is a review of secondary information from food retail and surveillance literature, popular new media, dystopian literature, and academic publications. The methodology conforms to a historical review of the development of a process.

Findings - The paper traces the evolution of surveillance systems and theory in general, highlighting it in the retail sector, and ultimately, defining what retail surveillance is.

Research limitation/implications - A more in-depth examination (through a mixed-methodology approach) of the consumer in a retail setting is needed.

Originality/value of the paper - Surveillance studies are varied, fragmented, and scholars often disagree. Consequently, this paper attempts to provide a clearer picture of surveillance methods and theory by reviewing the history of surveillance literature and theory, and ultimately focusing on the retail sector and the impact of the use of surveillance on both the retailer and the consumer. A tentative definition of retail surveillance is also developed. Foreseen contributions encompass helping scholars, retail managers, and policy makers gain a better understanding of the impact of smart retail technologies on consumer behaviour.

Keywords - Surveillance; Retailing; Surveillance theory; Panoptic, Amazon Go

Classification - General review

Introduction

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)

Although the roots of modern surveillance could be traced as early as the 15th century (see the next section on the Emergence of Surveillance Studies), the practice and concept could be found in ancient civilizations where records were kept for purposes such as taxation, military service, immigration, and apportioning land, among others (Lyon 1994, pp.22–24). 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,’ Lyon defines 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)

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)

In the Routledge Handbook of Surveillance Studies, on the other hand, 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 the preindustrial societies, which tended to stay local and compartmentalized, and the centralized “surveillance” that emerged with the industrial society and the bureaucratic record keeping (e.g., a police officer trailing a suspect). Marx then goes to identify both the “surveillance agent” (i.e. the watcher/observer/seeker/inspector/auditor/tester) who can be a sponsor, data collector, or secondary/initial 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 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, have become more comprehensive, intensive, and extensive, and its emphasis has expanded beyond the individual to systems and networks (p. 57). This has led us to head towards a “maximum security society” in which surveillance is ubiquitous and its traditional borders that formerly protected personal information were weakened or obliterated by new technologies (p. 2). Marx, moreover, 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 (2016b, pp.66–69).

In today’s world, surveillance has become an intrinsic part of daily life. The dependency on communication and information technologies for administrative and control processes have turned societies into “information societies” (Lyon 1998) and “surveillance societies” where everyday, normal life is closely monitored (Lyon 2001, p.1; Lyon 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 2006a)). Agencies, organizations and governments pursue our detailed personal information; 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 the 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 highways. 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, highlighting their authoritarian control, and ultimately, reviving the talk of “Big Brother.” A pre-emptive approach in security and policing is Big Data surveillance, whose related trends include control, faith in technology, public-private synergies, and user involvement. 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 US proposed new rules governing bulk data collection by the NSA of the phone calling habits of Americans (Lyon 2014; Bauman et al. 2014).

Biometric surveillance (a form of biosurveillance) is increasingly found in different sectors, such as: retails loss prevention, transportation security, law enforcement, 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 2001, pp.77–81; Nelkin & Andrews 2003). 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. Prevention/protection surveillance is used in public health sectors, for example, the Centres for Disease Control and the World Health Organization use surveillance to avoid or contain epidemics and contagious diseases by monitoring individuals and environmental conditions, 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).

Retailers, on the other hand, 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; radio frequency identification (RFID) tags that has revolutionized the efficiency, effectiveness, and security of the supply chain and inventory management (Jones et al. 2004); and floor personnel and shop detectives (Bonfanti 2014, p.302). Marx names such scrutiny of outsiders/customers the “external constituency surveillance” (2012, p. xxv). In order to profile and track current and potential customers, database marketing has grown to become a multi-billion-dollar industry that collects personal data on consumers’ spending habits, preferences, and lifestyles (Lyon, 2003, p. 162). Dataveillance is now used to make individuals’ data become visible to organizations through data-mining. In conclusion, 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, generating a new dimension of virtual geography (Crang et al. 1999).
Due to space limit and the vastness of the field of surveillance studies, providing a comprehensive history of surveillance in general is beyond this research. Consequently, this paper seeks to explore the use of surveillance in the retailing sector, and its effect on the consumers, both positively and negatively. The rest of the paper is organized as follows: Section 2 provides a brief literature overview of the relation between consumerism and surveillance, the different surveillance systems employed in the retail sector, the customers’ perception of surveillance, the shoppers’ perceptions of surveillance, and the debate regarding the question of ethics. Section 3 follows the emergence of surveillance studies, starting from the 15th century and until today. Finally, Section 4 presents the conclusion and expected contributions.

