Volume 4 (1) 2022 https://doi.org/10.5204/lthj.2088

Retail Analytics: Smart-Stores Saving Bricks-and-Mortar Retail or a Privacy Problem?

Helen Gregorczuk
The University of Queensland, Australia

Abstract

'Bricks-and-mortar' retailers are increasingly looking to retail analytics as a way of staying competitive with online counterparts. Retail analytics is a subset of big data analytics, and proponents contend that its use can provide a greater understanding of customer behaviours and patterns. To achieve this, retail analytics requires 'smart-stores' to collect and store as much data as possible about in-store customers, and to build detailed consumer profiles that can be used to sell products on an increasingly individualised basis. At the same time, enhanced efficiencies are gained by a better matching of staff resources and design of store layout that directly correspond to customer behaviours. The range of data collection and analysis technologies used in retail analytics is evolving and currently includes facial recognition software and video analytics, specially designed sensors, Bluetooth beacons, Wi-Fi data collections and point-of-sale systems, including loyalty cards. When these collection technologies are combined, a smart-store can, thus, resemble a sophisticated consumer surveillance system entailing numerous collectors and re-users of consumer-generated data. This article argues there is a disproportionate impact on privacy when compared to the benefits for retailers. It outlines the developing sphere of retail analytics and its manifestation through smart-stores. It considers some of the key privacy issues that emerge through retail analytics and the consequent surveillance and 'datafication' of everyday life. This includes the issue of whether collected data is personal information, the degree to which individuals can understand the multifaceted data collection processes of smart-stores, and the importance and weight to be attributed to privacy in any decision-making by stores in the uptake of various technologies.

***Keywords**:* Retail analytics; privacy; big data; datafication; surveillance; personal information; disproportionality.

I. Introduction

This article contends that large-scale data-gathering and processing by bricks-and-mortar retailers, known as 'retail analytics', can be a significant privacy problem in the way it normalises surveillance and the datafication of daily life. It argues that there is a disconnect between the legitimate commercial objectives of retailers and shopping centres and the extent of the impact on an individual's privacy, as well as the erosion of privacy at a societal level. The article contributes to the literature by outlining retail analytics practices and their purposes with the aim of promoting greater awareness of them. It further highlights the importance of considering privacy in any decision-making about the implementation of data-gathering and processing technologies. In particular, it argues that there is an overreach by retailers in their data-gathering activities—that there is a disproportionate approach adopted when the objective of the retailer is greater customer convenience or engagement, but the result is a widespread surveillance system in bricks-and-mortar retail outlets. It argues that any consideration of privacy needs to honour privacy's value and importance in order to attribute appropriate weight in decisions around the appropriateness of particular retail analytics practices and their implementation.

Bricks-and-mortar retailers face significant commercial competition from online outlets, particularly at this time of pandemic restrictions. Both shopping centres and stores now attempt to provide a more personalised, customer-centric in-store shopping experience for customers.[1] They are attempting to better understand customer behaviours to improve and personalise the shopping experience. In wanting to learn more about their customers, bricks-and-mortar retailers are employing store-based technologies that essentially mimic the behavioural tracking capabilities of e-commerce and, in some instances, go beyond it. While consumers may be aware of the use of cookies on websites, which allow a retailer to know how often they visit a website or webpage and what they purchase, they may be surprised to know the extent to which they may be tracked in a real-world 'smart-store' or 'smart shopping centre'.[2] Indeed, it has been argued that for retailers to be successful they must break down the silos of the online and bricks-and-mortar components of their business.[3] The extensive data collection of 'cyberspace' written about more than two decades ago[4] has become reality. In some instances, store mannequins have been fitted with high-resolution video cameras and facial recognition technology that can be used to detect the age, gender, race and facial expressions of customers.[5] Customers with smartphones who log into free Wi-Fi, or just have their phone switched on, can be tracked as they move around a store or a shopping centre.[6] Bluetooth beacons allow retailers to contact customers in real time with targeted marketing offers but have people-tracking as a side effect.[7] For example, the data gathered and mined by the department store Target about a teenager's shopping habits allowed it to predict that she was pregnant before her family knew.[8] The days in which a customer browsing in a bricks-and-mortar mall could experience relative anonymity are fast coming to an end.

The growth of the smart-store and its data collection requirements is heralding the advent of a new analytical industry: retail analytics. 'Analytics' has been defined as the process of transforming raw data into actionable knowledge,[9] and typically uses statistics, algorithms, computer programming, and explanatory and predictive models to gain insights into the data[10] and improve decision-making.[11] 'Retail analytics' refers to a range of data-gathering, data-processing and analysis services utilised by retailers with the aim of making better commercial use of that data and adding value to their business.[12] However, to reach that goal of useful business insight, a huge amount of data collection on shopping patterns, store use and individual behaviours is required. The capacity to collect, store and analyse enormous quantities of data with tremendous speed and negligible cost is known as 'big data'.[13] Retail analytics is one example of big data.

This article outlines these forms of in-store data collection and the purposes of retail analytics to highlight privacy concerns. It argues that while the 'smart-store' and its dependence on retail analytics may provide a more enhanced customer experience, there are likely negative consequences from the 'datafication' of the everyday shopping experience of customers in bricks-and-mortar outlets. 'Datafication' refers to the transformation of human life so that its elements can be a continual source of data.[14] That is, things that never used to be recorded (such as walking through a shopping centre) can now be captured, aggregated and analysed.[15] Datafication intensifies privacy concerns such as the normalisation of surveillance.[16]

Section II outlines the data collection techniques and strategies that are starting to emerge, and Section III underscores the purpose of analytical operations. Section IV outlines examples of retail analytics from Target, Amazon Go, Westfield, Cadillac Fairview and 7-Eleven, highlighting the privacy implications of datafication and the normalisation of surveillance activities, as well as the importance of privacy in any decisions about the implementation of data-gathering technologies. The case studies demonstrate the capacity of retail analytics technology for capturing data and creating systems of surveillance where people may not expect it, and that retailers' perception of their practices does not always accord with that of the public or the relevant privacy commissioner. In particular, the case studies show how a retailer's practices are in many instances disproportionate in their effects on privacy when compared to the legitimate objective of greater customer engagement, tailored marketing, or gauging customer demographics, which a retailer may be pursuing. Section V concludes by outlining the balance struck between the requirements of the *Privacy Act 1988* (Cth) and customers' privacy against the ability of bricks-and-mortar retailers to remain profitable. Under the *Privacy Act*, the obligations to treat information in accordance with the Australian Privacy

[1] Corrigan, "Target," 159.
[2] Farshidi, "The New Retail Experience," 15.
[3] Bullard, Style and Statistics, 11.
[4] Kang, "Information Privacy in Cyberspace Transactions," 1193.
[5] Shopsmart, "Retail Stores Are Spying."
[6] Little, "Someone to Watch Over You," 169.
[7] Max, "Nineeteen Technologies of People Track People," 6.
[8] Duhigg, "How Companies Learn Your Secrets."
[9] Das, Computational Business Analytics, 1.
[10] Educause, "What Is Analytics?"
[11] LeClaire, Business Analytics in Retail for Dummies, 3.
[12] For example, see Mohanty, Big Data Imperatives.
[13] Tene, "Judged by the Tin Man," 351.
[14] Mejias, "Datafication," 1.
[15] Mayer-Schönberger, Big Data, 73.
[16] Strandburg, "Monitoring, Datafication, and Consent," 17.

Principles (APP) only arise where the information is 'personal information' as defined in the Act. The challenge in retail analytics is that collections of information are not always going to obviously be personal information in the statutory sense. The definition of personal information is context-specific and, therefore, changes over time. It is possible for a piece of data to not be personal information in one context; however, when combined with other data it may become personal information.

