Chapter 3
Privacy in Location-Sensing Technologies

Andreas Solti, Sushant Agarwal, and Sarah Spiekermann-Hoff

Abstract Data analysis is becoming a popular tool to gain marketing insights from heterogeneous and often unstructured sensor data. Online stores make use of click stream analysis to understand customer intentions. Meanwhile, retail companies transition to locating technologies like RFID to gain better control and visibility of the inventory in a store. To further exploit the potential of these technologies, retail companies invest in novel services for their customers, such as smart fitting rooms or location of items in real time. In such a setting, a company can not only get insights similar to online stores, but can potentially also monitor customers. In this chapter, we discuss various location-sensing technologies used in retail and identify possible direct and indirect privacy threats that arise with their use. Subsequently, we present technological and organizational privacy controls that can help to minimize the identified privacy threats without losing on relevant marketing insights.

3.1 Introduction

The era of sensing technologies has already begun. We use smart devices (e.g., smart phones, smart watches, smart cars, smart clothes) in our daily lives and we often cannot imagine life without internet and being online every day. The acceleration of technological progress offers ever new use cases of sensing technologies. Organizations that heedlessly implement novel use cases as they become technically feasible without considering the privacy implications to users or employees risk losses in reputation and trust [6]. Therefore, it is crucial to be aware of the privacy implications of the used technologies. Privacy risks caused by the use of information technology are rooted in operators' ability to permanently save and link information about sensed individuals [76, 83]. The anxiety of the general public with

A. Solti · S. Agarwal (✉) · S. Spiekermann-Hoff
Vienna University of Economics and Business, Vienna, Austria
e-mail: solti@ai.wu.ac.at; sagarwal@wu.ac.at; spiek@wu.ac.at

A. Gkoulalas-Divanis, C. Bettini (eds.), *Handbook of Mobile Data Privacy*,
https://doi.org/10.1007/978-3-319-98161-1_3

these technologies is exemplified in newspaper articles that use the term “privacy snatchers” [16] to refer to organisations monitoring workers or customers.

Throughout this chapter, we will look at the everyday example of how brick-and-mortar retailers use locating technologies to gain a better understanding of their customers. In contrast to online retailers that can tap into a rich source of information in terms of browsing behaviour of customers through click stream analysis, brick-and-mortar retailers are only recently investigating location-sensing technologies for gaining similar insights about the physical movements and behaviours of customers in shop floors. For example, radio-frequency identification (RFID) technology can detect with which items customers interact on their shopping trip. An information that is very interesting for retailers from a marketing perspective. Additionally, location-sensing technologies enable novel services for customers (e.g., locating an item, automating checkout). While such services may be interesting for the company, they often come at the risk of compromising privacy of users. This is especially the case, as the locating-technologies used are pervasive and do not generally alert the users when information is collected from them. From the legal perspective, companies need to avoid unlawful handling of privacy sensitive data. Otherwise, they risk not only a loss in reputation and trust, but also substantial fines. In the EU, for example, the new regulation extends the upper limit of fines for privacy infringements to 20 million EUR, or 4% of the annual world-wide turnover of an organisation (whichever is greater) [81]. For both organisations and users it is, however, crucial to be aware of the interplay between different technologies, the use cases supported, and the direct and indirect privacy threats entailed by using these novel technologies. In this chapter, we investigate this interplay to offer an overview and also present privacy controls that can help to minimise the identified privacy threats without losing on relevant information. Organisations that use these technologies have the responsibility to make customers aware about the technologies used and the information gathered by them. The chapter is organised as follows. Section 3.2 presents use cases that are enabled by location-sensing technology in the retail sector. In Sect. 3.3, we introduce various location-sensing technologies and compare them. We also list the privacy threats that are associated to automated location-sensing. Section 3.4 exemplifies the interplay of technology, usecases and associated privacy threats in popular scenarios in retail. Specifically, we focus on RFID and WiFi and their combination. Last, in Sect. 3.5, we present privacy controls. These controls minimise the possible privacy threats using location-sensing technologies in different scenarios. We conclude this chapter in Sect. 3.6.

3.2 Use Cases of Location-Sensing Technologies in Retail

Retailers are interested in improving their service quality to increase customer satisfaction [72], and in maximising their profits. In this chapter, we focus on how location-sensing technologies enable location-based services. To clarify terminology, location-based services belong to the general class of context-based services, where context is defined by Abowd et al. [2] as:

> "any information that can be used to characterize the situation of entities (i.e., whether a person, place or object) that are considered relevant to the interaction between a user and an application, including the user and the application themselves"

We restrict our analysis to *location* as one of the most important contextual feature in this chapter, but also discuss features that can be derived from location-sensing technology. For a broader discussion on context-aware systems, we refer to the survey by Baldauf et al. about context-aware systems and their support for security and privacy [14] and the textbook in the field of ubiquitous computing edited by Krumm [50].

Location-sensing technologies create novel use cases to increase service quality, or assist existing use cases by gaining more transparency about the customer behaviour in the retail environment.

While online retailers rely on a rich information source of customer behaviour through click-stream analysis to provide recommendations (e.g., by analysing the online browsing and search histories), brick and mortar retailers are often blind to their customers' behaviour in their shops. For decades, they employed market researchers who would follow customers around in stores to better understand the needs of customers. With location-sensing technologies, brick and mortar retailers can automatically gain insights into the interests of customers, and can react to their location context. We distinguish management use cases, marketing use cases, and operational use cases.

3.2.1 Management Use Cases

Management is typically interested in the aggregate performance of a store and the trend of the performance over time. Several *performance indicators* can be supported with location-sensing technologies. For some of them, point of sales data needs to be integrated [18]. Generally, the behaviour before, during and after the consumption can be defined as product information browsing, consumption and product usage, respectively [69], and this behaviour information can be collected using location-sensing technologies. Management use cases include any type of analysis of this information. We briefly sketch the most important use cases here that can be based on location-sensing:

Conversion rates One of the simplest location-based indicators are conversion rates. For example, a measure of interest is the conversion rate of passersby into shop visitors [17]. Another important measure is the fraction of entering customers that purchases products. When location-sensing technologies track customers' behaviour in the shop, it is possible to gather more fine-grained information and these conversion rates can be partitioned into product categories [89]. One example is to measure the number of visitors to a store section (e.g., the area where jackets are on display) and relate it to the number of purchases that contained the category (e.g., jackets).

Length of stay Other interesting insights that can be of managerial relevance are length of stay of customers. This measure positively correlates with the probability of making a purchase (e.g., through impulse buying). Being able to automatically measure the length of stay as an indicator can help for example to select background music that increases the length of stay [61].

Queuing times Location-sensing technologies can be used to extract waiting times of the location data. Of particular interest are the queuing times at service stations like the point of sales, or also fitting rooms in the context of fashion retail. Studies show that waiting time influences perceived service quality [51]. Therefore, timely control of these measures is important to balance service quality and resource utilisation.

Store layout optimisation The optimisation of the store layout is important to maximise profit [55]. The layout can profit from additional location information that is available, when customer movement patterns are analysed. Furthermore, novel layouts can be quickly tested for operational efficiency by analysing the changes in customer movement patterns.

3.2.2 Marketing Use Cases

For marketing purposes, we consider interactions with the customer. We exemplify a few location-based use cases here, and refer to the survey of Adomavicius and Tuzhilin [4] and the handbook by Ricci et al. [71] for more general recommendation concepts.

Geofencing The idea of geofencing, that is triggering notifications based on entering or leaving a defined area boundary (i.e., the geofence) belongs to location based services [17]. Geofencing in retail environments resembles traditional market places, where the passing customers heard the voices of the nearby sellers advertising special deals, when getting closer the their booths. The difference is that the marketing is now automated, and the customers that are detected in the defined areas get push notifications on their smart devices.

Context-aware browsing More subtle than getting push notifications, when entering an area, context-aware browsing changes the services offered when browsing the web based on the context of the user [20, 29, 63]. In the retail domain, this can for example be applied to smart screens in the store that react on the items carried by the customer. Also the online shop offering to customers accessing the store with their mobile devices can be adapted based on the customer's location. Here, changing the order of items or recommendations in the online shop based on the shopper's distance to the items.

3.2.3 Operational Use Cases

Location-based sensing technology enables further use cases besides management and marketing that support daily operations. We mention some of the more common use cases in the following.

Preventing theft Location sensing of items in a brick and mortar retail environment can be used to trigger an alarm, when items pass the boundaries of the defined shopping area without having checked them out before [86].

Locating products When location-sensing technology [41] is harnessed to track the whereabouts of products, the primary novel use case is locating the products in case a client is looking for it. This use case is often supported by RFID technology based on passive RFID tags, as it is affordable to equip every item with a unique identifier. In case an item is requested, the system can be asked about the assumed position of that item, to potentially avoid a time consuming search, when the item is not at its allocated position.

Replenishing products Location-sensing applied to products has another important use case, which is replenishment of items. Typically, an item needs to be replenished, when items are sold to customers and this type of replenishment does not depend on location-sensing technologies. However, there are further reasons for items disappearing from the sales floor, which is referred to as retail shrinkage (e.g., stolen items). In these cases, location-sensing technologies can help to detect shrinkage and allow more timely replenishment in that case [27]. Furthermore, if the item is only misplaced, locating technologies can prevent unnecessary orders of available items.

Path/Layout optimization When multiple tasks need to be performed at different locations (e.g., the items of an order need to be collected from different positions) workers can be assisted to save time and traveled distance by optimizing their paths through the shop or back room [85]. Location-sensing technology can assist here to adjust the proposed path to the items and the worker's current positions. Also customer paths can be analysed and taken into consideration for store layout optimization [23].

Waiting time estimation Knowing the expected waiting time at a queue has a positive influence on perceived service quality (as long as the expectations are reliable) [51]. A good waiting time estimator in stable systems is asking the last person that exited the queue about their waiting time. There are systems that measure the waiting time by requiring customers to draw a number from the system, when they enter the queue to measure the time. Location-based sensing allows us to collect the information from the location data and enables the use case of informing customers about their expected waiting time in front of fitting rooms or checkout.

Automated checkout Perhaps one of the technically more advanced use cases that use location sensing is the automated checkout of items at the point of sale. RFID technology is an enabler for this technology, and mobile applications installed on smart devices allow identification of customers. Recently, prototypes for this use case have emerged [87].

