

Privacy issues of mobile phone companies' usage of Ultra-Wideband (UWB) technology

Analysing the use of UWB in mobile phones from a multi-actor perspective, magnifying privacy concerns and formulating guidelines



Privacy

Privacy is a fundamental human right. Your devices are important to so many parts of your life. What you share from those experiences and who you share it with, should be up to you. Products should be designed to protect your privacy and give you control over your information. It's not always easy. But that's the kind of innovation we should believe in.

DELFT UNIVERSITY OF TECHNOLOGY

MASTER THESIS

Privacy issues of mobile phone companies' usage of Ultra-wideband (UWB) Technology

Analysing the use of UWB technology in mobile phones from a multi-actor perspective, magnifying privacy concerns and formulating guidelines

Mohamed Adeeb Ahmed
5126207
Faculty of Technology, Policy and Management
TU Delft

Keywords: mobile phones, Ultra-Wideband technology, radio technology, privacy, thematic analysis

Graduation committee:
Chair: Dr.ir. C. (Carlos) Hernandez Ganan
1st Supervisor: Dr. F.S. (Seda) Gürses
2nd Supervisor: Dr.-Ing. T. (Tobias) Fiebig



Delft University of Technology

Acknowledgements

Throughout the duration of the last 5 months, I have received immense support. I would like to take some time to thank the people without whom this thesis would not be possible. Even though it is just my name on the second page of this document, it was definitely a combined effort especially mentally during a pandemic.

First, I would like to thank my supervisor Dr. Seda Gurses. You peaked my interest in the idea of privacy during my first year. You helped me pick a topic that is relevant to the society around us. You created invaluable space for me to conduct research, helping me bounce ideas off you but at the end of the day, pushing me to find my own voice. I greatly appreciate the freedom you gave me to find my own path while writing my first thesis. You gave me guidance throughout and supported me, EVEN on one leg. You will definitely be able to see more of Adeeb in what he does.

I would like to also thank my other committee members, Dr. ir. Carlos and Dr. Ing. Tobias. Thank you for first agreeing to be on my committee, but also investing time and providing valuable feedback. I feel honoured, proud and happy that you accepted to do so. We may have only met through this thesis but it has been a pleasure discussing and presenting ideas to you, albeit only virtually.

I cannot thank them personally for privacy reasons, but I am greatly indebted to all my expert and user interviewees. Without your effort, time, knowledge, creativity and ability to answer questions while put on the spot, this thesis would quite literally be only halfway written. To all the emails sent back and forth, the rescheduling, the consent forms and finally, the actual interviews, it has been a pleasure getting to know you. Your insight has been invaluable in writing this document and I hope we can meet again in a more personal space.

I would like to thank all the professors that have taught me during the last two years. While this thesis may represent the end of my education cycle at TU Delft, it has been an absolute pleasure to sit in your classes. You have taught me about philosophy, law, ethics, behaviour modeling, negotiation, supply chain management, the works. You have helped mould me into a Complex Systems Engineer that cannot look at anything without analysing the different processes it needs to go through to come to fruition. Thank you for your support, help, guidance and overall friendly attitude. If anything, the TU has been an embodiment of Dutch culture where the faculty are the main representatives. You have always had your door open to my concerns and for that, I will truly be indebted.

I have to thank who I consider to be my closest friend, Manoviraj. You have helped me throughout the duration of my thesis, whether it comes to the thesis templates, thesis procedures, discussing ideas, sharing low budget dinners or sharing the doom and gloom of the pandemic. You have been a friend of the truest definition of the word. Thank you for your support because without you, the last 5 months or even 24 months may have been a lot tougher. There's also a whole list of friends I want to mention who showed me life is not all about work but rather the memories that you make. We have met through the TU but our bonds will definitely outlast our time here.

