University of Zurich^UZH

Estimote UWB Beacons Privacy and Functionality Analysis

Seyyid Ökkes Palta
Zurich, Switzerland
Student ID: 20-742-524

Supervisor: Katharina Müller, Prof. Dr. Burkhard Stiller
Date of Submission: August 7, 2024

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

BACHELOR THESIS – Communication Systems Group, Prof. Dr. Burkhard Stiller

Bachelor Thesis
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmuehlestrasse 14, CH-8050 Zurich, Switzerland
URL: http://www.csg.uzh.ch/

Declaration of Independence

I hereby declare that I have composed this work independently and without the use of any aids other than those declared (including generative AI such as ChatGPT). I am aware that I take full responsibility for the scientific character of the submitted text myself, even if AI aids were used and declared (after written confirmation by the supervising professor). All passages taken verbatim or in sense from published or unpublished writings are identified as such. The work has not yet been submitted in the same or similar form or in excerpts as part of another examination.

Zürich, 06.08.2024

Signature of student

Abstract

Im Zusammenhang mit dem Internet der Dinge (IoT) wurden viele verschiedene Technologien entwickelt, um die Genauigkeit der Lokalisierung in Innenräumen zu erhöhen und gleichzeitig die Energieeffizienz zu erhalten. Da diese Technologien jedoch in unseren Häusern eingesetzt werden, werfen sie verschiedene Fragen zum Datenschutz auf. Da es sich um ziemlich neue Technologien handelt, ist der Datenschutzaspekt dieser Technologien noch nicht gründlich erforscht worden. Vor diesem Hintergrund zielt diese Arbeit darauf ab, die Datenschutzaspekte von Estimote UWB Beacons zu analysieren, die die Ultrabreitbandtechnologie (UWB) nutzen. Dazu wurden sowohl technische als auch theoretische Ansätze umgesetzt. Die Beacons wurden mit einem UWB-fähigen Smartphone verbunden, und die Ergebnisse dieser Verbindung wurden mit einem Software Development Kit (SDK) beobachtet. Auf der Grundlage der Beobachtungen wurden die offiziellen Anwendungsfälle dieser Beacons, die von Estimote Inc. veröffentlicht wurden, analysiert, um die Datenschutzlücken zu schließen. Es wurde festgestellt, dass das Estimote-Ökosystem ganz ähnliche Datenschutzprobleme aufweist wie das Apple-Ökosystem mit AirTags. Obwohl also viele Anforderungen an den Datenschutz erfüllt wurden, konnte das Estimote-Ökosystem wesentliche Datenschutzanforderungen nicht erfüllen.

In the context of the Internet of Things (IoT), many different technologies have been developed to increase the accuracy of indoor localization while maintaining energy efficiency. However, since these technologies operate in our homes, they raise several privacy questions. As the technologies can be quite new, the privacy aspect of these technologies has not been researched thoroughly. Considering this, this thesis aims to analyze the privacy aspects of Estimote UWB Beacons that use ultra-wideband (UWB) technology. Thus, both technical and theoretical approaches were implemented. The beacons were connected with a UWB-enabled smartphone, and the results of this connection were observed in a Software Development Kit (SDK). Based on the observations, the official use cases of these beacons released by Estimote Inc. were analyzed to address the privacy gaps. It was found that the Estimote ecosystem has quite similar privacy issues as the Apple ecosystem with AirTags. Therefore, although many privacy requirements were fulfilled, the Estimote ecosystem failed to fulfill significant privacy requirements.

Acknowledgments

Above all, I want to express my appreciation to my supervisor, Katharina O. E. Mueller, for her invaluable support, guidance, and constructive feedback while writing this thesis. I also extend my thanks to Prof. Dr. Stiller and the Communication Systems Group at the University of Zurich for offering me an engaging topic for my Bachelor's Thesis.

Contents

Chapter 1

Introduction

Every day, new and different types of technology emerge, which may change our habits and how we live and interact with our surroundings. In 1887, when Heinrich Hertz was researching electromagnetism, he also became the first to generate Ultra-Wide Band (UWB) signals [1]. Hence, it can be stated that this technology is both old and new [1].

UWB is one of the most promising wireless sensor networks, which is robust with high-precision capabilities [2]. The use case of UWB varies a lot. In one case, UWB technology is used and analyzed in the automotive industry by [3] and in another case, it is used for miniaturization technique by [4]. Therefore, the use case of UWB is quite broad, and this technology can be used in many different ways for different purposes.

As UWB technology is used in many fields, one should consider its functionality and privacy. Current UWB literature does not focus on privacy, and there has not been any specific research done on Estimote UWB beacons [5].

In this thesis, the functionality and privacy aspects of Estimote Beacons will be analyzed. These beacons use UWB technology to locate indoor devices and send information or data to nearby devices with the UWB feature. Estimote UWB beacons are three small devices that emit UWB signals that compatible devices, such as the newest smartphones, can detect. These beacons can measure the distance with high precision in indoor environments, and their batteries can last more than six months [6].

As previously mentioned, more research needs to be done on the privacy aspect of these beacons. This thesis should shed light on this aspect and analyze how privacy is preserved in these beacons within their technology.

1.1 Motivation

People have been working to make daily life more accessible than ever by introducing new technologies such as washing machines and dishwashers. The Internet of Things (IoT) concept primarily describes situations in which network connectivity and computational power are expanded to objects, sensors, and everyday items not typically viewed as computers. This allows these objects to produce, share, and use data with little human involvement. However, there is no universally accepted definition [7]. As IoT has become increasingly popular in recent years, analyzing this area would answer some questions that IoT users may ask in the coming years [8]. These questions arise as new technologies emerge because humans gradually worry about losing privacy. Therefore, privacy has been more important in recent decades [9]. Additionally, such technologies can also be used for malicious purposes. These will be explained further in later chapters of this thesis. These malicious purposes use cases and the risks they can pose to a user must be addressed.

1.2 Thesis Goals

This thesis aims to analyze the functionality and privacy of Estimote UWB beacons based on data that can be retrieved from them. This should allow the readers to understand and provide them with actionable insights on making the most of this technology in their daily lives. Furthermore, privacy analysis aims to answer possible privacy-related questions that may arise shortly [8].

Functionality analysis will help us address the privacy questions. This analysis includes quantifiable factors like range and signal strength and other qualifiable aspects, such as the signal passing through an obstacle and its possibility. Based on these features of beacons, this thesis aims to address and answer privacy-related questions and highlight the risks involved in using this technology. Additionally, more than two hundred use cases were released recently by Estimote Inc. [10]. These use cases will also be analyzed based on the privacy mapping discussed later in Chapter 2.

1.3 Thesis Outline

The introductory chapter provides background information regarding the functionality and privacy analysis of Estimote beacons. Chapter 2 conducts further research on the background and technology pertaining to the functionality and privacy of these beacons and shows which related work has been published. Chapter 3 provides a possible design for use cases of Estimote Beacons. Chapter 4 shows the implementation of the analyses in more detail and technical. After the design and implementation in the previous chapters, Chapter 5 evaluates the results and analyzes the functionality and privacy aspects of Estimote beacons. Last but not least, chapter 6 mentions final considerations, summarizes the work, concludes the results, and suggests future work.

Chapter 2

Fundamentals

2.1 Background

This thesis focuses on the functionality and privacy analysis of Estimote beacons. Privacy has always been a research area, as its meaning increased with the emergence of new technologies [9]. Firstly, the types of tracking technologies that are used when analyzing privacy will be explained. Later, privacy regulations and frameworks such as GDPR, NIST, and nFADP will be explained. These different regulations and frameworks will be combined in a privacy mapping, and the details of this combination will be explained. This privacy mapping generalizes these privacy regulations and frameworks and was first introduced by [11].

2.1.1 Tracking Technologies

What is UWB and How Does it Work?

Ultra-wideband (UWB) is a communication protocol that uses a large part of the radio spectrum to transmit data over short distances with deficient power consumption [12]. This makes Estimote beacons use much less energy; hence, they can last longer and be used for longer periods. UWB signals have extremely short pulses and occupy a bandwidth much wider than traditional radio signals, allowing UWB to achieve high data rates and precise indoor positioning capabilities with short pulses of about 2 nanoseconds each [12, 13]. UWB technology is used in various applications such as wireless communication, indoor positioning and tracking, radar systems, and IoT devices. Below is the graph that shows the band in which the UWB operates.

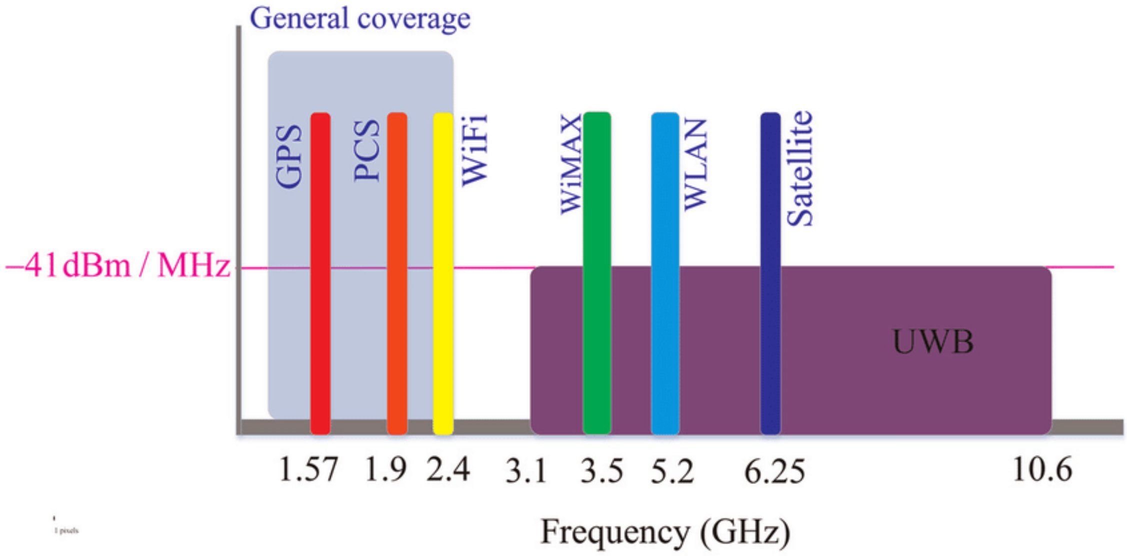


Figure 2.1: Bandwidth of UWB [14]

The wide band comes from its frequency range, which varies between 3.1 and 10.6 GHz. UWB's frequency is also above the general coverage, which makes it unique and different from other signals such as GPS, PCS, and WiFi.

Packets are sent when Estimote beacons are connected to the phone via UWB, and these packets represent the communication between the phone and the beacon. The diagram below shows, in detail, what the UWB frame structure looked like during this communication.

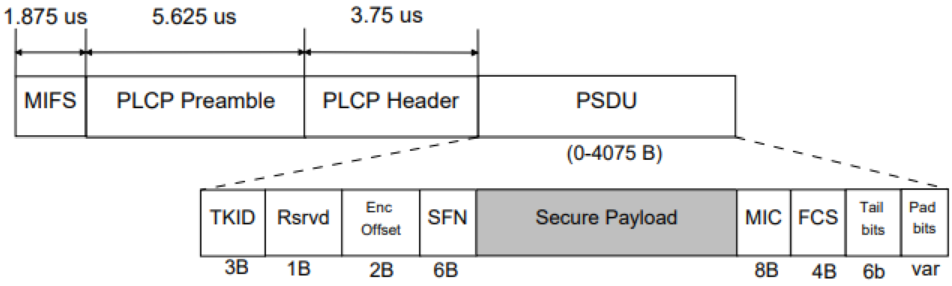


Figure 2.2: UWB Frame Structure [15]

Compared to the normal mode, this frame structure has less overhead, a shorter preamble, and minimum inter-frame space (MIFS). This is important as it minimizes the data transmission and, hence, decreases the power consumption. Furthermore, the payload is secured after the Physical Layer Convergence Protocol (PLCP) Header in the Physical Layer Service Data Unit (PSDU). Thanks to these reliable methods for delivering the secure payload, bursty packet errors are avoided, and the packet error rate can be decreased [15].

UWB technology has many potential applications, from healthcare to customer service. Although its primary application is in indoor positioning technologies, it offers many advantages since the UWB is significantly more accurate than other indoor positioning technologies [16]. Its application can vary from museums and airports to restaurants, and UWB is being used for navigating and helping the customers or visitors on-site [17]. A more detailed examination of the current application and the research conducted on this technology will be presented in a subsequent chapter 5.

The operational concept is straightforward. Once a device equipped with an ultra-wideband (UWB) radio, such as a smartphone, wristband, or smart key, enters the range of another UWB device, ranging commences. The ranging is accomplished by implementing time of flight (ToF) measurements between the devices [13]. The time of flight (ToF) is calculated by measuring the round-trip time of challenge/response packets. This calculation is depicted below 2.3. The device's precise location is calculated by either the mobile or the fixed UWB device, depending on the application type (e.g., asset tracking or device localization). Suppose the device is operating an indoor navigation service. In that case, its relative position in relation to the fixed UWB anchors must be ascertained, and its position on the area map must be calculated [13].

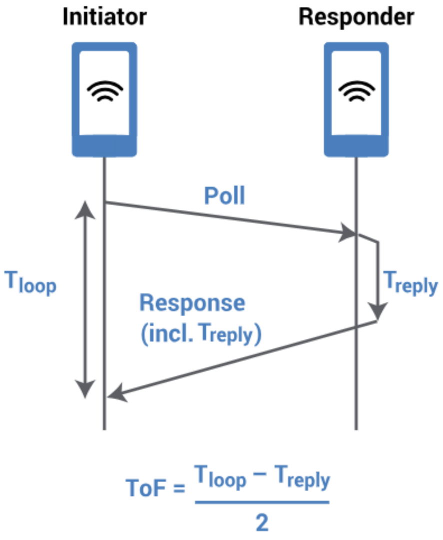


Figure 2.3: UWB Time of flight calculation [13]

BLE Technology

The Estimote UWB beacons use BLE technology as well 3.4. This technology uses much less energy than other Bluetooth technologies, increasing the battery life of Estimote beacons. However, this technology has a limitation that restricts the amount of data that can be transmitted, allowing only a limited number of data to be sent [18]. Despite its restrictions on data transmission, BLE technology has been gradually applied more in our daily life [18] since its advantages outweigh its disadvantages. A more detailed explanation can be found in the diagram below.

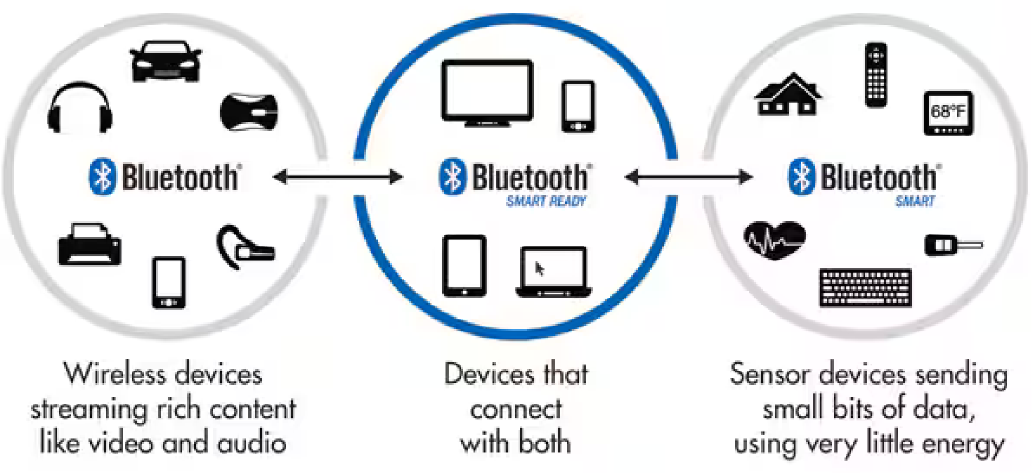
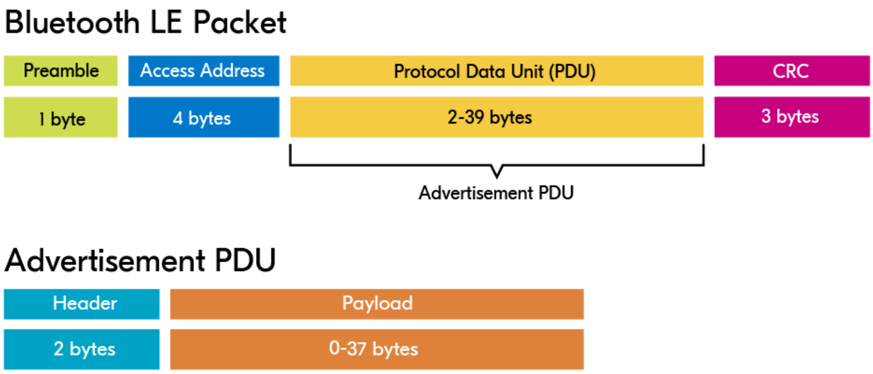

Bluetooth
Bluetooth SMART READY
Bluetooth SMART
68°F
Wireless devices streaming rich content like video and audio
Devices that connect with both
Sensor devices sending small bits of data, using very little energy

Figure 2.4: Types of Bluetooth devices [19]

The diagram above shows Bluetooth devices can be classified into three groups. Devices that stream rich content, such as audio or video, can be classified into one group. In the second group, some devices can connect with different devices that utilize Bluetooth technology. Lastly, there are Bluetooth sensor devices with a minimum energy requirement. Estimote beacons can be grouped in the last group here as they transmit as little data as possible to save energy. Therefore, this technology is called Bluetooth Low Energy. This allows Estimote beacons to last longer, as discussed previously.

The performance of BLE was measured on a radio developed by Nordic Semiconductor, and the maximum data rate is limited to 125 kbit/s [18]. Additionally, BLE enables angle-of-arrival estimations, increasing Estimote beacons' accuracy [20].



Bluetooth LE Packet

Preamble	Access Address	Protocol Data Unit (PDU)	CRC
1 byte	4 bytes	2-39 bytes	3 bytes

Advertisement PDU

Advertisement PDU

Header	Payload
2 bytes	0-37 bytes

Figure 2.5: BLE Packet Structure [21]

The diagram 2.5 shows how Bluetooth Low-Energy (BLE) packets are structured. There is a one-byte preamble and an access address of four bytes. This is followed by the Protocol

Data Unit (PDU), which contains the payload. A Cyclic Redundancy Check (CRC) is included at the end of the packet to prevent data redundancy. The primary component of the packet is the PDU, which includes a header comprising two bytes. This is then followed by the payload. The payload can consist of 0 to 37 bytes depending on the packet.

Comparison of BLE and UWB

Considering the accuracy of both technologies, UWB has been proven to be more accurate in indoor localization [20]. At the same time, BLE can have a localization error of up to a few meters [20]. From [20], the following significant differences can be inferred.

a. **Bandwidth** UWB has a much wider bandwidth, which varies depending on the channel. BLE's bandwidth, on the other hand, is limited to 40 different 2 MHz channels

b. **Frequency bands** UWB can operate in sub or gigahertz, while BLE operates in the 2.4 GHz frequency band.

c. **Power consumption** The difference in power consumption between these two technologies is considerably high. While BLE consumes ten mW on average, UWB uses 280.5 mW.

Even though UWB is much more flexible than BLE regarding the bandwidth and frequency bands, BLE is more advantageous under certain circumstances [20]. If BLE is not affected severely by multipath interference, it can achieve high accuracy. Another reason for the usability of BLE is its ubiquitousness. UWB technology cannot be found on every smartphone, and only very few have this technology installed, while BLE can be found in almost every smartphone [20].

Combining these technologies allows Estimote UWB beacons to improve their accuracy [22]. As BLE is not very accurate and its calculation is based on the signal strength, UWB technology will enhance the accuracy through objects such as walls [22].

2.1.2 Privacy Regulations

What is GDPR?

The European Union's General Data Protection Regulation (GDPR) took effect in 2018 as new technologies that use big data were developed [23]. GDPR is a detailed and the world's strictest privacy and security law [24]. Although it came into effect in 2018, previous versions of GDPR were first released before the 2000s [24].

As technology progressed further, modern problems emerged. These modern problems require modern solutions. Hence, GDPR came into existence to protect privacy and security. However, these laws are only valid in GDPR countries and only apply to people living in these countries [25]. Other countries not in the EU, such as Switzerland and New Zealand, adopted similar data protection laws [25]. Moreover, some countries are in Europe but do not implement GDPR [25]. These recent developments in privacy and security laws worldwide imply the importance of creating GDPR-compliant systems and new technologies.

History of GDPR

In 1950, the European Convention on Human Rights addressed the right to privacy [24]. As the technology advanced more in the coming decades and the Internet was invented, the EU recognized the need for an update in data protection. In 1995, the EU enacted the European Data Protection Directive, setting the minimum data privacy and security standards, which each member state used as a foundation to develop its own implementing legislation [24]. However, even then, the Internet was transforming into a data vacuum as it is today.

In 1994, the first banner ad appeared online [24]. Privacy became even more critical after tech giants like Facebook and Google emerged. A Google user sued the company in 2011 for scanning her emails, and two months after that, the EU decided to update the directive introduced back in 1995 [24]. The GDPR took effect in 2016 after passing the European Parliament, and as of 2018, all organizations must comply with the GDPR [24, 26].

Data Protection Principles

When it comes to data protection, the GDPR introduces seven protection and accountability principles [26]:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and Confidentiality
7. Accountability

These principles align well with other privacy frameworks such as NIST and privacy regulation nFADP. This alignment helps to consider all the privacy frameworks and regulations collectively and to analyze the Estimote UWB beacon's compliance with these.

Lawfulness of Data Processing

Data processing can only be lawful under certain conditions according to Article 6 in the GDPR [27]:

a. there exists consent from data subject to the processing of their personal data for at least one specific purpose

b. processing is required for fulfilling a contract to which the data subject is a party or for taking steps at the request of the data subject before entering into a contract

c. processing is required to comply with a legal obligation that the controller is bound by.

d. processing is essential to safeguard the vital interests of the data subject or another individual

e. processing is required for the execution of a task performed in the public interest or the exercise of official authority assigned to the controller

f. processing is necessary for the legitimate interests pursued by the controller or a third party, except when those interests are outweighed by the interests or fundamental rights and freedoms of the data subject that require the protection of personal data, especially if the data subject is a child

As long as the technology complies with one of these conditions, its data processing is considered lawful [27]. These conditions are set by Article 6, and Estimote beacons will be analyzed with respect to these points.

New Federal Act on Data Protection

In Switzerland, the Federal Act on Data Protection was adopted in 1992 [28]. Since then, many technological advancements and changes in data usage and purposes have occurred. In the past 30 years, this federal act has been updated, and consequently, the New Federal Act on Data Protection (nFADP) was published in September 2023 [28]. The nFADP delineates seven fundamental tenets pertaining to the handling and processing of personal data [28, 11]:

1. Personal data must be discussed **lawfully**.
2. The processing must be carried out in **good faith** and be **proportionate**.
3. Personal data may only be collected for a **specific purpose** that the data subject can **recognize**; personal data may only be further processed in a manner that is **compatible with this purpose**.
4. They shall be **destroyed** or **anonymized** as soon as they are **no longer required** for the purpose of processing.

5. Any person who processes personal data must satisfy themselves that the data are **accurate**. They must take all appropriate measures to correct, delete, or destroy incorrect or incomplete data insofar as the purpose for which they are collected or processed is concerned, The appropriateness of the measures depends, in particular, on the form and the extent of the processing and on the risk that the processing poses to the data subject's personality or fundamental rights.