II. Data Collection Techniques, Technologies and Strategies

Data-gathering by retailers is not new. Store loyalty cards, credit card payment information and purchase history analysis have been around for decades. However, the development of the 'smart-store'[17] and the large range of collection technologies and analytical techniques associated with 'big data' have taken things to another level.[18] Retailers are collecting data from many sources including in-store Wi-Fi, mobile phones, mobile apps, kiosks, digital signage, social media and online search engines. In some cases, the data collection is about improving store layouts and inventory management, managing security and staffing levels, and curating the right mix of brands and goods to entice the likely customer.[19] The data that can be captured and analysed at an aggregate and anonymous level, or is attached to products rather than people, is less concerning from a privacy perspective. However, where the data collection is focused on decision-making at the individual customer level, then different considerations apply. The shift from aggregate to individual-level data analysis, enabled by tracking technologies, is seen by marketers as highly desirable, as it allows for much more granular targeting.[20] Sometimes it is not clear whether the data collection is focused solely at the aggregated level or whether it could be utilised at an individual customer level. For example, a store may have the tools to do a 'shopping basket analysis' to determine its discounting strategy across the board—an aggregated analysis may reveal that 50% of customers purchase socks and underwear at the same time such that it is more profitable to only discount one of these at a time. However, if the ability is retained to drill down at an individual customer level, then offers may be targeted to particular customers based on their past purchase history, and this may trigger privacy concerns.

In the case of supermarkets, customers' every move can be tracked with devices such as radio frequency identification (RFID) tags on products or shopping trolleys, as well as a range of global positioning system (GPS) tracking-based technologies, handheld price checkers, and thermal scanners in the ceiling.[21] GPS relies on satellites to provide accurate latitude, longitude, altitude and time, and is accurate to between four metres and fifteen metres.[22] Video cameras are also sometimes fitted with facial recognition technology, which allows for the comparison of a captured image at a predetermined location to a predetermined set of definitions (a template) typically tied to customer demographics. The power of this data-gathering comes from combining technologies such as GPS and phone network triangulation and Wi-Fi to provide the most precise location information. Other examples of combinations of technologies include RFID and digital touchscreens (such as kiosks)[23] fitted with facial recognition cameras, and beacons using Bluetooth technology to send offers to a customer's phone.[24] The facial recognition cameras are sometimes used in a 'face detection' way—that is, not to identify individuals by matching them to a database of photographs but instead to group them under demographic categories such as age, gender and race.[25] Detailed insights into individual customers can be captured through these cameras by recognising their emotions, detecting and measuring facial expressions, and even analysing their eye movements.[26] Advertisements can be targeted to billboards based on the demographic information and mood of the group walking past, evident in the Westfield example discussed in Section IV(C).[27]

Cameras fitted with retail analytics software facilitate 'video analytics'. The video analytics process is designed to detect, track and recognise 'objects of interest' from multiple videos while interpreting their behaviour.[28] An 'object' can be a face, a head, a human or a queue of people.[29] The behaviour can include dwelling time, attention or movement across different sections.[30]

[17] A smart-store is a bricks-and-mortar retailer that utilises a range of new technologies and modern marketing concepts; see Hyunwoo, "Smart Store."
[18] For example, see Pantano, Smart Retailing, 70.
[19] Randhawa, "Retail Analytics," 601.
[20] Bradlow, "Big Data," 85.
[21] Cox, Retail Analytics, 17.
[22] Cheung, "Location Privacy," 43.
[23] Kiosks are a secure cabinet consisting of touchscreens, a computer and a printer with a credit card reader. They can be found in airports, retail stores and malls, hotels and banks. Inman, "Shopper-Facing Retail Technology," 9.
[24] Ventura, "Retail in the Digital Era," 20.
[25] Sightcorp, "Face Analysis Technologies."
[26] Sightcorp, "Face Analysis Technologies."
[27] Edwards, "Smile for the Camera."
[28] Shan, Video Analytics for Business Intelligence, vi.
[29] Shan, Video Analytics for Business Intelligence, vi.
[30] Cazzato, "Pervasive Retail Strategy," 24.

The objective of video analytics is to describe the behaviour of shoppers and the effectiveness of ads, shelf space and product displays, and is generally done by calculating a range of indexes for attraction (viewing), attention (amount of time a customer spends looking at an item), relevance (how interesting) and engagement (derived from the correlation between relevance and attention).[31] 'Gaze tracking', which can give information about the focus of attention,[32] underpins these indexes.

Location is a particularly rich source of data.[33] It has been described as one of the most sensitive forms of personal information because of the way it implicates other kinds of personal information and allows for inferences to be drawn.[34] In other words, it can be used to deduce many other things about an individual.[35] Section A explores in greater detail the techniques and technologies associated with location analytics.

A. Location Analytics and Customer Tracking

Location analytics, in the context of retail, has been defined as the process or ability to gain insight from the location or geographic component of business data.[36] Transactional data, when laid out in a geographic information system, can result in new insights. In the context of retailers, it has been particularly used to identify historical spending habits of people from different geographical locations and to allow for targeted advertising and better product distribution.[37] It can be used to improve sales and store layouts with the ability to track customer movement, creating greater efficiencies in staffing and cleaning of high traffic areas.[38]

Max goes further in explaining the context for location analytics in a retail setting.[39] She argues that the concept emerged from a combination of disciplines, notably web analytics, where offline (bricks-and-mortar) retailers have wanted to emulate the success of online retailers such as Amazon, as well as the desire for targeted marketing, which is based on the assumption that personalised promotions to customers will increase conversion (the rate at which browsing customers convert to customers who purchase something). The data largely comes from a smartphone collecting its location from a variety of wireless technologies such as GPS and mobile cell phone towers, and is sometimes referred to as 'mobile location analytics'.[40] In-store tracking is a prominent example of mobile location analytics. The term is often understood as referring to a range of technological solutions that integrate retail infrastructures with sensor technologies, with the aim of continuously tracking and analysing customers' activities in or near a venue.[41] A retailer may rely on a range of technologies including GPS, Wi-Fi, and Bluetooth beacons to this end.[42]

One increasingly common data collection technology being used in retail analytics is Bluetooth Low Energy (BLE) beacons, sometimes referred to as Bluetooth smart beacons. The primary objective of beacon use in retail analytics is for location tracking and targeted marketing to promote customer loyalty and impulse buying, and to increase customer spending.[43] Beacons allow retailers to directly contact customers and to send personalised advertisements and offers when they are in the vicinity of the store,[44] or even in a specific part of the store; they also allow for tracking movements, behaviours and frequency of visits.[45] Beacons are small radio transmitters that can be fixed throughout the retail environments or even built into displays or tablets.[46] The beacons send a signal that can then activate a smartphone app installed on a customer device.[47] BLE tracking is becoming increasingly commonplace because it is now built into Apple and Android devices without customers having to download an application; they only need to opt in to 'anonymous tracking'.[48]

[31] Testori, "Video Analytics," 9.
[32] Cazzato, "Pervasive Retail Strategy," 24.
[33] Cheung, "Location Privacy," 43.
[34] Michael, "Überveillance," 220.
[35] Gilley, Mobile Device Tracking.
[36] Max, "A Brief History of Location Analytics," 23.
[37] Technopedia, "Location Analytics."
[38] Cox, Retail Analytics, 21.
[39] Max, "A Brief History of Location Analytics," 1.
[40] Gassen, "Mobile Location Analytics," 1.
[41] Gassen, "Mobile Location Analytics," 1.40
[42] Gassen, "Mobile Location Analytics," 1.
[43] Max, "Nineteen Technologies to Track People," 7.
[44] Milesi, Navigating the New Digital Divide.
[45] Tickto, "Behavioural Analytics."
[46] ComQi, "Programming Your Store," 31.
[47] ComQi, "Programming Your Store," 31.
[48] Max, "Nineteen Technologies to Track People," 7.

Max contends that location analytics was initially used in retail for ‘people counting’.[49] However, retailers soon realised that location analytics could be used not only for the generation of in-store population statistics, but also for tracking individual customer behaviours. As such, location analytics could provide insight on population-based sales conversion rates, but it could also be used to generate data on how to increase this rate.[50] Even at this early stage, the original locational solutions to track customer behaviours in a store were a blend of laser, thermal and video technologies.[51]

Thus, locational tracking techniques have developed into ‘people-tracking technologies’ that seek to capture customer and employee activities in the physical store and allow retailers to better understand traffic patterns, manage queues and demand, measure sales conversion and empower marketing.