Last but not least, I would like to thank my family. To my brother, who has been a true role model, who I try to do as much as I can to learn from and replicate. To my parents, for believing in me, for supporting me and for truly being there through the last 5 months. Thank you for everything you have done for me, beyond the confines of my education alone.

Abstract

Ultra-Wideband (UWB) technology became unregulated within the EU in 2007. Most recently, it was integrated into mobile phones in 2019, notably Apple and Samsung adding it to all their newer models. While UWB is characterised as a radio technology with any signal above 500 MHz, it operates within the 6-9 GHz range in mobile phones. This allows for fast data rate, low power secure communication, multipath facilities and accurate localization. While the integration of UWB is mostly advantageous to users and innovators, its ability of accurate localisation may lead to severe privacy concerns.

The aim of the thesis is to understand the privacy concerns of UWB's integration into mobile phones by answering the main research question: how do experts and users perceive privacy concerns of UWB usage in mobile phones; and how can they be mitigated? It was subsequently broken down into three sub-research questions: 1. What are the possible applications of UWB in mobile phones? Phones have other incumbent radio technology embedded such as Bluetooth (BLE) and Wi-Fi, however it seems like UWB is being integrated to serve additional purposes. The answer to this question seeks to understand from gray and research literature how UWB can be used in mobile phones and what advantage it gives over incumbent technology. Research shows UWB gives phones the ability for indoor navigation, gesture-based control, foot traffic analysis for smart retail, teleconference systems, proximity-based localization, key-less entry among others.

This leads to research question 2. What are the potential privacy concerns associated with UWB? The incorporation of new technology capable of accurate localization leads to privacy concerns. All privacy issues were categorised on the basis of three paradigms: social, surveillance and institutional mentioned in Gurses and Diaz, 2013. This was initially done by interviewing experts from the three groups of privacy experts, policy regulators and technology experts. Analysis of their answers showed that UWB privacy concerns seem relatively similar to BLE and Wi-Fi localization, albeit with higher granularity. UWB allows mobile phone companies, third parties and governments track people accurately indoors, push advertisements depending on location, obtain relative relationships between people based on distance leaving people with no place to hide. Subsequently, user interviews were carried out to see if they could identify the same concerns of UWB. Results showed that from the data of users interviewed, all of them believed that accurate data localization of people is crossing a line that users cannot push back on. A majority of them saw most of the same privacy issues as the experts showing that, as people get more adept with technology they understand how it can affect their privacy. A common question that was asked across all the interviews was how can we protect our privacy in the face of such penetrating innovation as time lapses.

Which is the final sub-research question: 3. What are technical and societal approaches to address privacy concerns? Experts provided solutions that were more industry oriented which included decoupling UWB from other location-based services, provision of opt-out settings on a more prominent basis, reworking license agreements, industry wide discussion and self-regulation in terms of privacy. However, users gave answers that were more user-centric and gave more control to the common public. This included users negotiating their own privacy agreements, compensation models for loss of privacy, a more holistic regulation process and finally, trying to break the control of big tech companies. This shows that users and experts have very similar understanding of privacy issues but very different views on how privacy should be protected. Perhaps, it may be time for regulators to pay heed to user suggestions. These suggestions were then compared with privacy mitigation strategies mentioned in literature. Notably, the most overarching concept that needs to be incorporated is the concept of Privacy-by-design which can then be broken down into technical and societal strategies. Technical approaches included concepts such as obfuscation, k-anonymiser, differential privacy, dummy localization and access control mechanisms. All the technical strategies seemingly had the same issue of requiring third-party applications to function. Sophisticated security measures and privacy statements would then be needed to ensure these companies do not choose monetary gain over user privacy. Societal approaches included concepts of data-for-all, technical regulatory bodies and finally, breaking up of big tech companies. As time passes and innovations become more pervasive, it may be too late to incorporate privacy protection actively. The time to protect privacy is now.