6. If the **consent** of the data subject is required, such consent is only valid if given **voluntarily** for one or more specific instances of processing based on appropriate information.

7. The consent must be explicitly given for:

   (a) processing **sensitive personal data**;

   (b) high-risk profiling by a private person; or

   (c) profiling by a federal body.

According to article 5, paragraph c of the nFADP, sensitive personal data is partially defined, such as health [28, 11]. As can be seen from the principles of GDPR and nFADP, these regulations are very similar, yet some categories have minor differences.

2.1.3 Security & Cybersecurity

Security is often intertwined with privacy as they are closely related. Derek E. Bambauer states in his article that privacy and security should be treated as distinct concerns [29]. In one case, a data mining company, Acxiom, provided the social security numbers of some of their customers to a defense contractor, and these numbers were then made public [29]. It was revealed that the company had been responsible for exposing sensitive customer data on three occasions, causing considerable concern among privacy advocates. However, this article argues that this case should be considered a privacy rather than a security issue [29]. The reason for this is the disclosure of data. The disclosure of data is related to the concept of privacy, whereas the hacks are related to the security field. Nonetheless, as previously stated, security and privacy concepts are inextricably linked. Consequently, a lack of security inevitably results in a lack of privacy.

NIST Cybersecurity Framework

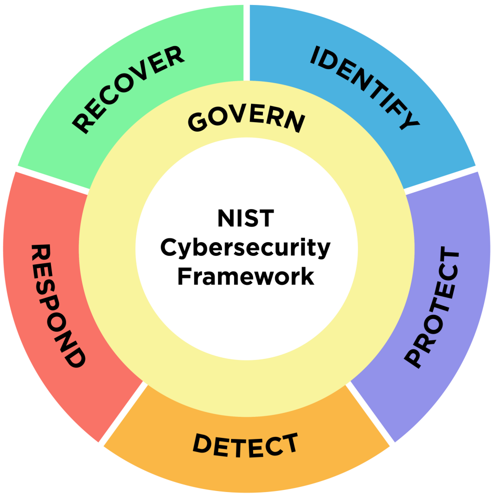


Figure 2.6: NIST Cybersecurity Framework [30]

The diagram above shows us five fundamental functions of the NIST cybersecurity framework (NIST CSF). NIST CSF is a more technical definition of the General Data Protection Regulation (GDPR), which was explained previously in detail. It is a set of guidelines and best practices developed by the National Institute of Standards and Technology (NIST) in 2014 [31, 32]. It aims to help organizations manage and reduce their cybersecurity risk. The framework is designed to be adaptable and scalable to different types and sizes of organizations. The five fundamental functions of the NIST cybersecurity framework are continuous and concurrent [32], and these five functions are the core of NIST CSF.

1. **Identify:** Develop an organizational understanding of managing cybersecurity risks to systems, assets, data, and capabilities. This function includes asset management, risk assessment, and risk management strategy.

2. **Protect:** Develop and implement appropriate safeguards to ensure the delivery of critical infrastructure services. This function consists of access control, data security, maintenance, etc.

3. **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. Activities included in this function consist of anomaly events and detection processes.

4. **Respond:** Develop and implement appropriate activities to take action on a detected cybersecurity incident. Activities such as mitigation, analysis, and improvements can be performed to apply this function.

5. **Recover:** Develop and implement appropriate activities to maintain resilience plans and restore any capabilities or services impaired due to a cybersecurity incident.

2.1.4 Privacy Mapping

In order to comply with GDPR, NIST, and nFADP, the privacy analysis in this thesis will be based on a recently published bachelor thesis from the University of Zurich [11]. The reason is that this mapping combines different regulations and frameworks. Once it can be determined that the Estimote environment complies with this privacy mapping, it can be stated that it complies with GDPR, NIST, and nFADP. According to the mapping boundaries thesis, the privacy mapping is as follows [11]:

(1) Awareness: The data subject is aware that personal data are being collected and processed.

- GDPR, Lawfulness, Fairness and Transparency: *Personal data shall be processed [...] in a transparent manner in relation to the data subject.*
- NIST, Control: Data Processing Policies, Processes, and Procedures: *Policies, processes, and procedures for authorizing data processing (e.g., [...] individual consent) [...] are established and in place.*
- nFADP, Consent: *If the consent of the data subject is required, such consent is only valid if given voluntarily for one or more specific instances of processing based on appropriate information.*

(2) Transparency: The data subject is aware of the specific data processing purposes.

- GDPR, Purpose Limitation: *A data subject should be able to know who is using its information and for what purposes.*
- NIST, Communicate: Communication Policies, Processes, and Procedures: *Transparency policies, processes, and procedures for communication data processing purposes [...] are established and in place.*
- nFADP, Data Collection for specific purposes: *Personal data may only be collected for a specific purpose that the data subject can recognize [and] [...] only be processed in a manner that is compatible with its purpose.*

(3) Confidentiality: Personal information is stored with appropriate security measures.

- GDPR, Integrity, and Confidentiality: *Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.*
- NIST, Protect: Protective Technology: *Mechanisms [...] are implemented to achieve resilience requirements in normal and adverse situations.*

(4) Accountability: The data subject can hold the controllers for their actions accountable.

- GDPR, Accountability: *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1*
- NIST, Govern: Governance Policies, Processes, and Procedures:
  (a) Roles and responsibilities for the workforce are established with respect to privacy
  (b) Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders

(5) **Data Minimization:** The personal data acquired is kept to a bare minimum and proportionate.

- GDPR, Data Minimization: *Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.*
- NIST, Control:
  (a) Data Processing Management: *Data are managed consistent with the organizational's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles*
  (b) Disassociated Processing: *Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles*

(6) **Accuracy:** The personal data stored must be accurate and correct.

- GDPR, Accuracy: *Personal data shall be accurate and, when necessary, kept up to date.*
- NIST, Control-P: *Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, [and] manage data retention).*
- nFADP, Accuracy: *Any person who processes personal data must satisfy themselves that the data are accurate.*

(7) **Storage Limitation:** The data may only be stored for as long as necessary.

- GDPR, Storage Limitation: *Personal Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*
- NIST, Control: Data Processing Policies, Processes, and Procedures: *A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.*
- nFADP, Data Removal: *[Personal data] shall be destroyed or anonymized as soon as they are no longer required for the purpose of processing.*

(8) **Lawfulness:** Data processing is done lawfully.

- GDPR, Lawfulness, Fairness and Transparency: *Personal data shall be processed lawfully [...] in relation to the data subject.*

- NIST, Govern: Governance Policies, Processes, and Procedures: *Legal, regulatory, and contractual requirements regarding privacy are understood and managed.*
- nFADP, Lawful data processing: *Personal data must be processed lawfully.*

(9) Anonymity: Personal data should limit the possible identification of the subject.

- NIST, Control: Disassociated Processing: *Data are processed to limit the identification of individuals.*

(10) Unlinkability: Connecting personal information back to the data subject should be impossible.

- NIST, Control: Disassociated Processing: *Data are processed to limit the observability and linkability.*

(11) Unobservability: The use of services by the data subject is not visible to third parties.

- NIST, Control: Disassociated Processing: *Data are processed to limit the observability and linkability.*

(12) Good Faith: Personal data must be processed in good faith.

- nFADP, Good Faith: *The processing must be carried out in good faith.*

Based on this mapping of principles from different regulations and privacy frameworks, this thesis aims to cover as many principles as possible. Hence, this privacy mapping will further evaluate Estimote beacons and their environment.

2.2 Related Work

This chapter will review the existing literature related to UWB and BLE beacon technologies. Previous research on indoor positioning systems, developments in beacon technologies, and privacy concerns in IoT devices will be explored.

Beacon technology has evolved significantly since its inception. Early implementations heavily relied on Bluetooth Classic. However, recent developments have shifted towards BLE and UWB for improved accuracy and energy efficiency. Only a few resources could be found that researched Estimote beacons.

2.2.1 Indoor Positioning Systems

Kolakowski et al. [33] researched using UWB and BLE technologies to track and evaluate older adults' behavior. It mainly focuses on the transmission and synchronization of UWB packets and their range. In addition, it performs experiments and calculates error rates when using these technologies. But, the privacy concerns still need to be addressed here. The importance of privacy is briefly mentioned here, but research still needs to be done in detail.

2.2.2 Beacon Technologies

Jimenez and Seco [22] thoroughly analyzed the UWB technology in a museum-like use case. They focused on the performance and range of UWB. Therefore, this is a profoundly technical analysis. However, privacy concerns with UWB and BLE devices were not mentioned here. They conducted their analysis with commercially available devices from Bespoon and Estimote [22].

In addition, Eder [34] conducted an analysis and evaluation of UWB technology and its architecture with a focus on privacy-preserving characteristics. Her master thesis states that the UWB technology is often considered a sufficient privacy-preserving mechanism. While her discussion of UWB technology and its architectural features with respect to privacy-preserving capabilities is extensive, and despite mentioning Estimote's beacons, there is a paucity of research on Estimote's UWB beacons, which integrate BLE technology.

2.2.3 Privacy in IoT Devices

Furthermore, another article from the Communication Systems Group (CSG) at the University of Zurich is available. Mueller and her team analyzed the privacy ontology to preserve privacy in UWB technologies [5]. This analysis shows that the privacy aspect of UWB technology has been analyzed in depth. The paper provides an ontology and a detailed categorization concerning the UWB protocol with a sole focus on privacy [5]. However, although this paper sheds light on the structure that preserves privacy in UWB technologies, it doesn't set its focus on Estimote beacons and their interoperability with both UWB and BLE technologies. BLE is briefly mentioned as one of the communication tools that can be used for smart home environments. While this paper might show that UWB's privacy ontology is secure and preserves privacy, using BLE technology in Estimote beacons can decrease privacy protection.

Another work related to UWB is a book [12] from 2006. In this book, Benedetto and her team comprehensively overview UWB communication systems. Similar to previous papers and research that were examined, this research also explained and focused on the technical aspects of UWB technology. Similar technical issues such as ranging are also mentioned and were compared to other technologies [12]. Per contra, no mentions of privacy or privacy concerns were found. As the book came out earlier than Estimote Beacons, it cannot be expected to see an analysis of Estimote Beacons. However, analyzing privacy issues with new technologies would still be possible. Since this has yet to be done, this research cannot answer questions and concerns related to privacy.

While significant research has been done on individual beacon technologies, limited work has been done on their combined use with BLE. This thesis aims to fill this gap by exploring the integration of UWB and BLE in beacon systems, focusing on enhancing functionality and addressing privacy concerns.

The existing literature provides a foundation for understanding beacon technologies and their applications. This chapter has highlighted critical studies and identified gaps this thesis will address. The following chapter will detail the methodology used in our research.

Chapter 3

Design

This chapter contains designs for the different methods of experimenting with Estimote beacons. Section 3.1 highlights which use cases are possible and can be concerning regarding privacy. Section 3.2 explains how the analysis with a sniffer device is performed. Last, the design to test the beacons' functionality regarding their range and signal strength will be shown.

3.1 Privacy Use Cases

In this section, different privacy use cases will be considered. These cases can be grouped under two main categories: normal and malicious use. In these two different groups, many different cases can be thought of; however, only one case for each group will be focused for now.

1. **Normal Use:**

   In this case, beacons access the phone to send data according to its use case, such as in the museum or at the airport. In addition, beacons receive data from the phone to track its location and position in space. These are the normal and intended use of beacons.

2. **Malicious Use:**

   Beacons can be deployed to send malicious data to phones or receive data from the phone that goes beyond its intended use. This malicious data may damage the phone and violate privacy regulations such as GDPR. Equally, receiving personal data without consent or beyond the previously declared purpose violates the GDPR.

Estimote's website has more than 200 use cases given [17]. Although a thorough analysis of all these use cases seems impossible, this thesis aims to analyze some essential and commercially viable use cases concerning their privacy. This will help us pinpoint which use cases can violate privacy regulations and what type of malicious can be observed in these use cases.

3.2 Sniffer Analysis

This section briefly explains what can be achieved by using a sniffer device. Later in the implementation chapter, a sniffer device will be employed. This device can track the data transmission between the UWB-enabled phone and the beacons. The findings allow us to analyze the transmission and determine what kind of data is being used and how much data flows between the phone and the beacons. The sniffer device will also help us identify privacy issues related to this data transmission. However, the sniffer device must be improved since the beacons are also connected to a cloud system. Therefore, the analysis will also include the cloud system and further data storage on the cloud will be tracked, which goes beyond the sniffer's capabilities.

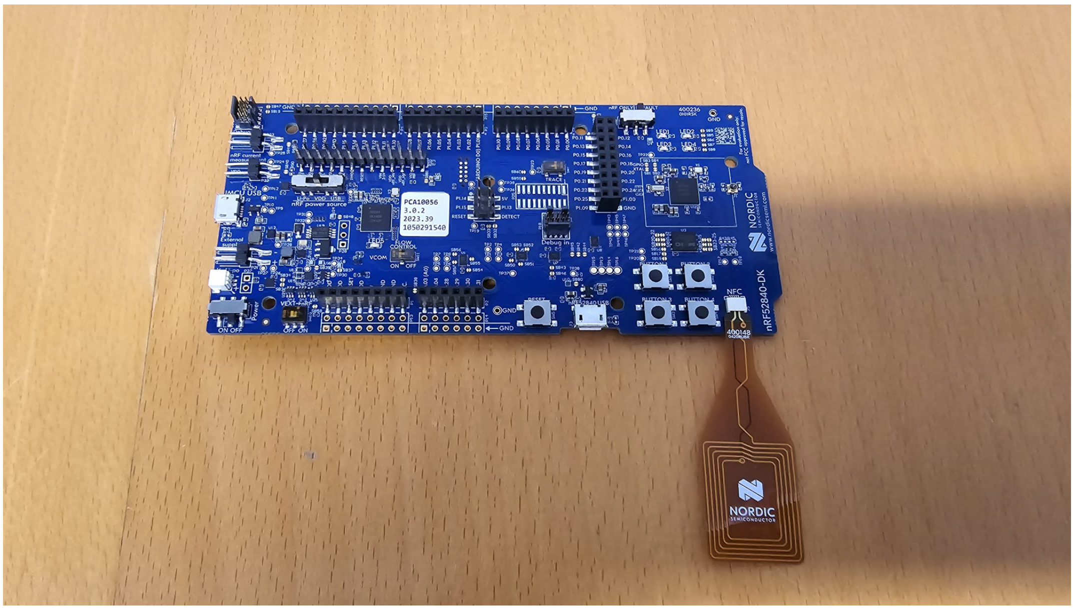


Figure 3.1: nRF52840

The picture above shows the sniffer's development kit, which Nordic Semiconductor developed. This development kit also includes a Near Field Communication (NFC) antenna, which can be connected to an internal or external power supply via a USB cable. Then, this kit will be connected with a Qorvo sniffer. Qorvo sniffer is shown in the image below.

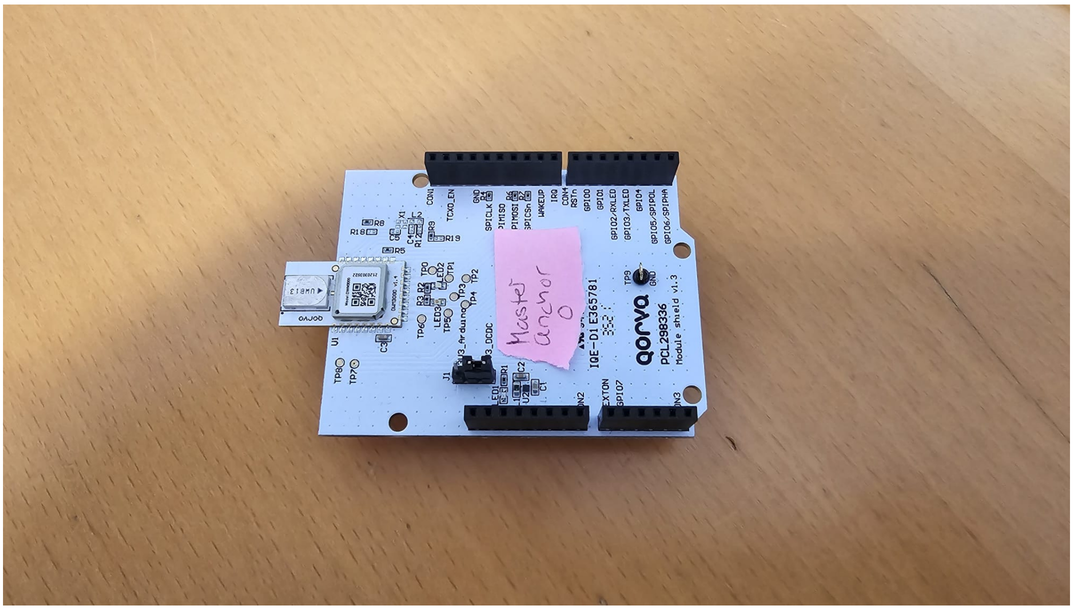


Figure 3.2: Qorvo DWM3000EVB

If configured correctly, this sniffer can be combined with the nRF52840 above, and they can sniff data transmission nearby. This combination is shown in the image below.

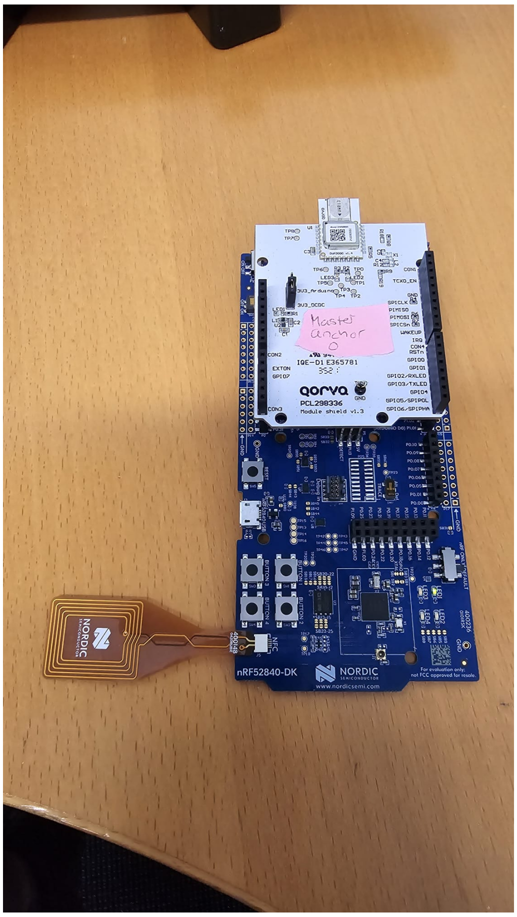


Figure 3.3: Combination of nRF52840 and DWM3000EVB

3.3 Ranging and Signal Strength Experiments

This section will explain how this thesis's technical aspect is built and what components it exists from. First, the technical setup will be explained with the Software Development Kit (SDK) provided by Estimote Inc. and how this generally works with the UWB-enabled phone and Estimote beacons. Then, subsection 3.4.2 will describe how to interpret the range and explore the beacons' range limits. Lastly, the signal strength measurement will be shown for Estimote beacons.

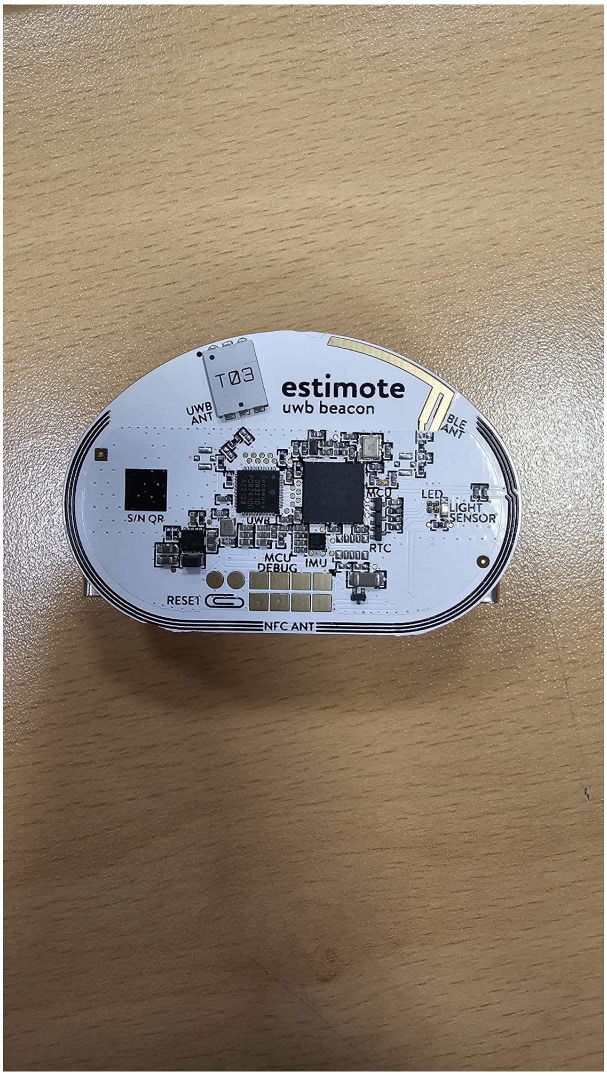


Figure 3.4: Inside of a UWB beacon designed and produced by Estimote Inc.

The image above shows that the beacon has two antennas for UWB and BLE, respectively. This combined use of UWB and BLE antennas allows these beacons to be precise with indoor localization by using UWB technology and to last longer and use less energy by using BLE technology. Additionally, these beacons have an NFC antenna, and phones can use their NFC technology.

3.3.1 Technical Setup

First, the SDK environment will be set up locally. Later, this SDK can be run on the phone to connect it to nearby beacons. This requires a phone with a UWB feature. Unfortunately, this feature is not as ubiquitous as BLE and can't be found on every smartphone [20]. Hence, it requires a very recent smartphone with this particular feature.

In addition, an Android phone is being used, and the environment set up by Estimote Inc. does not allow Android devices to connect to multiple UWB beacons simultaneously [35]. This can be achieved using an iOS-supporting phone that provides UWB features. Therefore, this limits the research here with multiple beacons simultaneously, and the focus will be set on working with one beacon at a time.

3.3.2 Ranging

According to the official documentation of SDK, the range of the Estimote beacons is quite accurate and can calculate the distance to 10 cm [36]. The thesis aims to test the range and determine the range limit. It is unknown how far these beacons can connect to a phone. The reason to test the range is that, in a wide range, some passers-by might not be aware of the usage of UWB beacons, and their phones can still be connected to these beacons. In this case, the data subject is not aware of being a data subject and that their phone is connected to a beacon. This case violates the GDPR guidelines that are explained previously in detail.

3.3.3 Signal Strength

In terms of functionality, the strength of the signal will be analyzed by creating different conditions in which the strength of the beacon signal will be tested. It is intended to conduct the tests in the following manner:

1. Placement of a single beacon right next to the smartphone
2. Placement of a single beacon away from the smartphone at the following distances: [5cm, 10cm, 15cm, 20cm, 25cm, 50cm and 100cm]
3. Placement of a single beacon at the following distances between the smartphone and the beacon: [1.5m, 2m, 2.5m, 3m, 3.5m, 4m, 4.5m and 5m]
4. Placement of a beacon with various obstructions in between, such as walls or human bodies.

Last but not least, it is important to note that only one beacon can be tested simultaneously. Due to technical restrictions, once a beacon is connected to the phone, other beacons cannot connect, and only one beacon can transmit data to the phone. This restriction comes from Estimote's Android design, which cannot be changed currently. However, this does not cause any problems since the beacons are identical, and the findings for one beacon will be similar to those with another. This test aims to determine under what circumstances these beacons can violate privacy regulations such as GDPR. This can happen if walls or other obstacles do not limit the range, and the beacons can still get data from nearby phones. In this instance, it is anticipated that the individual in possession of the intelligent mobile phone may not be aware of the utilization of ultra-wideband (UWB) technology in the vicinity, thereby rendering their smartphone susceptible to data collection, which contravenes the regulations of the protection of personal data.