**Literature Background**

*Consumerism and surveillance*

Consumption is considered a sphere of surveillance, for “the key traits are visible, and in the consumer sphere a particular pattern of growth is evident” (Lyon 2007, p.2). Consumer surveillance is, therefore, a technological enhanced development of capitalist management (Lyon 2001, p.43). It is noteworthy that consumer surveillance has surpassed Orwell’s (1989) dystopian vision of the nation state’s possession of the power of surveillance and control. However, although much consumer surveillance practices may resonate with Taylorist or panoptic methods, the leading principle of the consumer order is pleasure, not pain or coercion (Lyon 1994, pp.155–157).

Some techniques of market research, such as political polls and crude market surveys, could be traced back to the mid-19th century in the U.S. (Lockley 1950). One of the landmarks in early market research was in the 1920s when Alfred Sloan, who worked for General Motors, used scientific management principles for commodity markets and consumer behaviour. By the 1930s, and with the help of International Business Machines Inc. (IBM), demographic and socio-economic data on buying habits were collated to build profiles on consumers and manage their activities. Such “social Taylorism” was viewed as a subtle form of social control. 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 zipcodes 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 database marketing could be considered the first phase of computer-assisted consumer surveillance. The second phase 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 trails of customer interests (Lyon 2001, 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 et al. 2015). Thus, obtaining information on the consumer from his/her current and past purchase history has become an important aspect of marketing practice that has a tremendous potential for improving profitability (Rossi et al. 1996; Scranton et al. 2012).

In his classic The Panoptic Sort (1993), 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 certain potential consumers (i.e. what marketers call marketing strategy, consisting of segmentation, targeting, and positioning). 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 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 target cellphone users (Lyon et al. 2005). Throughout the development of those three phases, the practice of customer relationship management (CRM) has grown; corporations now manage the flow of data between service representatives and marketing department in order to offer differential treatment to different kinds of customers, those whose history demonstrates greater or lesser profitability for the company (Lyon 2007, pp.40–44).

**Surveillance in retailing**

In the U.S., retailers experience an average shrink rate of 1.44%, which costed the economy $48.9 billion in 2016, furthermore, about one-fourth of retailers have inventory shrinkage rates of 2% or more and the average cost per shoplifting incident has doubled to $798.48 (Anon 2017b). One in eleven people in the U.S. is a shoplifter, and more than 10 million people have been apprehended for shoplifting over the past five years (Shoplifting Statistics). In total, organized Retail Crime (ORC) costs the retail industry approximately $30 billion each year, in addition to losses incurred by shoplifting (Anon 2017a). To combat that threat, many retail stores install surveillance systems which are designed to help in identifying incidents of retail crime, such as shoplifting, robberies and violence.

Retail surveillance could be overt or covert. On the one hand, some retailers prefer not to hide cameras, mounting them visibly in public spaces, 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. 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.

Surveillance methods employed in the retail sector include: (1) closed circuit television (CCTV); (2) internet protocol (IP); (3) audio analytics; (4) biometric surveillance with facial recognition algorithm; (5) virtual guards; (6) electronic article surveillance (EAS), also known as tagging; (7) collecting customers’ phone numbers and emails; (8) customer loyalty cards that enable the tracking of purchases, that are replacing discount punch or stamp cards and proprietary currency; (9) tracking technology of free Wi-Fi and Bluetooth services; (10) personalized advertising; (11) return rewards; (12) radio frequency identification (RFID) that provides retailers with tighter control and management of the supply chain and of inventory management; and (13) geofencing. In Geofencing, retailers use Wi-Fi and/or bluetooth to automatically be alerted to the customer’s presence when s/he approaches, enters, and browses the store. One of the retailers on the cutting edge of this technology is Target, who provides their customers with offers once they use Target’s app, Cartwheel, installed on the smartphone. On January 22, 2018, Amazon Go opened its first pilot store to the public (Fig. 2). A prototype grocery store operated by the online retailer Amazon, Amazon Go has four locations in Seattle, Washington, three in Chicago, Illinois, and two in San Francisco, California as of January 2019; it is partially-automated, with customers able to purchase products without using a cashier or checkout station. The store concept is seen as a revolutionary model that relies on the prevalence of smartphones and geofencing technology to streamline the customer experience, as well as supply chain and inventory management. However, 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 the increased surveillance in the store, some worry about eliminating interpersonal connections and what it means for the future of city life.