B. Wi-Fi Location Analytics

It is now increasingly common practice for retailers and shopping centres to offer free Wi-Fi to customers as part of the customer tracking exercise. Wi-Fi is the technology standard for exchanging data over a wireless local area network.[52] Wi-Fi-enabled devices continually send ‘probe requests’ to find networks to join within range.[53] The probe requests and responses contain an identifier known as the media access control (MAC) address unique to the device, and this identifies devices in a network.[54] The MAC address is assigned by a manufacturer to a Wi-Fi-enabled device and is visible in communications between devices irrespective of whether the wireless connection is encrypted.[55] This means that a retailer can utilise wireless technologies and infrastructures to collect probe requests, then extract the MAC address and link it to a specific location.[56] It becomes possible to track customers by monitoring the signal strength received by the Wi-Fi access point, which can then be used to estimate the distance of the device from the access point.[57] The technology functions well indoors and is used more widely than GPS, despite not being as accurate as GPS.[58] Moreover, if the device is within the range of several access points, then this further increases the accuracy with which a retailer can pinpoint the device’s location. Monitoring of the device location can occur over time, thus, building a profile of a customer’s behaviour. This occurs even if the device is not connected to Wi-Fi, as it is sufficient for the device’s Wi-Fi feature to be turned on.[59]

Thus, Wi-Fi is a people-tracking technology that is ideal for capturing unstructured movement in large venues.[60] This is becoming increasingly important because Wi-Fi sensors can monitor radio waves from smartphones and can cover a range of approximately 10,000 square metres.[61] The technology can in this way be used to track customer behaviour over a relatively broad location through the combination of different Wi-Fi access points, both in-store and out. For example, journalists visited a Canberra shopping centre, utilised the free Wi-Fi and then requested the collected data. The data revealed which websites they had visited on their iPhones as well as where the phone had been and noted details of what section of the centre the device was in, for how long and on what floor.[62]

III. The Purpose of Analytical Operations

Since the technologies are evolving, collection strategies are likely to develop considerably over the short and medium terms. It is appropriate to consider the purpose of these analytical operations at a more general level. The main function of retail analytics is personalisation. There are three categories of practices overlapping to some extent, but can be identified as:

- personalisation and targeted ads to enhance in-store customer experience and to increase sales and loyalty
- audience measurement information and demographics to improve the efficient use of store resources and to facilitate personalisation
- profiling interests and behaviours to facilitate a more personalised customer service.

[49] Max, “A Brief History of Location Analytics,” 23.
[50] Max, “A Brief History of Location Analytics,” 2.
[51] Max, “A Brief History of Location Analytics.”
[52] Max, “Nineteen Technologies to Track People,” 7.
[53] Information Commissioner’s Office, “Wi-Fi Location Analytics,” 3.
[54] Though the MAC address can be altered. See Information Commissioner’s Office, “Wi-Fi Location Analytics,” 3.
[55] Burdon, “Google Street View,” 702.
[56] Cheung, “Location Privacy,” 44.
[57] Cheung, “Location Privacy,” 44.
[58] Cheung, “Location Privacy,” 44.
[59] Information Commissioner’s Office, “Wi-Fi Location Analytics,” 4.
[60] Max, “Nineteen Technologies to Track People,” 6.
[61] Max, “Nineteen Technologies to Track People,” 6.
[62] O’Mallon, “Westfield Is Watching.”

The different types of analytical function that are starting to emerge from smart-stores provide insight into the development of dense and multiple data collection networks. The analytical function of the smart-store is predicated on omnibus-style data collection to fulfil the main purpose of the analytical exercise: personalisation. This section outlines key facets of personalisation, and, in doing so, examines how proponents of retail analytics justify the collection of data for a more enhanced and personalised customer experience. This is achieved in three ways: targeted marketing to customers, increasing audience measurement, and enhanced customer profiling.

A. Targeted Marketing

Personalisation in the form of targeted marketing is one of the ultimate drivers for retail analytics. The logic seems to be that customers are more likely to buy a product or service if it is relevant to them; to know this, retailers must collect as much data as possible to build a clear picture (profile) of their customers.[63] According to EKN, retailers are using analytics to gain a deeper understanding of their customers' behaviours, needs and preferences to build a more personal relationship. This greater knowledge of customers is supposed to improve marketing effectiveness by micro-targeting, which ultimately leads to offers that increase the likelihood of a purchase.[64] Similarly, Gassen and Fhom describe the motivation for retail analytics as better understanding customers' shopping patterns, which, in turn, leads to improved customer engagement and marketing, optimised product placement and the ability to run targeted campaigns towards user groups who share similar profiles.[65]

B. Audience Measurement Information and Demographics

While targeted marketing can focus on individual customers, it is becoming increasingly common for retailers to now target broader population demographics. A customer's physical characteristics, such as their height, weight, gender, and skin and clothing colour—sometimes referred to as 'soft biometrics'[66]—are captured by video cameras fitted with facial recognition and video analytics technology. These 'soft biometrics' can be used to describe the essential characteristics of an individual without (it is argued) uniquely identifying them.[67] The technology has evolved to the point at which a person's emotional state and eye movement can be collected.[68]

In some instances, the cameras are concealed within mannequins.[69] Mogg argues that while stores generally have security cameras that could be fitted with the facial recognition technology, the advantage of having it within the mannequins is that it improves the accuracy of the data, given the close proximity of the camera to individual customers.[70] In addition to picking up these demographic details, the cameras are also able to register how long someone is looking at an item,[71] and it is possible that the mannequins may be fitted with microphones to pick up customers' conversations about the products displayed.[72]

C. Profiling Interests and Behaviours

As outlined, retailers are investing in more resources to better target both individuals and broader populations of customers. Indeed, this means that the interests and behaviours of customers can be profiled to a significantly greater depth than previously. Hildebrandt defines profiling as the process of knowledge discovery in databases by means of pattern recognition.[73] The patterns emerge from data-mining, and after interpretation and testing, they can be used for predicting the behaviour of the subjects being profiled[74] or for predicting preferences and attitudes.[75]

In the context of retail analytics, behavioural advertisers use customer profiling for direct marketing purposes.[76] Advances in tracking technologies have enabled advertisers to construct personal profiles to target customers individually, thus, creating more relevant advertising and efficient advertising spending.[77] However, this can give rise to some significant privacy concerns. King and Jessen identify a range of privacy concerns with profiling, including interference with customers' rights to adequate

[63] Cox, Retail Analytics, 29.
[64] EKN, The Future of Retail Analytics.
[65] Gassen, "Mobile Location Analytics," 1.
[66] Shan, Video Analytics for Business Intelligence,28 vii.
[67] Denman, "Identifying Customer Behaviour," 199.
[68] Cazzato, "Pervasive Retail Strategy," 23; Farinella, "Face Re-Identification," 41.
[69] ShopSmart, "Retail Stores Are Spying."
[70] Mogg, "It's No Dummy."
[71] ShopSmart, "Retail Stores Are Spying."
[72] Roberts, "Bionic Mannequins."
[73] Hildebrandt, "Who is Profiling Who?" 241.
[74] Hildebrandt, "Who is Profiling Who?" 241.
[75] King, "Profiling the Mobile Customer," 456.
[76] King, "Profiling the Mobile Customer," 456.
[77] King, "Profiling the Mobile Customer," 457.

notice of the collection of their personal information and pervasive and non-transparent commercial observation of consumer behaviour, as well as the increased generation of unwanted marketing material.[78] In fact, unauthorised creation of consumer profiles was one of the fastest growing consumer complaint categories in the United States, rising by 193% from 2007 to 2008.[79]

IV. Privacy Concerns: Datafication and Normalising Surveillance

The privacy concerns arising from customer profiling are not specific to one technological development, but are instead representative of a wider concern: datafication and the normalisation of surveillance practices through everyday automation. Under the *Privacy Act*, smart-store retailers subject to the legislation[80] must comply with the APP in the collection, handling and processing of personal information. Personal information is defined as:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
> (a) whether the information or opinion is true or not; and
> (b) whether the information or opinion is recorded in a material form or not.[81]