Chapter 4

Implementation

This chapter first shows our implementation and how the analysis is conducted. In this functionality analysis, the range and signal strength of the Estimote beacons were tested. Later, the privacy aspect of these beacons will be analyzed. As mentioned, the findings will be reviewed based on the GDPR requirements. The evaluation of our findings will be explained in more detail in the next chapter.

4.1 Software Development Kit

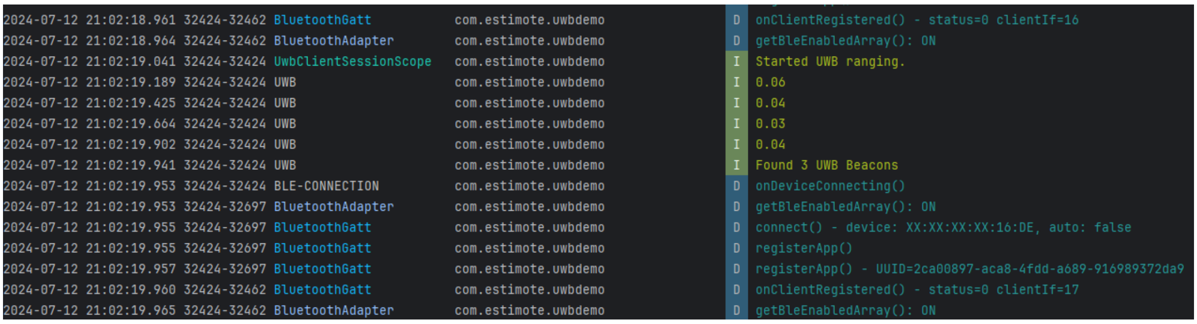
The Software Development Kit (SDK) provided by Estimote Inc [36] was used for the testing. This allowed us to use their Estimote UWB environment directly and connect our phones to their beacons.

```
uwbManager.init(
        activity = this
    )

requestPermissions(
    arrayOf(
        Manifest.permission.BLUETOOTH_SCAN,
        Manifest.permission.BLUETOOTH_CONNECT,
        Manifest.permission.UWB_RANGING
    ),
    1
)
```

Listing 4.1: Code snippet of permission requests.

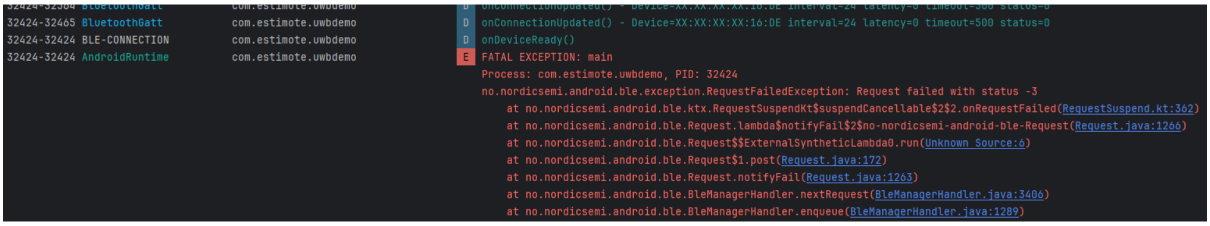
As shown in the code snippet above, permissions were initially requested from the UWB-enabled phone. Bluetooth was enabled, and before the beacon could connect via UWB, it had to communicate with BLE first. Once the Bluetooth connection was successful, the UWB ranging was started. As explained before, only one beacon at a time could be detected due to the technical restrictions on Android phones. If multiple UWB beacons were connected simultaneously, the following result is shown.



```
2024-07-12 21:02:18.961 32424-32462 BluetoothGatt          com.estimote.uwbdemo     D  onClientRegistered() - status=0 clientIf=16
2024-07-12 21:02:18.964 32424-32462 BluetoothAdapter       com.estimote.uwbdemo     D  getBleEnabledArray(): ON
2024-07-12 21:02:19.041 32424-32424 UwbClientSessionScope  com.estimote.uwbdemo     I  Started UWB ranging.
2024-07-12 21:02:19.189 32424-32424 UWB                    com.estimote.uwbdemo     I  0.06
2024-07-12 21:02:19.425 32424-32424 UWB                    com.estimote.uwbdemo     I  0.04
2024-07-12 21:02:19.664 32424-32424 UWB                    com.estimote.uwbdemo     I  0.03
2024-07-12 21:02:19.902 32424-32424 UWB                    com.estimote.uwbdemo     I  0.04
2024-07-12 21:02:19.941 32424-32424 UWB                    com.estimote.uwbdemo     I  Found 3 UWB Beacons
2024-07-12 21:02:19.953 32424-32424 BLE-CONNECTION         com.estimote.uwbdemo     D  onDeviceConnecting()
2024-07-12 21:02:19.953 32424-32697 BluetoothAdapter       com.estimote.uwbdemo     D  getBleEnabledArray(): ON
2024-07-12 21:02:19.955 32424-32697 BluetoothGatt          com.estimote.uwbdemo     D  connect() - device: XX:XX:XX:XX:16:DE, auto: false
2024-07-12 21:02:19.955 32424-32697 BluetoothGatt          com.estimote.uwbdemo     D  registerApp()
2024-07-12 21:02:19.957 32424-32697 BluetoothGatt          com.estimote.uwbdemo     D  registerApp() - UUID=2ca00897-aca8-4fdd-a689-916989372da9
2024-07-12 21:02:19.960 32424-32462 BluetoothGatt          com.estimote.uwbdemo     D  onClientRegistered() - status=0 clientIf=17
2024-07-12 21:02:19.965 32424-32462 BluetoothAdapter       com.estimote.uwbdemo     D  getBleEnabledArray(): ON
```

Figure 4.1: UWB finds three beacons at the same time

In this case, the phone is connected to one beacon via BLE and UWB. However, other UWB beacons were also found. Later, this application crashes as it does not support multi-device connections for Android phones. The code snippet below shows the regular error message was received when trying a multi-device connection.



```
32424-32384 BluetoothGatt          com.estimote.uwbdemo     D  onConnectionUpdated() - Device=XX:XX:XX:XX:16:DE interval=24 latency=0 timeout=500 status=0
32424-32465 BluetoothGatt          com.estimote.uwbdemo     D  onConnectionUpdated() - Device=XX:XX:XX:XX:16:DE interval=24 latency=0 timeout=500 status=0
32424-32424 BLE-CONNECTION         com.estimote.uwbdemo     D  onDeviceReady()
32424-32424 AndroidRuntime         com.estimote.uwbdemo     E  FATAL EXCEPTION: main
                                                               Process: com.estimote.uwbdemo, PID: 32424
                                                               no.nordicsemi.android.ble.exception.RequestFailedException: Request failed with status -3
                                                                   at no.nordicsemi.android.ble.ktx.RequestSuspendKt$suspendCancellable$2$2.onRequestFailed(RequestSuspend.kt:362)
                                                                   at no.nordicsemi.android.ble.Request.lambda$notifyFail$2$no-nordicsemi-android-ble-Request(Request.java:1266)
                                                                   at no.nordicsemi.android.ble.Request$$ExternalSyntheticLambda0.run(Unknown Source:6)
                                                                   at no.nordicsemi.android.ble.Request$1.post(Request.java:172)
                                                                   at no.nordicsemi.android.ble.Request.notifyFail(Request.java:1263)
                                                                   at no.nordicsemi.android.ble.BleManagerHandler.nextRequest(BleManagerHandler.java:3406)
                                                                   at no.nordicsemi.android.ble.BleManagerHandler.enqueue(BleManagerHandler.java:1289)
```

Figure 4.2: Error message during multi-device connection

The CEO of Estimote Inc. was contacted regarding this issue and to find a solution. A temporary solution was found, and the firmware of the beacons was updated. However, further investigation showed that multi-device connection was still unavailable for Android phones. Therefore, the research had to continue using a single beacon and turn off the others. This might be enabled in the future, and more work can be done. This will be mentioned in the later chapters.

4.2 Functionality Analysis

In this section, the range and signal strength of UWB beacons were tested. The range can raise some privacy questions, which will be analyzed in the next chapter as the findings will be evaluated.

4.2.1 Ranging

In order to test the range, the following commands were used in the SDK.

```
uwbManager.rangingResult.onEach { rangingResult ->
    when (rangingResult) {
        is EstimoteUWBRangingResult.Position -> {
            Log.i("UWB", rangingResult.position.distance?.value.toString())
            }
        is EstimoteUWBRangingResult.Error -> {
            Log.i("UWB", "Error: ${rangingResult.message}")
        }
        else -> Unit
    }
}.launchIn(lifecycleScope)
```

Listing 4.2: Code snippet of UWB ranging.

This range helped us determine the phone's position. The values here can be interpreted in two different ways:

1. Phone's position with respect to the beacon
2. Beacon's position with respect to phone

The research is independent of which interpretation is used. However, the former interpretation is preferred to be used in real-life applications; these beacons are fixed onto a wall or surface, and phones will be moving in 3D space with their users and tracked. A further limitation necessitates a cable connecting the mobile phone and the laptop to run the software development kit (SDK). In other environments, the WiFi connection can also run the SDK on the phone and test the UWB connection between the phone and the beacon. However, this doesn't affect the setup, and the movement of a smartphone can be simulated in a 3D space by moving the beacons while the phone is fixed due to a cable connection.

4.2.2 Signal Strength

The beacons' signal strength will be measured using the same code snippet above. This will show the values received from the ranging function. Signal strength will also be measured under certain circumstances, as explained in the previous chapter 3.3.3. In figure 4.1, it can be seen that the program has already started with ranging before finding 3 UWB beacons. A similar output format is expected when conducting signal strength experiments.

4.3 Privacy Analysis

In this section, a use case analysis will be explained and highlighted, highlighting which cases using UWB may violate privacy regulations and frameworks. Estimote Inc. has recently published more than 200 use cases on their website [17]. These use cases will be thoroughly analyzed and categorized. More than ten use cases were found that are related to our research question and can raise specific privacy concerns. They will be thoroughly evaluated in the next chapter. These chosen use cases are representative and represent each use case category, such as healthcare, active tracking, marketing, and workplace. In addition, they have different characteristics, such as outdoor or indoor. These use cases can be found in the appendix. Furthermore, pertinent privacy regulations will be used to evaluate these use cases. These different privacy regulations were mapped onto a privacy mapping in 2.1.4.

Chapter 5

Evaluation

This chapter will evaluate the technical findings of UWB beacons and smartphones. The technical findings include range and signal strength tests. These criteria will help us address privacy concerns when using these beacons with UWB technology. Later, the preservation of privacy in our SDK setup will be evaluated. This is followed by a pervasive analysis of different UWB technology use cases that Estimote Inc. gives. This analysis will evaluate every use case in detail and show where and under what circumstances they lack privacy. The lack of privacy will be analyzed based on the privacy mapping explained in 2.1.4. Finally, an overview of the privacy evaluation will be presented based on an in-depth analysis of the use cases.

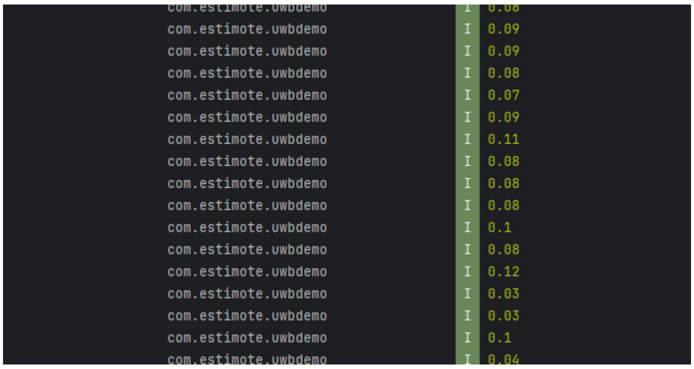
5.1 Technical Findings

Our technical findings highlight the privacy issues that can occur when UWB beacons are operated with smartphones nearby. In this section, the range and signal strength were tested. Signal strength is based on the wrong range during the tests. This will be shown in more detail in 5.1.1.

5.1.1 Range & Signal Strength Test Results

The methods used to test the beacons and their signal strength can be found in 3.3.3. These methods help us understand privacy concerns when using UWB technology in different cases.

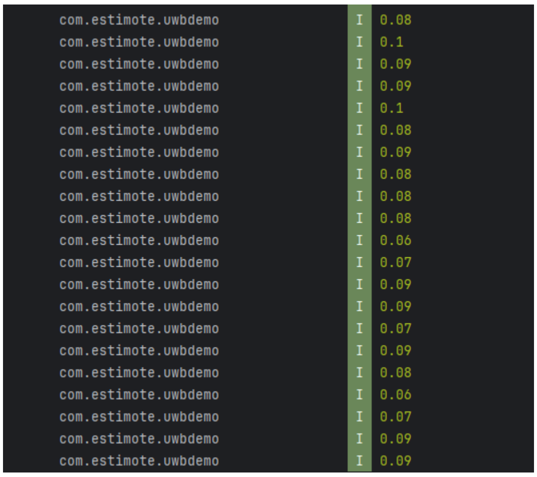
Range Testing



```
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.09
com.estimote.uwbdemo                    I  0.09
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.07
com.estimote.uwbdemo                    I  0.09
com.estimote.uwbdemo                    I  0.11
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.1
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.12
com.estimote.uwbdemo                    I  0.03
com.estimote.uwbdemo                    I  0.03
com.estimote.uwbdemo                    I  0.1
com.estimote.uwbdemo                    I  0.04
```

Figure 5.1: UWB Beacon test close range less than 10 cm

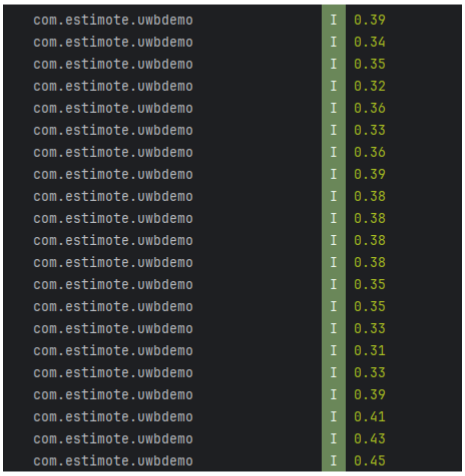
In the figure above 5.1, it can be seen that UWB ranging can find the phone and measure the distance. In this test, the beacon was placed close to the phone, and the distance was measured precisely. According to Estimote Inc., the precision of these beacons is 10 cm [36], and in this distance, this statement seems correct. The test range is between 0.12 and 0.03 meters. The difference between the highest and the lowest measured distance is 0.09 meters or 9 cm. The average is 0.08 meters, calculated by adding all the measurements and dividing by the number of results.



```
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.1
com.estimote.uwbdemo                    I  0.09
com.estimote.uwbdemo                    I  0.09
com.estimote.uwbdemo                    I  0.1
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.09
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.06
com.estimote.uwbdemo                    I  0.07
com.estimote.uwbdemo                    I  0.09
com.estimote.uwbdemo                    I  0.09
com.estimote.uwbdemo                    I  0.07
com.estimote.uwbdemo                    I  0.09
com.estimote.uwbdemo                    I  0.08
com.estimote.uwbdemo                    I  0.06
com.estimote.uwbdemo                    I  0.07
com.estimote.uwbdemo                    I  0.09
com.estimote.uwbdemo                    I  0.09
```

Figure 5.2: Estimote UWB Beacon test close range 10 cm

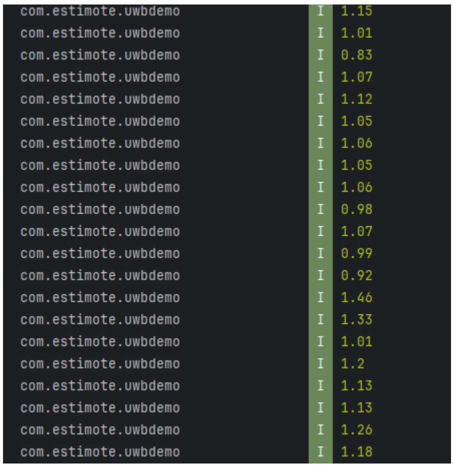
In this test 5.2, the beacon was placed further than in the previous test, and the test results were more accurate. The test result range varies between 0.06 and 0.1 meters. The average is 0.082 meters, and this measurement is quite accurate. However, there can be more variation in the test results in future tests.



```
com.estimote.uwbdemo    I  0.39
com.estimote.uwbdemo    I  0.34
com.estimote.uwbdemo    I  0.35
com.estimote.uwbdemo    I  0.32
com.estimote.uwbdemo    I  0.36
com.estimote.uwbdemo    I  0.33
com.estimote.uwbdemo    I  0.36
com.estimote.uwbdemo    I  0.39
com.estimote.uwbdemo    I  0.38
com.estimote.uwbdemo    I  0.38
com.estimote.uwbdemo    I  0.38
com.estimote.uwbdemo    I  0.38
com.estimote.uwbdemo    I  0.35
com.estimote.uwbdemo    I  0.35
com.estimote.uwbdemo    I  0.33
com.estimote.uwbdemo    I  0.31
com.estimote.uwbdemo    I  0.33
com.estimote.uwbdemo    I  0.39
com.estimote.uwbdemo    I  0.41
com.estimote.uwbdemo    I  0.43
com.estimote.uwbdemo    I  0.45
```

Figure 5.3: Estimote UWB Beacon test range 35 cm

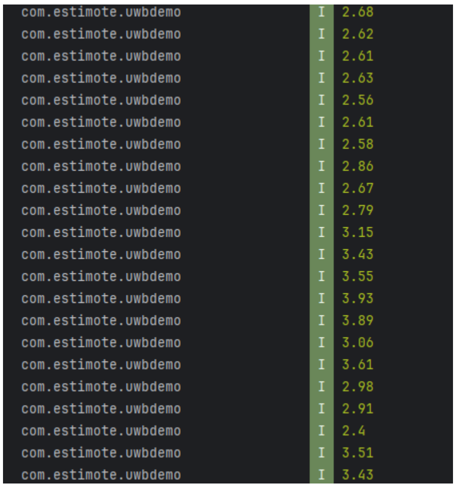
In the results above 5.3, the numbers are more precise than the results before. As these beacons are made to connect to the phones from a distance, their very close-range test results can be more inaccurate than mid-range test results. The smallest distance measured is 0.31 meters, and the highest is 0.45 meters. The average is 38 cm, which is very close to our actual distance of 35 cm.



```
com.estimote.uwbdemo    I  1.15
com.estimote.uwbdemo    I  1.01
com.estimote.uwbdemo    I  0.83
com.estimote.uwbdemo    I  1.07
com.estimote.uwbdemo    I  1.12
com.estimote.uwbdemo    I  1.05
com.estimote.uwbdemo    I  1.06
com.estimote.uwbdemo    I  1.05
com.estimote.uwbdemo    I  1.06
com.estimote.uwbdemo    I  0.98
com.estimote.uwbdemo    I  1.07
com.estimote.uwbdemo    I  0.99
com.estimote.uwbdemo    I  0.92
com.estimote.uwbdemo    I  1.46
com.estimote.uwbdemo    I  1.33
com.estimote.uwbdemo    I  1.01
com.estimote.uwbdemo    I  1.2
com.estimote.uwbdemo    I  1.13
com.estimote.uwbdemo    I  1.13
com.estimote.uwbdemo    I  1.26
com.estimote.uwbdemo    I  1.18
```

Figure 5.4: Estimote UWB Beacon test range 1 meter

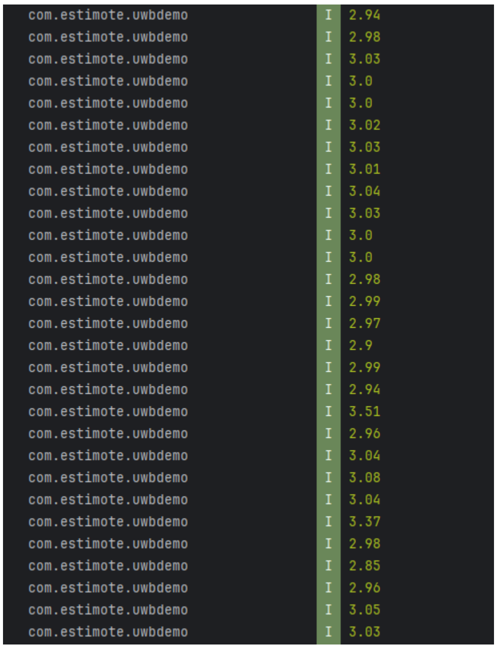
In the figure above 5.4, the distance was increased to 1 meter to determine how precise the distance between the phone and the beacon can be measured. Our lowest value here is 0.83 meters, and the highest is 1.46 meters. The average is 1.09 meters, which seems to be as precise as what Estimote stated about the accuracy of these beacons [36]. However, it is important to note that these tests were conducted in a room with furniture and items around, and these items and furniture can impact the measurements negatively.



```
com.estimote.uwbdemo                     I  2.68
com.estimote.uwbdemo                     I  2.62
com.estimote.uwbdemo                     I  2.61
com.estimote.uwbdemo                     I  2.63
com.estimote.uwbdemo                     I  2.56
com.estimote.uwbdemo                     I  2.61
com.estimote.uwbdemo                     I  2.58
com.estimote.uwbdemo                     I  2.86
com.estimote.uwbdemo                     I  2.67
com.estimote.uwbdemo                     I  2.79
com.estimote.uwbdemo                     I  3.15
com.estimote.uwbdemo                     I  3.43
com.estimote.uwbdemo                     I  3.55
com.estimote.uwbdemo                     I  3.93
com.estimote.uwbdemo                     I  3.89
com.estimote.uwbdemo                     I  3.06
com.estimote.uwbdemo                     I  3.61
com.estimote.uwbdemo                     I  2.98
com.estimote.uwbdemo                     I  2.91
com.estimote.uwbdemo                     I  2.4
com.estimote.uwbdemo                     I  3.51
com.estimote.uwbdemo                     I  3.43
```

Figure 5.5: Estimote UWB Beacon test range 2 meters

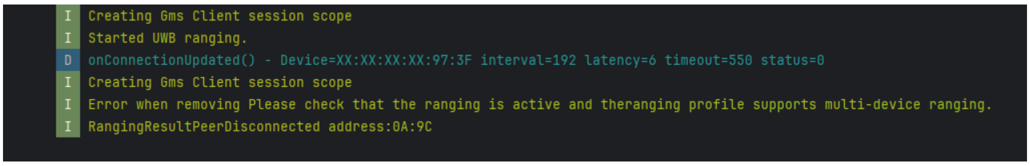
One of the least accurate measurements recorded was testing an Estimote beacon from 2 meters. In the figure 5.5, it can be seen that all values lie above 2.4 meters. Therefore, this test result is insignificant. The possible correction of this result is removing any items between the phone and the beacon.



```
com.estimote.uwbdemo                     I  2.94
com.estimote.uwbdemo                     I  2.98
com.estimote.uwbdemo                     I  3.03
com.estimote.uwbdemo                     I  3.0
com.estimote.uwbdemo                     I  3.0
com.estimote.uwbdemo                     I  3.02
com.estimote.uwbdemo                     I  3.03
com.estimote.uwbdemo                     I  3.01
com.estimote.uwbdemo                     I  3.04
com.estimote.uwbdemo                     I  3.03
com.estimote.uwbdemo                     I  3.0
com.estimote.uwbdemo                     I  3.0
com.estimote.uwbdemo                     I  2.98
com.estimote.uwbdemo                     I  2.99
com.estimote.uwbdemo                     I  2.97
com.estimote.uwbdemo                     I  2.9
com.estimote.uwbdemo                     I  2.99
com.estimote.uwbdemo                     I  2.94
com.estimote.uwbdemo                     I  3.51
com.estimote.uwbdemo                     I  2.96
com.estimote.uwbdemo                     I  3.04
com.estimote.uwbdemo                     I  3.08
com.estimote.uwbdemo                     I  3.04
com.estimote.uwbdemo                     I  3.37
com.estimote.uwbdemo                     I  2.98
com.estimote.uwbdemo                     I  2.85
com.estimote.uwbdemo                     I  2.96
com.estimote.uwbdemo                     I  3.05
com.estimote.uwbdemo                     I  3.03
```

Figure 5.6: Estimote UWB Beacon test 3 meters

This time, the measurement is considerably more precise. In the test above 5.6, our test result varies between 2.85 and 3.51 meters. The average is 3.02 meters, which is accurate as it is less than 10 cm from the actual distance.



```
I  Creating Gms Client session scope
I  Started UWB ranging.
D  onConnectionUpdated() - Device=XX:XX:XX:XX:97:3F interval=192 latency=6 timeout=550 status=0
I  Creating Gms Client session scope
I  Error when removing Please check that the ranging is active and theranging profile supports multi-device ranging.
I  RangingResultPeerDisconnected address:0A:9C
```

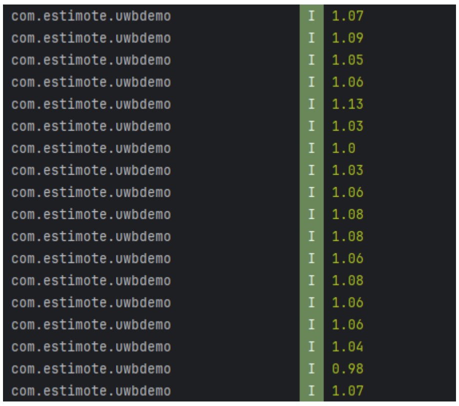
Figure 5.7: Estimote UWB Beacon test 5 meters

When the test is conducted from 5 meters, connection problems can be seen between the phone and the beacon in 5.7. Although it is unclear why this problem occurs, multiple Estimote UWB beacons can prevent it. However, this is impossible in our current setup as Android phones are used.