Fig. 2 – Amazon Go app in the App Store

Smart retail technologies have the potential to improve the customer retail experience by providing a new, mobile-enabled, real-time, superior, and personalized retail services. Research findings indicate that smart customer experience directly enhances satisfaction and reduced 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 et al. 2017). Nevertheless, such practices, whilst giving targeted users access to discounts and services directly customised to their consumption patterns, 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 obligate supermarkets to prevent certain customers purchasing a product (for example, customers with tendencies to obesity buying doughnuts) when accessed profiles combine medical with purchasing data (Lace 2005, p.208).

**Customers’ perception of surveillance**

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 trialability, and deliver unique benefits to consumers (Tamilia & Reid 2007; Tamilia 2011). Nowadays, retailers’ investments in store design, staff training, and technological systems can ensure adequate security levels without compromising customers’ 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 Experience (CSE)—while ensuring a high level of sales environment surveillance without interfering with the shopping experience (Bonfanti 2014). Despite the fact that open merchandising 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, and economic losses (Bonfanti 2014, p.298). Since shoplifting is the main cause of shrinkage, retailers have to monitor the shoplifters’ intentions 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 (p. 298). To create an attractive shopping experience that is capable of meeting the customers’ latent sensorial, emotional, and psychological expectations, retailers have to employ surveillance solutions that are both secure and appealing to shoppers, for example: store design, locking and security systems, personnel training, and technological systems.

Retailers can also leverage 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). Packaging design (Coles & Kirwan 2011), in addition to its aesthetic, also 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 tags, it becomes a means of retail loss prevention.

In today’s world, technological advancements have a direct effect on consumer expectations. Consumers now expect products to be almost instantaneously available and their shopping experience to be seamless, as they oscillate between online and offline channels during the purchase journey. However, such technological advancements in the shopping experience come hand in hand with the advancement in surveillance, to which consumers react differently.

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 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 his or her personal information (p. 73). According to the survey, both who are well informed (i.e. informed resisters) and who were ignorant of surveillance knowledge (i.e. alienated skeptics) are the most fearful of surveillance. On the other hand, those who 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).

In the field of retailing, some consumers might argue that surveillance should be preventive, dissuasive, and educational rather than punitive in nature, thus, the purpose of any security system should be to dissuade people from stealing rather than to catch and punish them. Kajalo and Lindblom (2010, 2016) use the crime prevention through environmental design (CPTED) theory to study how consumers view various formal and informal surveillance practices in the context of shopping malls. They employ the CPTED approach that divides surveillance into “formal” (e.g. CCTV and motion detectors) and “informal” (which maximizes visibility and fosters positive social interaction) (Fig. 3).

Fig. 3 – Formal and informal surveillance: Definitions and practical implications at the store level (Kajalo & Lindblom, 2011)

<table>
<thead>
<tr>
<th>Form of surveillance</th>
<th>Definition</th>
<th>Practical implications at the store level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal surveillance</td>
<td>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</td>
<td>Arranged proper security training for sales staff Hire private security guards Invest in security hardware (e.g. CCTV surveillance systems)</td>
</tr>
<tr>
<td>Informal surveillance</td>
<td>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</td>
<td>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</td>
</tr>
</tbody>
</table>

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 (Lin et al. 1994). 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 et al. 2009). Based on their view regarding formal and informal surveillance practices, consumers can be grouped into different clusters, each indicating the basis of 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 (Kajalo & Lindblom 2016).