The challenge is that many of the retail analytics practices may not on their face necessarily be characterised as being 'about' an identified individual or even 'about' an individual who is 'reasonably identifiable' under the current terms of the Act. Whether or not metadata generated by a mobile device in the hands of retailers is personal information in Australia is a grey area.[82] Whether or not cameras that are used for face detection (cf. facial recognition) are making an individual reasonably identifiable is also questionable. This means that retailers may not necessarily consider that what they are doing falls under the protections in the *Privacy Act* and, therefore, remains largely unregulated. The *Privacy Act* and the definition of personal information were under review by the Australian Government in 2020 and 2021. While the definition of personal information is intended to be expansive,[83] the Australian Attorney-General's Department describes 'it is somewhat unclear in its application to technical information'.[84] The review is not expected to be finalised until later in 2022; however, an amendment to the definition of personal information to make clear the *Privacy Act*'s application to technical information may address concerns about how data is collected across the digital economy.[85]

Even where a retailer's collection practices are clearly for 'personal information', it is questionable whether those collection practices will meet the requirements in the APP. For example, collecting personal information is accepted only where it is reasonably necessary for a retailer's functions (APP 3.2); by fair and lawful means (APP 3.5); with the individual's consent where the information is also 'sensitive information' (APP 3.3), and with reasonable notification of the collection practices (APP 5); and where managing the information is done in a transparent manner in line with a published privacy policy (APP 1). The case studies outlined in Sections A–E illustrate these points.

A key effect of the extended use of retail analytics is that bricks-and-mortar stores are essentially emulating the data-gathering and customer surveillance abilities of online retailers. Turow et al. argue that physical bricks-and-mortar retailers are playing catch-up with their online counterparts in their ability to provide 'individualised relevance'.[86] They define this as presenting the shopper with products that reflect that person's interests, encourage the person to investigate the products on-site, and that offer goods at personalised prices that reflect the person's comfort zone. In fact, much of the existing literature on retail analytics extols the positive virtues of personalisation for retailers through targeted marketing as a means to increase sales.[87] Turow et al. offer a different perspective in that they contend that this individualised relevance comes at the rarely detected cost of continual surveillance.[88]

Similar sentiments are found in other works regarding the wider context of surveillance activities. For example, Michael and Clarke refer to the emergence of 'dataveillance' through the widespread storage of personal data on computers through the

[78] King, "Profiling the Mobile Customer," 459.
[79] King, "Profiling the Mobile Customer," 458.
[80] Most retailers will be subject to the legislation, provided they are not small businesses (i.e., have a turnover above AUD$3 million). See section 6D of the *Privacy Act 1988*.
[81] *Privacy Act 1988* (Cth) s 6.
[82] *Privacy Commissioner v Telstra* (2017) 249 FCR 24. However, note the clarification provided by the *Telecommunications (Interception and Access) Act 1979* (Cth) s 187 for telcos.
[83] Explanatory Memorandum, *Privacy Bill 1988* (Cth), 11.
[84] Attorney-General's Department, Privacy Act Review, 21.
[85] Attorney-General's Department, Privacy Act Review, 21.
[86] Turow, "Data Mining," 472.
[87] For example, Huang, "A Unified Framework."
[88] Turow, "Data Mining," 471.

1970s and 1980s. They contend that monitoring people through their digital personae is much more economical than physical observation and, hence, it has become more widespread.[89]

They also refer to the concept of 'überveillance' as the sum total of point in time, predictive, real-time and retrospective types of surveillance, and the deliberate integration of an individual's personal information for the continuous tracking and monitoring of identity and location in real time.[90] This can be contrasted with 'locational privacy', which can be defined as an individual's expectation that when they are moving in a public space in normal circumstances, their location is not being systematically and secretly recorded for later use.[91] The tension between überveillance and location privacy is that information arising at different times, and from different forms of surveillance, can be combined to offer a more complete picture of a person's activities, and to enable more inferences to be drawn, or suspicions generated.[92] This combining of information can be thought of as 'datafication'. Beyond digitisation, datafication puts information into a quantified format so that it can be tabulated and analysed.[93] Datafication allows for more sophisticated information analysis and facilitates analyses across large data sets.[94] It seems to be driven by the desire to turn 'human behaviour … into an analysable form',[95] and has led to 'the wider transformation of human life so that its elements can be a continual source of data'.[96]

Referring back to retail analytics, Turow's et al. focus on how understanding the retail industry's strategies for organising and 'naturalising' information-gathering about customers is important. Bricks-and-mortar retailers in trying to remain competitive are normalising information-gathering about their customers to the extent that they are becoming 'cultural routines'.[97] The period of the mid-1980s through to the 2010s is referred to as a 'great data transition', with customers no longer viewed through a broad demographic lens but as individuals giving off streams of data often in real time.[98] The development of the internet and the success of online sales of books and music are seen as decimating their real-world counterparts.[99] Bricks-and-mortar retailers' perception was that their long-term survival depended on migrating to the digital world themselves, embracing the tracking potential of new technologies and the 'actuarial' potential of the data collected.[100] These retailers are seeking to find an optimum 'loyalty and analytics' combination, describing this as the need to integrate data mining and surveillance into their sales areas.[101] The requirement is to mimic the online sites' ability to follow people around and tailor offers to them, which will generate repeat business.

This constant wide-scale data-gathering becoming entrenched in 'real-world' smart-stores, and the consequent surveillance and datafication in which it results, do not sit comfortably with privacy. Such erosion of privacy through immense data-gathering and processing capacity in the most ordinary of everyday environments (shopping centres) runs the risk of becoming entrenched as a cultural norm. The loss of privacy in this incremental way should be acknowledged so that privacy may be given its proper weight in decisions about how data-gathering and processing technology is utilised.

Giving privacy its proper weight requires some articulation of its meaning and value. Although privacy is widely considered notoriously difficult to define,[102] its value is generally understood in terms of 'promoting personal dignity and autonomy in ways that are important for individual personality, healthy civic discourse, and democratic governance'.[103] Where privacy is lost, it has been said that much else is lost, due to privacy's centrality to the whole structure of human interaction.[104] In the context of retail analytics, the most relevant privacy interests can be summarised as freedom from surveillance and manipulation, and the 'right to be let alone' and to be protected from the unreasonable intrusiveness of others.[105] The 'right to be let alone' suggests a sphere in which it is possible to be anonymous and unobserved,[106] an objective that is increasingly

[89] Michael, "Überveillance," 218.
[90] Michael, "Überveillance," 220.
[91] Blumberg, On Locational Privacy.
[92] Michael, "Überveillance," 219.
[93] Mayer-Schönberger, Big Data, 78.
[94] Mai, "Big Data Privacy," 193.
[95] Mayer-Schönberger, Big Data, 93–94.
[96] Mejias, "Datafication," 2.
[97] Turow, "Data Mining," 465.
[98] Turow, "Data Mining," 468.
[99] Turow, "Data Mining," 469.
[100] Turow, "Data Mining," 469.
[101] Turow, "Data Mining," 469.
[102] For example, Lindsay, "Conceptual Basis of Privacy," 135.
[103] Spencer, "Privacy and Predictive Analytics," 638.
[104] Simmel, "Isolated Freedom," 71.
[105] For example, Wacks, Privacy, 38.
[106] Karyda, "Privacy and Fair Information Practices," 195.

difficult to achieve in a world where retail analytics and big data collection methods are used. Despite this, there is arguably the expectation of individuals in public places still seeking and finding freedom from identification and surveillance.[107] Being free from certain kinds of intrusion is at the core of privacy, and this is understood through social and legal norms that specify 'when, where, and in what ways we may and may not be observed, listened to, questioned, and in other ways kept track of'.[108] Those legal norms may be found in information privacy legislation such as the *Privacy Act*. The real objective of information privacy regulation has been described as protecting individuals against unjustified interferences in their private life by protecting them against unjustified collection, storage, use and dissemination of their personal information.[109] The question becomes whether smart-store retailers' data-gathering and processing is justified. It could arguably be viewed as manipulation with the enhanced ability to not only target consumer preferences, but also exploit individual vulnerabilities.[110]

The following case studies illustrate actual examples of retailers' data-gathering practices and highlight some of the privacy implications from those practices. They demonstrate that the extensive data-gathering and processing practices of retailers—while potentially offering useful insights for stores, or convenience for customers—come at a disproportionate cost to individual privacy through unnecessary surveillance and datafication.