So far, the tests above have been conducted in the same room, and the surrounding items have barely affected the signal strength. In the next part, the tests were conducted behind a wall, and these test results without line-of-sight will help us address privacy questions when using the Estimote UWB beacons.

Signal Strength

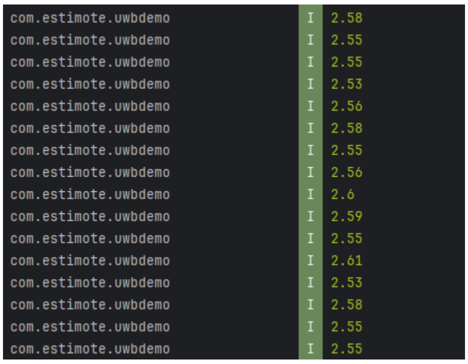
The tests above were also conducted without any obstacles. A wall was used between the phone and the Estimote UWB beacon in the following test cases. The goal is to discover what kind of effects can be observed when there is a connection between the phone and the beacon. It is important to note that the wall between them was 10 cm thick, and in some other use cases, the walls can be thinner or thicker, depending on the building and wall type.



```
com.estimote.uwbdemo                I  1.07
com.estimote.uwbdemo                I  1.09
com.estimote.uwbdemo                I  1.05
com.estimote.uwbdemo                I  1.06
com.estimote.uwbdemo                I  1.13
com.estimote.uwbdemo                I  1.03
com.estimote.uwbdemo                I  1.0
com.estimote.uwbdemo                I  1.03
com.estimote.uwbdemo                I  1.06
com.estimote.uwbdemo                I  1.08
com.estimote.uwbdemo                I  1.08
com.estimote.uwbdemo                I  1.06
com.estimote.uwbdemo                I  1.08
com.estimote.uwbdemo                I  1.06
com.estimote.uwbdemo                I  1.06
com.estimote.uwbdemo                I  1.04
com.estimote.uwbdemo                I  0.98
com.estimote.uwbdemo                I  1.07
```

Figure 5.8: Estimote UWB Beacon from 1 meter behind a wall

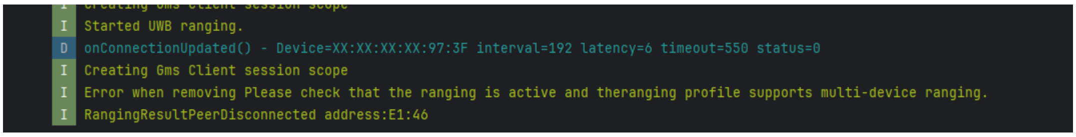
In the figure above 5.8, the results vary from 0.98 and 1.13 meters. The average is 1.06 meters, below the accuracy threshold given by Estimote [36]. Even though the beacon is behind a wall, the accuracy of these results is quite high.



```
com.estimote.uwbdemo                 I  2.58
com.estimote.uwbdemo                 I  2.55
com.estimote.uwbdemo                 I  2.55
com.estimote.uwbdemo                 I  2.53
com.estimote.uwbdemo                 I  2.56
com.estimote.uwbdemo                 I  2.58
com.estimote.uwbdemo                 I  2.55
com.estimote.uwbdemo                 I  2.56
com.estimote.uwbdemo                 I  2.6
com.estimote.uwbdemo                 I  2.59
com.estimote.uwbdemo                 I  2.55
com.estimote.uwbdemo                 I  2.61
com.estimote.uwbdemo                 I  2.53
com.estimote.uwbdemo                 I  2.58
com.estimote.uwbdemo                 I  2.55
com.estimote.uwbdemo                 I  2.55
```

Figure 5.9: Estimote UWB Beacon from 2.5 meters behind a wall

The test results above 5.9 show that the accuracy remains as the distance between the beacon and the phone gets more significant. Although all values lie above 2.5 meters, the average is 2.56 meters. This is significantly accurate, given that the average accuracy is 10 cm.



```
I  Creating Gms Client session scope
I  Started UWB ranging.
D  onConnectionUpdated() - Device=XX:XX:XX:XX:97:3F interval=192 latency=6 timeout=550 status=0
I  Creating Gms Client session scope
I  Error when removing Please check that the ranging is active and theranging profile supports multi-device ranging.
I  RangingResultPeerDisconnected address:E1:46
```

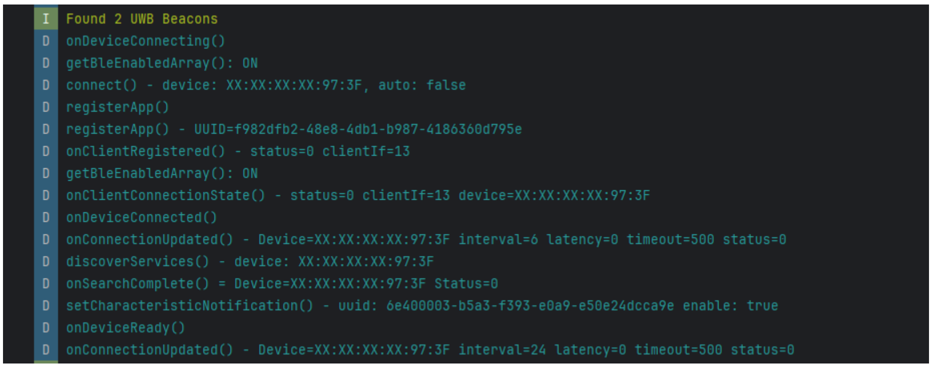
Figure 5.10: Estimote UWB Beacon from 4 meters behind a wall

In 5.10, the SDK raised an error. The phone found the UWB beacon. However, the connection could not be set up. Multi-device ranging cannot be used currently, so a single UWB beacon fails to connect from 4 meters. It is important to note that the beacons can still connect from 4 meters or more when using multi-device ranging as they can be detected by the phone through a wall.

5.1.2 Preservation of Privacy

MAC Addresses

The medium access control (MAC) addresses are hidden in our SDK.



```
I  Found 2 UWB Beacons
D  onDeviceConnecting()
D  getBleEnabledArray(): ON
D  connect() - device: XX:XX:XX:XX:97:3F, auto: false
D  registerApp()
D  registerApp() - UUID=f982dfb2-48e8-4db1-b987-4186360d795e
D  onClientRegistered() - status=0 clientIf=13
D  getBleEnabledArray(): ON
D  onClientConnectionState() - status=0 clientIf=13 device=XX:XX:XX:XX:97:3F
D  onDeviceConnected()
D  onConnectionUpdated() - Device=XX:XX:XX:XX:97:3F interval=6 latency=0 timeout=500 status=0
D  discoverServices() - device: XX:XX:XX:XX:97:3F
D  onSearchComplete() = Device=XX:XX:XX:XX:97:3F Status=0
D  setCharacteristicNotification() - uuid: 6e400003-b5a3-f393-e0a9-e50e24dcca9e enable: true
D  onDeviceReady()
D  onConnectionUpdated() - Device=XX:XX:XX:XX:97:3F interval=24 latency=0 timeout=500 status=0
```

Figure 5.11: Hidden MAC addresses

Before the program crashes when using a multi-device connection as in 4.2, it can be seen in the output that the device MAC addresses are listed in 5.11. It helps us identify different beacons with their visible ending numbers, such as 97:3F. However, the rest of the MAC address is censored with ”X” to preserve the privacy of these beacons and prevent unauthorized or unintended access to them.

5.2 Privacy Analysis in Different Use Cases

This section analyzes the use cases mentioned in 4.3 based on the privacy mapping in 2.1.4. The use cases were categorized into four different groups: healthcare, active tracking, marketing, and workplace. The detailed categorization of all use cases can be found in A.1. These use cases were categorized to discover the possible application fields of these UWB beacons and address privacy issues.

5.2.1 Healthcare

Use Case #1

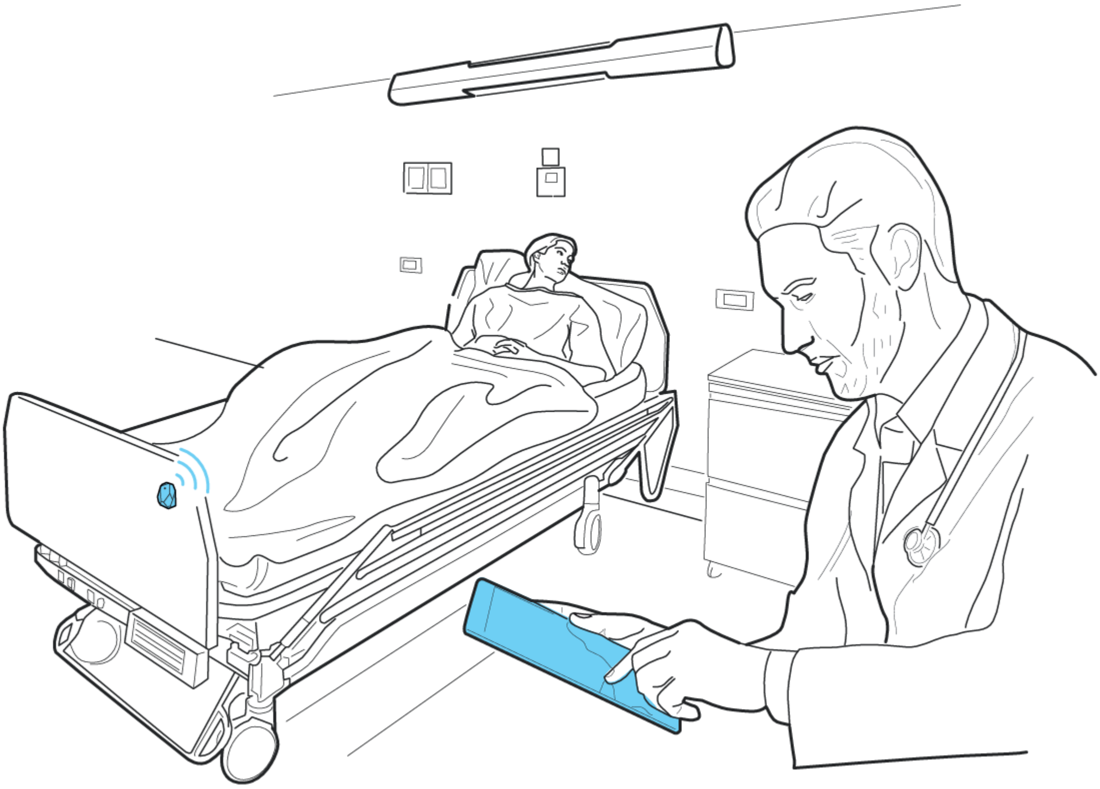


Figure 5.12: Retrieving patient data [10]

In this case, the healthcare personnel can retrieve and access patient data on their tablet. They can access personal health data stored on the hospital's servers.

1. **Awareness:** The patient can be aware if it is told verbally. The patient then knows that their data are collected and can be accessed by personnel.
2. **Transparency:** The patient can be told why their data are being used and for what purposes.
3. **Confidentiality:** As it can be seen in 3.4, there is no data storage on UWB beacons. However, patient data can be stored in the cloud or servers, depending on the hospital's policies.
4. **Accountability:** In this case, the patient can hold the hospital or the facility responsible for their actions. In case of any data breach or loss, the hospital can be sued.
5. **Data Minimization:** Estimote UWB beacons also use BLE technology, so their data usage is limited [17]. In this case, the UWB beacon can only inform the personnel which patient they are treating, and patient data can be retrieved from their server.

6. **Accuracy:** Patient data can be kept accurate when using Estimote UWB beacons and updating patient data directly from a tablet used by personnel.

7. **Storage Limitation:** The only data that can be stored is the patient's identifier. This identity can help personnel find and access the data of a specific patient. Therefore, data storage is quite limited to the patient's identifier.

8. **Lawfulness:** The test result in 5.11 shows that the MAC addresses of these beacons are hidden. This protects the Estimote UWB beacon and limits its data processing.

9. **Anonymity:** Personal patient data is limited in identifying the subject (patient). However, the identity of the patient is disclosed. Therefore, the anonymity principle does not apply.

10. **Unlinkability:** It is possible to connect personal information back to the data subject. Although linkability depends on the hospital's database tables, in most cases, the personal information has an identifier that can be traced back to the patient.

11. **Unobservability:** It is unclear which devices can connect to a patient's UWB beacon. The connected device can belong to non-personnel, violating personal data privacy.

12. **Good Faith:** Patient data is used in good faith here, as the intention is to access the patient data and offer the personnel ease in dealing with many different patients throughout the day.

Use Case #2

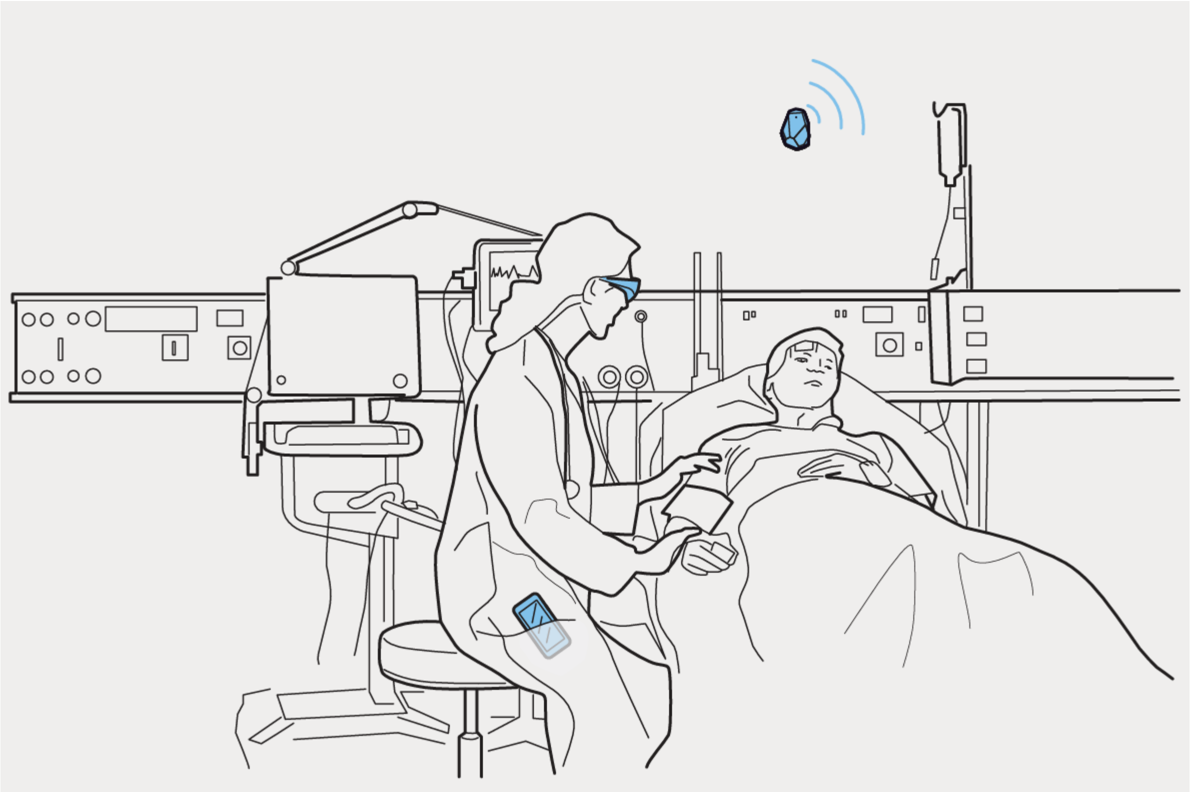


Figure 5.13: Accessing patient information [10]

Health personnel can access a patient's health data via the UWB beacon. They can see the information on their glasses with the help of their smartphone.

1. **Awareness:** Patients can be told verbally that their data are being used while getting treatment.

2. **Transparency:** Depending on the patient's condition, the patient can know the specific data processing purposes. However, as the patient's condition may prevent them from knowing the purposes of their data processing, this use case may need to be more transparent.

3. **Confidentiality:** Similar to the previous use case, the confidentiality of data storage depends on the hospital's technical infrastructure, as there is no data storage on UWB beacons.

4. **Accountability:** In this case, the hospital can be held liable for any data breach or loss, as data storage is the hospital's responsibility.

5. **Data Minimization:** Data is minimized due to the technical limitations of BLE technology.

6. **Accuracy:** Data accuracy depends on the hospital as well. However, if a third party accesses the UWB beacon and can alter the data, the data can be manipulated and may no longer be accurate.

7. **Storage Limitation:** As discussed, data storage on UWB beacons is quite limited. UWB beacon helps other devices identify the patient and retrieve their personal information.

8. **Lawfulness:** Patient data can be processed lawfully, as the UWB beacons hide their MAC addresses like in our test in 5.11.

9. **Anonymity:** Patient information is used while their identity is disclosed as well. While this is very helpful when used by healthcare personnel, it can also be used for malicious purposes behind the wall of another hospital room. This is possible as our UWB-enabled smartphone could set up a connection with UWB beacons behind a wall in 5.9.

10. **Unlinkability:** Due to the identification of personal data at the hospital, the personal information can be linked to the data subject (patient).

11. **Unobservability:** Third parties can see patient data if they can successfully connect to the UWB beacon. This raises significant privacy issues.

12. **Good Faith:** Like the previous use case, this data processing is intended to be done in good faith.

5.2.2 Direct Tracking

Use Case #3

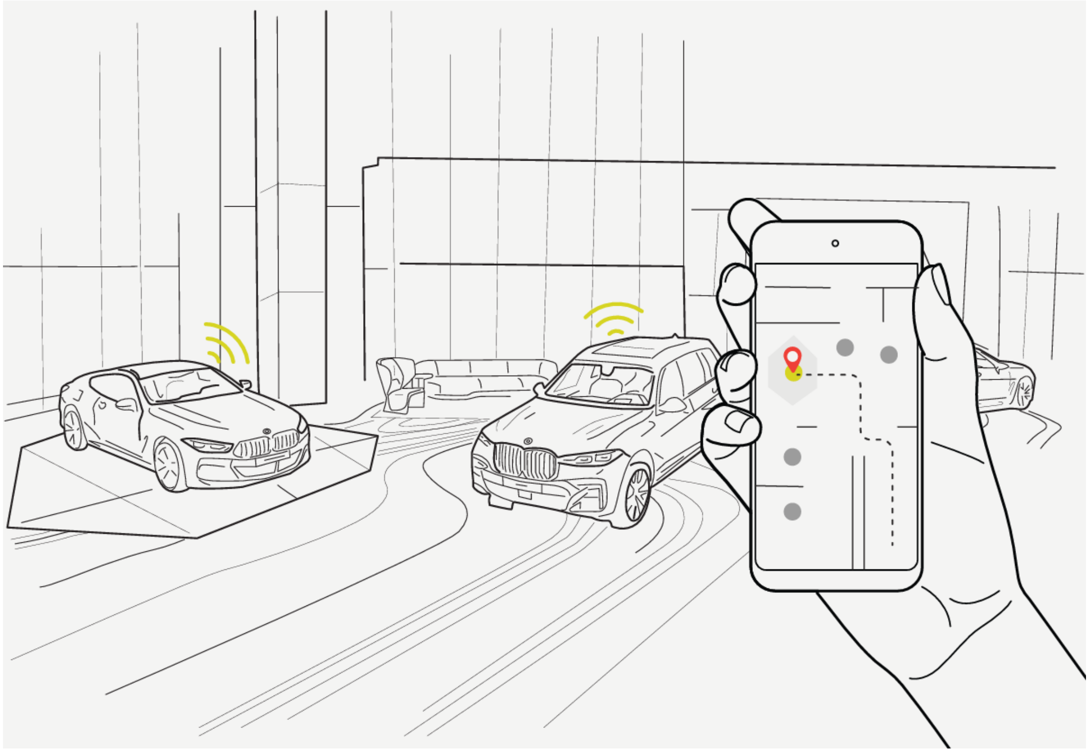


Figure 5.14: Finding the way to a car [10]

The car owner can find their way to their car. Multiple cars have UWB beacons or tags; however, the personal vehicle is displayed on the phone. This can be especially helpful in a crowded parking lot. The car's last location is saved on the phone.

1. **Awareness:** The user who placed the UWB beacon inside the car is aware of its data usage. This can be achieved when buying the UWB beacons, and there is detailed information on Estimote's website [17].

2. **Transparency:** The Estimote Inc. is transparent on their website about data processing purposes [17]. This includes how data is used and how it can be stored.

3. **Confidentiality:** In this case, personal information consists of the location of their vehicle. So far, it is unclear whether other parties can track this car.

4. **Accountability:** If the location of the personal vehicle is compromised, Estimote Inc. can be held responsible by the data subject for this data breach.

5. **Data Minimization:** Data minimization is fulfilled as data consists of the vehicle's location only.

6. **Accuracy:** The vehicle's location is kept accurate on the smartphone by UWB beacons.

7. **Storage Limitation:** Storage is limited to the location and navigation on the phone. This limitation is based on the goal of this use case.

8. **Lawfulness:** Data is processed lawfully as the addresses of these beacons are hidden from the public.

9. **Anonymity:** Although it is unclear whether the UWB beacon reveals the owner of a vehicle, it might be possible to trace this down. Therefore, the anonymity cannot be guaranteed all the time.

10. **Unlinkability:** Similar to the point before, the information can be linked to the data subject.

11. **Unobservability:** If third parties connect to UWB beacons, they can track the vehicle's location and use this information for other purposes.

12. **Good Faith:** The original intention of using this technology is in good faith.