According to Bonfanti (2014), in-store security systems can be either positively or negatively perceived by consumers depending on how it emotionally affects their 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, shopping habits and basic demographics 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
The question of ethics

Surveillance always has 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 face of surveillance is how surveillance should be conceived in ethical terms. In the late 1990s, Canadians (outside Quebec) 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,"). 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 May 2013, and after the American department store Nordstrom put up a sign announcing that they had been piloting the technology of tracking the 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 directly to their store but also on social media (Clifford & Hardy 2013; Datoo 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 upon on one of the mall’s directories, exposing facial-recognition software that was running in the background of the digital map. The mall’s parent company, Cadillac Fairview, 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 video 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 sued for other purposes, hence, negative privacy implications (Rieger 2018; Heydari 2018).

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.” (Datoo 2014). However, since data protections law(s) is usually challenged when attempting to control the desire of organizations to amass ever increasing levels of information, there is a marginal impact on surveillance societies (Lace 2005, p.215). As a result, and in the face of the spread of surveillance, four kinds of approaches have emerged: institutional regulation, everyday resistance, social movements, and human rights advocacy (Ball et al. 2012, p.363). Marx (2016b, pp.166–168) 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). 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 (Fig. 4). Since then, he has been lobbying for the Mann-Wassell 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 2004; Mann 1998; Mann 2012; Mann et al. 2003), a “counter-surveillance,” 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). 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 (Fig. 5).
Fig. 4 – 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/

Fig. 5 – The eight veillances as discussed by Steve Mann (2012)

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.” This creates a need for greater awareness (among governments, business, 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.

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)

Consumers, therefore, need mutually beneficial exchanges built on informed consent. The 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.

**Surveillance Studies**

“Man is born free, and he is everywhere in chains.”

(Jean-Jacques Rousseau’s *The Social Contract*, 1762)

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. At the turn of the 21st century, routine and systematic surveillance practices evolved from individuation and bureaucratic organization (Dandeker 1990) to becoming more technological and computer-based.

Expanding beyond the control of minorities by police and intelligence services, and initiated by sociologists such as Gary Marx (2012, 2016) and David Lyon, surveillance studies 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 Marx (2016b),

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, and although there is currently a myriad of studies regarding surveillance, there is a lack of integration among literatures; surveillance studies are varied, fragmented, and scholars often disagree. Marx (2016b) calls for an “increased communication between fields, improved definition and operationalization of concepts, and nuanced abstractions filled with systematic empirical content” (p. 140). This paper, therefore, attempts to provide a clearer picture of surveillance methods and theory by reviewing the history of surveillance literature and theory, and ultimately focusing on the retail sector
and the impact of the use of surveillance on both the retailer and the consumer, and developing a tentative
definition of retail surveillance.

**Historical Foundations Between the 15th and 19th Centuries**

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, and 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 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 (Boyne 2000). During
plagues, surveillance was 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.

In the late 18th century, philosopher and social theorist Jeremy Bentham designed the panopticon, an
institutional building and a system of control (Fig. 6) that could be applied to any penitentiary house
(Fig. 7). 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, 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, supplanting earlier coercive and brutal methods, and secondly,
focusing on classificatory schemes with which sovereign power was capable of locating and
differentiating the treatment of different prisoners (Lyon 2006a, p.3). The architectural plan conceived
by Bentham was first constructed by his brother Samuel, an engineer, in 1787 for a factory at Critchef
in Russia (Zuboff 1988, p.320). In the 19th century, and with the growth of bureaucracy and the regulated
states, the content of surveillance kept expanding (Marx 2016b, p.43). Although Bentham’s panopticon
was never built, contemporary prisons far surpass his original vision of coercion without the use of
violence (Rhodes 1998). More importantly, panopticism would later serve as a key theoretical frame of
surveillance studies (Elmer 2012).

Fig. 7 – Bentham’s *Panopticon; or, The Inspection-Houses* book cover (scanned by Google).
The Foucauldian Discipline and Its Impact

Bentham’s prison architectural design, centred around the illusion of an omniscient surveillant, became a stepping stone for the French philosopher and social theorist Michel Foucault’s work on surveillance. 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)

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. The trap of permanent visibility assures the automatic functioning of power (just think about the rapid spread of surveillance and visibility of social media nowadays (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)

Thus, 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 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 [panopticism] 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 confining architectures instill a form of discipline in the individual, making him/her act independently, conforming to his/her modern, industrial, democratic society, hence, an illusion of freedom.