To sum up, the new use cases of location-sensing technology are manifold, and more and more of them emerge, as combinations of different technologies and information sources are explored. In the next section, we provide an intuition on the methods for location sensing and compare technologies that can be used for this purpose.

3.3 Location-Sensing Technologies and Entailed Privacy Threats

We first introduce location sensing technologies and compare them to each other. An organisation wanting to deploy location-sensing technologies has to be aware of the ensuing privacy issues and legal demands. Thus, we discuss and categorise privacy issues by focusing, in particular, on concrete privacy threats arising on the technical level.

3.3.1 Introduction to Location-Sensing Technologies

Location sensing refers to the process of obtaining location information of a mobile agent with respect to a set of reference positions in a predefined space [35, 56]. The most common techniques for location sensing are trilateration and fingerprinting. In this section, we discuss on a high level how these two techniques work and discuss different technologies with which they can be enabled.

3.3.1.1 Locating Objects by Trilateration and Fingerprinting

Trilateration is a method to determine absolute or relative location of an object based on measurement of distances from three known points [84]. Figure 3.1 illustrates the process where for an object the distance is known with reference to three points X1, X2 and X3. With respect to point X1, see Fig. 3.1a, the radial distance is r1 and based on this information the item lies somewhere on the circumference of the highlighted circle. Then if we consider the distance from the second point X2, as shown in Fig. 3.1b, the item can lie on either points of intersection of the two circumferences, marked by A and B. Finally, if distance from all the three points is considered, as shown in Fig. 3.1c, then location of the item can be concluded, marked as B. This illustration works for location-sensing in a 2D space. If the position of an object is to be estimated in 3D space, we need a fourth reference point. In practice there are usually imprecisions regarding the distance to a reference point, which affect the accuracy of the estimated position [13, 58]. Therefore, more than three reference points are often used to increase the accuracy.

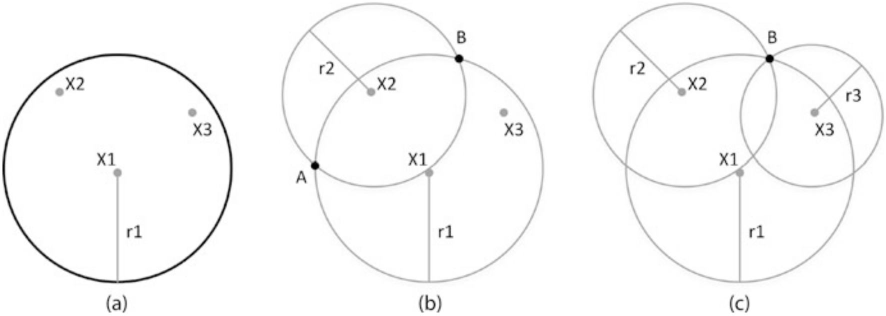

Fig. 3.1 Illustration for trilateration

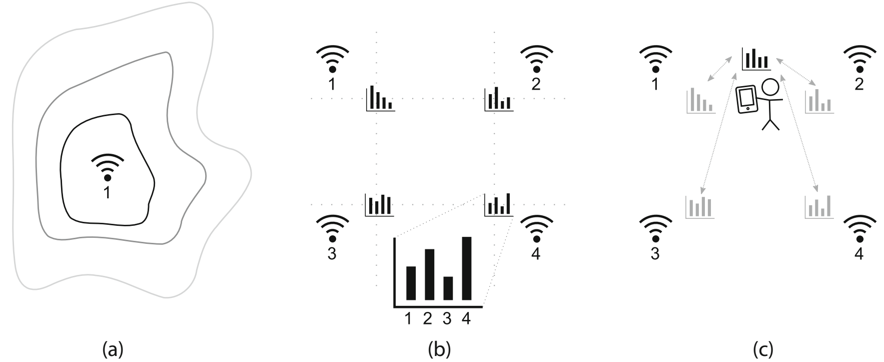

Fig. 3.2 Illustration for 2-step fingerprinting. (**a**) and (**b**) depict the first step for training and (**c**) shows the second step for positioning

The process of trilateration can be used in different ways to estimate the location: For satellite-based applications, estimation is done through measuring the time taken for a radio signal to travel from the transmitting satellites to a receiver and then multiplying it with the speed of the wave [68]. For applications like WiFi and Bluetooth it is done via measuring the received signal strength (RSS), a measurement of the power present in a received radio signal [90]. Trilateration generally works well outdoors. But due to obstacles like walls, street canyons, roofs, floors etc. the radio signals do not propagate linearly and get attenuated indoors. As a result, accuracy levels for location estimation goes down.

To attain better accuracy, a 2-step process called *fingerprinting* is used [12]. To model the attenuation, multiple reference points are considered and parameters (like signal strength) are calculated for these points. This step is called the training or calibration stage. The second step is the positioning stage where the parameters are recorded at the device's location and these parameters are then compared to the reference points to estimate the location. In other words, in the training step a fingerprint for the signals is created and in the positioning stage, the parameters are measured and compared with the fingerprints to ascertain the location. Figure 3.2

shows the two stages of fingerprinting for radio signals (such as WiFi, bluetooth or cellular signals). For the first stage, received signal strength (RSS) is measured for the radios, Fig. 3.2a shows the distorted radio signal in a field that is attenuated by obstacles. Figure 3.2b shows the training phase, where measurements at known positions (for example in a grid) are taken and recorded. Then, in the second stage, the RSS values are measured for a user (Fig. 3.2c) and compared with the data collected in the training stage. Thus, by comparing the RSS data with training data, the location is estimated.

In the following, we describe a multitude of technologies that allow location-sensing by a system with the help of trilateration and explore their feasibility of use. As outlined above, We will approach these technologies from the perspective of brick-and-mortar retail shops.

3.3.1.2 Satellite-Based Location Sensing

Smart devices capable of satellite based navigation have an integrated receiver to communicate with the satellites. The most commonly used navigation system as of 2017 is the Global Positioning System (GPS). To get an estimation of the position, the receiver needs to be in line of sight of at least satellites and solid objects like buildings, caves etc. attenuate the signals drastically. Hence, satellite navigation works well outdoors but cannot be used extensively for indoor location tracking. Also, as there is only a receiver in the devices for satellite communication, no information is directly transmitted to the satellites or any server. Thus to gain location information of such a device, a retailer has to request customers to install an app or visit their website where the device owner (customer) grants the retailer access to the device's location.

3.3.1.3 WiFi Based Location Sensing

WiFi technology enables devices to connect to a network wirelessly. Every networking chip or interface in these devices has a unique identifier called media access control (MAC address) which is broadcasted to wireless access points in range if WiFi is turned ON in the device. Uniqueness of the MAC address can be used to ascertain if a WiFi enabled device is in a proximity. For instance, it can be used to count unique customers (with a WiFi enabled device) in stores [5]. This method can further be extended by keeping two WiFi access points (A and B) and then analysing the pattern of movement of customers/devices, such whether A or B has a higher count or are customers spending more time around A or B etc. This can further be extended if an array of WiFi access points are setup. In this case, based on trilateration (similar to satellite-based location sensing systems) and the received signal strength indicator (RSSI) for each connection, location can be estimated as well as tracked [57]. Thus, by just measuring the signal strengths and the MAC addresses, the retails can track location as well as movement of customers who carry a WiFi enabled device without requesting the customer to install any extra application for such a purpose. This only works though if the WiFi is switched ON in a device. An American fashion retailer, Nordstrom, used this technology in 2012–2013 to track the customers in 17 of its stores [24] and that hampered the retailer's brand-image. Though Nordstrom ended WiFi tracking after the protests, based on the media reports, WiFi tracking is still harnessed in thousands of retail stores around the world [48].

3.3.1.4 Bluetooth Based Location Sensing

Bluetooth beacons are low-power radio transmitters which send signals in immediate vicinity using bluetooth. Martin, in his article in Harvard Business Review, refers to beacons as the *missing piece in the mobile-shopping puzzle* as they allow precise targeting of customers in a certain area [60]. Using beacons, retails can push a message, advertisement or even coupons to a customer's device. Similar to WiFi based sensing, if a cluster of these beacons are used then RSSI can be analysed for computing the location of a device [52]. In retail, beacons are currently used for pushing offers, but places like Eldheimar museum, Iceland use bluetooth beacons for indoor location sensing [77].

3.3.1.5 Cellular Tower Based

Trilateration or 2-stage fingerprinting can also be used based on the analysis of RSSI from the cellular network antennas to calculate locations of devices with cellular radios [42]. Research has shown that by just using four different location points calculated using the RSSI, more than 90% of the individuals can be uniquely identified[26]. Thus, just by sensing the location of a device, a few times in a day, there is a potential to differentiate or uniquely identity that device in a database of thousands of other devices. This method is not popular in the field of retail, however, emergency services generally use this information to estimate location of devices [34].

3.3.1.6 Ultrasonic Waves Based

Interestingly, even speakers/microphones present in smart devices can be used to track the location. Using ultrasonic sounds (inaudible to humans), it is possible to estimate distances based on the sound volume of the received signal. Thus, unlike other technologies they use sound instead of radio signals. Based on the arrangement, a customer's device can either act as a transmitter if it generate the sound signal or as a receiver if it listens to such sounds through the microphone. However, for sensing location using this technology, retailers need to convince their customers to install app with privileges to access the microphone and or speakers. In the recent past, this technology was exploited to provide analytics for

TV based advertisements [8]. In the advertisements, firstly some unique ultrasonic sound signals were attached. Secondly, malicious apps were pushed on devices like computers, tablets and cellphones which were listening and analysing ultrasonic sound signals 24 hours a day. Based on the analysis of received sound signals, the company provided rich insights like % of people watching the advertisements etc. [8].

3.3.1.7 RFID Based Location Sensing

By analysing the RSSI of the RFID tags, it is possible to estimate the rough distance of the tag from a reader [22]. If an array of RFID readers are used then through trilateration, location of tags can be estimated. Such systems, tracking location in real-time are referred to as RFID enabled Real-Time Locating Systems (RTLS) [75]. In retail, RFID tags can be added to loyalty cards, shopping baskets or even with the items on sale (either as price tags or integrated in the items) [33].Thus, movement of RFID tags could relate to the movement of people and provide additional insights to the retailers. In addition to retail, RFID tags have been used in hospitals to track movement of customers [46] and in schools to monitor the students [49].