Use Case #4

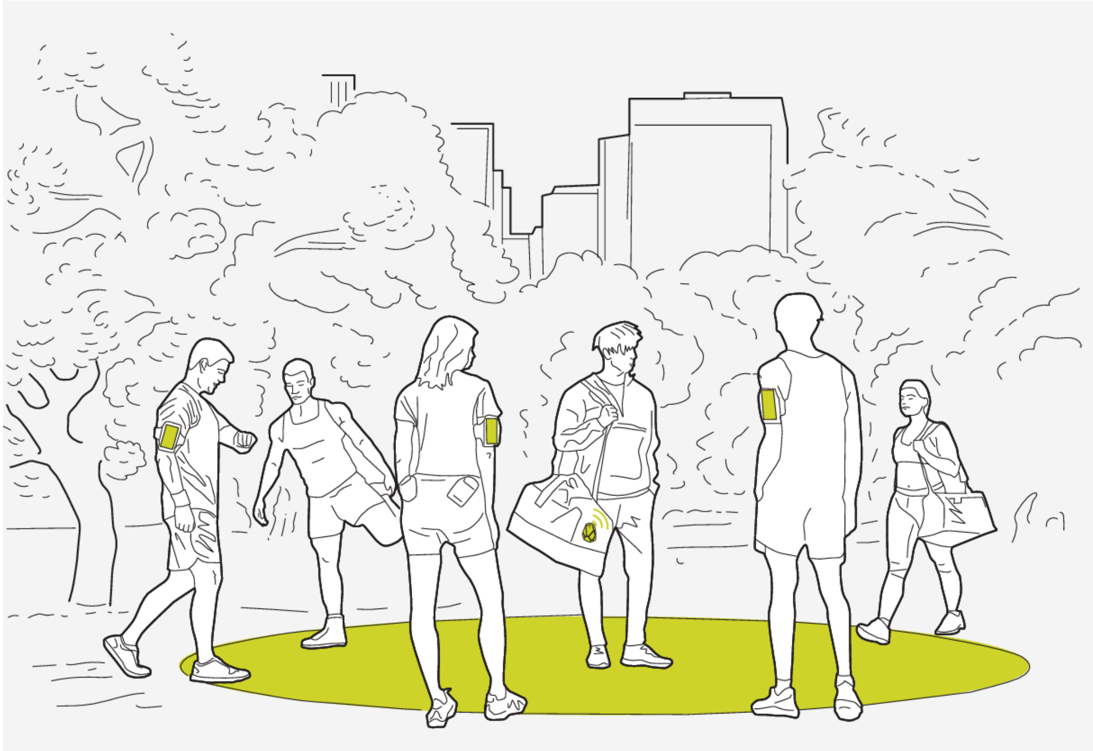


Figure 5.15: Athletes' phone connected to a UWB beacon [10]

The coach can keep track of the attendees and the number of people attending the exercise session. For instance, this data can then be stored on the coach's phone.

1. **Awareness:** The coach can tell the athletes that their phones are connected to a UWB beacon. Then, the data subjects will be aware of the data processing and collection. However, since this is a verbal communication, misunderstandings or negligence can occur, and some people who join the exercise later may not be aware of the data processing and collection via UWB beacon. A similar situation applies to by-passers. Their phone might also connect, but they may not be aware of the data collection.

2. **Transparency:** The coach can inform the athletes about the specific data processing purposes. Then, the transparency principle will be fulfilled. However, similar to the previous point, the coach might lack information about the purpose, or there might be miscommunication. In this case, the purpose would not be transparent.

3. **Confidentiality:** So far, there is no known data storage during this use case. If so, fulfilling this principle depends on the coach's cloud infrastructure.

4. **Accountability:** If the coach uses the data collected from athletes for different purposes, the athletes can hold the coach accountable for their actions.

5. **Data Minimization:** The data needed is minimized depending on the purpose. If we keep track of the proximity of athletes, then the needed data is their current distance.

6. **Accuracy:** According to our test results in 5.6, a single UWB beacon can accurately track the distances in close range.

7. **Storage Limitation:** The storage is limited as there is only one UWB beacon in use.

8. **Lawfulness:** The data processing is lawful.

9. **Anonymity:** It is unclear if Estimote UWB beacon keeps track of the phones anonymously.

10. **Unlinkability:** If the previous point is not fulfilled, the information can be linked to the data subjects, violating this principle.

11. **Unobservability:** Third parties can observe and use this activity as its usage occurs outside, and unauthorized access can occur.

12. **Good Faith:** The intention of this use case is in good faith.

Use Case #5

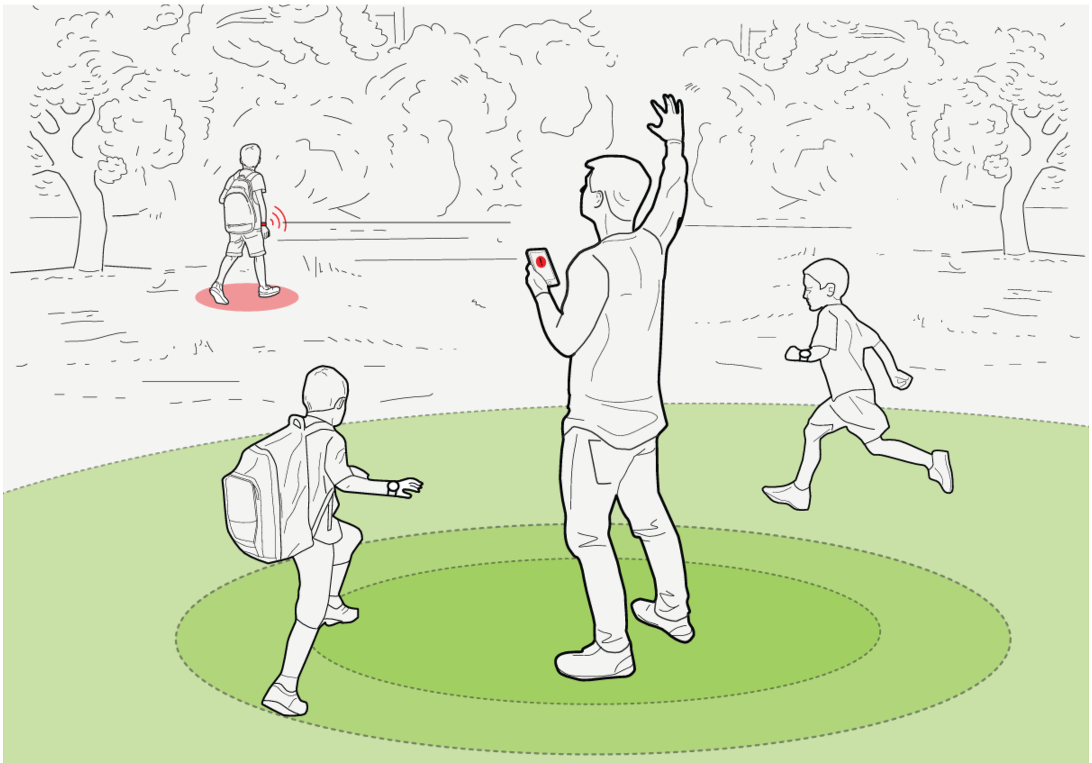


Figure 5.16: Tracking people who leave a specified zone [10]

The teacher can see if any child is leaving a specified zone for security reasons.

1. **Awareness:** The teacher can inform the children that they are being tracked by UWB beacon. However, as mentioned in previous use cases, a similar issue can occur here, such as miscommunication or a lack of information.

2. **Transparency:** It is possible to be transparent about the data processing purposes. Since children might lack comprehension, the parents of the children can be informed properly before using UWB.

3. **Confidentiality:** In this use case, there is no data storage. Therefore, it is not possible to assess if this principle is fulfilled. However, trivially, the confidentiality of data storage is fulfilled as there is no threat.

4. **Accountability:** The parents of the children can hold the teacher accountable if the technology is used for undeclared purposes.

5. **Data Minimization:** The only data that is acquired is the children's location. This is the only data needed for its purpose, so data usage is minimized.

6. **Accuracy:** As there is no known data storage in this case, the accuracy of stored data is trivially fulfilled.

7. **Storage Limitation:** There is no known data storage in this use case. Therefore, the storage limitation is trivially fulfilled.

8. **Lawfulness:** The data is being processed lawfully as the UWB beacons are not directly accessible, and their MAC addresses are not shown during the connection like in 5.11.

9. **Anonymity:** The anonymity of the data subject is open to discussion as each child is marked with their own device here. Therefore, this principle is not fulfilled.

10. **Unlinkability:** The activities of children's devices can be linked back to the children. This is because the anonymity of the data subject is not fulfilled. As a result, unlinkability is not fulfilled either.

11. **Unobservability:** Since it is unclear which devices can track the children's devices using UWB, the unobservability of this use case is questionable.

12. **Good Faith:** The intention of this use case is in good faith.

Use Case #6

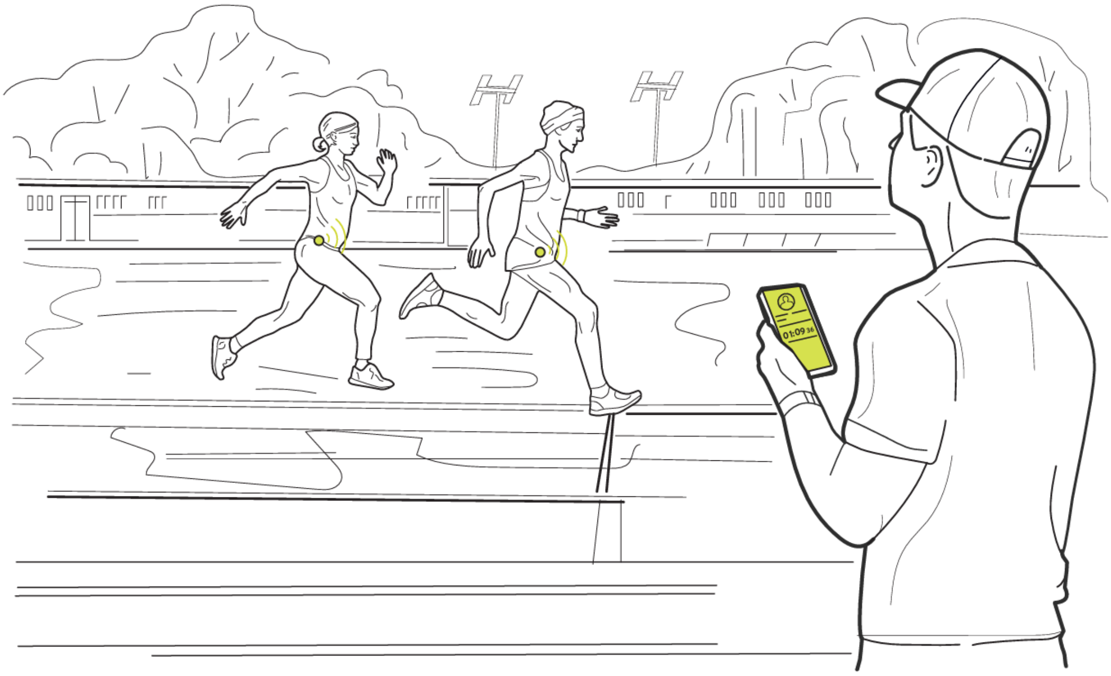


Figure 5.17: Athletes' performance is tracked by trainer's phone [10]

The trainer can track the athletes' performance. Later, this data can be stored on their phone or a server. Over time, the trainer can keep track of the athletes' progress after several training sessions.

1. **Awareness:** Since the athletes are wearing a small UWB beacon, they are aware of the data processing.
2. **Transparency:** This case is transparent if the coach tells the athletes about the data collection purposes.
3. **Confidentiality:** Given that the data can be stored on the coach's phone, it allows it to be stored with appropriate security measures. However, if no password is required to unlock the phone, the confidentiality of personal information cannot be guaranteed.
4. **Accountability:** The athletes can hold the coach accountable for any misuse or data breach.
5. **Data Minimization:** If the purpose is solely to collect data about the athletes' performance, then the data collection is kept to a bare minimum.
6. **Accuracy:** The data kept is accurate and correct as UWB beacons can precisely track the distance as in 5.6.

7. **Storage Limitation:** The storage limitation depends on the coach. If the coach prefers to keep the data longer than necessary, this violates the storage limitation.

8. **Lawfulness:** Data processing is done lawfully, as the beacons are protected from direct breaches as in 5.11.

9. **Anonymity:** The data is not collected anonymously. Each athlete's data will be collected and stored.

10. **Unlinkability:** Due to the lack of anonymity, the personal information can be linked back to the athletes.

11. **Unobservability:** Unobservability is not guaranteed since the UWB beacons can connect to phones other than the coach's.

12. **Good Faith:** The data processing is carried out in good faith.

Use Case #7

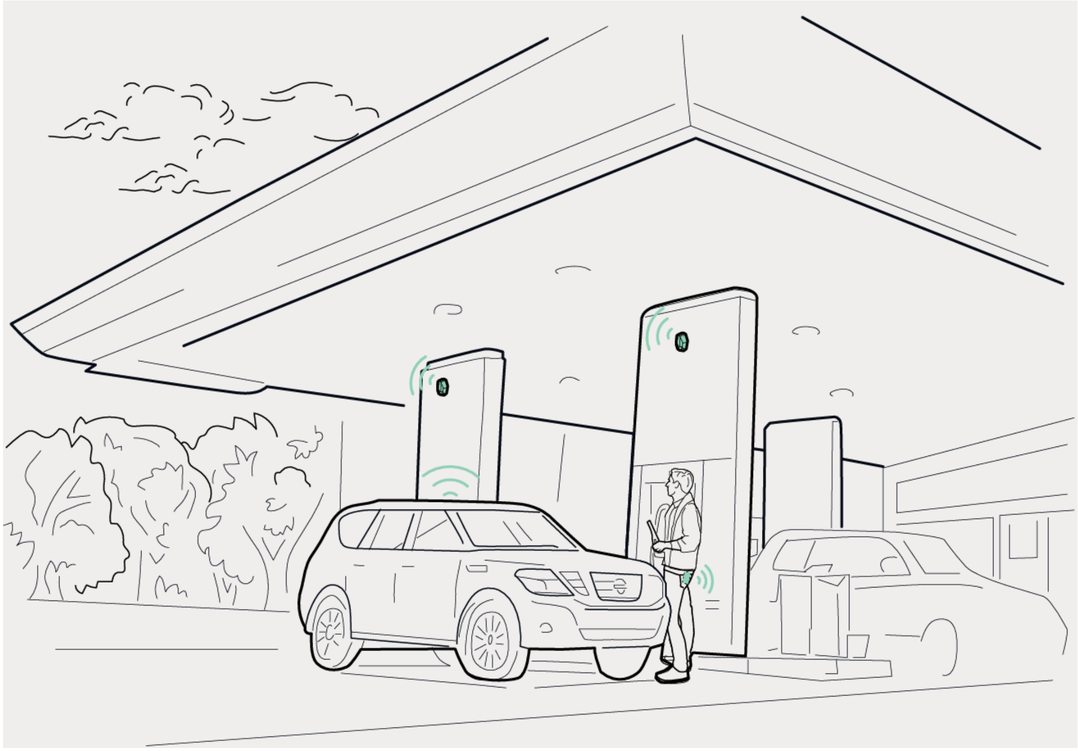


Figure 5.18: Tracking person and their car at gas station [10]

The gas company keeps track of the vehicles and customers visiting their gas stations. They can create statistics and track individual customers to offer a loyalty bonus upon revisiting.

1. **Awareness:** Drivers can be informed by a sign stating that UWB technologies are in use. However, only some drivers can see this sign, as some drivers can be in a rush and might need more time to check out. This makes it difficult to make people aware of the data processing.

2. **Transparency:** If the principle above is fulfilled, the transparency principle can be fulfilled similarly. The reasons and purposes for using UWB beacons can be listed on the sign. However, a similar problem was encountered: only some drivers might see and read the sign.

3. **Confidentiality:** The company that operates the gas station can store information on who visited the station and for how long on its servers. Therefore, confidentiality depends on the company's policies. As some companies may allow other companies to use their data, i.e., subsidiary companies, it is questionable whether the confidentiality is fulfilled.

4. **Accountability:** The customers at the gas station can sue the company for its actions when handling their personal information.

5. **Data Minimization:** Data collection is minimized depending on the purpose. If the company intends to use the data for statistical purposes, it can store data related to the statistics, such as how long the customer stayed and how much they paid.

6. **Accuracy:** UWB beacons help the company update the customer data upon each visit and stay. Therefore, accuracy is fulfilled.

7. **Storage Limitation:** Depending on the purpose, the data is stored as long as needed. However, in this case, the companies might keep the data for future use, violating storage limitations.

8. **Lawfulness:** Similar to 5.11, the MAC addresses of connected devices and vehicles are hidden to process the data lawfully. Additionally, consent can be given by using the services at the gas station.

9. **Anonymity:** As briefly mentioned in data minimization, the data kept must be anonymous to prevent direct identification of customers. However, anonymity is violated since the company can collect data for other purposes, such as marketing.

10. **Unlinkability:** As anonymity can be violated, the information can be linked

11. **Unobservability:** As many devices are connected to UWB beacons here, it is not easy to preserve unobservability. Since it is unclear if the company can prevent third parties from observing, we state that the unobservability is not fulfilled.

12. **Good Faith:** The UWB beacons are used in good faith.

Use Case #8

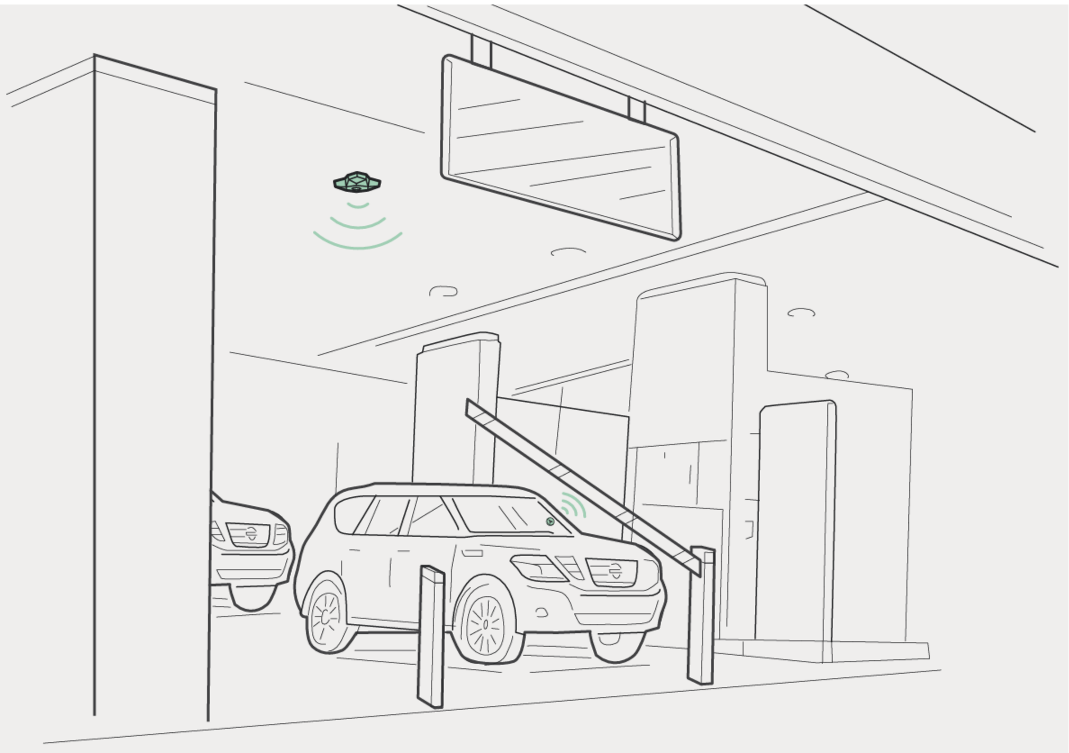


Figure 5.19: Tracking cars at border controls or toll gates [10]

Border control tracks the vehicles passing through the barrier and stores this information on the servers provided by the government. The reason for storing is security and safety.

1. **Awareness:** Drivers can be informed by using a sign when crossing the checkpoint.

2. **Transparency:** Drivers can be informed by using a sign that lists data processing purposes. However, as this use case takes place at a checkpoint, it cannot be expected that the drivers take their time to read a sign with a list. Therefore, transparency may not be fulfilled properly.

3. **Confidentiality:** Border control checkpoints work with the government and may use a central database provided directly by the government [37]. In this case, confidentiality can be adequately fulfilled as governments are strict with the security of their databases.

4. **Accountability:** Vehicle owners can sue the state in case of any data breach or sensitive data loss and hold the state accountable for its actions.

5. **Data Minimization:** Data minimization can be achieved by limiting the data collection to passing vehicles only. However, it is also possible to utilize UWB for malicious tracking.

6. **Accuracy:** The accuracy can be reached by updating the database as vehicles pass through the barrier.

7. **Storage Limitation:** It is unclear how long the data will be stored. Hence, storage is unrestricted, yet the authorities can limit it.

8. **Lawfulness:** Data is processed lawfully, as consent must be given when crossing the border.

9. **Anonymity:** The anonymity is not fulfilled as each vehicle has a different identity and connects to the UWB beacon.

10. **Unlinkability:** Due to the lack of anonymity, unlinkability is not fulfilled either, as information, such as the license plate number, can be linked to the data subject (the vehicle owner).

11. **Unobservability:** The authorities can allow third parties to access data when there is a security issue. Therefore, the unobservability is not fulfilled.

12. **Good Faith:** The data is processed in good faith, such as allowing vehicles to pass quickly, which pass the checkpoint every day.

Use Case #9

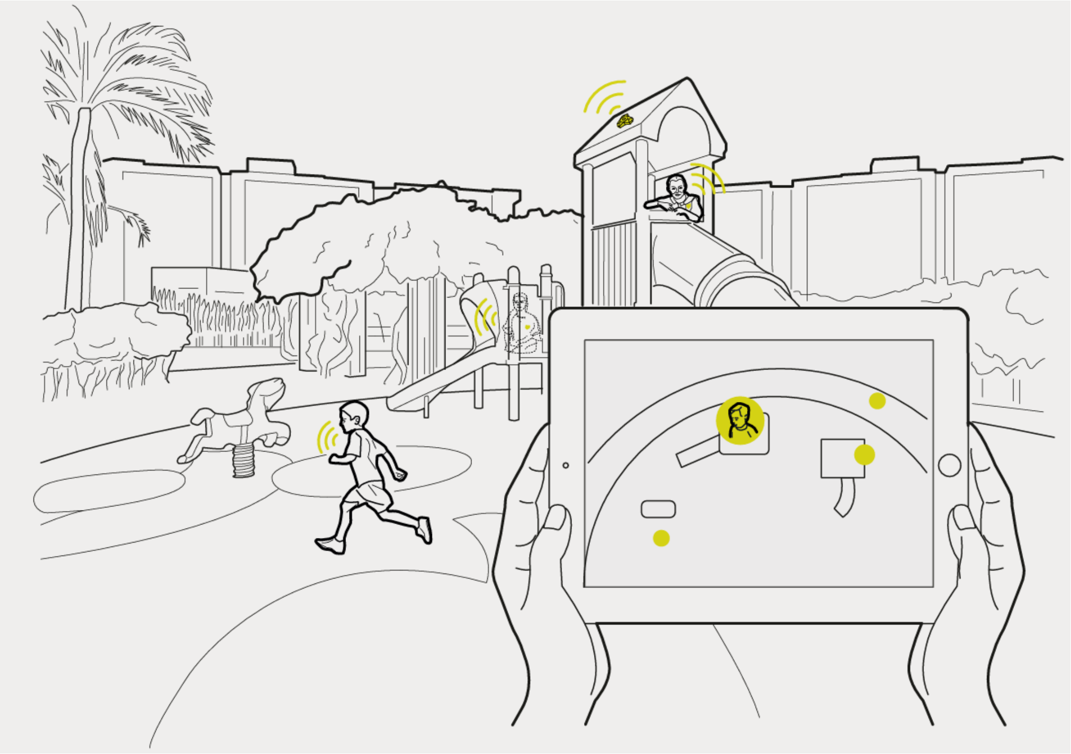


Figure 5.20: Tracking children on a playground [10]

Parents keep track of their children on a playground so they can easily find them if they get lost. Other children can also be seen on the tablet. There is no data storage here as it is only meant for active tracking for the current.