A. Case Study 1: Target

The department store Target's data analytics system rose to prominence when it was revealed in a 2012 *New York Times* article that it was able to predict that a young woman was pregnant before her family knew.[111] The woman's father had gone to the store to complain about Target sending his teenage daughter discount vouchers for maternity items, but, as it transpired, Target were indeed correct that she was pregnant.[112]

Target had collected data about the young woman's purchase history for twenty-five unique products, which were analysed together, producing a 'pregnancy prediction' score.[113] The analysis included comparison of the purchase history of customers who had joined its baby registry with its wider customer database.[114] The young woman in this case had not joined the baby registry, but because her purchases were similar enough to customers' in the registry, Target was able to infer that she was pregnant.[115] Indeed, Target had perfected the technique to the extent that they were able to know what customers bought at different stages of the pregnancy, and to target the personalised offers more precisely.[116]

The example is striking for several reasons. In particular, it reveals how the decisions of others (those joining the baby registry) affect the privacy of individuals (who have not joined the baby registry or volunteered their information). Barocas and Nissenbaum suggest that only 20% of a particular population needs to disclose that they possess a certain attribute for an adversary to then identify all the other members in the population who also have this attribute.[117] As such, it implies that the value of the consent of the other 80% of that population is significantly weakened.[118] The choices of the individual about their information will not be determinative.

The other striking aspect of this example is that Target capitalised on marketing research, which shows that when someone is going through a significant life event (such as the birth of a child) they are more susceptible to marketing offers.[119] Target marketing staff apparently stated that 'new parents are a retailer's holy grail', and that if they could identify and target women in their second trimester (which is when most expectant mothers begin buying items such as maternity clothing and vitamins), this would increase their chances of securing them as long term-customers.[120] Marketing staff were also able to demonstrate that when a child is born, the parents are so exhausted and overwhelmed that whoever they are shopping with at the time is likely who they will stay with over many years, and not just for maternity items but also other goods.[121]

[107] Westin, Privacy and Freedom, 34.
[108] Scanlon, "Thomson on Privacy," 315.
[109] De Hert, "Data Protection," 4.
[110] Manwaring, "Digital Consumer Manipulation," 142.
[111] Duhigg, "How Companies Learn Your Secrets."
[112] Corrigan, "Target," 159.
[113] Mai, "Big Data Privacy," 192.
[114] Barocas, "Big Data's End," 44.
[115] Barocas, "Big Data's End," 44.
[116] Duhigg, "How Companies Learn Your Secrets," 8.
[117] Barocas, "Big Data's End," 62.
[118] Barocas, "Big Data's End," 62.
[119] Duhigg, "How Companies Learn Your Secrets."
[120] Duhigg, "How Companies Learn Your Secrets."
[121] Duhigg, "How Companies Learn Your Secrets."

Target's prediction of the young woman's pregnancy was not a random exercise but a calculated business decision. If privacy is understood as more than just protection of information but in terms of personal privacy and the desire to be let alone and to be free from unwarranted intrusion and manipulation or domination by others,[122] then it is particularly striking in the way the company targeted pregnant customers. One's susceptibility to change brands to Target due to exhaustion and overwhelm, and their value as long-term customers, meant their identification as pregnant customers was important to the store precisely because they were vulnerable and could be more readily manipulated. It highlights the power imbalance between retailers and individuals and how retailers can exploit this for their own ends.

While the huge volume and granularity of the data collected by retailers may increase their competitiveness and the personalised service they can offer customers, it also provides the vehicle through which surprising and intrusive inferences can be made about those customers.

B. Case Study 2: Cadillac Fairview

Cadillac Fairview is a North American commercial property company. It owns at least a dozen large shopping malls in Canada where it had installed facial detection technology in its digital directories/information kiosks.

Cadillac Fairview's privacy policy did not make any mention of using facial recognition (or detection) technology.[123] Cadillac's practice of using facial recognition (detection) technology without gaining individual consent was the subject of a joint investigation by the Canadian federal, Alberta and British Columbia privacy commissioners ('the Privacy Commissioners').[124] The main focus was on the issue of whether Cadillac's use of 'anonymous video analytics' (AVA) technology in its interactive digital directories resulted in the collection, use or disclosure of personal information and, if so, whether Cadillac obtained adequate consent for the collection, use or disclosure of that information, including whether Cadillac retained the information longer than necessary. Cadillac argued that its practice in relation to the AVA software was not the collection of personal information because the stored gender and age estimates generated by the system are anonymous and could not be used, alone or in combination, with other information to identify an individual. The company is quoted as stating that its goal was to analyse the age and gender of shoppers and not to identify individuals.[125] This demonstrates that the emphasis on 'identifiability' means there are practices that organisations may not be recognising as the collection of personal information and requiring compliance with the *Privacy Act*.

The Commissioners found that the AVA technology:[126]

(i) took temporary digital images of the faces of any individual within the field of view of the camera in the directory [and that this was] retained in computer memory briefly during processing

(ii) used facial recognition software to convert those images into biometric numerical representations of the individual faces [which is] sensitive personal information that could be used to identify individuals based on their unique facial features

(iii) used that information to assess age range and gender.

The Commissioners noted that while they did not find any evidence that Cadillac had used the biometric information, including any of the retained numerical representations, for identification purposes, there had been the collection and use of personal information through the AVA technology without the requisite notice or consent.[127] It did not matter that the captured images of individual faces were kept only for a very short time. Further, the images captured by the technology were used to generate additional personal information including numerical representations, age range and gender of individual faces, which were then collected and retained for a much longer time period.[128] The Privacy Commissioners reasoned as follows:

> We accept that the demographic output generated by the AVA Technology, such as age and gender assessments, would not on their own, constitute personal information for the purposes of the Acts. That said, non-identifying information can be 'personal information' in context, and in this case, the demographic output was retained with other information including biometric information, location, and a timestamp. It is our view that the combination of this information raises a likelihood … that the individual could be identified. This is the case even though we found no evidence that CFCL attempted to

[122] Wacks, Privacy, 38.
[123] Cadillac Fairview, "Privacy Policy."
[124] Office of the Privacy Commissioner of Canada, "Joint Investigation of Cadillac."
[125] Office of the Privacy Commissioner of Canada, "Cadillac Fairview."
[126] Office of the Privacy Commissioner of Canada, "Joint Investigation of Cadillac," para. 2.
[127] Office of the Privacy Commissioner of Canada, "Joint Investigation of Cadillac," para. 2.
[128] Office of the Privacy Commissioner of Canada, "Joint Investigation of Cadillac," [71].

> identify individuals from this collected personal information. It is therefore our position that the demographic output also constitutes personal information in this context.

The ability to combine identifying information with non-identifying information is enough, then, to make information personal and subject to the protection of privacy legislation. Even if the step of identifying individuals is never taken, it is the potential to do so that means the information should be treated as personal information.

A secondary issue investigated by the Commissioners was whether Cadillac's use of mobile device geolocation technologies resulted in the collection, use or disclosure of personal information. The Commissioners found in this instance that Cadillac did not collect the location information of identifiable individuals through mobile device tracking technology. This was because there was no practical prospect of associating a hashed and randomised MAC address (device identifier) and the non-granular 'zone' geolocation information collected using Wi-Fi triangulation with a logged-in Wi-Fi account or an anonymous shopper journey. However, they noted that as a general principle, device identifiers can constitute personal information where they render a specific individual identifiable either alone or in combination with other information.[129] This case study demonstrates the contextual nature of the definition of personal information and how organisations will not always consider what they are doing to be subject to the *Privacy Act*.

C. Case Study 3: Westfield

Westfield (now known as Scentre Group) is a large shopping centre company with shopping centres throughout Australia and New Zealand. The media has reported on Westfield's use of digital advertising billboards to capture the age, gender and mood of passing customers to tailor advertisements.[130] According to Westfield's privacy policy:[131]

> audience measurement information collected passively using in centre technologies such as SmartScreen Advertising Units which utilise image processing software to aggregate data such as shopper numbers and demographics. These technologies do not identify individual shoppers, or record or retain images of individual shoppers.