3.3.1.8 Comparison of Technologies' Sensing Accuracy and Prerequisites

Following Table 3.1, based on Hazas et al. paper [42], compares the discussed technologies based on the requirements, accuracy and ability to track indoors. For a

Table 3.1 Comparison of different technologies for location tracking [43]

Tech	Accuracy	Indoors	Whats tracked	Prerequisites for customers to be tracked
Satellite	5–10 m	No	Devices	• Device with appropriate receiver • Application with location access internet access • Internet to share location information
WiFi	10–50 m	Yes	Devices	• Device with WiFi capability • WiFi turned on
Bluetooth	5–10 m	Yes	Devices	• Bluetooth enabled device • Some application with internet access to communicate with beacons • Internet to share beacon information
Cell tower	50–100 m	Yes	Devices	• Device with cellular capability • Some application with access to internet and network information • Internet to share network information
Ultrasonic	1–10 m	Yes	Devices	• App with permission to send/listen ultrasonic signals • Internet to share beacon information
RFID	1–10 m	Yes	Tagged items	None

more exhaustive analysis, survey by Liu et al. can be referred where they discuss 20 different solutions for indoor location sensing [56].

For the discussed use cases, Satellite based tracking is not the preferred option for the retail sector as it does not performs well in indoor conditions. Similarly, cell tower based tracking has low accuracy which makes it unattractive for the retail purpose. For Bluetooth and ultrasonic based tracking, the customers, currently need to install an extra application on their smart devices to enable the retailers for tracking them. On the other hand, WiFi and RFID based tracking are two options which do not require any extra application on customers' smart devices for retailers to track them. For WiFi, the main limitation is that the customers must carry a WiFi enabled smart device with WiFi radio turned on. This is increasingly common as many users want to connect to their home WiFis automatically and therefore keep their WiFi access enabled on their phones. For RFID, there is finally no user access activity required. The infrastructure can be set up and used by the retailers without customer knowledge and involvement. For instance, attaching RFID tags to shopping carts or simply tagging the shelved products, retailers can locate and track the movement of customers. Thus, for this chapter, we focus on WiFi and RFID based tracking as these technologies can potentially be used without any active consent of the customer.

3.3.2 Associated Privacy Threats

In IT, a threat is commonly defined as a *potential cause of an incident that may result in harm of systems* [44]. A privacy threat can therefore be understood as a potential cause of an *incident*, which may again cause *harm* to an individual's privacy. We focus on the technical causes or activities resulting in privacy harms without considering the impact of harm. Impact is subjective and varies on a case by case basis, depending on the type of data involved, privacy expectations etc. Thus, first, we discuss the different activities which lead to privacy harms. Second, we present a general overview about how these activities materialise for RFID and WiFi based location sensing. For further reading, we refer to extensive survey works on the topic of privacy threats with RFID and wireless technologies [38, 45, 53, 88].

3.3.2.1 Classification of Privacy Harms

Privacy is defined as an elusive concept [74] and there is a little agreement on how to define it [62]. As such, this makes it difficult to base the threats to privacy on its definition. Solove [73] instead of defining privacy, discusses different activities which lead to privacy harm and classifies them. He categorises the activities that cause privacy harm in four high level groups which are then further classified into 16 different forms [73].

Information collection relates to the process of data gathering
Surveillance—watching, sensing or recording an individual's activities or
Interrogation—questioning or probing the individual for information

Information processing relates to the activities involving storage of the collected information, its manipulation and the use
Aggregation—combining different pieces of information about an individual
Identification—linking the information to the identity of individuals
Insecurity—carelessness in protecting the collected information
Secondary Use—using the collected information for a different purpose
Exclusion—keeping individuals unaware about their collected information

Information dissemination relates to the activities involving revealing, sharing or spreading information about the individuals
Breach of confidentiality—breaking a promise to keep individual's information confidential
Disclosure—revealing true information about an individual
Exposure—revealing intimate information such as nudity, grief etc.
Increased accessibility—easing the accessibility of information by third parties
Blackmail—threatening to disclose the information
Appropriation—faking the individual's identity for mala fide interests
Distortion—disseminating false and misleading information about individuals

Invasion impinging privacy by other means, not necessarily with the use of information
Intrusion—disturbing an individual's solitude
Decisional interference—government's unwanted incursion into an individual's decisions about their private life

As such, for the chapter we focus on a retail scenario and so we discuss only the threats which are directly related to the technology. Thus, we rule out interrogation and blackmailing as they are not directly related to RFID or WiFi. Also intrusion and decisional interference are not considered as these are not dependent on the use of information. We use this classification in the next section to understand the associated privacy threats. After discussing what can cause privacy harm, let us now focus on specific technologies, WiFi and RFID to understand how these harms are materialised.

3.3.2.2 Realisation of Privacy Harms Using RFID and WiFi

For RFID based tracking, companies track the items with RFID tags and then later associate with the customers. For WiFi, a customer's device is tracked to estimate the location. Privacy of customers is compromised not only by sensing the exact location but also due to processing which combines other data sources as well for rich insights about customers, for e.g. inferring preferences of customers based on the time spent in different areas of the store. Thus, we discuss the activities described by Garfinkel et al. [38] through which privacy can be comprised with the use of RFID in retail through:

Action movement of an item triggers an action, for e.g. the disappearance of items from sensors could yield in an action of a photograph taken

Association individuals are correlated with the RFID tags they interact with, e.g. customers are associated with items they pick in a store

Location individual's position is tracked, e.g. in a retail store if an individual picks an item then movement of the item can give information about location of the individual

Inferred preferences individual's preferences are estimated by associating the carried RFID tags, e.g. if an individual picks up sports garments then RFID tag of the garment can provide information about the possible preferences of that individual

Estimation of constellation a combination of several tags used lead to a unique digital fingerprint [91] e.g. combination of different items can lead to the uniqueness of the shopping basket, creating unique constellation or group of items which can differentiate individuals

Transaction transactions or relations can be inferred based on the movement of tags from one constellation to the other, e.g. individuals shopping together can be identified if they exchange some products during a shopping trip

"Breadcrumbs" wrong association or association of discarded items can lead to false inference, e.g. if an individual picks up an item and later discards it then in case another individual picks up that same item, latter can be wrongly associated with the identity of the first individual

For WiFi based location sensing, only the customers' devices can be tracked. As customers are already uniquely identified based on the devices, *estimation of constellation* and *associations* are not applicable. Similarly, *transactions* cannot be identified as device exchange during a trip cannot be analysed and *actions* affecting privacy are difficult to trigger. On the other hand, *location* of the devices can be tracked, time spent in different sections can lead to *inferred preferences*. *Breadcrumb* threat is still valid if different customers carry the same device at different times (e.g. families or friends sharing a device, customers selling devices to others etc.). The activities harming privacy by using WiFi are hence a subset of the list discussed for RFID. Thus, the classification by Garfinkel et al. provides an exhaustive list for the ways through which privacy can be possibly compromised by using RFID as well as WiFi based tracking. Let us now consider some specific scenarios where RFID and WiFi based tracking is used for the use cases discussed in Sect. 3.2.

3.4 Analysis of Popular Location-Sensing Scenarios in Retail

We consider different scenarios that are relevant for brick-and-mortar retailers that plan to use, or already use location-sensing technologies, and are also relevant to customers confronted with these technologies in their daily life. We introduce the scenarios in order of increasing amount of accumulated location information about customers. Therefore, we first investigate RFID-based scenarios, then turn to WiFi-based scenarios and last consider the combination of the two technologies. The use cases supported by these scenarios and the associated privacy threats are outlined for each scenario.

3.4.1 RFID Locating Systems

The adoption of RFID technology in retail is the subject of a major ongoing privacy debate. The reason is the combination of three of its technological traits that raise consumer fears: First, humans have always been afraid of the invisible. This invisibility is manifest in many kinds of RFID that use chips too tiny to be recognised by the human eye, and communicate information without a line of sight through fabrics and even walls. Second, RFID cannot be "switched off", as other technologies. Last but not least, RFID technology is expected to be ubiquitously deployed and present on or embedded in all products and product components carrying barcodes today. This means that the technology will most likely become omnipresent in the near future.

Here, we first consider RFID data with statically installed gates and handheld readers. On an item level, we distinguish two cases. The first case is that an RFID tag is attached to the price tag of an item, which is typically removed after purchase. The second case is that RFID tags are integrated into items, such that removal becomes impossible without damaging the items. We also look at whether additional RFID enabled interaction points are existing in the retail area. For example, interactive smart kiosks allow customers to find more information about an item by presenting it to an attached reader.[1]

3.4.1.1 RFID Without Integrated Tags and Without Interaction Points

The customer interaction with the RFID system is limited to the checkout at the point of sales and potential reading at the exit (also *electronic article surveillance (EAS)*) gate, illustrated in Fig. 3.3. Sometimes, a customer brings back an item for returns at the customer centre. In such instances, there are additionally two data reads (at the EAS gate, and at the point of sales). The data collected through the RFID system in this case does not contain identifying patterns and only shows that there were items bought and perhaps returned.

[1] In the context of fashion retail, these interaction points can be inside the fitting room. Typically the users can interact there with a touch screen or also a smart mirror [7].

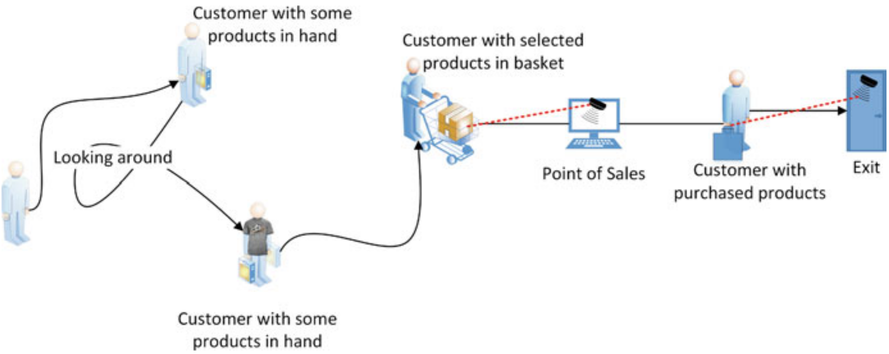
Customer with some products in hand
Customer with selected products in basket
Looking around
Point of Sales
Customer with purchased products
Exit
Customer with some products in hand

Fig. 3.3 An illustration of a shopping trip with RFID readers at a point of sales and an exit gate

Supported Use Cases

This scenario shown in Fig. 3.3 does not allow for many customer specific use cases. Nevertheless, it supports the use case of *preventing theft* (as outlines in Sect. 3.2.3). The EAS gates can automatically signal that an item has passed the gate that was not paid for to alert employees or security personnel. Additionally, as items are tagged with RFID technology, the use case of *locating products* (cf., Sect. 3.2.3) becomes possible. When the replenishment gate between back room and shop floor is RFID-enabled, the system knows whether items are on the sales floor or in the back room. Additionally, searching for misplaced items can be facilitated by handheld RFID scanners that can detect hundreds of items per second. Taking inventory with RFID technology can be sped up by handheld scanners, or fully automated (e.g., by robots). The use case of *replenishing products* (see Sect. 3.2.3) in case of retail shrinkage is supported by the updated inventory reports.