1. **Awareness:** The children or their parents can be informed about the tracking of their location. This has to be done according to the GDPR Article 8 [38], as these children are likely below 16 years old.
2. **Transparency:** The device must inform the parents about the data processing purposes. However, the device can also track other children, and this may not be wanted, or other parents would not want to allow it. Therefore, the transparency principle is violated.
3. **Confidentiality:** To the author's understanding, there is no data storage in this use case. Therefore, the confidentiality is fulfilled trivially.
4. **Accountability:** Legal action can be taken if a parent notices that another parent is using this service for purposes other than safety.
5. **Data Minimization:** Data collection is minimized to the children's location only.
6. **Accuracy:** The accuracy principle is not applicable as this use case has no data storage.

7. **Storage Limitation:** It is not applicable as there is no data storage.

8. **Lawfulness:** Data is processed lawfully via parents' consent.

9. **Anonymity:** Although the parent can track a specific signal on their tablet, the children can be tracked anonymously. Additionally, other devices on the playground are not shown with the children's names.

10. **Unlinkability:** Linking it back to the data subject is impossible as personal information is not stored.

11. **Unobservability:** The use of services by the data subject or subjects (children and their parents) is visible to third parties, such as other parents.

12. **Good Faith:** The data processing is in good faith, such as tracking one's child for safety purposes.

5.2.3 Marketing

Use Case #10

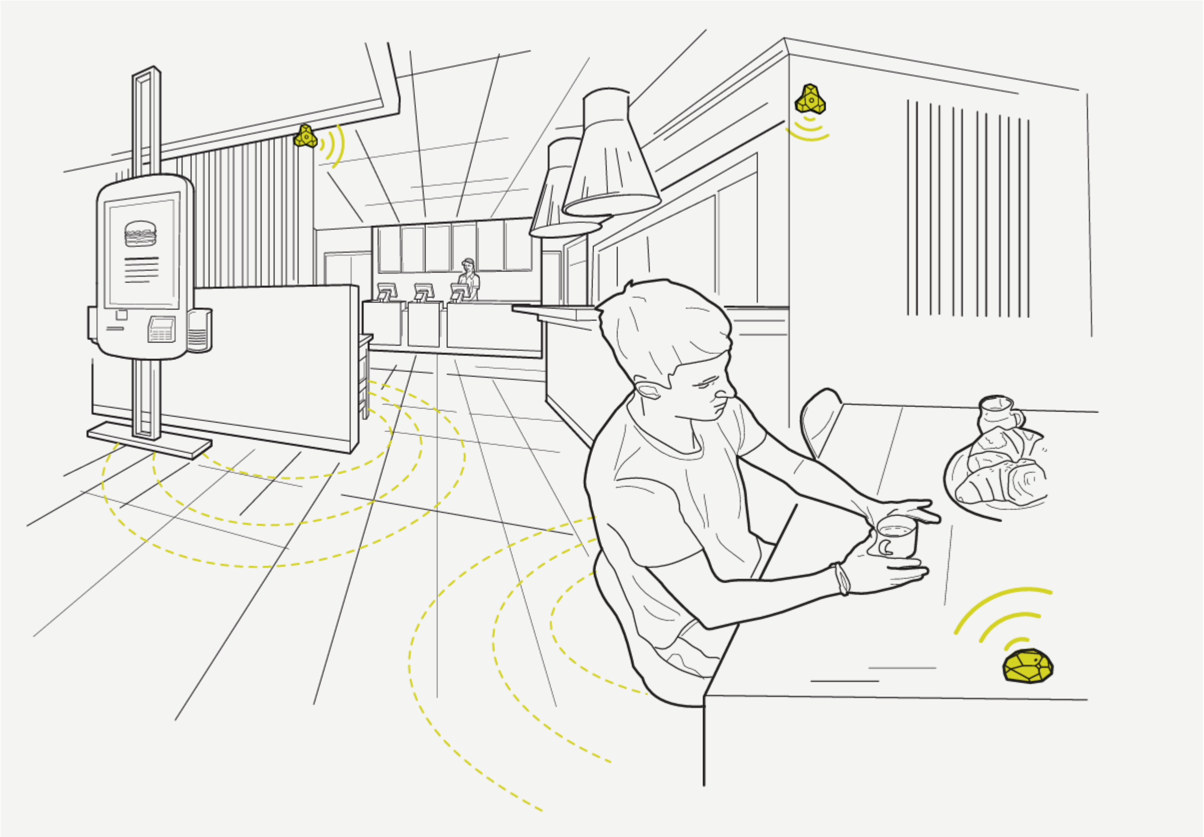


Figure 5.21: Tracking customers' presence in restaurant [10]

A fast-food restaurant puts UWB beacons throughout their restaurant, and they track customers' proximity.

1. **Awareness:** Customers are informed about the presence of UWB beacons with a sign, and consequently, awareness can be satisfied.
2. **Transparency:** Customers are informed of the presence of UWB beacons and the reasoning for that. Then, the transparency principle is satisfied.
3. **Confidentiality:** In this use case, the data is stored on the company's servers; therefore, the confidentiality of data processing is up to the company's policies. Most fast-food chains operate internationally and must comply with international privacy regulations.
4. **Accountability:** Customers can sue the fast-food chain operator for any misuse or data breach.
5. **Data Minimization:** Data is minimized to analyze the traffic inside the restaurant.

6. **Accuracy:** Data is kept accurate on the servers by updating the information via UWB beacons in the restaurant.

7. **Storage Limitation:** The company can limit the data storage for a certain period and then delete the data. However, data can be used for future purposes, such as marketing or new advertisements. Therefore, the storage limitation can be violated in the future.

8. **Lawfulness:** Data is processed lawfully when customers agree to be subject to UWB data collection when they enter the restaurant.

9. **Anonymity:** As there is no phone on track, the names and identities of the customers do not matter and are not considered.

10. **Unlinkability:** As anonymity is fulfilled, unlinkability is satisfied.

11. **Unobservability:** Unobservability is satisfied. The services used by data subjects are not visible to third parties.

12. **Good Faith:** The intention of this use case is in good faith.

Use Case #11

Figure 5.22: Tracking customer's phone when selling [10]

The store owner can offer a loyalty bonus to customers who visit their store regularly. The UWB beacon can automatically detect which customer visits and when.

1. **Awareness:** The customer is aware of UWB beacons in the shop, which have a sign at the entrance.
2. **Transparency:** During a terse conversation when selling products, explaining the data collection purposes of UWB beacons is impossible.
3. **Confidentiality:** Customer data is stored on the company's secure cloud via UWB beacon.
4. **Accountability:** Customers can sue the company and hold it accountable for any actions with their data.
5. **Data Minimization:** Data is minimized to the customers who visit the shop and how much time they spend there.
6. **Accuracy:** Accuracy is provided by constant updates via UWB beacons upon a customer's visit.

7. **Storage Limitation:** Storage is limited to the company's purpose and will be discarded when the data is unused or if the customer cancels their subscription.

8. **Lawfulness:** Data is processed lawfully with the customer's consent when creating their loyalty program.

9. **Anonymity:** Anonymity is not satisfied as each customer's information is saved with their identity and name.

10. **Unlinkability:** Due to the failure to satisfy the previous principle, unlinkability cannot be provided.

11. **Unobservability:** Third parties can use this technology in this use case to promote their products or suggest other products. This can include the company's or shop's partnership with third parties.

12. **Good Faith:** The use case is in good faith and aims to provide a better service to the customer.

Use Case #12

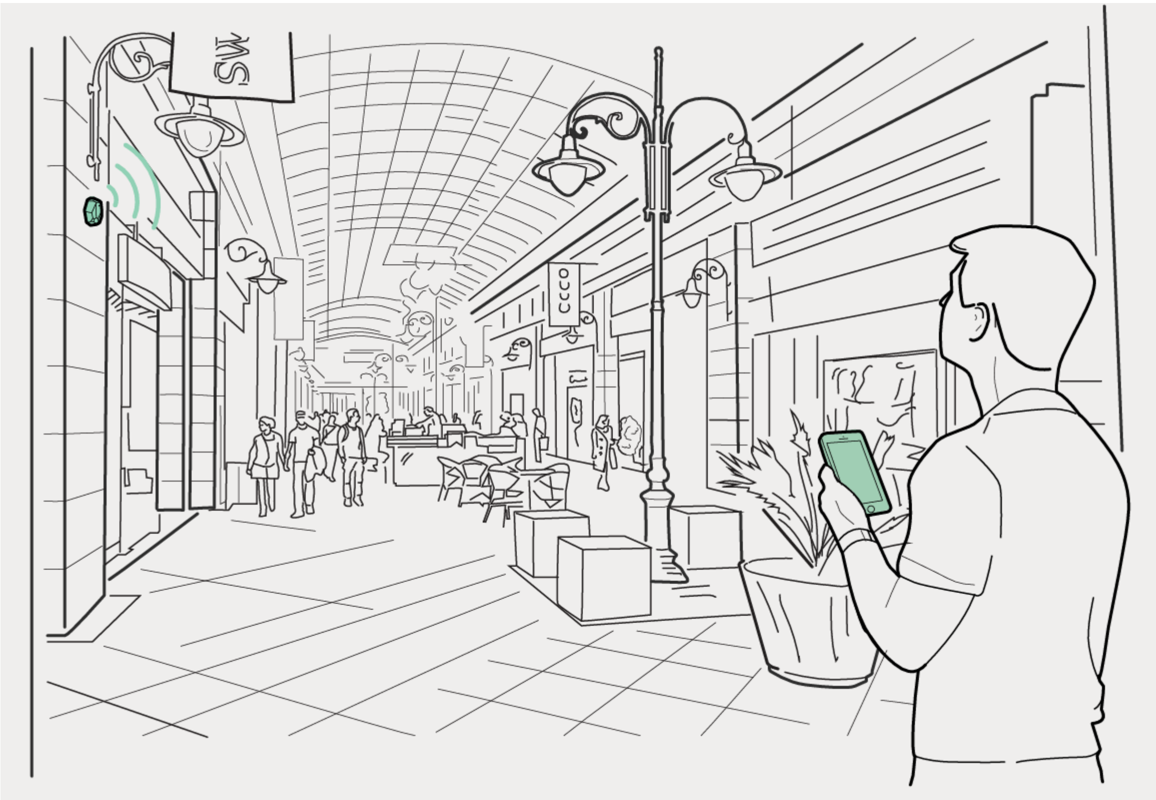


Figure 5.23: Tracking visitors' phone in mall [10]

Mall managers can track the customers who visit the mall. They can see where their customers spend most of the time during the visit. This can help them improve their advertising. Additionally, this service can help customers navigate the mall.

1. **Awareness:** The customer is aware of the UWB beacons. These beacons are not hidden, and a sign informs the customers when they enter the mall.
2. **Transparency:** Mall operators are transparent about their purposes when implementing and placing UWB beacons.
3. **Confidentiality:** The mall stores customers' data in a secure cloud.
4. **Accountability:** Customers can sue the mall administration for their actions with their data.
5. **Data Minimization:** Data collection is not minimized, as many stores can profit, and it becomes difficult to track which stores need which types of data.
6. **Accuracy:** The data in the database can accurately be updated via active tracking with UWB beacons in the mall.
7. **Storage Limitation:** Data storage is limited to the store's current purposes, and data will not be stored for any possible future purposes.

8. **Lawfulness:** The data processing is lawful as intentions or explanations of purposes are not misleading.

9. **Anonymity:** Anonymity is not provided as personal smartphones are connected to the UWB beacons, and the mall and store operators can track these phones.

10. **Unlinkability:** Due to the previous point, unlinkability is not satisfied, and personal information can be connected to customers.

11. **Unobservability:** The use of services is visible to third parties, as any company that sells products in the mall can track where most customers are and place its advertisements there for marketing purposes.

12. **Good Faith:** The use case is in good faith since tracking people can help people navigate in the mall.

Use Case #13

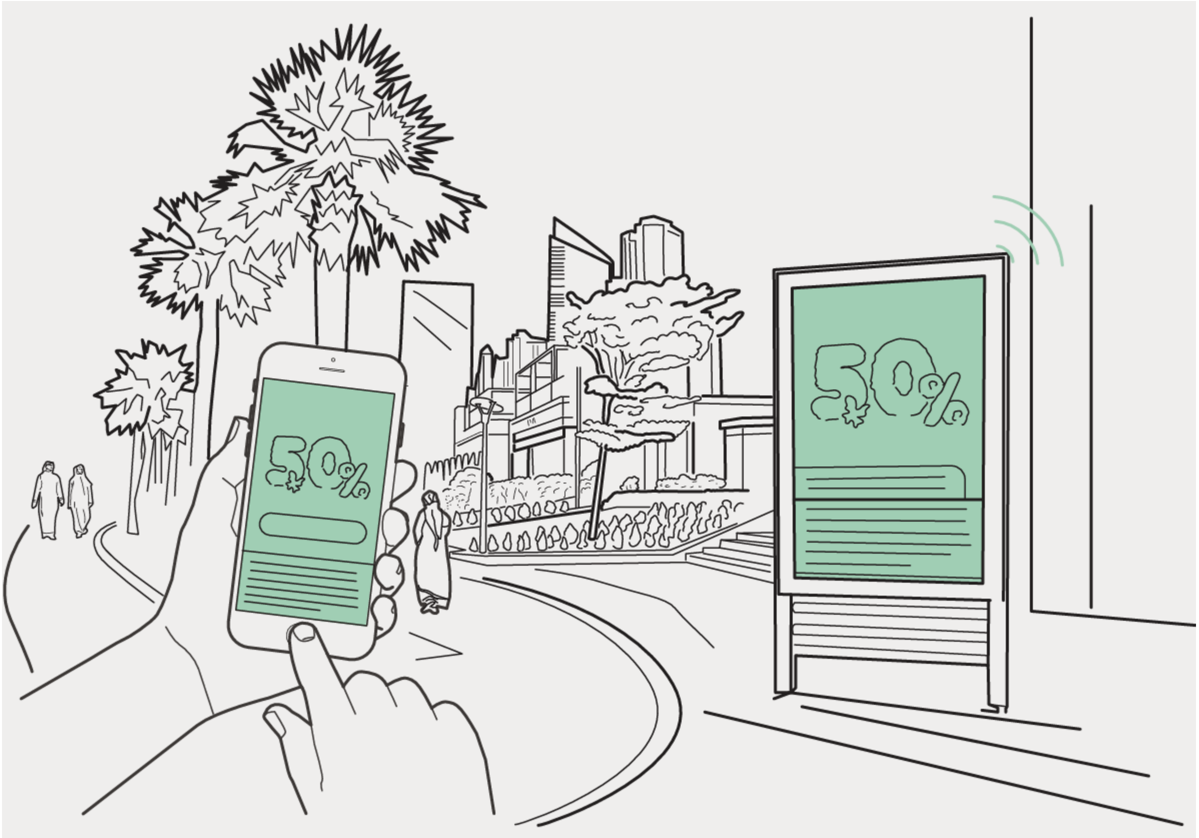


Figure 5.24: Showing advertisements from billboard to phone [10]

Billboard advertisements can also be shown on personal smartphones via UWB beacons by measuring the proximity of the smartphones. The advertisements can then reach a broader spectrum, and more people can be informed about the discount or deal. In addition, the advertisement includes a footnote on how the proximity data is being used and for what purposes. There is no data collection.

1. **Awareness:** The smartphone owner is aware of the data processing as their smartphone is connected in proximity.

2. **Transparency:** The usage of UWB is transparent here, as the advertisement explains data processing purposes in a footnote.

3. **Confidentiality:** There is no data collection; hence, the confidentiality principle is trivially satisfied.

4. **Accountability:** Phone owners can hold the company accountable for misusing the data should the company take such actions.

5. **Data Minimization:** Data is minimized to the proximity of smartphones only.

6. **Accuracy:** The accuracy of stored data is trivially fulfilled as there is no data collection.

7. **Storage Limitation:** The storage is limited as there is no data storage.

8. **Lawfulness:** Lawfulness is not satisfied. The smartphone owner was not asked for permission, nor did they consent to see advertisements on their phone.

9. **Anonymity:** The smartphone's proximity is calculated. However, the smartphone's owner is not included in the data processing. The anonymity is satisfied.

10. **Unlinkability:** The information cannot be linked to the data subject because the anonymity is satisfied.

11. **Unobservability:** Third parties cannot observe which services the smartphone's owner uses.

12. **Good Faith:** The use of UWB beacons is not in good faith. The advertisements may not be wanted to be seen by the data subject. However, they are not offered any choice. The advertisement pops up on their phone without their consent.

Use Case #14

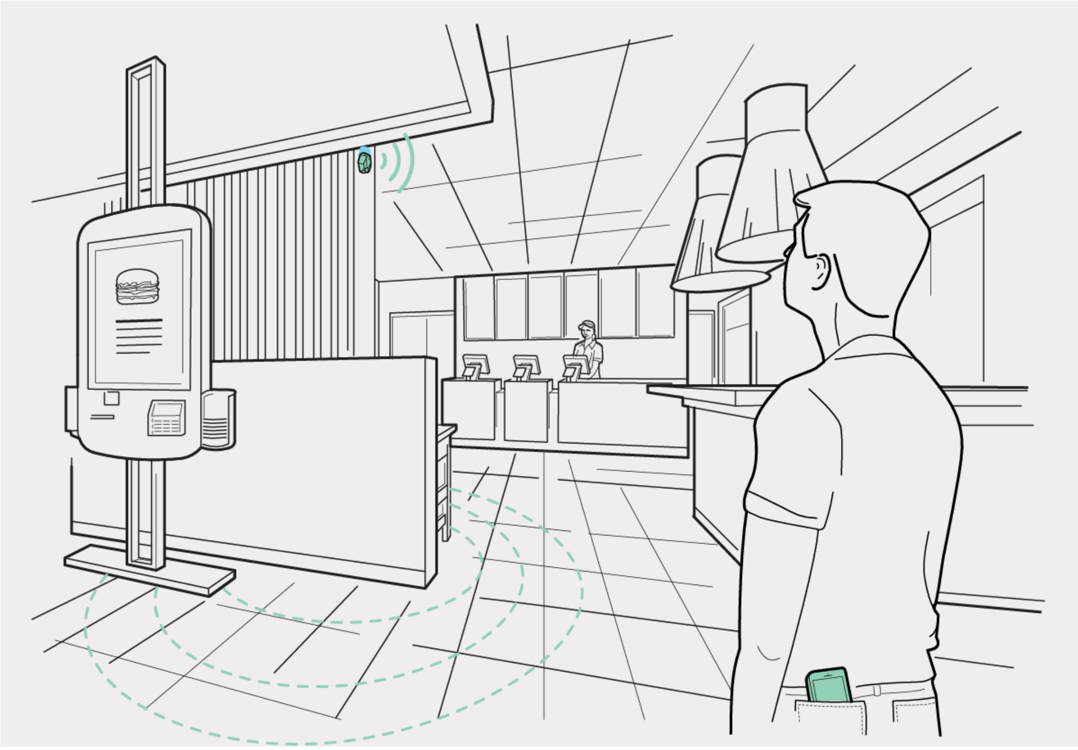


Figure 5.25: Tracking customers entering the restaurant [10]

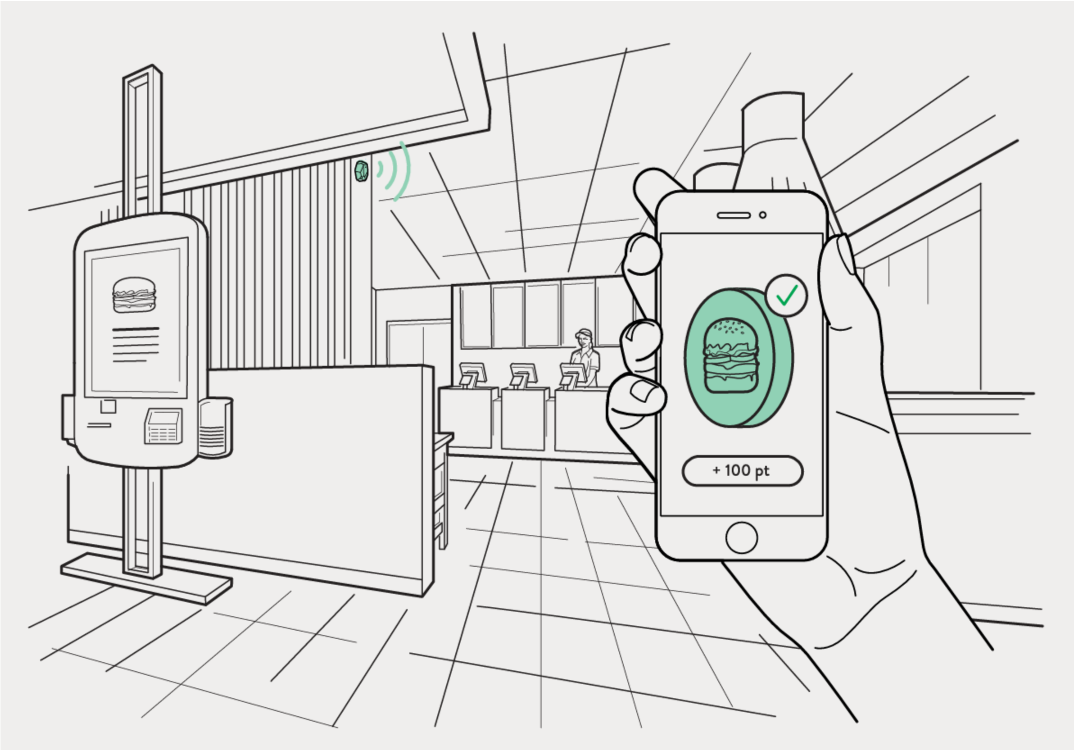


Figure 5.26: Earning points upon entering a restaurant [10]

Figure 5.27: Customer doesn't earn points for not entering [10]

The UWB beacons detect the customers' smartphones when they enter the restaurant. This helps employees keep track of the customers and provides some statistical information such as the peak hours and average time spent in the restaurant for marketing purposes in 5.25. The restaurant can offer a loyalty bonus for regular visits in 5.26, and customers can earn points for their next visit when they revisit the restaurant. If the customers decide not to visit the restaurant, they will not earn any points as in 5.27. The customer data is stored securely on the restaurant's servers.

1. **Awareness:** The customers who visit the restaurant are aware of the data processing. However, the customers who visited before are passing by this time and are unaware of the data processing. This violates the awareness principle.

2. **Transparency:** The company is clear with its data processing purposes. However, similarly to the previous point, customers who are only passing by the restaurant are not informed about the data processing purposes. As shown in 5.9, the UWB beacons can detect the phones behind a wall.

3. **Confidentiality:** The collected data is stored with appropriate security measures.

4. **Accountability:** The customers can hold the restaurant accountable for their actions with personal data.

5. **Data Minimization:** Data collection is minimized to marketing purposes only, such as the number of visits, points collection, etc.