Contents

Acknowledgements	i
Abstract	ii
List of Figures	3
List of Tables	4
1 Introduction	5
1.1 Problem definition	5
1.2 Research overview	6
1.2.1 Literature survey	6
1.2.2 Discussion	6
1.2.3 Research Question	7
1.2.4 Research Sub-Questions	7
1.3 Potential challenges	8
1.4 Thesis structure	8
2 Methodology	10
2.1 Real time technology assessment	10
2.1.1 Sub-questions breakdown	11
2.2 Privacy methodology	12
2.3 Interviewee selection	13
2.3.1 Expert Interviews	13
2.3.2 User Interviews	14
2.4 Thematic analysis	14
3 Technology and Regulatory Specifications	16
3.1 Ultra-Wideband Technology	16
3.2 Comparison with other wireless technology	18
3.2.1 Bluetooth	19
3.2.2 Wireless Fidelity (Wi-Fi)	19
3.2.3 Technical characteristics comparison	19
3.2.4 Functionality comparison	19
3.3 Radio technology regulatory bodies	20
4 UWB Applications	22
4.1 UWB research use cases	23
4.2 Mobile phone companies use cases	26
4.3 Discussion	27
5 Privacy and radio technology	29
5.1 Potential privacy issues of UWB integration in mobile phones	29
5.2 Privacy issues of location monitoring capabilities of radio technology	31
5.2.1 Social privacy concerns-	31
5.2.2 Surveillance privacy concerns-	32
5.2.3 Institutional privacy concerns-	33
6 Expert Interviews	35
6.1 Expert Interviewees	35
6.2 UWB regulation within the EU	36
6.3 Privacy concerns	37
6.3.1 How does UWB differ from other incumbent radio frequency technology?.	37

6.3.2	What are the major issues seen with AirTags (and Android equivalent)?	38
6.3.3	What are the concerns with 5G UWB being introduced?	38
6.3.4	What might be some security concerns?	39
6.3.5	What are some surveillance privacy concerns?.	39
6.3.6	What are some social privacy concerns?	40
6.3.7	What are some institutional privacy concerns?.	41
6.3.8	What can be done to protect privacy?	42
6.4	Discussion	43
7	User Interviews	45
7.1	Interview procedure	45
7.2	Interview questions	46
7.3	Personal identifiers	46
7.4	Surveillance privacy.	48
7.5	Social privacy	50
7.6	Institutional Privacy.	51
7.7	Privacy protection suggestions	52
7.8	Discussion	53
8	Privacy mitigation strategies	55
8.1	Privacy-by-design	55
8.2	Technical approaches	56
8.3	Societal approaches.	58
9	Conclusion	62
9.1	Main findings	62
9.2	Limitations	63
9.3	Recommendations for future research	64
A	Appendix	65
A.1	Ethics	65
	Bibliography	70

List of Figures

1.1	Different domains of research papers	6
1.2	Report structure	8
3.1	A sinusoidally shaped UWB pulse	16
3.2	Difference between narrowband and UWB transceivers (Kshetrimayum, 2009)	17
3.3	Stakeholders responsible for UWB usage	21
4.1	Application domains	23
4.2	Use cases for Apple's UWB devices (Evans, 2021)	27
7.1	Surveillance privacy concerns thematic analysis	48
7.2	Social privacy concerns thematic analysis	50
7.3	Institutional privacy concerns thematic analysis	51
A.1	Information sheet for experts	66
A.2	Consent form options for experts	67
A.3	Information sheet for users	68
A.4	Consent form options for users	69

List of Tables

1.1	Search hits across three academic websites	6
2.1	Revised RTA for this research	11
6.1	Expert Interviewee details	35
6.2	Different privacy concerns of UWB incorporation	42
7.1	Breakdown of interview questions	46

1

Introduction

1.1. Problem definition

There has been widespread research to build on a wireless technology that is capable of short range data transfer. Ultra-wideband (UWB) technology has emerged to the forefront with great promise to satisfy this growing demand for low-cost, high data rate and short range wireless transmission (Zin and Hope, 2010). It is a radio technology that can use very low energy levels for short-range, high-bandwidth communications over a large portion of the radio spectrum (K. Zhang et al., 2018). This means that it is able to operate – like WiFi and Bluetooth – through radio waves at a very high frequency and uses a wide spectrum of several gigahertz (GHz).