Privacy Threats

For this scenario, a major privacy threat arises from not restricting the RFID readers to only read the company's tags. This may lead to *surveillance* and *aggregation* of additional information, if there exists no mechanism to block reading of third party tags. Processing the aggregated information could be considered as a *secondary use* if the company is not transparent about it. Identifiers from the third party tags can lead to indirect *identification*. This aggregated information can further reveal more information about the individual *through association* of purchases with the unauthorised tag reads [88]. For instance, consider a customer, who carries a RFID smart card for public transportation, shops in such a store. When she leaves, not only the items bought would be recorded but also the identifier from the RFID smart card. This unauthorised read of the card is then a case of secondary use and the aggregated information leads to surveillance as retailer would gain knowledge about her shopping pattern i.e. when all does she visits the store. Additionally, the unauthorised tag can also be associated with the RFID tags of the bought items providing a personal identifier for them. Companies like *Integrity For You* have used such RFID chips in loyalty cards [19] which leads to the discussed threats if read by an authorised party.

3.4.1.2 RFID with Integrated Tags

When RFID tags are integrated into items for an increased theft protection level, they remain in the sold items without removal by the customer. In this scenario, the retail companies should take measures to deactivate (destroy, or send to sleep) the integrated tags after purchase [21], especially if the sold items are worn or carried around by customers. Otherwise the tags can be used to identify customers at later points in time or track them at other places where RFID technology is used. It is worth noting that other stores, but also any other organisation employing RFID-readers, can track people carrying or wearing items with enabled integrated tags [38].

Supported Use Cases

The supported use cases are the same as in Sect. 3.4.1.1 above (i.e., *preventing theft*, *locating* and *replenishing products*). However, there is a notable increase in protection against theft in this scenario [83]. An attacker can no longer simply remove the price tag from the product, or destroy a tag that is attached to the outside of the product. As the tags are embedded in the products, their removal becomes infeasible for most thieves.

Privacy Threats

The threats are similar to that discussed for the previous Sect. 3.4.1.1. However, in the long run for customers, all threats listed in Sect. 3.3.2.1 exist as the tags can be read by any interested party for malicious intentions. Some tags can be clipped [47] or ripped off to ensure they are not read, but such possibilities do not exist in all kinds of tagging. For instance, if tags are sewn-in with brand labels in garments then ripping them off might damage the garment. Thus, it becomes difficult to block the unwanted tag reads.

3.4.1.3 RFID with RFID-Enabled Interaction Points

When interaction points (like smart kiosks, mirrors, esp. in fitting rooms) are equipped with RFID readers, customers can benefit from more information about

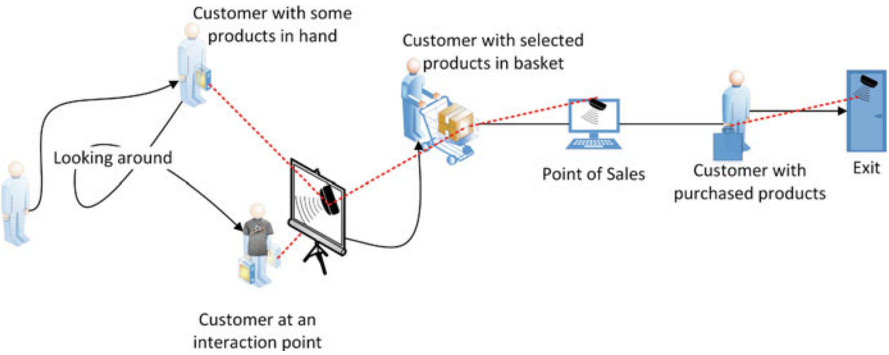
Customer with some products in hand
Customer with selected products in basket
Looking around
Point of Sales
Customer with purchased products
Exit
Customer at an interaction point

Fig. 3.4 An illustration of a shopping trip with RFID readers at an interaction point, a POS and an exit gate

the items of their choice [7]. The scenario is illustrated in Fig. 3.4. From a privacy perspective, novel information can be gathered from customers. It is possible to collect the information about items that a person was interested in, but decided to not buy. This is the case, when the sets of items that are brought to an interaction point overlap with the items that are finally bought by the customer. Additionally, the number of visits to the interaction points can be inferred to a certain degree. Prerequisite is that each subsequent visit to the interaction point has a given certain overlap in items (e.g., in the case of smart fitting rooms).

Supported Use Cases

Besides the operational use cases mentioned in Sect. 3.4.1.1 (i.e., preventing theft, locating and replenishing products), this scenario allows for additional managerial and marketing use cases. The use case of capturing *conversion rates* (as illustrated in Sect. 3.2.1) is partly supported in this scenario. In fact, the conversion rates of items that customers brought to the interaction point can be computed. In this way, it is possible to separate the items of interest that are also sold from those, that are interesting but not sold. For marketing, the use case of *context-aware browsing* (see Sect. 3.2.2) is supported. That is, the smart screens at interaction points can show the information pages according to the products detected that a customer brings there.

Privacy Threats

In addition to the threats discussed in Sect. 3.4.1.1, through *aggregation* of additional RFID data from interaction points could lead to even richer inferences about customers. The data *discloses* details of items that customers interact with which could be used for other *secondary uses*. Items brought to the interaction point reveal *inferred preferences* i.e. types of items picked up and brought there and possibly *transactions* for the customers shopping together [45]. For example, if two customers A and B come on a shopping trip then RFID tags would be read at interaction points as well as at the POS. Aggregated RFID tag reads can provide information about items which customers picked and did not buy. Also, if there exist some exchanges of items among the customers then those exchanges or transactions can also be inferred i.e. if many tags were read for customer A at an interaction point and then for B at a POS then either both have similar preference or they are shopping together.

3.4.1.4 RFID Real-Time Locating Systems

RFID real-time locating systems (RTLS) enable full visibility of inventory at all times. Usually the data is polled in periodic intervals for economic reasons. An illustration for RFID RTLS is shown in Fig. 3.5. If a retailer deployed an RTLS, it becomes possible to track customers indirectly by tracking moving items that are finally checked out [54]. It is theoretically possible to classify item movements into customer movements and employee inventory actions. For example, a large group of items moved from one area to the other on the sales floor indicates employee replenishment or store assortment activity. In contrast, smaller groups of items travelling through the shop and eventually ending at the checkout counter, could indicate customer movement. This information can be traced back to the point of the first picked up item. If customers always carried at least one item with them on their path, trading that item allows to reconstruct the customer's path. Furthermore,

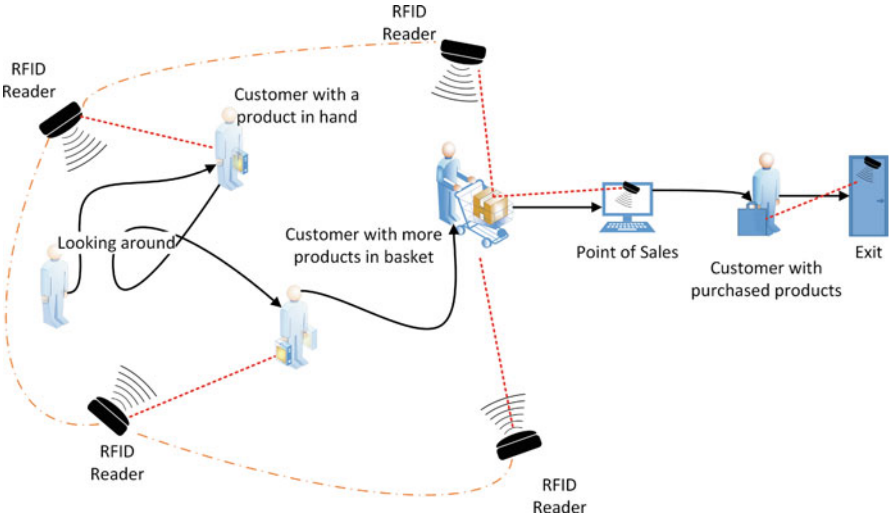
RFID Reader
RFID Reader
Customer with a product in hand
Looking around
Customer with more products in basket
Point of Sales
Customer with purchased products
Exit
RFID Reader
RFID Reader

Fig. 3.5 An illustration of a shopping trip with RFID RTLS, a POS and an exit gate

if the customer carries an integrated RFID tag that is technically compatible with the RTLS, the mentioned correlation anchor is unnecessary. It can be replaced by the integrated tag. The entire path of the customer can be traced in this case. Note that even the RFID RTLS data of a store that itself does not offer any items with integrated RFID tags, could potentially track customers, as they might carry integrated tags from other organisations.

Supported Use Cases

This scenario supersedes the scenario with only limited interaction points in Sect. 3.4.1.3. That is, many additional use cases are supported here. The management use cases of *conversion rates* (see Sect. 3.2.1) extend beyond bringing an item voluntarily to an interaction point to picking up an item. The queuing times (see Sect. 3.2.1) of customers can be monitored indirectly by observing that items queue in front of the point of sale. Also the *store layout optimisation* (see Sect. 3.2.1) can benefit from the movement patterns of customers through the shop. The marketing use cases mentioned in Sect. 3.2.2 are not supported directly by this scenario. However, when interaction points exist in the store (e.g., smart kiosks) these can offer *context-aware browsing* that can react on the items present. Furthermore, items that accompanied the items on their movement paths (e.g., a second picked up item that was again dropped) can be included in the context. All operational use cases are supported, except the use case of *automated checkout* (see Sect. 3.2.3). Notably, *theft prevention* (see Sect. 3.2.3) is in place and even suspicious movement patterns can be detected. For instance, when a product suddenly disappears from the sensing infrastructure, this might indicate a destruction of a tag. Also, *locating products* (see Sect. 3.2.3) is supported to the highest degree, as the system is aware of the locations in real time.