6. **Accuracy:** The accuracy of stored data is provided by constantly updating the database with the data received via UWB beacons.

7. **Storage Limitation:** The data storage is limited to the customer's account usage. Customers' data is erased if they want to delete their accounts.

8. **Lawfulness:** The personal data is processed lawfully as consent is given by visiting the restaurant.

9. **Anonymity:** The data collection is not anonymous, as each customer's name is also saved in the database.

10. **Unlinkability:** Due to the lack of anonymity, the unlinkability is not fulfilled either. Personal data can be traced back to the data subjects.

11. **Unobservability:** The ecosystem used by the restaurant is closed. Therefore, the unobservability is satisfied, and the activities cannot be observed by third parties.

12. **Good Faith:** The intention of this use case is in good faith. It offers discounts and loyalty points to customers and allows them to eat at a cheaper price.

Use Case #15

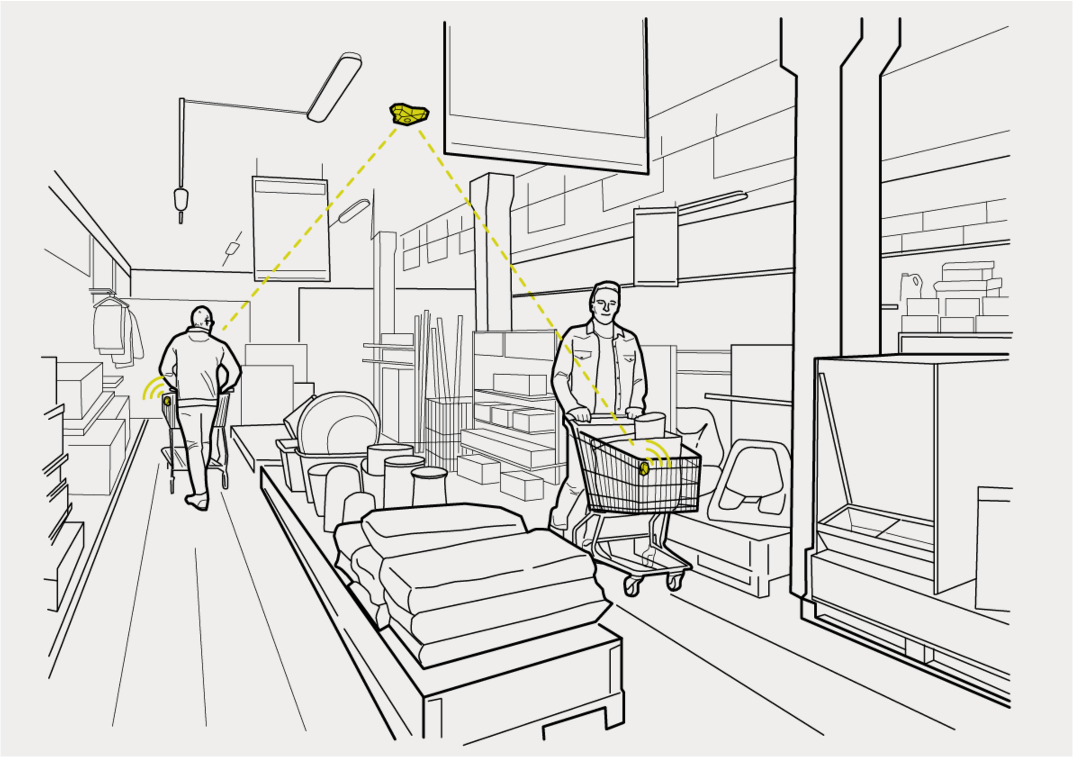


Figure 5.28: Tracking shopping carts [10]

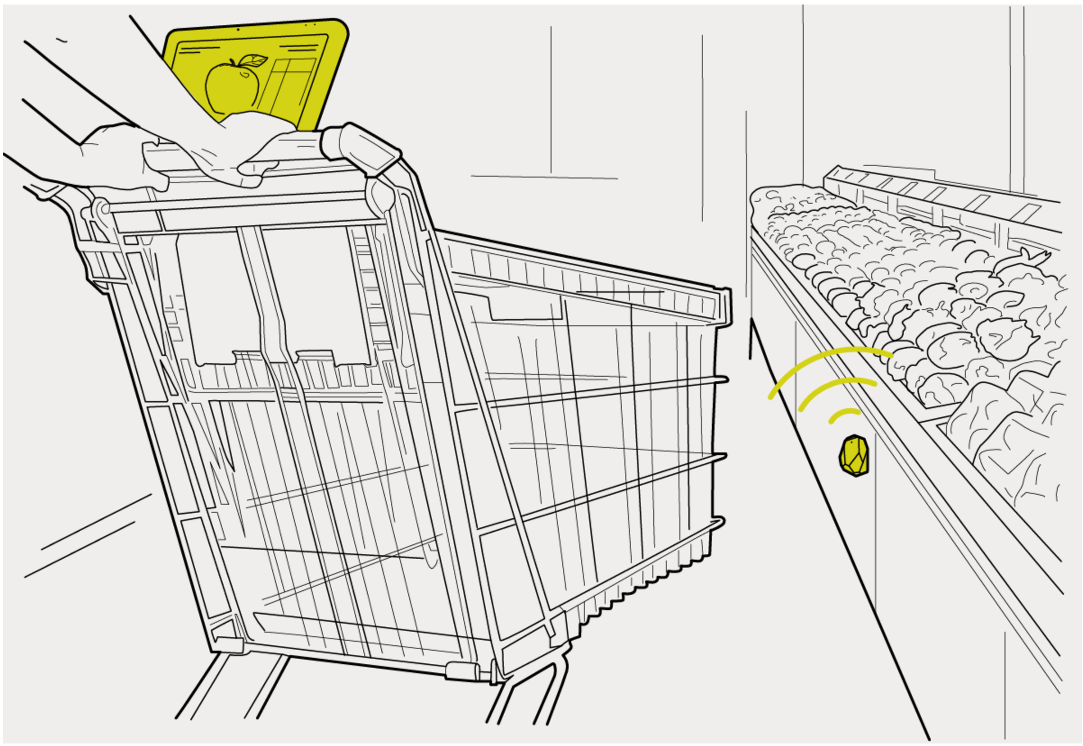


Figure 5.29: Reminding customer to buy an item [10]

In this use case, the customers are informed with a sign about the presence of UWB beacons in the supermarket. This sign also explains the purpose of the implementation of UWB beacons. Data, such as the shopping carts' location and movement, is kept in a secure database. Data collection and storage are minimized by collecting information merely about the carts. The customer is informed about a specific item when the shopping cart gets close to a UWB beacon. This can also remind customers what they want to buy. Additionally, the tablets on the carts can be used to add a shopping list, and the UWB beacons can help customers find items in the store.

1. **Awareness:** Customers know the data processing because a sign at the supermarket entrance says that UWB technologies are used here.
2. **Transparency:** The sign that informs customers about UWB usage in the supermarket also tells them about the specific purposes.
3. **Confidentiality:** The data is stored in a secure database.
4. **Accountability:** The customers can hold the supermarket managers accountable for their actions.
5. **Data Minimization:** Data is minimized by only collecting and storing data on carts' movement and locations.
6. **Accuracy:** UWB beacons constantly update the statistical data.
7. **Storage Limitation:** The data from the carts' movements does not include any personal information. Therefore, there is no storage limitation.
8. **Lawfulness:** The data processing is lawful, and no consent is required, as no personal data is involved.
9. **Anonymity:** The data collected is anonymous.
10. **Unlinkability:** As the data is anonymous, the information is also unlinkable.
11. **Unobservability:** The third parties can track the activities of data subjects anonymously.
12. **Good Faith:** The use case is in good faith, making shopping easier for the customers.

5.2.4 Workplace

Use Case #16

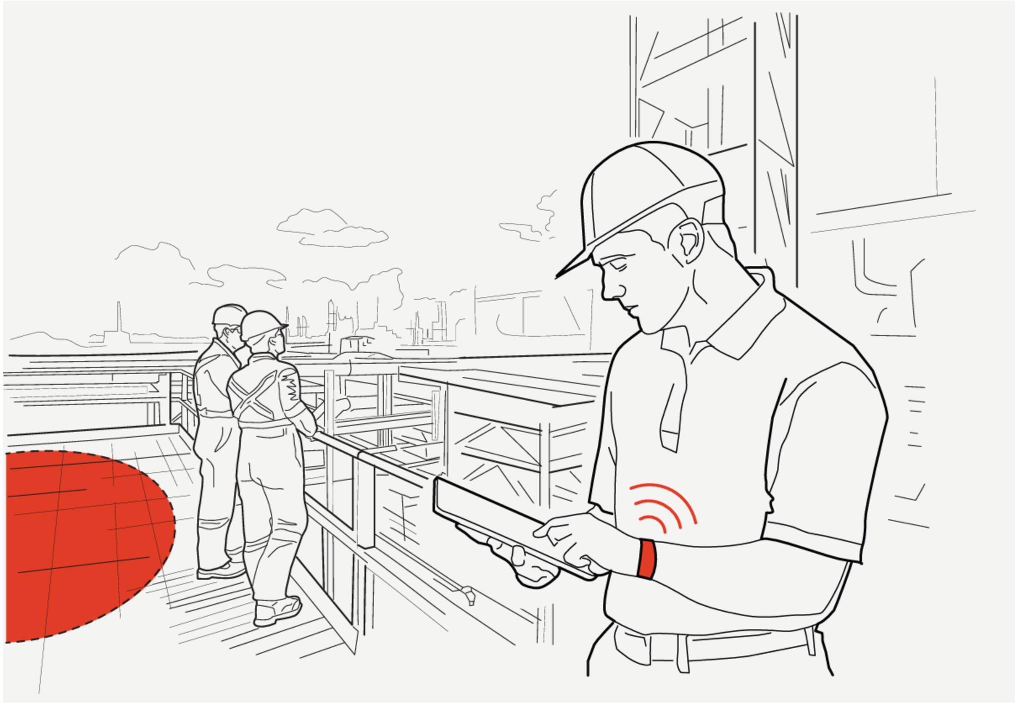


Figure 5.30: Tracking coworker at construction [10]

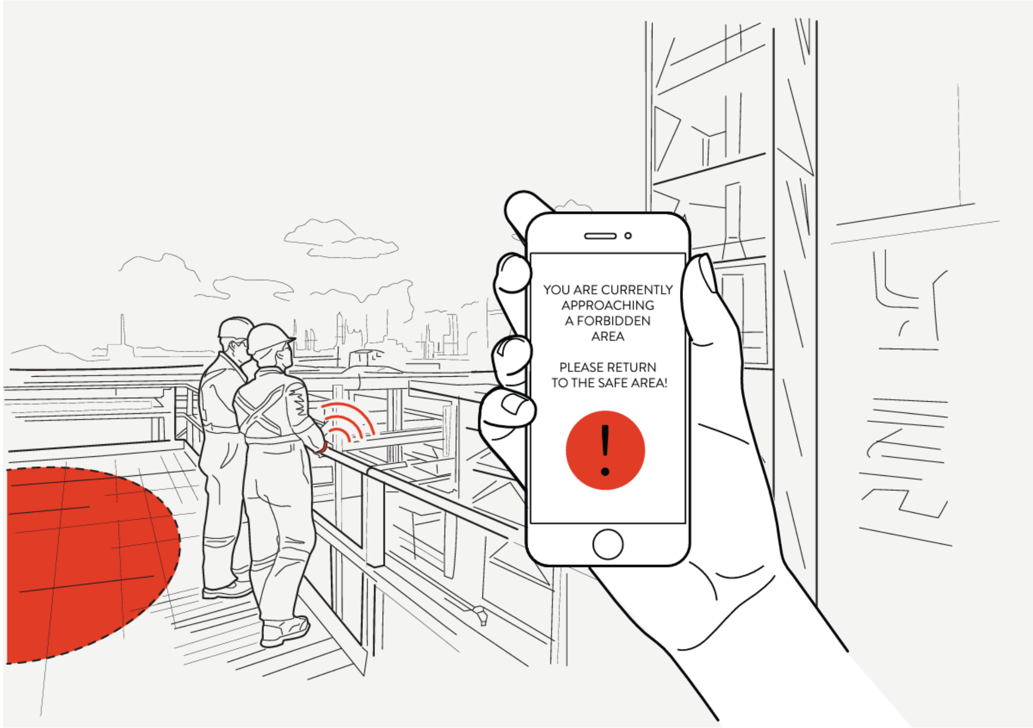

YOU ARE CURRENTLY APPROACHING A FORBIDDEN AREA
PLEASE RETURN TO THE SAFE AREA!
!

Figure 5.31: Coworker enters forbidden area [10]

UWB technology tracks employees at a construction site, and if they get too close to an unsafe or forbidden area, they are warned on their phones. This requires sending data to their phone to warn. The location of the employee is tracked via their watch. There is no data storage.

1. **Awareness:** The employee is aware of the processing of personal data. This is declared by the employer when signing the contract.
2. **Transparency:** Like the previous point, the employer informs the employees that their location will be tracked to prevent any harm.
3. **Confidentiality:** There is no storage of personal information. This principle is fulfilled trivially.
4. **Accountability:** The employee can hold the employer accountable for their actions if their data is used for other purposes.
5. **Data Minimization:** Data is minimized to the employees' location.
6. **Accuracy:** There is no data storage. Therefore, the accuracy of stored data is provided trivially.
7. **Storage Limitation:** Storage is limited as no storage is needed for active tracking.
8. **Lawfulness:** The data is processed lawfully with the employees' consent.
9. **Anonymity:** The data is not anonymous; each employee has a different identifier, and these must be tracked individually at the construction site.
10. **Unlinkability:** Unlinkability is not fulfilled as the personal information, such as authorization, can be connected to the data subject.
11. **Unobservability:** The UWB ecosystem is closed; no third parties can observe employees' activities.
12. **Good Faith:** The data processing is in good faith, as it prevents any harm.

Use Case #17

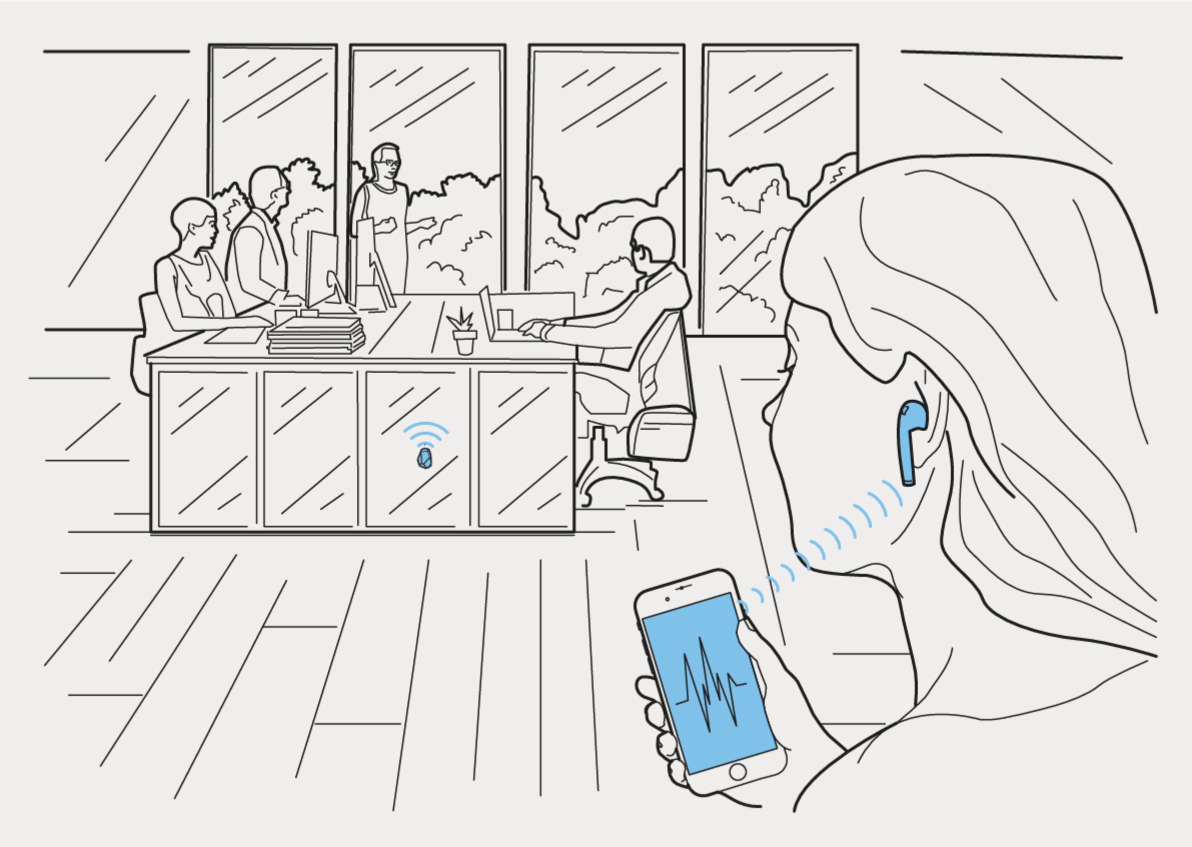


Figure 5.32: Coworker can follow the meeting from outside [10]

The UWB beacon in the meeting room connects to the coworker's phone outside. She is currently not in the meeting, so she can follow the meeting from outside without actively joining and participating. As discussed in the chapter 2, the UWB beacons are energy efficient and are provided by using as little data as possible. Therefore, rich data, such as audio, cannot be sent to the coworker's phone directly. However, new Estimote UWB beacons can achieve this by using an external power supply and transmitting rich data to nearby phones as well [17]. Meeting participants are informed that their meeting can be listened to by third parties and for what purposes. However, the audio will not be recorded and will only be transmitted live.

1. **Awareness:** This use case fulfills the awareness principle as the participants are aware of data processing.
2. **Transparency:** The purposes of audio transmission are clear, and meeting participants are informed.
3. **Confidentiality:** This is not applicable since there is no data storage.
4. **Accountability:** The participants can hold the company accountable for any misuse of this technology.

5. **Data Minimization:** Data is minimized to audio-only.

6. **Accuracy:** This is not applicable since there is no data storage.

7. **Storage Limitation:** This is not applicable as there is no data storage.

8. **Lawfulness:** Consent is given when participating in the meeting. Therefore, lawfulness is satisfied when processing the data.

9. **Anonymity:** The audio transmission does not identify the speaker directly; therefore, anonymity is kept.

10. **Unlinkability:** The audio is not unlinkable if other employees know the participants and can identify them from their voices.

11. **Unobservability:** Unobservability is heavily violated as third parties can easily connect to the UWB beacon and listen to the meeting while not actively participating. Removing or disabling the UWB beacon should not be forgotten if the meeting is confidential. Otherwise, sensitive information can spread among unauthorized personnel.

12. **Good Faith:** The use case is in good faith, supporting other coworkers in joining the meeting passively.

Use Case #18

Figure 5.33: Technician gathering technical data from a plane [10]

The technician can access the plane's technical data during maintenance. This helps the technician find all the relevant information directly on his tablet. Additionally, the technician can update the changed or maintained parts so that a future technician can see which parts were replaced or maintained and when. The plane's technical data is stored on the airline's cloud. Whenever the plane is in the hangar and surrounded by other UWB beacons, it can update its data on the cloud. There is no personal data involved. Because of that, several principles from the privacy mapping in 2.1.4 are skipped as they are not related anymore and satisfied trivially. The only concern here is the unobservability. As these UWB beacons stay in the cockpit also during the flight, any passenger or an unauthorized person can access the plane's technical data and pose a threat. Such data can be used maliciously for other purposes.

Use Case #19

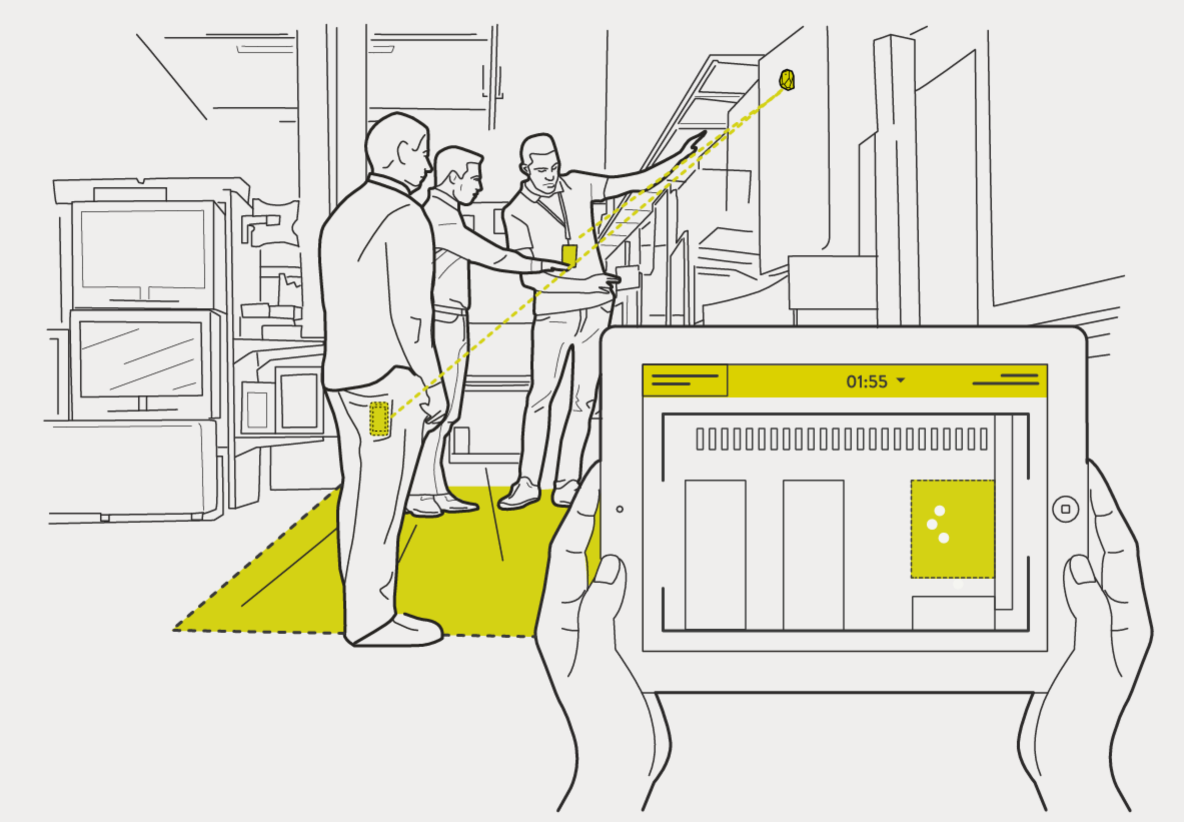


Figure 5.34: Tracking coworkers in a warehouse [10]

In this last use case, the UWB beacon placed in a warehouse can track people standing in one designated area. Then, another coworker can see these people on their tablet and track them. Coworkers are informed about the UWB usage here and its purposes. In this case, the company can designate this area as sensitive, and coworkers must pay attention to who visits, as there might be a dangerous product or a confidential unfinished prototype. People who have been to the designated area are identified and put in a secure database to track who visited the area and for how long for security reasons.

1. **Awareness:** The employees are informed about the UWB beacons' data processing.
2. **Transparency:** The employees are informed about the purposes of UWB beacons.
3. **Confidentiality:** Confidentiality is fulfilled as the database is secured.
4. **Accountability:** The employees can hold the company accountable for their actions with their data.
5. **Data Minimization:** Data is minimized to the designated zone only.
6. **Accuracy:** The database is constantly updated with new data coming from the UWB beacon.