After considerable technical development since the early 2000s, UWB has recently received a lot of attention because it can provide centimetre-level positioning accuracy (K. Zhang et al., 2018). This can be translated into ethical issues and privacy concerns as mobile phone companies seek to adopt them into their mobile phones, as Apple has done so in the latest iPhone 11 and all subsequent models (Alliance, 2020). The Ultra-wideband Alliance¹ provided a report to the Federal Communications Commission (FCC), detailing the reasons why this technology may be commercially advantageous. This included applications of high-accuracy tracing for CoVID-19, heart-rate monitoring, temperature monitoring, universal smart remote controls (Alliance, 2020). However, it has to be noted that all the applications mentioned have commercial advantages whereas, the proverbial 'flip side of the coin' was not made mention of.

Historically, UWB was used for its military propositions of accurate radar and radio frequency positioning (Fowler et al., 2017). Nowadays, UWB applications in research has extended to:

1. utilisation of infrastructure-free vehicle localisation (K. Zhang et al., 2018)
2. target person tracking for robots (Feng et al., 2018)
3. precise positioning within huge vessels that include ships or submarines (K. Zhang et al., 2018)
4. wireless body area network (WBAN) which can be placed on a person to provide adaptable healthcare (Ullah et al., 2009) and,
5. medical applications including cardiology and obstetrics imaging (Vishwesh and Raviraj, 2018)

However, Apple provides a completely different reason for incorporating UWB: spatial awareness, where you can precisely locate other UWB-equipped devices and operate it as GPS at the scale of your living room. The Apple website states that this enables faster localization and file-sharing using AirDrop, their short range file transfer capability. These applications show the technical capability of UWB but also its potential for intrusion into people's lives. Considering how Apple, Samsung, Huawei and all major mobile companies want to incorporate UWB technology into their devices, issues of privacy and location monitoring are imminent. Since a vast majority of the human population requires a mobile phone for day-to-day activities, UWB technology may have unregulated and unchecked applications if big technology companies promote it effectively.

¹Ultra-wideband Alliance is a group of 25 members (companies) that advocate for UWB technology usage and promote verticals that show the value of UWB for IoT and Industry 4.0.

Regulators may need to move faster if this is the case. This is the research domain for this thesis to look at from a multi-actor perspective that includes technology experts, privacy researchers, governmental regulators and users. It seeks to determine the trade-off between privacy and technological innovation.

1.2. Research overview

1.2.1. Literature survey

An initial literature survey was done to highlight the issues of privacy, if any, when it comes to UWB technology. The search terms included 'UWB (Ultra wideband technology)' and 'privacy.' Additional terms included 'Location monitoring' AND 'ethics/ privacy.' Presented below are the number of hits across the three search engines used.

Search terms	Google Scholar	Web of Science	Scopus
"UWB" and "Privacy"	16400	39	76
"Location monitoring" and "privacy/ ethics"	75000	611	8

Table 1.1: Search hits across three academic websites

There were three main domains which characterised the research of UWB technology as shown in the figure below. In the health domain, the main areas of research were assisted living conditions and Wireless Body Area Networks (WBAN) to help maintain health levels of individuals. Within the domain of comparison, UWB was compared with other wireless technologies such as Bluetooth, Wi-Fi and GPS under different criteria. Finally, within the last domain, there are several location-based possibilities of UWB usage which are being researched for novel applications.