Privacy Threats

As this scenario supersedes the previous scenario discussed in Sect. 3.4.1.3, here we can assume that a store is full of interaction points revealing the data. In this scenario, analysing the movement pattern for a group of items can correlate to the movement of customers in the store. Thus through *estimation of constellations* or groups of items, *location* information can be inferred for the customers. Thus, in addition to the threats discussed in previous Sect. 3.4.1.3, the processing of RFID data threatens *exclusion* if customers are not made aware of location sensing processing. Also, as the analysis for grouping the items or estimation of constellations is based on correlations, there exists a possibility to infer *distorted* information. For instance, wrong relations or *transactions* can be concluded between customers if a customer picks up some item left by some other customer (*"breadcrumbs"* issue) [53].

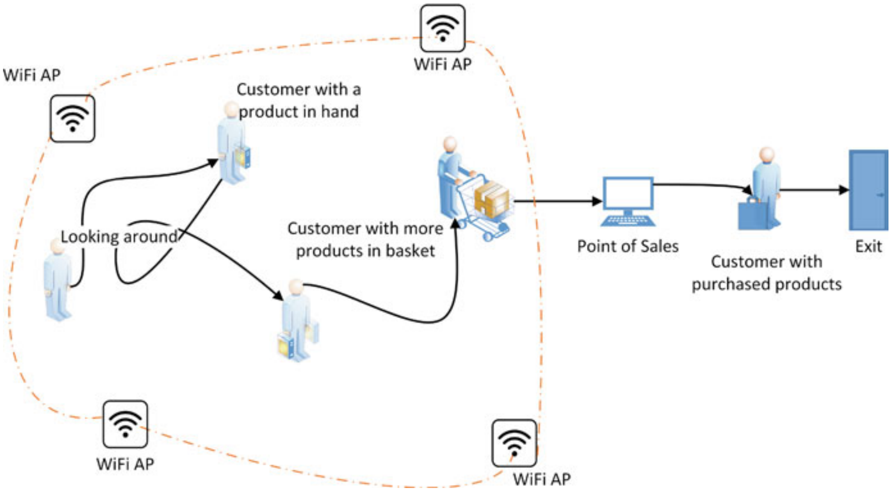
WiFi AP
WiFi AP
Customer with a product in hand
Looking around
Customer with more products in basket
Point of Sales
Customer with purchased products
Exit
WiFi AP
WiFi AP

Fig. 3.6 An illustration of a shopping trip with WiFi locating system

3.4.2 Wi-Fi Locating Systems

While RFID systems focus on the identification of (passive) tags, Wi-Fi positioning systems allow identification of communication devices. These systems allow to sense the location of smart phones using a cluster of Wi-Fi access points (AP), as shown in Fig. 3.6. If customers use the wireless network of an organisation, they leave traces with the MAC address of their device, which constitutes a unique identifier to track the owner [25]. Even when they do not actively use a wireless network, the communication devices often send polling requests for currently available networks. Mostly, this happens even when Wi-Fi is set to disabled on the devices. These polling requests can be used to locate the source device by means of triangulation or fingerprinting [3]. To avoid the possibility of being tracked in this way, recent device operating systems feature a random assignment of MAC addresses for every new connection of a device to wireless networks. However, a recent study has shown that these mechanisms are not fully functional yet, and it is possible to track devices at least over the duration of a visit [80].

In Wi-Fi locating system, the frequency of gathered data points is determined by the device model and its operating system. The probe request intervals range from 10 s, when the device is active, to 500 s when the device is inactive [28]. The granularity of the data impacts the quality of conclusions that can be drawn from it. The more fine grained the resolution is, the more privacy sensitive the gathered data becomes [15].

Supported Use Cases

This scenario is the only one supporting the capturing of the *conversion rates* (see Sect. 3.2.1) of passersby into customers that enter the shop. However, there is a bias, as only the customers that have a Wi-Fi enabled device are reflected in this rate. The *length of stay* (Sect. 3.2.1) of customers can be accurately measured, as customers become visible to the system from the moment they enter a store. As in the scenario of real-time locating systems based on RFID, the queuing times can be extracted from the data. Wi-Fi technology can also be used in mobile apps to support *geofencing* (Sect. 3.2.2), although for this particular use case Bluetooth is the more common technology. The use case of context-aware browsing can be supported at interaction points, by reacting to the areas that a customer visited on their path before starting the interaction. As far as the operational use cases are concerned, this scenario only supports *path optimisation* (Sect. 3.2.3) to a limited degree, as the customer paths can be seen, but to fully understand what the customers were looking for in their paths, further information is required. The *waiting time estimation* (Sect. 3.2.3) can be supported and displayed to customers.

Privacy Threats

In general, a log for MAC addresses is maintained for technical troubleshooting. However, the *aggregation* of unique MAC addresses if used for location sensing, leads to *surveillance* as location can be tracked and sensed for every shopping trip undertaken by customers if they leave Wi-Fi turned ON. Thus, this leads to *secondary use* of the collected data. Moreover if there is lack of transparency regarding the collection and processing of MAC addresses then it also leads to *exclusion*. Through the tracked *location*, retailers can *infer preferences* of their customers based on the time spent in different sections of the store. Also, MAC addresses can provide information about the devices being used customers and could be used for marketing, for instance is a customer using a new device or a fairly old device, if it is expensive or relatively cheap etc. For an example of this scenario, consider a big mall which provides free Wi-Fi. Through the collected information, one can analyse different paths taken by customers along with the time spent in certain areas of the mall. This information *discloses* probable preferences of a customer e.g. whether she visits more of sports stores, fashion retail store etc. Additionally, if WiFi location sensing is used by retailers then they can also understand the movement paths of the customers in their store and time spent in different sections similar to the mall example.

3.4.3 Analysis of Combinations of RFID and Wi-Fi

The combination of RFID and Wi-Fi data sources is of particular interest. The scenario is illustrated in Fig. 3.7. The reason is that RFID tags are typically attached

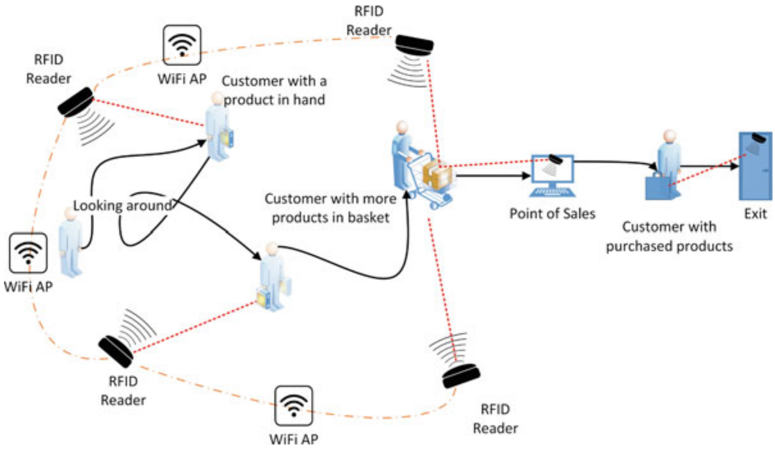

Fig. 3.7 An illustration of a shopping trip with RFID RTLS, Wi-Fi locating system, a POS and an exit gate

to items, whereas Wi-Fi is associated with actors (e.g., personnel, customers) interacting with items. In this way, when combining these two sources of information, it becomes possible to not only track a moving actor, but also track the items with which that actor is interacting. For example, the items picked up and dropped along the path are available for analysis.

Supported Use Cases

This combination of data sources enables all the use cases outlined in Sect. 3.2. Among others, specially tailored personalised marketing campaigns can take items of interest into account to tailor advertisements, and provide recommendations. Also, retailers can analyse the paths of customers for optimal shop floor layout, estimate waiting times, etc.

Privacy Threats

For this scenario, threats are simply a combination of those discussed for RTLS (Sect. 3.4.1.4) and Wi-Fi (Sect. 3.4.2). First of all, it leads to high level of *surveillance* as not only the location is sensed and continuously tracked but also information about items which are picked and carried or picked and later left are also associated with the location data. Thus, the *aggregated* information *discloses* fine-grained information about a customer's shopping trip. This scenario is comparable to the online cookies for analytics. Analytics cookies provide information about the browser used, mouse clicks, pages visited, count of visits etc. Similarly, this scenario provides information about the device used by a customer, path which they took in the store, items that were picked up and later bought, items that were picked and not bought etc. Thus, the scale or level of surveillance is much higher as compared to the previous scenarios.

3.5 Privacy Controls for Location Sensing Technologies

After having discussed the threats to privacy in different scenarios, we now turn to legal requirements and technical controls.

3.5.1 Legal Requirements

For the legal requirements, we base our analysis on the upcoming EU General Data Protection Regulation (GDPR) [81]. The GDPR supersedes the previously applied EU Data Protection Directive [82] and raises data protection standards by adapting rules in line with the recent technological developments. Based on the general principles discussed in the regulation, companies should ensure overall *lawfulness, fairness and transparency* for processing along with appropriate security measures to ensure *integrity and confidentiality*. Personal data should be only collected for specified and explicit purpose for establishing *purpose limitation*. Then, data collection should be relevant and limited to what is essential such that *data minimisation* is achieved. Next, the collected data should be kept accurate and up to date such that *accuracy* is ensured. Last, the personal data should be deleted or anonymised after the purpose has been fulfilled to assure *storage limitation*. While ensuring the basic principles for processing personal data, companies have broadly three different paths to ensure compliance: They can either (1) anonymise the data, (2) obtain informed consent for processing or (3) perform a balancing act to check if their processing can be considered as part of their legitimate interests.