Westfield refers to this information in its policy as 'other information we collect', an indication that they do not consider it 'personal information' but still pertinent enough to include in their privacy policy. The technology is not facial recognition but rather face detection, such that the collection of information is limited to age and gender rather than precise photo-matching databases to identify who customers are.[132] Even so, the technology would likely come as a surprise to most customers, particularly as, according to *The Guardian*, 'once the billboards have your attention they hit record, sharing your reaction with advertisers'.[133]

As the practice does not identify individuals or make them 'reasonably identifiable', it is unlikely to trigger the provisions of the *Privacy Act* because there is no capture of 'personal information' on a surface examination. However, there is the broader question of whether privacy is still infringed in circumstances in which an individual is not identified but is being targeted as part of a group and surveilled without their full awareness of the practice. Without a detailed explanation of how the technology works, it is possible that it is similar to the Cadillac Fairview example, in which the Canadian Privacy Commissioners found there were enough pieces of information retained by the software system to make the information personal in that context, despite Cadillac's lack of intention to identify people. If the cameras have the ability to recognise the mood of the passing individuals, then this suggests that at some stage in the process, a photo with good resolution must be taken to make that association.[134] This case demonstrates that privacy policies may not always make retail analytics practices entirely clear and that much depends on the company's interpretation of whether they are collecting personal information and, therefore, subject to privacy legislation.

D. Case Study 4: Amazon Go

Online retail giant Amazon has opened its own bricks-and-mortar convenience stores 'Amazon Go'. They follow a self-service model with no checkouts or cashiers. Patrons download the 'Amazon Go' app onto their device, link it to their Amazon account and scan their device as they enter the store.[135] The technology involves an array of cameras on the ceiling and on the shelves,

[129] Office of the Privacy Commissioner of Canada, "Joint Investigation of Cadillac," [144].
[130] Gillespie, "Are You Being Scanned?"
[131] Westfield, "Privacy Policy."
[132] Gillespie, "Are You Being Scanned?"
[133] Gillespie, "Are You Being Scanned?" para. 3.
[134] See generally on soft biometrics Denman, "Identifying Customer Behaviour," 202.
[135] Polacco, "The Amazon Go Concept," 79.

and sensors that detect which products are picked up from (or returned back to) the shelves[136] and adjust the customer's bill accordingly.[137]

The primary appeal for consumers seems to be the absence of queues to pay for goods, with an apparently seamless and fast shopping experience. However, the volume of data collected in the process, together with the privacy risks that this brings, is the trade-off.[138] Amazon Go has automated much of the purchase, checkout and payment steps associated with buying food.[139] The technology in combination is known as 'Just Walk Out Technology' and is responsible for keeping track of items taken from, and in some cases returned to, the store's shelves, and keeps track of the customer's virtual cart.[140] 'Just Walk Out' is comprised of:[141]

- an app using location-based services
- QR code IDs
- integrated payment
- image recognition
- multiple sensor technology
- artificial intelligence
- machine learning
- similarity to web shopping through just one click.

However, the extent of the privacy impact is more readily understandable with Miles's description of the technology:

> Amazon's convenience stores rely heavily on location technology to track consumers' movements inside buildings. Cameras analyze shopping behaviors, strategically placed microphones listen to conversations, and information about consumers' shopping habits is stored in a central database that Amazon can reference for future operational and strategic planning.[142]

This case study demonstrates the convenience offered by a 'just walk-out' smart-store is only possible through extensive data-gathering across several channels. If this style of store were rolled out more widely, then it seems that extensive surveillance would indeed be normalised and privacy concerns intensified. Customer convenience is unlikely to justify the reach of such surveillance infrastructure.

E. Case Study 5: 7-Eleven

Convenience store 7-Eleven has approximately 700 stores across Australia. Its practice of collecting customer facial images upon completing a customer survey was assessed by the Australian Office of the Information Commissioner (OAIC) in 2021.[143] Across mid-2020–2021, 7-Eleven administered a survey about customers' in-store experience via a tablet device. Each tablet included a camera that took facial images of the customer as they completed the survey. Facial images were stored on the tablet for about twenty seconds before being uploaded to a cloud-hosted service and deleted from the tablet. 7-Eleven's service provider processed the facial images by converting each facial image to an encrypted algorithmic representation of the face (faceprint), and then assessed and recorded inferred information about the customer's approximate age and gender. The faceprint was then sent to another piece of software along with all other faceprints generated by responses entered on the same tablet for the last twenty hours. This software searched for faceprints that were similar; if there was a high probability match, then this was flagged in the results. The objective was to identify responses that were not genuine and exclude them from the results. By March 2021, approximately 1.6 million survey responses had been registered.[144]

First, the Commissioner found that this was a collection of sensitive biometric information. She then held that risks associated with the collection of such information were not proportional to the function of understanding and improving customers' in-

[136] Browne, "Amazon Go Grocery."
[137] "Amazon Go Transforms Checkout."
[138] Miles, "Cashierless Stores."
[139] Ives, "Amazon Go?" 2.
[140] Polacco, "The Amazon Go Concept," 82.
[141] Ives, "Amazon Go?" 2.
[142] Miles, "Cashierless Stores," para. 3.
[143] *Commissioner Initiated Investigation into 7-Eleven Stores (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021).*
[144] *Commissioner Initiated Investigation into 7-Eleven Stores (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021)* [6].

store experience.[145] In particular, there were other ways in which the retailer could have identified potentially non-genuine responses and collected demographic information, which would have had a lesser privacy impact on individuals.[146] The OAIC was not satisfied that the large-scale collection of customers' facial images (sensitive biometric information) through 7-Eleven's feedback survey was 'reasonably appropriate and adapted' to understanding and improving customers' in-store experience.[147] The benefit to 7-Eleven 'was disproportionate to, and failed to justify, the potential harms associated with the collection and handling of sensitive biometric information'.[148] The Commissioner noted that biometric information is of particular sensitivity due to the risk of adversity to individuals where the information is misused or compromised, and that it cannot be reissued or cancelled like other forms of compromised information.[149] She found that this was in violation of APP 3.3, as the collection was not 'reasonably necessary' for 7-Eleven's functions.[150] Further, there was no evidence that individuals expressly consented to the collection of their facial images or faceprints.[151]

The case shows the OAIC using proportionality as a mechanism for assessing the necessity and legitimacy of a retailer's practice when assessing it against APP requirements for the collection of personal information. It is an example of a retailer's data-gathering practices being disproportionate in its effects on privacy when compared to the benefit it is aiming to pursue. Further, it demonstrates how retailers do not necessarily regard what they are doing as the collection of personal information. 7-Eleven had submitted that the facial images and faceprints were not personal information 'because they are not used to identify, monitor or track any individual'. The Commissioner did not accept this. The *Privacy Act*'s definition of personal information does not make any reference to the intentions of an organisation about what it is going to do with the information; the facial images here could identify individuals even if this was not what 7-Eleven intended to do with them.

V. Conclusion

These considerations highlight that the processes of data collection, storage and analysis that pervade the construct of the 'smart-store' lead to the creation of a sophisticated surveillance apparatus that is designed to monitor all aspects of customer behaviour and store use. The combination of technologies and the lack of transparency of collection practices is what distinguish retail analytics from traditional paper-based and in-person collection techniques. As argued, a key concern that arises from the use of retail analytics is that the implementation of the technology and retailers' legitimate commercial objectives come at a disproportionate cost to privacy, with often less intrusive measures being available. In particular, the case studies demonstrate how these practices entrench surveillance and datafication to such an extent that there is an erosion of privacy. The case studies also show the capacity of those technologies and how the average individual is largely unaware of the level of individual tracking that is taking place. Most individuals would be surprised to know that a retailer could deduce their pregnancy just from their shopping history, or that their image was taken and assessed biometrically when passing a digital screen at a shopping centre, or filling in a customer satisfaction survey. This article has argued that the smart-stores' intent of enhanced 'individualised relevance' is ultimately a privacy problem with its emphasis on datafication and the normalisation of surveillance through hyper-individualised targeting, tracking and monitoring. This overreach by retailers may be tempered by a better understanding of the value and importance of privacy in any decision-making about the implementation of particular retail analytic technologies.