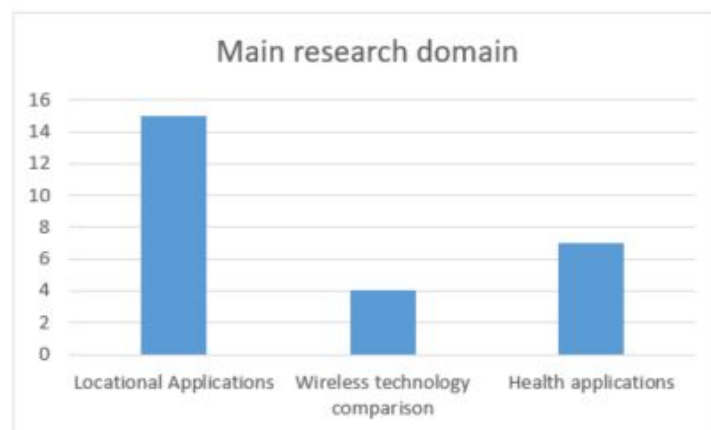


Figure 1.1: Different domains of research papers

1.2.2. Discussion

UWB has seen the same history as Global Positioning System (GPS), being firstly used for military applications and banned by the European Conference of Postal and Telecommunications Administration (CEPT) for market usage (Fowler et al., 2017; Karim, 2004). [The CEPT is the governing body for all telecommunications technology in the European Union (EU).] This was done because they interfered with medium-wave receivers. However, research over time showed that UWB uses lower power and hence, medium-wave and UWB receivers can co-exist. This 'discovery' led to the CEPT regulating commercial usage of UWB in 2007 (Karanja et al., 2018) which has been added within Apple and Samsung mobile phones in 2019. The timeline of UWB usage in the EU and United States has been different and has been governed by different bodies. This means there are different regulations, data protection regimes and harmonization standards for the two regions. For the purpose of this research, the European Union is the focus of the analysis.

Since its inception in the early 2000s, UWB has been seen as a technology that can be used for location discovery and device ranging (Alliance, 2020). Device ranging refers to the process of establishing object

distance. It is with this premise that research has looked at the possible wide-scale commercial applications of UWB. The probable commercial applications of UWB will be mentioned in detail in chapter 4, referencing different research conducted in the last ten years. There are five main domains that these applications will be broken down into: medicine, localization, penetrability, connectivity and crowd-sourcing. These seem to show that UWB is a largely invasive technology.

Centimetre level accuracy of UWB helps in accurately locating stationary and moving objects, which can include antiquities and autonomous robots. UWB technology also consumes relatively low power. While these may be highly advantageous, research has not considered scenarios where these capabilities are aggregated in a personal smartphone. There is a cluster of personal information on a personal phone that raises considerable privacy concerns which a majority of papers have failed to address. Cheng et al., 2020, Kim et al., 2012 and Ruan et al., 2018 are the only papers from the initial literature review that briefly mention privacy issues which is not adequate in this day and age where the sense of privacy is deteriorating. This is the knowledge gap that this thesis seeks to magnify and dive into.

1.2.3. Research Question

The papers within the first query did not yield any privacy risks of UWB within hand-held devices, thus the second query of location monitoring and ethics was carried out. The results further showed that there is not a lot of prominent research in the last five years. Wang and Loui, 2009 states that from the offset, location information may not very be indicative or intrusive. But the aggregated information that is stored in mobile phones serves as a huge privacy concern. It is with this centralised aggregated information that mobile phone companies can piece together an entire profile about a customer. This could reveal results pertaining to race and political views. If this is combined with the amount of information social media apps are selling to third parties, it raises a serious concern of what information is actually protected by mobile phone companies.