3.5.1.1 Anonymisation

ISO defines anonymisation as a process by which personally identifiable information (PII) is irreversibly altered in such a way that an individual can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party [1]. For anonymisation of personal data, through the techniques of randomisation and/or generalisation, personally identifiable part is removed from data sets. Article 29 in their paper on anonymisation have discussed various techniques to achieve the non-identifiability of individuals [9]. Along with the explanation of different techniques they have also provided with strengths and weaknesses as well as common mistakes and failures related to their use. Like the ISO definition, they also emphasise on the importance of irreversible non-identifiability. If an individual can directly or even indirectly be identified in a dataset (for instance, through a reference to an identifier such as a name, number, location data) then that dataset has to be considered as personal data. Hence, MAC addresses used for Wi-Fi tracking is to be considered as personal data as individuals can be indirectly identified based on the uniqueness of the devices carried by them. Similarly, if RFID tags can be associated with customers based on comparison of fields like timestamps (which are also generally associated with purchase history) then RFID data also becomes personally identifiable. To remove the personally identifiable part, in the literature, a lot of techniques have been defined for anonymisation for example noise addition [32], k-anonymity [78], l-diversity [59], differential privacy [31] etc. As individuals cannot be identified in a well anonymised dataset, it falls out of the scope of data protection and reduces the legal obligations for the companies.

However, it is quite complicated to achieve a level of anonymisation that guarantees privacy. Researchers like Ohm have discussed the failures of anonymisation in ensuring privacy [67]. There exist a number of techniques to de-anonymise data [64] i.e. reidentifying individuals from a data set which was previously believed to be anonymous. The complication arises from the tradeoff between utility and privacy [70]. Higher levels of anonymisation increase privacy but in turn decrease the utility of a dataset. Thus, it is important to attain an equilibrium where utility and privacy parameters are well balanced [39]. If anonymisation techniques are chosen intelligently based on the context (type of data involved) then adequate level of privacy can be achieved while conserving useful utility of the dataset.

Anonymisation can be used in two broad ways—(1) Collecting information which is anonymous, (2) Collecting personal information and later anonymising it for a further purpose. For the first case, the collected information should not be personally identifiable. Hence, if collected data is considered as anonymous then companies should ensure that the dataset cannot be linked to existing datasets such that it is not possible to de-anonymise the data. For the second case, if data is later anonymised then best available techniques for anonymisation have to follow suit [66], including a regular inspection of the dataset for potential re-identifiability. This becomes specially important as location traces using the discussed technologies, in general, create quite distinct traces for individuals. For instance, Montjoye et al. found that by using only four different data points for coarse location and time during a day per individual, 95% of the 1.5 Million individuals could be uniquely identified [26]. Thus, location data can easily become personally identifiable.

3.5.1.2 Obtaining Consent

If a company values the utility of a dataset with personal information or if anonymisation is not adequately maintaining privacy then it can try to obtain the consent for processing from datasubjects. For obtaining consent, a company must explain, in a transparent way, the purpose of processing along with distinguishable information on the possibility of withdrawing consent in the future. Being transparent is crucial since consent must be given in an informed manner. Friedman et al. have developed a model providing broad guidelines for informed consent provision [36, 37]. Based on their model, there are six components to be considered:

Disclosure Providing accurate information about the processing along with harms and benefits involved with the processing. For example, companies should mention details like what information is collected, who will have access to it, how long would it be stored etc.

Comprehension Understandability of the information such that individuals are able to accurately interpret the information disclosed to them. Thus, it is not only important to provide all the information about processing but to also ensure that the information is easy to understand for the data subjects.

Voluntariness Ensuring that the action of giving consent is not forced on the individuals i.e. companies should not make data processing compulsory if data is not essential for the purpose. For instance, a marketing survey collecting information on a Pizza delivery service should be voluntary and service of delivering pizzas should not be affected if a customer chooses not to take part in the survey.

Competence Mental, emotional and physical competence (capability) of the targeted data subjects should be considered to ensure that they give an informed consent. For example, if information is provided such that the font which is not readable for an average individual then the consent will not be counted as readability (vision competence) was not properly considered.

Agreement Clear options must be provided for data subjects to provide consent for the data processing. Moreover, the GDPR adds that the process of revoking consent should be as simple as giving consent.

Minimal distraction All the above criteria must be met in such a way that individuals are not unduly diverted from their task at hand. For instance, if a company asks customers to read a 50 page document before they shop in a smart store then customers would tend to ignore the information and make uninformed decisions. This becomes quite challenging to implement as all information should be provided to customers and at the same time it should not distract them from their main task. For this reason, the GDPR recommends the use of Privacy Icons that are simpler to process by users.

After a company obtains an informed consent for processing, the customers must then be given options to access their data as well as the possibility to rectify some parts if logged incorrectly. Furthermore, options to erase their personal data or withdrawing consent for further processing have to be provided, along with ensuring adequate security in order to ensure compliance with the GDPR. In the context of security of personal information, pseudonymisation is referred to as a recommended technique.

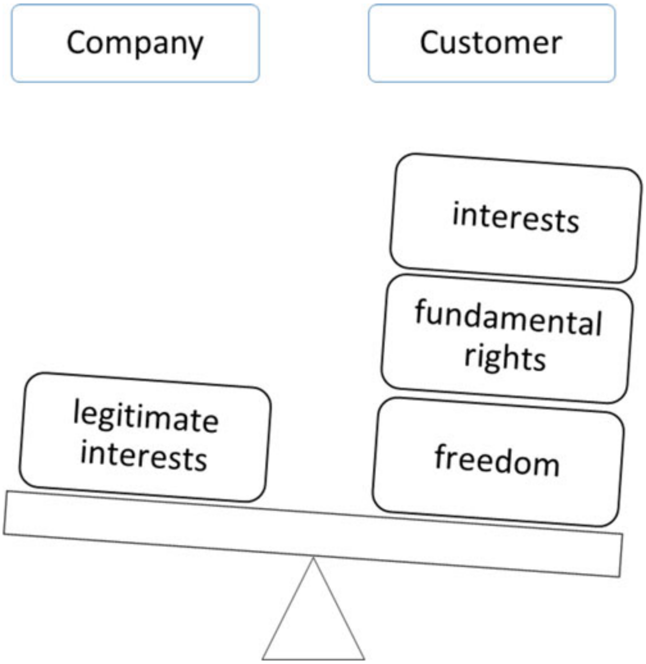

Fig. 3.8 Balancing act for legitimate interests as defined in the GDPR [81]

3.5.1.3 Legitimate Interests

Processing can also be considered lawful if done within the scope of legitimate interests of a company [10]. Legitimate interests can only be argued when the following three points are fulfilled:

1. The considered legitimate interests of the company are balanced against the interests or fundamental rights and freedoms of the data subjects, as illustrated in Fig. 3.8.
2. Processing is lawful (following other applicable legal regulations).
3. Processing represents a real and present interest. This means that data cannot just be collected for speculative reasons (i.e. for some future use). Scenarios like the engagement in *conventional direct marketing and other forms of marketing or advertisement* or the provision of *IT and network security* are two examples where the legitimate interests argument can be used as a valid legal ground for the processing. If legitimate interests are used as a legal ground, however, then a company needs to provide information about its data processing activity in a transparent way. Also, customers must be given an option to object to such processing in case they believe that their freedom is negatively affected by it.

3.5.2 Implementation of Privacy Controls

Technical controls, available in our context, deal mainly with anonymisation to avoid location data being personally identifiable, pseudonymisation for enhancing security and transparency to ensure informed consent. Location anonymity is given, when the location information is dissociated from an individual, while pseudonymisation links location information to a pseudonym that is disconnected from the individual [30]. Though pseudonymisation does not provide adequate promises of privacy and is considered as personally identifiable data, it is still considered as a recommended technique for ensuring security of personal data along with other techniques like encryption. In the following, we discuss possible privacy controls for the outlined scenarios in Sect. 3.4. Note that in all these scenarios, the location sensing is taking part on the provider side and not on the user side. Location-sensing system providers should consider implementing these controls to minimise the associated privacy threats.

3.5.2.1 Privacy Controls for RFID Systems

Blocking Unknown RFID Reads to Ensure Data Minimisation

To ensure data minimisation, companies should collect only relevant data. Thus, RFID tags, which are not associated with the company should not be read. This control can simply be implemented by maintaining *a whitelist* of the inventory of tagged items that the company owns or issues. More specifically, such a whitelist includes Electronic Product Codes (EPCs) that are supposed to be in the store according to the inventory system. This would lead to discarding the reads of unknown or unexpected EPCs that were not deactivated by other organisations and could potentially identify individuals. Also, the EPCs of sold items should also not be read, if the purpose to use RFID in store was mainly to enhance the visibility of the inventory.

Deactivating/Destroying Integrated Tags in Sold Products to Safeguard Customers' Confidentiality

As discussed in Sect. 3.3.2.1, through estimation of constellations, RFID tags may provide unique personal identifiers related to customers. Thus, to prevent such threats, companies should either destroy or deactivate the tags. A lot of different techniques have been discussed in the literature for achieve this [11, 47].

Securing RFID Enabled Loyalty Cards

If a company decides to put RFID tags in their loyalty cards then the deactivation of such tags is not longer an option. Read range of 1–10 m also amplifies the associated privacy threats. In that case, companies should ensure that the chips on the cards are only using Near-Field Communication (NFC) [65] where the read range is no more than 1 m and there exist ways to prevent unauthorised reads. Since, read range for NFC is less than 1 m, it becomes comparatively difficult to read tags in an unauthorised way.

Anonymisation of Tag Reads for RFID Enabled Interaction Points

As RFID data from RFID enabled interaction points (e.g., smart fitting rooms, kiosks etc.) can be correlated to items that customers bought (indirectly identifying them). Hence, RFID data has to be considered as personal data. Thus, companies can either anonymise the data and remove any personally identifiable information or obtain an informed consent from the customers for the processing of such data. For ensuring that the RFID data is anonymous, temporal cloaking (e.g., reducing the time granularity from seconds to days) can be applied on the read RFID enabled items suggested by Gruteser and Grunwald [40]. By making the time information less precise, the data can be turned into *k-anonymous* data. *k-anonymous* means that individuals'information is sufficiently imprecise in order to make them indistinguishable from at least $k-1$ other individuals. In this way, the system can still count how often a given article type was brought to interaction points (e.g., fitting rooms) in a broader time range (e.g., day, week). If temporal information is cloaked to days, this measure hides the information of the number and times of visits to the interaction points per individual, maintaining anonymity of visitors per day. By doing this, the individual level information is lost but marketing insights about the ratio of fitting room visits and effective sales can still be collected on an item level. Note that in settings with a high variety of article types, it might be possible that the assignment of the fact whether a customer was in the fitting room could still be reconstructed (e.g., if a rare item was sold on 1 day, and there was also one visit of that outlier item in the fitting room). In that case, it is possible to increase time censoring to weekly, monthly, or even coarser granularity [40].