Before the advance of surveillance technologies, and in 1949, George Orwell had his dystopian novel, *Nineteen Eighty-Four*, published. In his futuristic nation of Oceana, the “thought-police” is an agent of a centralized totalitarian state that uses surveillance primarily as a means to maintain social order and conformity. In the later decades, however, Orwell’s cautionary tale of “Big Brother” has been surpassed, and both state and non-state institutions are now involved in monitoring different populations (Haggerty & Ericson 2000). Foucault uses the term “panopticon” to describe both the development and the transformation of the Orwellian society from a society of 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 &
Foucault’s panopticism has been transported “from the penal institution to the entire social body” (1978, p.298).

Although Foucault prompted a new panaopticism in theorizing surveillance, others had different reactions to his work: doubting that Bentham’s approaches are present in the former’s work (Agamben 1998), that Foucault’s work is flowed (since it is fatalistic to apprehend and comprehend deviance by new ways of control) (Ignatieff 1978, p.220), or that there is a need to go beyond Foucault’s work to understand the contemporary electronic technology-dependent surveillance (Haggerty & Ericson 2000; Webster & Robins 1986; Zuboff 1988). Marx (2016b, 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 his analysis does not give sufficient attention to the multiplicity and fluidity of surveillance goals and the conflicts between them.

Describing surveillance as a “major form of power in the mode of information,” Mark Poster (1990, pp.85–98) advocated for a new “Superpanopticon,” a system of surveillance without towers, guards, walls, or windows, and means of controlling the masses in the postmodern, post-industrial mode of information.

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. (p. 93)

Thus, 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, moreover, would describe databases as “multiplication of the individual” instead of an invasion of privacy or a threat to a centred individual (p. 97); this description of an “additional self” will be later echoed in what Haggerty and Ericson (2000) describe as “data doubles” (see below). Diana Gordon (1987), on the other hand, argued that the term “electronic panopticon” better captures the nature of the contemporary situation.

Thomas Mathiesen (1997) argues that “synopticism” (where the many see and contemplate the few) now parallels Foucault’s panopticism (where the few see the many). His concept is based on the Greek word syn, meaning “together” or “at the same time,” and opticon, which has to the with the visual. Consequently, we live in a “viewer society.” 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, the reporters, and the stars who have become a new class in the public sphere (p. 219). He, however, does not disregard Foucault’s panoptic, 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 the 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. In the field of consumption, consumers synoptically watch the 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).

On the other hand, Bauman (2003) argues that the importance of the panoptic in the 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. Thus, 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).

The influence of Deleuze’s work

Foucault’s panoptic perspective would be later challenged. For example, 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 American novelist William Burroughs (1959) to dub the new system of power) where individuals are controlled by “passwords . . . a numerical language of control . . . made of codes that mark access to information” and where “marketing has become the center or the ‘soul’ of the corporation” and the operation of markets an instrument of social control (pp. 5–6). 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).

In conjunction with the French psychotherapist and philosopher Félix Guattari, Deleuze introduced a radical notion of multiplicity in the surveillance phenomena, which they called “surveillant assemblage” (Deleuze & Guattari 1987). 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). Deleuze and Guattari also introduced the “rhizomatic surveillance.” Rhizomes are plants that grow like weeds; 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. To them, the rhizome metaphor highlights two attributes of the surveillant assemblage: (1) the phenomenal growth through expanding uses, and (2) its leveling effect on hierarchies (Haggerty & Ericson 2000, p.614). Rhizomatic surveillance, 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).

Drawing on the works of Deleuze and Guattari, Haggerty and Ericson (2000) argue 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 “data double.”

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)

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.
The notion of data doubles could be also viewed as a departure from Marx’ 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 derived from the surplus information that different populations trail behind them in their daily lives” 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.

Building on the work of Foucault and Deleuze, Hardt and Negri, in their Empire (2001), investigate the emergent phenomenon of the “empire,” which they describe as a “political subject,” a “decentred” and “virtual” entity not specifiable by markers of land. To them, the older political power of the nation state is being replaced by a new empire that requires a new mode of self-regulation, changing societies of discipline to societies of control.

**Beyond the Panopticon**

Both Lyon (2006a) and Roy Boyne (2000) advocate for accepting the effect of 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.