The wide-scale usage of UWB within phones and its lack of adequate introduction to the common public will not curb these issues. This idea is supported by Michael et al., 2006 which states that companies sell the idea of these technologies by purporting 'possible' applications and uses while completely foregoing the very real threat of privacy that every human being has a right to. Even regulators seem to forget that this is a major concern. Michael et al., 2006 further mentions that any new technology must be analysed from a privacy perspective to help integrate it successfully into society, while devising privacy protection strategies. This raises the question: **how do experts and users perceive privacy concerns of UWB usage in mobile phones; and how can they be mitigated?**

This research question is relevant in the 21st century as technology is getting more invasive everyday. The concept of privacy is lost on big technology companies such as Apple, Samsung, Amazon, Facebook, etc. They continuously state that they prioritise user privacy. But whistleblowers and news articles alike, eventually reveal that this is not the case. This thesis aims to highlight and magnify, from a privacy perspective, a new technology that a large proportion of the public does not know about. This will help educate the public about the potential privacy issues of UWB and possibly serve as a starting point to improving privacy regulations or preserving strategies. Furthermore, this thesis aims to operate in the knowledge gap of no prior privacy research being conducted on UWB technology. Prior research has been conducted in the field of BLE and Wi-Fi. While this serves as a reference for chapter 5, this thesis serves as one of the first theses written on the privacy concerns of UWB. It is increasingly being integrated into more personal devices which is why its privacy concerns are important for the common public.

1.2.4. Research Sub-Questions

In order to answer the main research question, the research has been divided into three sub-research questions to streamline the data collection and analysis process. These are enlisted below with a justification on their relevance:

Q1. What are the possible applications of UWB within mobile phones?

Currently, mobile phones have incumbent wireless communication technologies which include Bluetooth and WiFi. From a business and user perspective, the incorporation of UWB within phones would need to improve a certain aspect of mobile phones. Apple states that this is for 'spatial awareness' which they describe as GPS on the scale of your living room (Apple website). Looking at the possible applications, it seems that UWB is capable of more than just spatial awareness. To answer this question, literature research will look at proposals and any research conducted to understand the wide-scale commercial applications of UWB. Purely academic research will be cross-referenced across uses mentioned by mobile phone companies. These use

cases will be gathered from patent papers, consortium documents and online articles.

Q2. What are potential privacy concerns associated with UWB?

In order to answer this question, two different groups will be interviewed. The first group involves experts within the domain of UWB. These interviews will help understand the policy regulations behind UWB, how it is harmonized within the EU and what potential privacy concerns are there with the applications. There are three main stakeholder groups considered for UWB: regulators, privacy researchers and mobile phone companies.

Regulators include organisations such as the European Conference of Postal and Telecommunications Administration (CEPT) and European Telecommunications Standards Institute (ETSI). Historically, they have been responsible in regulating similar wireless technology such as GPS and Bluetooth. Their input will help the reader understand how radio technology is regulated within the EU and if privacy is an important governing criteria. Privacy experts will help highlight any privacy concerns as seen in different UWB-mobile phone use cases. However the third stakeholder group of mobile phone company employees will not be interviewed as it seen as a conflict of interest. They are responsible for including UWB for a positive business perspective. Privacy issues largely reduce the potential positive impact they hope to have. Further, research has shown that company employees have largely refrained from talking about UWB in public interviews and research. The information obtained from stakeholder groups will be used to compare with user concerns and check if the same issues resonate with them. With the use of thematic analysis, user statements will be compared to find the most prominent privacy issues and whether they are consequential to them or not.

Q3. What are technical and societal approaches to address privacy concerns?

The output from the previous question will serve as guiding light to answer this question. In order to address and curb these concerns, some technical and societal privacy mitigation strategies will be presented. These can serve as privacy mitigation strategies for developers, regulators and users alike.