Ensuring Transparency for RFID Enabled Interaction Points

To avoid complications with the identifiability of outliers, companies can also rely on obtaining consent from customers. In that case, informing customers about RFID readers would be essential to ensure transparency. It can be easily achieved by using RFID logos at customer interaction points, such as shop entries. To provide a choice, there should be an option to use a non-RFID based interaction point. Alternatively, the RFID readers could only read the tags after the customer has confirmed that he or she wishes to use the underlying smart services.

3.5.2.2 Privacy Controls for RFID Real-Time Locating Systems

The main purpose of RTLS is to analyse the movement of tagged items. Thus, unless there is a specific purpose to identify and track customers using the technology, substantial efforts should be made by companies to avoid identifiability of customers in a RTLS dataset.

Discarding Historical Data to Ensure Storage Limitation and Data Minimisation

By only storing the latest position of tags, customer behaviour cannot be reconstructed. Furthermore, the RTLS information system should not store information about EPC tags that have been sold, or EPCs of other stores. This can be easily implemented with a whitelist mechanism. In this way, only the whereabouts of items currently available for sale in the shop are recorded.

Anonymising RFID Location Data

To make this data anonymous, companies would need to destroy the linkability between the RTLS and POS data sets. Here, the relation is not only based on temporal information (relating RFID read timestamps with POS timestamps) but also spatial information (relating different baskets of items moving around). For obstructing a correlation of space and time at checkout, temporal and spatial cloaking can be applied [30] without losing valuable information regarding position of items. A discussion of privacy-preserving techniques with provable privacy guarantees is presented in Chap. 5.

3.5.2.3 Privacy Controls for Wi-Fi Locating Systems

Wi-Fi based locating systems can be used for assisting customers for in-store navigation, analysis of most crowded and least crowded parts of store etc. Paths are uniquely identified by the MAC-address of the device which is considered as identifiable data. Simple *pseudonymisation* by replacing the MAC address by an identifier (e.g., a hash value of the address) does not suffice, as the data can still be correlated to individual's sales data through spatio-temporal overlaps of the purchase and the visit of the point of sale. However, even applying temporal and spatial cloaking for the visits on a daily basis is not enough as by looking at data created by multiple visits of a returning customer, the anonymity of that customer can be compromised. For example, consider the case where temporal cloaking to a daily resolution is applied. Looking at only 1 day of records, the customer is hidden in the anonymity of all the customers that visited that day. However, when looking at multiple days when that customer made purchases, the customer's identity is only hidden in the *intersection* of the sets of customers on these multiple days, which in turn allows singling out customers. Thus, if companies are interested in analysing location traces of identifiable customers then an informed consent must be obtained. Otherwise, anonymisation can also be used as it also supports a number of applications.

Anonymising WiFi Location Data

As even through spatio-temporal cloaking customers can be uniquely identified, we suggest using new identifiers for every *visit* instead of a single identifier per MAC address to disable possible linkability. Also, for anonymising location data, different techniques are defined in literature. The approach by Tang et al. [79] ensures privacy as individual's data is not stored but only anonymous visits to areas are recorded. An application of this method to Wi-Fi location-sensing technologies means to only count visits in areas or transitions from one area to another instead of entire uniquely identifiable paths. Further methods include the framework by Duckham and Kulik [30], where the authors propose to obfuscate information, that is, increase the imprecision of location information.

3.6 Conclusion

In this chapter, we first explained how location can be inferred by means of trilateration or fingerprinting. Subsequently, we discussed potential technologies that allow us to perform location-sensing. Then, we used the example of a brick-and-mortar retail organisation to illustrate and discuss the use cases empowered by location-sensing technologies. We found that many previously existing use cases benefit from this additional form of information, while some entirely novel use cases are only possible through location-sensing technologies.

From these use cases, we turned to the threats of privacy that location-sensing technologies entail and exemplified them in the retail domain after an introduction into an existing taxonomy and categorization of threats. Therefore, we discussed popular location-sensing scenarios ranging from only collecting location data at fixed positions to real-time locating systems that can surveil the entire store area. Finally, we discussed controls to mitigate the identified privacy threats from the perspective of the location-sensing system provider and presented controls that the users have in this setting.

We live in times, where new technologies pop up at an increasing rate and outperform previous technologies in terms of accuracy and efficiency, sometimes by magnitudes. It is difficult to cope with the privacy implications of these novel technologies, as even within a single technology the potential use cases become apparent only as time progresses. Furthermore, new combinations of technologies allow for unforeseen use cases. For example, there are first supermarkets, where the system fully automatically detects the picked up items and the customers' identities by facial recognition to entirely automate checkout and avoid queueing [87].

Therefore, adherence to existing and upcoming legislations, and responsible use of collected data of organisations is of utmost importance. When new information gathering systems are implemented in organisations, we need to ensure that privacy is built in by design, because afterwards it might be too late, and privacy breaches can dearly cost an organisation in both reputation, trust and also by legal fines. Thus, we urge the implementers of novel technologies and the users to consider privacy and ethics throughout their systems and processes.

References

1. ISO/IEC 29100:2011 - Information technology – Security techniques – Privacy framework. 2011.
2. G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles. Towards a better understanding of context and context-awareness. In *International Symposium on Handheld and Ubiquitous Computing*, pages 304–307. Springer, 1999.
3. S. Adler, S. Schmitt, K. Wolter, and M. Kyas. A survey of experimental evaluation in indoor localization research. In *Indoor Positioning and Indoor Navigation (IPIN), 2015 International Conference on*, pages 1–10. IEEE, 2015.
4. G. Adomavicius and A. Tuzhilin. Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. *IEEE transactions on knowledge and data engineering*, 17(6):734–749, 2005.
5. M. Afanasyev, T. Chen, G. M. Voelker, and A. C. Snoeren. Usage patterns in an urban WiFi network. *IEEE/ACM Trans. Netw.*, 18(5):1359–1372, 2010.
6. K. Albrecht and L. C. McIntyre. Scandal: Wal-mart, p &g involved in secret RFID testing, consumers against supermarket privacy invasion and numbering (caspian). Retreived on 10-01-2017 from http://www.spychips.com/press-releases/broken-arrow.html.
7. Y. Andreu-Cabedo, P. Castellano, S. Colantonio, G. Coppini, R. Favilla, D. Germanese, G. Giannakakis, D. Giorgi, M. Larsson, P. Marraccini, et al. Mirror mirror on the wall an intelligent multisensory mirror for well-being self-assessment. In *2015 IEEE International Conference on Multimedia and Expo (ICME)*, pages 1–6. IEEE, 2015.
8. Anonymous. Silverpush launches cross-device ad targeting with unique audio beacon technology. Retrieved on 14-01-2017 from http://www.steamfeed.com/silverpush-launches-cross-device-ad-targeting-with-unique-audio-beacon-technology/.
9. Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques, 2014.
10. Article 29 Data Protection Working Party. Opinion 06/2014 on Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 2014.
11. J. Ayoade. Roadmap to solving security and privacy concerns in rfid systems. *Computer Law & Security Review*, 23(6):555–561, 2007.
12. M. Azizyan, I. Constandache, and R. Roy Choudhury. Surroundsense: mobile phone localization via ambience fingerprinting. In *Proceedings of the 15th annual international conference on Mobile computing and networking*, pages 261–272. ACM, 2009.
13. R. Bajaj, S. L. Ranaweera, and D. P. Agrawal. GPS: location-tracking technology. *Computer*, 35(4):92–94, 2002.
14. M. Baldauf, S. Dustdar, and F. Rosenberg. A survey on context-aware systems. *International Journal of Ad Hoc and Ubiquitous Computing*, 2(4):263–277, 2007.

15. A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *IEEE Pervasive computing*, 2(1):46–55, 2003.
16. A. Bibby. Invasion of the privacy snatchers. *Financial Times, January*, 9, 2006.
17. R. R. Burke. The third wave of marketing intelligence. In *Retailing in the 21st Century*, pages 113–125. Springer, 2006.
18. J. D. Cai. Business intelligence by connecting real-time indoor location to sales records. In *International Conference on Web-Age Information Management*, pages 817–823. Springer, 2014.
19. M. T. Capizzi and R. Ferguson. Loyalty trends for the twenty–first century. *Journal of Consumer Marketing*, 22(2):72–80, 2005.
20. G. Castelli, A. Rosi, M. Mamei, and F. Zambonelli. A simple model and infrastructure for context-aware browsing of the world. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'07)*, pages 229–238. IEEE, 2007.
21. A. Cavoukian. Privacy guidelines for RFID information systems (RFID privacy guidelines), 2006. Information and Privacy Comissioner/Ontario, Toronto.
22. A. Chattopadhyay and A. R. Harish. Analysis of low range indoor location tracking techniques using passive UHF RFID tags. In *2008 IEEE Radio and Wireless Symposium*, 2008.
23. I. Cil. Consumption universes based supermarket layout through association rule mining and multidimensional scaling. *Expert Systems with Applications*, 39(10):8611–8625, 2012.
24. P. Cohan. How nordstrom uses WiFi to spy on shoppers. Retreived on 13-01-2017 from http://www.forbes.com/sites/petercohan/2013/05/09/how-nordstrom-and-home-depot-use-wifi-to-spy-on-shoppers/#2421d0ec3bf9.
25. M. Cunche. I know your MAC address: Targeted tracking of individual using Wi-Fi. *Journal of Computer Virology and Hacking Techniques*, 10(4):219–227, 2014.
26. Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel. Unique in the crowd: The privacy bounds of human mobility. *Scientific reports*, 3, 2013.
27. D. Delen, B. C. Hardgrave, and R. Sharda. Rfid for better supply-chain management through enhanced information visibility. *Production and Operations Management*, 16(5):613–624, 2007.
28. L. Demir. Wi-Fi tracking : what about privacy. Master's thesis, M2 SCCI Security, Cryptologyand Coding of Information - UFR IMAG, Sept. 2013. https://hal.inria.fr/hal-00859013.
29. A. K. Dey. Understanding and using context. *Personal Ubiquitous Comput.*, 5(1):4–7, Jan. 2001.
30. M. Duckham and L. Kulik. A formal model of obfuscation and negotiation for location privacy. In *International Conference on Pervasive Computing*, pages 152–170. Springer, 2005.
31. C. Dwork. Differential privacy: A survey of results. In *International Conference on Theory and Applications of Models of Computation*, pages 1–19. Springer, 2008.
32. C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography Conference*, pages 265–284. Springer, 2006.
33. Eileen P. Kelly G. Scott Erickson. RFID tags: commercial applications v. privacy rights. *Industrial Management & Data Systems*, 105(6):703–713, 2005.
34. European Emergency Number Association. Caller location in support of emergency services. *EENA Operations Document*, (2), 2014.
35. Z. Farid, R. Nordin, and M. Ismail. Recent advances in wireless indoor localization techniques and system. *Journal of Computer Networks and Communications*, 2013, 2013.
36. B. Friedman, E. Felten, and L. I. Millett. Informed consent online: A conceptual model and design principles. *University of Washington Computer Science & Engineering Technical Report 00–12–2*, 2000.
37. B. Friedman, P. Lin, and J. K. Miller. Informed consent by design. *Security and Usability*, (2001):503–530, 2005.
38. S. L. Garfinkel, A. Juels, and R. Pappu. RFID privacy: An overview of problems and proposed solutions. *IEEE Security & Privacy*, 3(3):34–43, 2005.
39. A. Ghosh, T. Roughgarden, and M. Sundararajan. Universally utility-maximizing privacy mechanisms. *SIAM Journal on Computing*, 41(6):1673–1693, 2012.