With panopticism comes resistance, yet resistance is not always liberatory and might even invite further control. 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 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.

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. 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 surveilance 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)

Even 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. E-commerce is dependent on the monitoring of consumers while surfing the internet.

The commodification of individuation (when people market themselves) is dubbed “participatory 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)

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 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). Thus, in the current capitalist economy, the new panopticon is more flexible, subtle, participatory, decentralised, and consensual (i.e. voluntary); people are seduced to conform by the pleasures of consuming, which substitutes the predecessors’ crudities and brutalities. To Lyon (2006a, p.8), such 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.”

Boyne proposes a new “post-panopticism” paradigm that has the following features: (1) forms of consumers 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) acts alongside the Panopticon (where the few watch the many), thus, relativising its effects; and (5) the Panopticon’s failure to produce docile subjects is a challenge to panoptic theory (Boyne 2000; Lyon 2007, p.60).

Rise of Popularity of Surveillance Studies

The field of surveillance studies in its modern form has started being of interest to scholars at least since the 1950s, with the rising awareness of human rights, the publishing of literary works by Huxley, Orwell, and Kafka, and the appearance of new technologies and their subsequent profound implications for social behaviour, organizations, and societies. Thus, since the mid-twentieth century, the surveillance landscape has altered dramatically. Since the 1980s, political-economic restructuring has helped to make all sorts of institutions, companies, agencies, and groups part of the process of governance alongside more formal government, and the chief tool in these processes is networked computer-based communications, which has ultimately fostered globalization, in which space becomes less of a barrier. Surveillance studies would, therefore, examine all manner of agencies using all manner of technologies (or none at all) that are involved in surveillance practices (Lyon 2010a). After 9/11 and the subsequent global war on terror (GWOT), surveillance studies would come to increased public and academic attention (Winseck 2009). This, moreover, coincided with the massive growth in surveillance capacities which paralleled the shift to computerized record-keeping, and the advancement in cloud technology (Mudassar et al. 2018), sensor technology (Foresti et al. 2009), and artificial intelligence (Vincent 2018).

Lyon (2003b) relates modern surveillance theory to those classical treatments that understand surveillance as an outgrowth of capitalist enterprises, bureaucratic organization, the nation-state, a machine-like technology, and the development of new kinds of solidarity, involving less “trust” or at least different kinds of trust. To simplify the processes of bureaucratic administration, the computerization of surveillance in the late 20th century has become a classic hallmark of modernity, upgrading Max Weber’s “iron cage” to an electronic one (Lyon, 2003, p. 165). Thus, in modern times, surveillance appeared as part of the political economy of capitalism (Marx), as a product of bureaucratic organization (Weber), and as a shift from punishment and spectacle to self-discipline (Foucault) (Lyon 2007, p.4). Giddens (1990, pp.58–59) writes that surveillance, based upon the control of information, is interrelated to three other dimensions of modernity: capitalism, military power, and industrialism (Fig. 8).

Lyon (2003b) argues that the rapid expansion of surveillance technologies in the later twentieth century is a central aspect of modernity and a putative shift toward more postmodern conditions. Surveillance is what lies behind the information, or the network, society. Postmodern surveillance, on
the other hand, deals with what William Staples (2000, p.11) thinks of as new forms of “vigilance and visibility” that are technology-based, body-objectifying, and everyday- and universal-kind of surveillance.

Fig. 8 – Anthony Giddens’ institutional dimensions of modernity (p. 59)

The growth of multi-disciplinary surveillance studies has also involved many fields, including: philosophy, criminology, social psychology, political science, geography, law, architecture/planning, history, economics, communications, cultural studies, computer, public administration, public health, business, marketing, science, technology and society studies (Marx 2012, p.xxvii), with sociology quite involved at every level (Lyon 2007, p.18). The contribution of surveillance studies, moreover, is to foreground empirically, theoretically and ethically the nature, impact and effects of a fundamental social-ordering process (Lyon et al. 2012). The importance of surveillance studies stems from the fact that without careful theorizing, the growth of contemporary surveillance will be seen only in relatively shallow and superficial ways in media accounts and policy reports that depend only on descriptive and statistical data (Lyon 2006a). In marketing history, the progress of surveillance parallels that of marketing and consumer behaviour: from the 1940s when “commercial 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, to the 1950s and 1960s when 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, to the 1970s when marketing icon Philip Kotler (1972) advocated for “customer satisfaction,” 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 et al. 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; Pridmore & Zwick 2013).