7. **Storage Limitation:** There is no known storage limitation, as the company can keep the data as long as it wants.

8. **Lawfulness:** The data is processed lawfully with the employees' consent.

9. **Anonymity:** The data is not anonymous, as the beacon can see which phone is connected.

10. **Unlinkability:** It is possible to link the data to the data subject by checking the phones that were connected to the beacon before.

11. **Unobservability:** Third parties from anywhere in the warehouse can observe the data subject with their tablet and can see the UWB beacon.

12. **Good Faith:** The use case is in good faith and tries to prevent the company from suffering harm or reputational damage from losing sensitive information.

5.3 Overall Evaluation

	Privacy Principles											
Use Cases with Categories	Awareness	Transparency	Confidentiality	Accountability	Data Minimization	Accuracy	Storage Limitation	Lawfulness	Anonymity	Unlinkability	Unobservability	Good Faith
Healthcare 5.12	✓	✓	✓	✓	✓	✓	✓	✓				✓
Healthcare 5.13	✓		✓	✓	✓		✓	✓				✓
Active Tracking 5.14	✓	✓		✓	✓	✓	✓	✓				✓
Active Tracking 5.15			✓	✓	✓	✓	✓	✓				✓
Active Tracking 5.16			✓	✓	✓	✓	✓	✓				✓
Active Tracking 5.17	✓	✓		✓	✓	✓	✓	✓				✓
Active Tracking 5.18				✓	✓	✓		✓				✓
Active Tracking 5.19	✓		✓	✓		✓		✓				✓
Active Tracking 5.20	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓
Marketing 5.21	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Marketing 5.22	✓		✓	✓	✓	✓	✓	✓				✓
Marketing 5.23	✓	✓	✓	✓	✓	✓	✓	✓				✓
Marketing 5.24	✓	✓		✓	✓	✓	✓		✓	✓		
Marketing 5.25, 5.26, 5.27			✓	✓	✓	✓	✓	✓			✓	✓
Marketing 5.28, 5.29	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Workplace 5.30, 5.31	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓
Workplace 5.32	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓
Workplace 5.33	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Workplace 5.34	✓	✓	✓	✓	✓	✓		✓				✓

Table 5.1: Results of the analysis

The table above 5.1 shows that there is a common pattern among the use cases. Principles such as accountability, data minimization, accuracy, storage limitation, and lawfulness can easily be fulfilled. Awareness and transparency principles depend on the way of communication and when. If the data subject is on the move or has limited time, it can be difficult to communicate clearly about the data collection and processing purposes. When setting up its servers and databases, confidentiality depends on the company's security measures. It is unclear to the author if the Estimote Cloud can also be used for data storage. Principles such as anonymity, unlinkability, and unobservability are the worst drawbacks of UWB beacons. The reason is that the UWB beacons connect to the phones with an identifier. Although the MAC addresses are hidden as in 5.11, the phone's owner can be detected by unauthorized persons if they track the location and the people on site. This raises similar privacy concerns mentioned in [11] with AirTags, and these UWB beacons can be used for malicious purposes. Therefore, it is shown that the Estimote ecosystem is similar to the Apple system when handling data with their beacons and AirTags, respectively.

Chapter 6

Final Considerations

The following chapter summarizes the topics, findings, and conclusive remarks discovered in this thesis. Furthermore, it outlines future work to be conducted in this research area.

6.1 Summary

The first step was to set up the SDK provided by Estimote Inc. After several debugging and firmware updates on Estimote UWB beacons, our phone could connect to the beacons by running the app from the SDK. This enabled us to track the connection, view the log output, and determine what processes are being executed. In the meantime, Estimote's website was updated, and Estimote Inc. published more than two hundred use cases for these UWB beacons. These beacons are incorporated with additional devices in some specific use cases. These use cases were then analyzed using the privacy mapping in [11].

6.2 Conclusions

This thesis thoroughly analyzes Estimote UWB beacon use cases and highlights privacy concerns based on their functionality and the privacy mapping provided before. These use cases were examined broadly by analyzing the privacy concerns based on the privacy requirements adopted from the privacy mapping, including three different regulations and frameworks for privacy, such as GDPR, NIST, and nFADP.

This thesis could address the privacy questions when using Estimote UWB beacons in different use cases. However, a technical issue was encountered when setting up the sniffer device. Due to the complicated setup and not sniffing any data from the data transmission between the phone and the beacon, this had to be left out. Therefore, the packets and data security could not be tested while data was transmitted between the phone and the beacon. Additionally, no further information could be retrieved when analyzing Estimote's cloud system, as the functionality was quite limited at the time of use.

6.2.1 Estimote's Adherence to the Privacy Requirements

This thesis showed that the Estimote environment has similar privacy concerns with Apple's AirTags in [11]. These concerns mainly arise from the data subjects' anonymity, unlinkability, and unobservability. Data subjects can be subject to any observations by third parties without awareness.

6.3 Future Work

As discussed in 3, this thesis used the SDK from Estimote Inc. for Android, and this UWB environment was not tested for iOS. This also allows for a multi-device connection, which is unavailable if Android phones are used. Additionally, when Estimote improves the UWB beacons, a similar functionality test can be conducted using multi-device connections for Androids. This can increase the accuracy and range of the test results in this thesis. As a result, more privacy concerns can arise from this increased accuracy and range.

Furthermore, the privacy regulations are evolving constantly with the introduction of new technologies. If any frameworks or privacy regulations should be updated, further privacy analysis should be conducted on these use cases. This includes updating the existing privacy mapping.

Similarly, new use cases can exist in different fields and have different characteristics. In this case, the use cases analyzed in this thesis may no longer be representative. So far, a sample was taken from over two hundred use cases and analyzed thoroughly. This analysis comprised use cases in four fields: healthcare, active tracking, marketing, and the workplace. Should new fields be introduced for these UWB beacons, these should be analyzed further based on the privacy requirements.

Lastly, Estimote UWB beacons can now work with Estimote UWB tags, which were not analyzed in this thesis. These UWB tags were released while UWB beacons were being analyzed, and they are pretty new technology. Additionally, they can work with UWB beacons to help them collect data. These Estimote UWB tags can also be analyzed technically for their function in an Estimote environment and which privacy requirements they fail to deliver based on the privacy mapping.

Bibliography

[1] M. Z. Win, D. Dardari, A. F. Molisch, W. Wiesbeck, and W. Jinyun Zhang, "History and applications of uwb." Institute of Electrical and Electronics Engineers, 2009.

[2] J. Zhang, P. V. Orlik, Z. Sahinoglu, A. F. Molisch, and P. Kinney, "Uwb systems for wireless sensor networks," *Proceedings of the IEEE*, Vol. 97, No. 2, pp. 313–331, 2009.

[3] M. G. N. Alsath and M. Kanagasabai, "Compact uwb monopole antenna for automotive communications," *IEEE transactions on antennas and propagation*, Vol. 63, No. 9, pp. 4204–4208, 2015.

[4] M. S. Khan, A.-D. Capobianco, S. M. Asif, D. E. Anagnostou, R. M. Shubair, and B. D. Braaten, "A compact csrr-enabled uwb diversity antenna," *IEEE antennas and wireless propagation letters*, Vol. 16, pp. 808–812, 2017.

[5] K. O. Müller, J. von der Assen, C. Feng, and B. Stiller, "An overview and ontology of privacy to preserve privacy in ultra-wideband networks," *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, pp. 2317–2324, 2022.

[6] W. Song, H. Lee, S.-H. Lee, M.-H. Choi, and M. Hong, "Implementation of android application for indoor positioning system with estimote ble beacons," *Journal of Internet Technology*, Vol. 19, No. 3, pp. 871–878, 2018.

[7] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," *The internet society (ISOC)*, Vol. 80, No. 15, pp. 1–53, 2015.

[8] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "Iot privacy and security: Challenges and solutions," *Applied Sciences*, Vol. 10, No. 12, p. 4102, 2020.

[9] J. Van den Hoven, M. Blaauw, W. Pieters, and M. Warnier, "Privacy and information technology," 2014.

[10] E. Inc., "Estimote Use Cases 2024," https://estimote.com/estimote-use-cases-2024.pdf, accessed:2024-07-23.

[11] D. Vogel, "Mapping Boundaries - An Analytical Dive into AirTags and Respective Privacy Concerns," 2024.

[12] M.-G. Di Benedetto, "Uwb communication systems: a comprehensive overview," 2006.

[13] F. Consortium, "How UWB Works," https://www.firaconsortium.org/discover/how-uwb-works, accessed:2024-08-01.

[14] "UWB Bandwidth Spectrum," https://www.researchgate.net/figure/The-comparison-between-the-UWB-spectrum-and-spectrum-of-currently-commercial_fig1_334820592, accessed: 2024-07-03.

[15] K. Dang, A. Mifdaoui, and T. Gayraud, "Design and analysis of uwb-based network for reliable and timely communications in safety-critical avionics," 05 2014, pp. 1–10.

[16] A. Schjørring, A. L. Cretu-Sircu, I. Rodriguez, P. Cederholm, G. Berardinelli, and P. Mogensen, "Performance evaluation of a uwb positioning system applied to static and mobile use cases in industrial scenarios," *Electronics*, Vol. 11, No. 20, p. 3294, 2022.

[17] "Estimote," https://estimote.com/, accessed: 2024-07-09.

[18] J. Tosi, F. Taffoni, M. Santacatterina, R. Sannino, and D. Formica, "Performance evaluation of bluetooth low energy: A systematic review," *Sensors*, Vol. 17, No. 12, p. 2898, 2017.

[19] "Bluetooth Low Energy Design 101," https://www.digikey.dk/da/articles/bluetooth-low-energy-design-101-from-chipsets-to-protocol-stacks-to-modules, accessed: 2024-07-09.

[20] L. Botler, M. Spörk, K. Diwold, and K. Römer, "Direction finding with uwb and ble: A comparative study," *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS).* IEEE, 2020, pp. 44–52.

[21] "BLE Advertisement Packet," https://academy.nordicsemi.com/courses/bluetooth-low-energy-fundamentals/lessons/lesson-2-bluetooth-le-advertising/topic/advertisement-packet/, accessed: 2024-07-09.

[22] A. R. Jiménez and F. Seco, "Finding objects using uwb or ble localization technology: A museum-like use case," *2017 International Conference on Indoor Positioning and Indoor Navigation (IPIN).* IEEE, 2017, pp. 1–8.

[23] H. Li, L. Yu, and W. He, "The impact of gdpr on global technology development," pp. 1–6, 2019.

[24] "What is GDPR, the EU's new data protection law?" https://gdpr.eu/what-is-gdpr/, accessed: 2024-05-22.

[25] "GDPR countries," https://www.gdpradvisor.co.uk/gdpr-countries, accessed: 2024-05-22.

[26] "General Data Protection Regulation (GDPR) Article 5," https://gdpr.eu/article-5-how-to-process-personal-data/, accessed: 2024-06-03.

[27] "General Data Protection Regulation (GDPR) Article 6," https://gdpr.eu/article-6-how-to-process-personal-data-legally/, accessed: 2024-06-03.

[28] T. P. P. for Federal Law, "New Federal Act on Data Protection," https://www.fedlex.admin.ch/eli/cc/2022/491/en, accessed: 2024-07-16.

[29] D. E. Bambauer, "Privacy versus security," *J. Crim. L. & Criminology*, Vol. 103, p. 667, 2013.

[30] "NIST Cybersecurity Framework," https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0, accessed: 2024-07-09.

[31] M. Scofield, "Benefiting from the nist cybersecurity framework," *Information Management*, Vol. 50, No. 2, p. 25, 2016.

[32] S. Almuhammadi and M. Alsaleh, "Information security maturity model for nist cyber security framework," *Computer Science & Information Technology (CS & IT)*, Vol. 7, No. 3, pp. 51–62, 2017.

[33] J. Kolakowski, V. Djaja-Josko, M. Kolakowski, and K. Broczek, "Uwb/ble tracking system for elderly people monitoring," *Sensors*, Vol. 20, No. 6, p. 1574, 2020.

[34] C. Eder, "Design and evaluation of ultra-wideband (uwb) architectures with a focus on privacy-preserving characteristics," Master's thesis, University of Zurich, 2023.

[35] "Estimote Forum," https://forums.estimote.com/t/cant-connect-to-multiple-uwb-beacons-on-android/12343, accessed: 2024-07-12.

[36] "Estimote Android SDK," https://github.com/Estimote/Android-Estimote-UWB-SDK, accessed: 2024-06-15.

[37] P. Bilski, J. Modelski, B. Kościug, J. Olejnik, I. Badaczewska, A. Malamou, and R. Makri, "Application of the RFID technology in the European Union border control system," *2017 IEEE International Conference on RFID Technology & Application (RFID-TA)*. IEEE, 2017, pp. 28–33.

[38] GDPR, "GDPR Article 8," https://gdpr-info.eu/art-8-gdpr/, accessed:2024-07-25.

Abbreviations

AWS	Amazon Web Service
BloSS	Blockchain Signaling System
BLE	Bluetooth Low-Energy
CIA	Confidentiality, Integrity and Availability
CRC	Cyclic Redundancy Check
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DoS	Denial of Service
DNS	Domain Name System
GDPR	General Data Protection Regulation
GHz	Gigahertz
GPS	Global Positioning System
IaaS	Infrastructure as a Service
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPFS	Inter Planetary File System
ISP	Internet Service Provider
MIFS	Minimum Inter-Frame Space
mW	Megawatt
nFADP	New Federal Act on Data Protection
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
P2P	Peer to Peer
PCS	Personal Communication Service
PDU	Protocol Data Unit
PLCP	Physical Layer Convergence Protocol
PSDU	Physical Layer Service Data Unit
REST	Representational State Transfer
RTT	Round Trip Time
SDK	Software Development Kit
SDN	Software-Defined Networking
SLA	Service Level Agreement
ToF	Time of Flight
UWB	Ultra-wideband
VNF	Virtualized Network Function
WiFi	Wireless Fidelity

List of Figures

List of Tables

Listings

Appendix A

Use Case Table

Table A.1: Categorization of Use Cases

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
1	Greeting upon entering				X	X	
2	UWB for conference				X	X	
3	Phone tracking at train station		X			X	
4	Showing price on the phone at train station		X			X	
5	Warning at train station		X			X	
6	Tracking patient	X	X			X	
7	Tracking coworkers		X		X	X	

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
8	Tracking storage facility				X	X	
9	Tracking forklift				X	X	X
10	Drive-Thru			X			X
11	Locating gadgets		X		X		X
12	Tracking in warehouse		X		X	X	
13	Navigation on train		X			X	
14	Emergency on train	X	X			X	
15	Tunnel construction				X	X	
16	Loading plane				X	X	
17	Border control		X				X
18	Tracking trains		X			X	
19	Police station				X	X	
20	Passengers connected to bus		X				X
21	Tracking pets		X			X	
22	Customer service				X		X
23	Navigation in stadium		X				X

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
24	Tracking coworkers at construction						X
25	Warning coworkers at construction		X				X
26	Tracking visitors in museum		X			X	
27	Tracking visitors in park		X				X
28	Finding car		X				X
29	Tracking shopping carts		X	X		X	X
30	Receiving information on factory				X	X	
31	Tracking trailer		X				X
32	Updating deliveries on cloud				X	X	
33	Tracking person in kitchen		X			X	
34	Finding person during emergency	X	X			X	
35	Contacting during emergency	X	X			X	

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
36	Locating person via radio station		X				X
37	Updating storage on cloud				X	X	
38	Housekeeping services				X	X	
39	Tracking athletes		X				X
40	Tracking child in the vicinity		X				X
41	Preventing child getting lost		X				X
42	Contacting child during emergency	X	X				X
43	Navigating to the car		X				X
44	Proximity in restaurant			X		X	
45	Locating in office				X	X	
46	Tracking taxi driver		X				X
47	Finding Uber driver		X				X
48	Using UWB in warehouse				X	X	

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
49	UWB at construction		X		X	X	X
50	Tracking emergency via UWB		X		X	X	X
51	Tracking coworkers in office		X		X	X	
52	Inter-connectivity in office				X	X	
53	Finding address				X		X
54	UWB in public place		X				X
55	Patient consultation	X				X	
56	Tracking patient	X				X	
57	Registering deliveries				X	X	X
58	Tracking coworker's condition		X		X	X	
59	Locating pallets in warehouse				X	X	
60	Inter-connectivity in warehouse		X		X	X	
61	Locating items in warehouse		X		X	X	

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
62	Tracking in coffee shop			X		X	
63	Tracking scouts on camp		X				X
64	Tracking person in warehouse		X	X	X	X	
65	Locating crate in construction				X	X	X
66	Tagging car with UWB		X			X	X
67	Connection between car and phone via UWB		X			X	X
68	Checking on patient	X			X	X	
69	Accessing patient data	X			X	X	
70	Tracking sensitive items		X		X	X	
71	Locating jewelry in shop		X	X		X	
72	Finding patient's device	X			X	X	
73	Finding car keys in office		X		X	X	

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
74	Finding car keys in repair shop		X		X	X	
75	Tagging pipes in warehouse				X	X	
76	UWB Phone in shop			X		X	
77	Locating gadgets in lab		X		X	X	
78	Tracking gadgets in lab				X	X	
79	Healthcare at home	X				X	
80	Tracking suitcases		X			X	
81	Wheelchair at airport		X			X	
82	UWB beacons in museum		X			X	
83	Retrieving data from athletes		X				X
84	Navigating at airport		X			X	X
85	Check-in at airport				X	X	
86	Tracking suitcases		X			X	
87	Bag-drop at airport		X			X	
88	Locating suitcase		X			X	

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
89	Self check-in at airport		X			X	
90	Security check				X	X	
91	Placing suitcases in plane				X	X	
92	Informing passengers		X			X	
93	Locating child at airport		X			X	
94	Information on wheelchair patient	X				X	X
95	Plane factory				X	X	
96	Warning about suitcase		X			X	
97	Tagging a suitcase		X			X	
98	Placing UWB device in public		X			X	
99	UWB in art gallery		X			X	
100	Attending meeting remotely				X	X	
101	Connectivity of devices in shop			X		X	

Index	**Name**	**Healthcare**	**Tracking**	**Marketing**	**Workplace**	**Indoor**	**Outdoor**
102	Informing customer on delivery				X	X	
103	Postal services		X		X		X
104	Package delivery		X		X		X
105	Security around warehouse				X	X	
106	Train operation				X		X
107	Retrieval of information on plane				X	X	
108	Tracking child at airport		X			X	
109	Tracking boarding on plane		X			X	X
110	Informing passengers at gate		X			X	
111	Retrieving patient data	X				X	
112	Proximity at dentist	X				X	
113	Tracking pets		X			X	
114	Phones connect to UWB beacon during exercise		X				X

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
115	Using UWB in stationery store			X		X	
116	UWB in a mall			X		X	
117	UWB in a shop at airport			X		X	
118	Tracking proximity in-store		X	X		X	
119	UWB in electronics store			X		X	
120	UWB for real estate			X			X
121	UWB for finding a person	X	X			X	
122	UWB beacons in museum		X			X	
123	UWB for sports		X				X
124	Passenger tracked by UWB		X				X
125	Tracking cars at gas station		X				X
126	Border controls		X				X
127	Drive-thru with UWB			X			X

Index	**Name**	**Healthcare**	**Tracking**	**Marketing**	**Workplace**	**Indoor**	**Outdoor**
128	Checking car condition				X	X	X
129	Public advertisement			X		X	X
130	Public ad from store			X		X	X
131	Advertisement in mall			X		X	
132	Promoting specific ad in-store			X		X	
133	Specified ad for customer			X		X	
134	UWB during support in-store			X		X	
135	Storage information				X	X	
136	UWB upon entering store		X	X			X
137	Proximity in restaurant			X		X	
138	Earning points in restaurant			X		X	
139	No points outside restaurant			X			X

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
140	Locating yourself in public space		X				X
141	UWB for customer support			X		X	
142	Locating tools in plane factory		X			X	
143	Tracking luggage cars		X				X
144	Navigating at airport			X			X
145	Finding car on parking lot		X	X			X
146	Car factory with UWB		X		X	X	
147	Tracking car parts in repair shop		X		X	X	
148	Tagging car parts in factory				X	X	
149	Tagging pallets in logistics				X	X	X
150	Locating containers in factory		X		X	X	
151	Tracking pallets in logistics				X	X	X

Index	**Name**	**Healthcare**	**Tracking**	**Marketing**	**Workplace**	**Indoor**	**Outdoor**
152	Tagging containers when shipping		X		X	X	X
153	Identifying excavator				X		X
154	Tracking pallets when loading truck		X		X	X	X
155	Registering trucks that enter facility				X		X
156	Positioning truck's position		X				X
157	Tracking forklifts in warehouse		X		X	X	
158	Locating trash and garbage truck				X		X
159	Tracking miners in mine		X		X	X	
160	Measurements in construction				X	X	X

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
161	Locating vehicles in construction		X		X	X	X
162	Finding the storage area				X	X	
163	Finding coworker in office		X		X	X	
164	Laptop and desk connection				X	X	
165	Locating car keys in office				X	X	
166	Tracking coworkers in room		X		X	X	
167	Contacting emergency in room	X				X	
168	Renting a bicycle		X				X
169	Finding rental scooter		X				X
170	Connecting scooter and phone		X				X
171	Tracking scooters in storage		X		X	X	X
172	Communication during sports event		X			X	X

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
173	Navigating in mall		X			X	
174	Navigation in park		X				X
175	Navigating via UWB in public		X				X
176	Checking data on ingredients				X	X	
177	Analyzing sales		X		X	X	
178	Locating place in mall			X		X	
179	Locating coworkers in warehouse		X		X	X	
180	Finding items in shop			X		X	
181	Navigating in stationery store		X	X		X	
182	Registering items in stationery store			X	X	X	
183	Tracking shopping carts		X	X		X	
184	Finding shopping carts		X		X	X	

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
185	Using robots via UWB				X	X	
186	Tagging a car for UWB		X			X	X
187	Reminding items to buy			X		X	
188	Car detects emergency	X	X			X	X
189	Checking car on phone		X			X	X
190	Locating the car		X				X
191	Tracking in workplace		X		X	X	
192	Locating gadgets in lab				X	X	
193	Tracking gadgets in lab		X		X	X	
194	Tracking small pieces in box		X		X	X	
195	Tracking beds in hospital	X	X		X	X	
196	Tagging beds in hospital	X	X		X	X	

Index	Name	Healthcare	Tracking	Marketing	Workplace	Indoor	Outdoor
197	Spotting coworker in hospital	X	X		X	X	
198	Retrieving room information in hotel				X	X	
199	Updating room information in hotel				X	X	
200	Vacuum informs UWB beacons upon cleaning				X	X	
201	Tracking person at home		X			X	
202	Tracking child in play area inside		X			X	
203	Tracking child on playground		X				X
204	Tracking children on playground		X				X
205	Tracking children taking bus		X				X
206	Tracking children on the bus		X			X	

Index	**Name**	**Healthcare**	**Tracking**	**Marketing**	**Workplace**	**Indoor**	**Outdoor**
207	Retrieving information on an animal				X	X	X
208	Checking equipment in barn				X	X	
209	Bartender using UWB				X	X	
210	Tracking in casino		X	X		X	
211	Tracking tools for news reporter		X		X	X	X
212	Identifying yachts		X				X
213	Tracking movements on the street		X				X
214	Retrieving information on soccer fields		X				X
215	Tracking children at school		X			X	
216	Sending data when shopping			X		X	
217	Turning on street lights when needed		X				X

Index	**Name**	**Healthcare**	**Tracking**	**Marketing**	**Workplace**	**Indoor**	**Outdoor**
218	Tracking scooter on the street		X				X
219	Retrieval of health information	X			X	X	