40. M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st international conference on Mobile systems, applications and services*, pages 31–42. ACM, 2003.
41. Y. Gu, A. Lo, and I. Niemegeers. A survey of indoor positioning systems for wireless personal networks. *IEEE Communications surveys & tutorials*, 11(1):13–32, 2009.
42. M. Hazas, J. Scott, and J. Krumm. Location-aware computing comes of age. *IEEE Computer*, 37(2):95–97, 2004.
43. M. Hazas, J. Scott, and J. Krumm. Location-aware computing comes of age. *Computer*, 37(2):95–97, 2004.
44. Information technology – Security techniques-Information security risk management. Standard, International Organization for Standardization, Geneva, CH, 2008.
45. A. Juels. RFID security and privacy: A research survey. *IEEE journal on selected areas in communications*, 24(2):381–394, 2006.
46. Kalyan S. Pasupathy, Thomas R. Hellmich. How RFID technology improves hospital care, 31-12-2015. Retreived on 14-01-2017 from https://hbr.org/2015/12/how-rfid-technology-improves-hospital-care.
47. G. Karjoth and P. A. Moskowitz. Disabling RFID tags with visible confirmation: clipped tags are silenced. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 27–30. ACM, 2005.
48. V. Kopytoff. For retailers, tracking shoppers brings new insights. Retreived on 13-01-2017 from https://www.technologyreview.com/s/520811/stores-sniff-out-smartphones-to-follow-shoppers/.
49. D. Kravets. Tracking school children with RFID tags? it's all about the benjamins. Retreived on 14-01-2017 from https://www.wired.com/2012/09/rfid-chip-student-monitoring/.
50. J. Krumm, editor. *Ubiquitous computing fundamentals*. CRC Press, 2016.
51. P. Kumar, M. U. Kalwani, and M. Dada. The impact of waiting time guarantees on customers' waiting experiences. *Marketing science*, 16(4):295–314, 1997.
52. A. LaMarca, Y. Chawathe, S. Consolvo, J. Hightower, I. E. Smith, J. Scott, T. Sohn, J. Howard, J. Hughes, F. Potter, J. Tabert, P. Powledge, G. Borriello, and B. N. Schilit. Place lab: Device positioning using radio beacons in the wild. In *Pervasive Computing, Third International Conference, PERVASIVE 2005, Munich, Germany, May 8-13, 2005, Proceedings*, pages 116–133, 2005.
53. M. Langheinrich. A survey of RFID privacy approaches. *Personal and Ubiquitous Computing*, 13(6):413–421, 2009.
54. J. S. Larson, E. T. Bradlow, and P. S. Fader. An exploratory look at supermarket shopping paths. *International Journal of research in Marketing*, 22(4):395–414, 2005.
55. M. Levy, B. A. Weitz, and D. Grewal. *Retailing management*. Irwin/McGraw-Hill New York, 1998.
56. H. Liu, H. Darabi, P. Banerjee, and J. Liu. Survey of wireless indoor positioning techniques and systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 37(6):1067–1080, Nov 2007.
57. H. Liu, H. Darabi, P. P. Banerjee, and J. Liu. Survey of wireless indoor positioning techniques and systems. *IEEE Trans. Systems, Man, and Cybernetics, Part C*, 37(6):1067–1080, 2007.
58. H. Liu, Y. Gan, J. Yang, S. Sidhom, Y. Wang, Y. Chen, and F. Ye. Push the limit of WiFi based localization for smartphones. In *The 18th Annual International Conference on Mobile Computing and Networking, Mobicom'12, Istanbul, Turkey, August 22–26, 2012*, pages 305–316, 2012.
59. A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam. l-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 1(1):3, 2007.
60. C. Martin. How beacons are changing the shopping experience. *Harvard Bus. Rev*, 2014.
61. A. S. Mattila and J. Wirtz. Congruency of scent and music as a driver of in-store evaluations and behavior. *Journal of retailing*, 77(2):273–289, 2001.
62. A. Moore. Defining privacy. *Journal of Social Philosophy*, 39(3):411–428, 2008.

63. D. Namiot. Context-aware browsing–a practical approach. In *2012 Sixth International Conference on Next Generation Mobile Applications, Services and Technologies*, pages 18–23. IEEE, 2012.
64. A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 111–125. IEEE, 2008.
65. P. V. Nikitin, K. Rao, and S. Lazar. An overview of near field UHF RFID. In *IEEE international Conference on RFID*, volume 167. Citeseer, 2007.
66. A. Novotny and S. Spiekermann. Personal information markets and privacy: a new model to solve the controversy. 2012.
67. P. Ohm. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA law review*, 57:1701, 2010.
68. R. Prasad and M. Ruggieri. *Applied satellite navigation-using GPS, GALILEO and augmentation systems*. 2005.
69. N. M. Puccinelli, R. C. Goodstein, D. Grewal, R. Price, P. Raghubir, and D. Stewart. Customer experience management in retailing: Understanding the buying process. *Journal of Retailing*, 85(1):15–30, 2009. Enhancing the Retail Customer Experience.
70. V. Rastogi, D. Suciu, and S. Hong. The boundary between privacy and utility in data publishing. In *Proceedings of the 33rd international conference on Very large data bases*, pages 531–542. VLDB Endowment, 2007.
71. F. Ricci, L. Rokach, and B. Shapira. *Introduction to recommender systems handbook*. Springer, 2011.
72. D. Y. Sha and L. Guo-Liang. Improving service quality of retail store by innovative digital content technology. In *2012 IEEE International Conference on Computer Science and Automation Engineering*, pages 655–660, June 2012.
73. D. J. Solove. A taxonomy of privacy. *University of Pennsylvania law review*, pages 477–564, 2006.
74. D. J. Solove. Understanding privacy. *Harvard University Press, GWU Law School Public Law Research Paper*, (420), May 2008.
75. J. Song, C. T. Haas, and C. H. Caldas. A proximity-based method for locating RFID tagged objects. *Advanced Engineering Informatics*, 21(4):367–376, 2007.
76. R. A. Spinello. Privacy rights in the information economy. *Business Ethics Quarterly*, 8(4):723–742, 1998.
77. steinunn. Discover a museum with BLE app for indoor location – Video from Eldheimar, 2014. Retreived on 14-01-2017 from https://locatify.com/blog/discover-a-museum-with-ble-app-for-indoor-location-video-from-eldheimar/.
78. L. Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.
79. K. P. Tang, P. Keyani, J. Fogarty, and J. I. Hong. Putting people in their place: An anonymous and privacy-sensitive approach to collecting sensed data in location-based applications. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 93–102, New York, NY, USA, 2006. ACM.
80. Z. Technologies. Analysis of iOS 8 MAC Randomization on Locationing. http://mpact.zebra.com/documents/iOS8-White-Paper.pdf, 2015. Zebra Whitepaper.
81. The European Parliament And The Council Of The EU. Regulation (eu) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). *Official Journal of the European Union*, L119/1, 2016.
82. The European Parliament, the Council and the Commission. Eu directive 95/46/ec on the protection of individuals with regard to the processing of personal data and on the free movement of such data: Eu directive 95/46/ec. pages 0031–0050, 1995.
83. F. Thiesse. RFID, privacy and the perception of risk: A strategic framework. *J. Strategic Inf. Sys.*, 16(2):214–232, 2007.
84. F. Thomas and L. Ros. Revisiting trilateration for robot localization. *IEEE Trans. Robotics*, 21(1):93–101, 2005.

85. J. P. Van Den Berg. A literature survey on planning and control of warehousing systems. *IIE Transactions*, 31(8):751–762, 1999.
86. R. Want. An introduction to RFID technology. *IEEE Pervasive Computing*, 5(1):25–33, 2006.
87. A. Wee. A supermarket without a checkout line-Amazon go, 2016. Zing Gadget http://en.zinggadget.com/a-supermarket-without-a-checkout-line-amazon-go.
88. S. A. Weis. Security and privacy in radio-frequency identification devices. Master's thesis, Massachusetts Institute of Technology, 2003.
89. A. Yaeli, P. Bak, G. Feigenblat, S. Nadler, H. Roitman, G. Saadoun, H. J. Ship, D. Cohen, O. Fuchs, S. Ofek-Koifman, et al. Understanding customer behavior using indoor location analysis and visualization. *IBM Journal of Research and Development*, 58(5/6):3–1, 2014.
90. C. Yang and H.-R. Shao. WiFi-based indoor positioning. *IEEE Communications Magazine*, 53(3):150–157, 2015.
91. D. Zanetti, P. Sachs, and S. Capkun. On the practicality of UHF RFID fingerprinting: How real is the RFID tracking problem? In S. Fischer-Hübner and N. Hopper, editors, *Privacy Enhancing Technologies - 11th International Symposium, PETS 2011, Waterloo, ON, Canada, July 27–29, 2011. Proceedings*, volume 6794 of *Lecture Notes in Computer Science*, pages 97–116. Springer, 2011.