Acknowledgement

I would like to thank Dr Andrew Fell and Associate Professor Mark Burdon for their input into this article. The views expressed in the article are my own and do not represent those of Queensland Health.

[145] *Commissioner Initiated Investigation into 7-Eleven Stores (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021)* [103].

[146] *Commissioner Initiated Investigation into 7-Eleven Stores (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021)* [103].

[147] *Commissioner Initiated Investigation into 7-Eleven Stores (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021)* [105].

[148] *Commissioner Initiated Investigation into 7-Eleven Stores (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021)* [105].

[149] *Commissioner Initiated Investigation into 7-Eleven Stores (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021)* [103].

[150] *Commissioner Initiated Investigation into 7-Eleven Stores (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021)* [107].

[151] *Commissioner Initiated Investigation into 7-Eleven Stores (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021)* [86].

Bibliography

"Amazon Go Transforms Checkout." *Mass Market Retailers*, 19 December 2016. https://www.massmarketretailers.com/amazon-go-transforms-checkout/

Attorney-General's Department. *Privacy Act Review Discussion Paper* (Australian Government, October 2021). https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf

Barocas, Solon and Helen Nissenbaum. "Big Data's End Run Around Anonymity and Consent." In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, edited by Julia Lane, Victoria Stodden, Stefan Bender and Helen Nissenbaum, 44–75. New York: Cambridge University Press, 2014.

Blumberg, Andrew J. and Peter Eckersley. *On Locational Privacy, and How to Avoid Losing It Forever* (Electronic Frontier Foundation, August 2009). https://www.eff.org/files/eff-locational-privacy.pdf

Bradlow, Eric T., Manish Gangwar, Praveen Kopalle and Sudhir Voleti. "The Role of Big Data and Predictive Analytics in Retailing." *Journal of Retailing* 93, no 1 (2017): 79–95. https://doi.org/10.1016/j.jretai.2016.12.004

Browne, Michael. "Amazon Go Grocery Expands Checkout-Free Shopping to Supermarket Concept." *Supermarket News*, 25 February 2020. https://www.supermarketnews.com/retail-financial/amazon-go-grocery-expands-checkout-free-shopping-supermarket-concept

Bullard, Brittany. *Style and Statistics: The Art of Retail Analytics*. Edited by Stacey Hamilton. Hoboken: Wiley, 2017.

Burdon, Mark and Alissa McKillop. "The Google Street View Wi-Fi Scandal and Its Repercussions for Privacy Regulation." *Monash University Law Review* 39, no 3 (2013): 702–738.

Cadillac Fairview. "Our Privacy Policy." Privacy Policy. Last modified 5 May 2021. https://www.cadillacfairview.com/en_CA/privacy.html#coverage3

Cazzato, Dario, Marco Leo, Paolo Spagnolo and Cosimo Distante. "Pervasive Retail Strategy Using a Low-Cost, Free Gaze Estimation System." In *Video Analytics for Audience Measurement*, edited by Cosimo Distante, Sebastiano Battiato and Andrea Cavallaro, 23–39. Cham: Springer, 2014.

Cheung, Anne. "Location Privacy: The Challenges of Mobile Service Devices." *Computer Law & Security Review* 30, no 1 (2014): 41–54. https://doi.org/10.1016/j.clsr.2013.11.005

ComQi. "Programming Your Store: Making the Most of In-Store Digital Technologies." *Journal of Retail Analytics*, no 1 (2015): 29.

Corrigan, Hope B., Georgiana Craciun and Allison M. Powell. "How Does Target Know So Much about Its Customers? Utilizing Customer Analytics to Make Marketing Decisions." *Marketing Education Review* 24, no 2 (2014): 159–166. https://doi.org/10.2753/MER1052-8008240206

Cox, Emmett. *Retail Analytics: The Secret Weapon*. Hoboken: Wiley, 2012.

Das, Subrata. *Computational Business Analytics*. Boca Raton: CRC Press, 2014.

De Hert, Paul and S. Gutwirth. "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action." In *Reinventing Data Protection?* edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt, 3–44. Dordrecht: Springer, 2009.

Denman, Simon, Alina Bialkowski, Clinton Fookes and Sridha Sridharan. "Identifying Customer Behaviour and Dwell Time Using Soft Biometrics." In *Video Analytics for Business Intelligence*, edited by Caifeng Shan, Shao-gang Gong, Tao Xiang and Fatih Porikli, 199–238. 1st ed. Berlin: Springer-Verlag, 2012.

Duhigg, Charles. "How Companies Learn Your Secrets." *New York Times*, 16 February 2012. http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Educause. "What Is Analytics?" Last updated 18 July 2012. https://www.youtube.com/watch?v=Gm-HbTvKw_0

Edwards, Charlotte. "Smile for the Camera: Creepy Billboards Are Tracking British Shoppers with Built-in Cameras That Target Ads Based on Your Mood." *The Sun*, 29 April 2019. https://www.thesun.co.uk/tech/8960640/creepy-billboards-track-with-cameras/

EKN. *State of the Industry Research Series: The Future of Retail Analytics* (EKN, 2013). https://www.sas.com/content/dam/SAS/en_us/doc/research2/ekn-report-future-retail-analytics-106717.pdf

Farinella, Giovanni, Giuseppe Farioli, Sebastiano Battiato, Salvo Leoniardi and Giovanni Gallo, 'Face Re-Identification for Digital Signage Applications' in *Video Analytics for Audience Measurement*, edited by Cosimo Distante, Sebastiano Battiato, Andrea Cavallaro, Springer 2014.

Farshidi, Ava. "The New Retail Experience and Its Unaddressed Privacy Concerns: How RFID and Mobile Location Analytics Are Collecting Customer Information." *Journal of Law, Technology and the Internet* 7, no 1 (2016): 15–38.

Gassen, Marius and Hervais S. Fhom. "Towards Privacy-Preserving Mobile Location Analytics." EDBT/ICDT 2016 Joint Conference, Bordeaux, France, 15 March 2016.

Gilley, Stephanie. *Mobile Device Tracking* (Federal Trade Commission, February 2014). https://www.ftc.gov/system/files/documents/public_events/182251/140219mobiledevicetranscript.pdf

Gillespie, Eden. "Are You Being Scanned? How Facial Recognition Technology Follows You, Even as You Shop." *The Guardian*, 24 February 2019. https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop

Hildebrandt, Mireille. "Who Is Profiling Who? Invisible Visibility." In *Reinventing Data Protection?* edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt, 239–252. Dordrecht: Springer, 2009.

Huang, Jiajin, Ning Zhong and Yiyu Yao. "A Unified Framework of Targeted Marketing Using Customer Preferences." *Computational Intelligence* 30, no 3 (2014): 451–474.

Hyunwoo, Hwangbo, Kim Yang Sok and Cha Kyung Jin. "Use of the Smart Store for Persuasive Marketing and Immersive Customer Experiences: A Case Study of Korean Apparel Enterprise." *Mobile Information Systems* 2017 (2017). https://doi.org/10.1155/2017/4738340

Information Commissioner's Office. *Wi-Fi Location Analytics* (ICO, February 2016). https://ico.org.uk/media/for-organisations/documents/1560691/wi-fi-location-analytics-guidance.pdf

Inman, Jeffrey and Hristina Nikolova. "Shopper-Facing Retail Technology: A Retailer Adoption Decision Framework Incorporating Shopper Attitudes and Privacy Concerns." *Journal of Retailing* 93, no 1 (2017): 7–28. https://doi.org/10.1016/j.jretai.2016.12.006

Ives, Blake, Kathy Cossick and Dennis Adams. "Amazon Go: Disrupting Retail?" *Journal of Information Technology Teaching Cases* 9, no 1 (2019): 2–12. https://doi.org/10.1177/2043886918819092

Kang, Jerry. "Information Privacy in Cyberspace Transactions." *Stanford Law Review* 50, no 4 (1998): 1193–1294. https://doi.org/10.2307/1229286

Karyda, Maria, Stefanos Gritzalis, Jong Hyuk Park and Spyros Kokolakis. "Privacy and Fair Information Practices in Ubiquitous Environments." *Internet Research* 19, no 2 (2009): 194–208. https://doi.org/10.1108/10662240910952346

King, Nancy J. and Pernille Wegener Jessen. "Profiling the Mobile Customer: Privacy Concerns When Behavioural Advertisers Target Mobile Phones, Part I." *Computer Law & Security Review* 26, no 5 (2010): 455–478. https://doi.org/10.1016/j.clsr.2010.07.001

LeClaire, Jennifer, Danielle Dahlstrom and Vivian Braun. *Business Analytics in Retail for Dummies*. 2nd IBM limited ed. Hoboken: Wiley, 2014.