There are many works that mapped the field of surveillance studies that guide us in the analysis of surveillance. Early social scientists discussed the modern disciplines of capitalist supervision (Marx), bureaucratic recordkeeping (Webber), the individual’s attempts at resistance in the urban metropolis (Simmel) and the disciplinary response to growing social inequality (Durkheim). Although the Foucauldian panopticon marks a shift towards modern surveillance, its generalizability is questionable, for after all, the panopticon is a prison. Post-panoptics—such as Agamben (1998) (Poster 2005; Hardt & Negri 2001; Deleuze 1992)—combine new technologies with political regimes and/or social control. Post-September 11, Greg Elmer and Andy Opel (2006) talk about a “survivor society,” or social control, a predetermined future with inevitable outcomes that can only be known by an elite class of sacred bureaucrats. Unlike the surveillance and control society theses which focus on the automation and
networking of technologies (such as databases, biometrics, face recognition cameras and software, etc.), the survivor society documents threats and shows an extensive use of surveillance beyond the conventional logic of automating and integrating new technological apparatuses. Didier Bigo (2006) writes about globalized surveillance after September 11, and proposes the notion of the “ban-opticon” that shows how the role of routines and acceptance of everyday life protects some over others (the latter becoming “targets”). Toshimaru Ogura (2006) stresses that the growth of contemporary surveillance is rooted in the expanding global capitalist system which, unlike military surveillance that has some obvious destructive and fatal aspects to it, is sometimes geared towards increasing efficiency and productivity. However, according to Lyon (2006a), surveillance theories lack attention to crucial dimensions, such as socio-economic class, gender, and ethnicity.

Conclusion
In the context of retailing, surveillance could be defined as following:

Surveillance in a 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, and shrinkage prevention. 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? Does it 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. 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, 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 et al. 2015). Surveillance has been commodified, where it (or the protection from it) is now a product to be purchased (Marx, 2012, p. xxvi)

Yet how can we, as consumers, differentiate appropriate from inappropriate uses of surveillance? Personal information defines our experience as consumers, however, though personal information economy offers us many benefits, it has a broader impact and poses many risks. To help consumers and interested stakeholders better understand the benefits and risks of information use, there should be a greater transparency about how organizations collect and use data potentially. 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). 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 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 and sectors (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.

Surveillance always carries with it some plausible justification that makes most of us content to comply. To Lyon (2001), the question of surveillance goes beyond the fear of data breach 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). By examining the origins of surveillance, both as theory and as practice in the field of retailing, this paper attempts to
further the understanding of the use of surveillance in the retailing sector, and its impact on both retailers and consumers.

**Expected Contributions**

This paper, and the planned subsequent mixed-methodology research, is expected to make three main contributions. First, in the field of theory, this paper provides a historic perspective on the development of surveillance studies and surveillance systems employed in retailing, and the effect of retailers’ use of technology and surveillance on retailing consumer behaviour, customer satisfaction, shopping effectiveness, and consumer well-being. Secondly, this study will be of significance to retail practitioners, for in order to grow and prosper, retailers have to follow the consumer and technology changes. Thirdly, the study will have social implications. Retail stores and supermarkets must be responsive to consumer changes; as consumers become more demanding for technology and convenience, the former must continue to provide those needs, otherwise, they will disappear from the competitive market.

**References**


Anon, Internal data from FaceFirst. *FaceFirst*. Available at: https://www.facefirst.com/company-overview/ [Accessed July 2, 2018b].


Heydari, A., 2018. Cellphone tracking has been used in at least 1 Canadian mall, former employee says. *CBC News*. Available at: https://www.cbc.ca/news/canada/calgary/cadillac-fairview-mall-location-
Hill, K., 2012. How Target figured out a teen girl was pregnant before her father did. Forbes.


189
Despite such lack of attention, there are some works that focus on such issues, for example, Oscar Gandy’s (2006) paper on racial profiling in the delivery of health care.