Lindsay, David. "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law." *Melbourne University Law Review* 29, no 1 (2005): 131–178. http://www5.austlii.edu.au/au/journals/MelbULawRw/2005/4.html

Little, Jonathon and Alexander Brown. "Someone to Watch over You." *Computer Law & Security Review* 22, no 2 (2006): 169–171. https://doi.org/10.1016/j.clsr.2006.01.001

Mai, Jens-Erik. "Big Data Privacy: The Datafication of Personal Information." *The Information Society* 32, no 3 (2016): 192–199. https://doi.org/10.1080/01972243.2016.1153010

Manwaring, Kayleen. "Will Emerging Information Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation." *Competition & Consumer Law Journal* 26, no 2 (2018): 141–181.

Max, Ronny. "A Brief History of Location Analytics." *LinkedIn*, 15 July 2016. https://www.linkedin.com/pulse/brief-history-location-analytics-ronny-max/

———. "Nineteen Technologies of People Tracking." Last updated 2021. http://www.behavioranalyticsretail.com/7-technologies-to-track-people/

Mayer-Schönberger, Viktor and Kenneth Cukier. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Mariner Books, 2014.

Mejias, Ulises A. and Nick Couldry. "Datafication." *Internet Policy Review* 8, no 4 (2019): 1–10. https://doi.org/10.14763/2019.4.1428

Michael, Katina and Roger Clarke. "Location and Tracking of Mobile Devices: Überveillance Stalks the Streets." *Computer Law & Security Review* 29, no 3 (2013): 216–228. http://doi.org/10.1016/j.clsr.2013.03.004

Miles, Stephanie. "Do Cashierless Stores Present a Privacy Risk to Consumers?" *Street Fight*, 30 January 2020. https://streetfightmag.com/2020/01/30/do-cashierless-stores-present-a-privacy-risk-to-consumers/#.X863a7NS-70

Milesi, Katherine, David White, Jean-Baptiste Vincent and Damien Ballesty. *Navigating the New Digital Divide: Digital Influence in Australian Retail 2015* (Deloitte Digital, 2015). https://www2.deloitte.com/content/dam/Deloitte/au/Documents/technology/deloitte-au-technology-digital-divide-140715.pdf

Mogg, Trevor. "It's No Dummy: Camera-Equipped Mannequins Being Used by Stores to Help Boost Sales." *Digital Trends*, 20 November 2012. http://www.digitaltrends.com/cool-tech/its-no-dummy-camera-equipped-mannequins-being-used-by-stores-to-help-boost-sales/

Mohanty, Soumendra, Madhu Jagadeesh and Harsha Srivatsa. *Big Data Imperatives: Enterprise Big Data Warehouse, BI Implementations and Analytics*. 1st ed. Berkeley: Apress, 2013.

Office of the Privacy Commissioner of Canada. "Cadillac Fairview Collected 5 Million Shoppers' Images." News release. 29 October 2020. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_201029/

———. “Joint Investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia.” Last modified 29 October 2020. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/

O'Mallon, Finbar. 'Westfield is Watching: Shopping Centre Wi-Fi Logs Location, Web Traffic' *Canberra Times* 3 March 2017. https://www.canberratimes.com.au/story/6036790/westfield-is-watching-shopping-centre-wi-fi-logs-location-web-traffic/

Pantano, Eleonora and Charles Dennis. *Smart Retailing: Technologies and Strategies*. Cham: Palgrave Pivot, 2019.

Polacco, Alex and Kayla Backes. “The Amazon Go Concept: Implications, Applications, and Sustainability.” *Journal of Business and Management* 24, no 1 (2018): 79–92. https://doi.org/10.6347/JBM.201803_24(1).0004

Randhawa, Ramandeep S. “Retail Analytics.” In *Essentials of Business Analytics*, edited by Bhimasankaram Pochiraju and Sridhar Seshadri, 599–622. Cham: Springer, 2019.

Roberts, Andrew. “Bionic Mannequins Spy on Shoppers to Boost Luxury Sales.” *Bloomberg*, 22 November 2012. http://www.bloomberg.com/news/articles/2012-11-19/bionic-mannequins-spy-on-shoppers-to-boost-luxury-sales

Scanlon, Thomas. “Thomson on Privacy.” *Philosophy and Public Affairs* 4, no 4 (1975): 315–322.

Shan, Caifeng, Fatih Porikli, Tao Xiang and Shao-gang Gong, eds. *Video Analytics for Business Intelligence*. 1st ed. Berlin: Springer-Verlag, 2012.

ShopSmart. “How and Why Retail Stores Are Spying on You.” *Consumer Reports*, March 2013. http://www.consumerreports.org/cro/2013/03/how-stores-spy-on-you/index.htm

Sightcorp. “Sightcorp Face Analysis Technologies: Overview.” https://sightcorp.com/technologies-overview/.

Simmel, Arnold. “Privacy Is Not an Isolated Freedom.” In *Privacy and Personality*, edited by J. Roland Pennock and John W. Chapman, 71–87. New Jersey: Transaction Publishers, 2007.

Spencer, Shaun B. “Privacy and Predictive Analytics in E-Commerce.” *New England Law Review* 49, no 4 (2015): 629–647.

Strandburg, Katherine. “Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context.” In *Privacy, Big Data, and the Public Good*, edited by Julia Lane, Victoria Stodden, Stefan Bender and Helen Nissenbaum, 5–43. Cambridge: Cambridge University Press, 2014.

Technopedia. “Location Analytics.” Last modified 22 August 2016. https://www.techopedia.com/definition/30338/location-analytics

Tene, Omer and Jules Polonetsky. “Judged by the Tin Man: Individual Rights in the Age of Big Data.” *Journal on Telecommunications & High Technology Law* 11, no 2 (2013): 351–368.

Testori, Matteo. “The Applications of Video Analytics in Media Planning, Trade and Shopper Marketing.” In *Video Analytics for Audience Measurement*, edited by Cosimo Distante, Sebastiano Battiato and Andrea Cavallaro, 3–20. Cham: Springer, 2014.

Tickto. “Behavioural Analytics: 5 Customer-Tracking Technologies.” 2016. http://tickto.com/behavioral-analytics-5-customer-tracking-technologies/#

Turow, Joseph, Lee McGuigan and Elena R. Maris. ‘Making Data Mining a Natural Part of Life: Physical Retailing, Customer Surveillance and the 21st Century Social Imaginary.” *European Journal of Cultural Studies* 18, no 4–5 (2015): 464–478. https://doi.org/10.1177/1367549415577390

Ventura, Richard. “Retail in the Digital Era: Combining Analytic Technologies with Digital Signage to Boost Sales and Engagement.” *Journal of Retail Analytics* 12, no 3 (2016): 19.

Wacks, Raymond. *Privacy: A Very Short Introduction*. 2nd ed. Oxford: Oxford University Press, 2015.

Westfield. “Security and Privacy Policy: Scentre Group Privacy Policies.” Last modified 1 December 2020. https://www.westfield.com.au/privacy-policy

Westin, Alan. *Privacy and Freedom*. New York: Atheneum, 1967.

Primary Legal Materials

Commissioner Initiated Investigation into 7-Eleven Stores (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021).

Explanatory Memorandum, *Privacy Bill 1988* (Cth).

Privacy Act 1988 (Cth).

Privacy Commissioner v Telstra [2017] 249 FCR 24.

Telecommunications (Interception and Access) Act 1979 (Cth).