1.3. Potential challenges

The biggest challenge of conducting research within the topic of UWB is the lack of literature. There is significant research conducted in the applications of UWB, how they can be commercialised and if there is a market for the same. However, as the literature review showed, there is very little information on the potential privacy concerns which is the central objective of this thesis. In order to ensure a suitable knowledge base could be obtained and provided to the reader, interviews were considered as the main data gathering process. Gray literature, company websites, company statements and patent papers are additional data gathering processes. The thesis aims to understand privacy concerns mentioned by experts and users alike by conducting interviews. This is a time consuming process. It involves the need to contact potential interviews, obtain their consent, officially interview them, transcribe interviews and then compare across participants. Furthermore, the data regulations within the EU need to be respected at all times, which is a stringent process. The TU Delft data supervisor was contacted to provide a suitable procedure that is adherent to the GDPR regulations. The entire ethical procedure followed for the research is shown in the appendix.

Finally, the research was conducted during the CoVID-19 pandemic. The communication between potential interviews was extended because of this. Further, the possibility of using the TU Delft campus for interviews was impossible. Teleconferencing applications became the main means of communications. There was the need for a schedule so that the potential interviews could feel comfortable giving consent and talking to someone who they haven't met before.

1.4. Thesis structure

The flow of the research will follow the same linear structure as the sub-research questions. The figure below shows the exact sequence and chapters of the report. The contents of each individual chapter is briefly discussed.

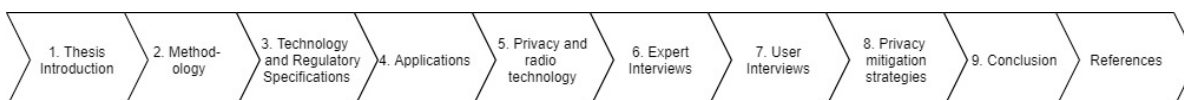


Figure 1.2: Report structure

1. **Chapter 2: Methodology** - The methodology for the entire research is laid out. This includes the core idea of real time technology assessment, the different privacy paradigms used for privacy issues characterization, how the interviews will be assessed and compared.
2. **Chapter 3: Technology and Regulatory Specification** - UWB is explained in the chapter. Since it is a very recent unlicensed technology, its capabilities and characteristics are discussed which is necessary to understand its working. It is then compared to Bluetooth and WiFi, two technologies that are most similar to its working and will work in tandem with, in a mobile phone.
3. **Chapter 4: Applications** - This chapter first looks into the applications academic research has considered. This is done through extensive desk research - mainly literature reviews for papers over the past ten years. This aligns with the timeline of UWB unregulated use in the EU, thereby progressing the idea that technical possibilities have exponentially grown recently. Then, the use cases of UWB in mobile phones are elaborated to see what phone companies have in mind.
4. **Chapter 5: Privacy and radio technology** - The main privacy issues of radio technology are introduced here. These issues of radio technology and location information are categorised on the bases of three paradigms to provide structure for interviews and thematic analysis.
5. **Chapter 6: Expert Interviews** - Expert interviews are required to gain an initial knowledge base and highlight potential privacy concerns. These are gathered from experienced individuals in the field of policy regulation, technical testing and privacy with respect to UWB. Their input will serve as a comparison to the findings obtained from users.
6. **Chapter 7: User Interviews** - User interviews are conducted to compare their concerns across experts. These serve as an outlook to present how the common public looks at privacy concerns. The analysis from interviews are broken down into the three privacy paradigms ameliorated with the results of the thematic analysis.
7. **Chapter 8: Privacy mitigation** - In order to answer the final sub-research question, potential technical and societal approaches to handling privacy concerns are discussed here.
8. **Chapter 9: Conclusion** - The final chapter discusses the main conclusions of the research, limitations and recommendations for future work in the field.

2

Methodology

In the previous chapter, a brief introduction was given on the problem and knowledge gap that the thesis aims to look at. This chapter seeks to provide details on an overarching methodology used for the thesis in section 2.1. Further, the different methods of data collection analysis are presented in sections 2.2-2.5.

2.1. Real time technology assessment

The research follows the overarching methodology of 'Real-time technology assessment (RTA)' theoreticized in Guston and Sarewitz, 2002. This is done within the realms of privacy alone and does not take into account other aspects such as interoperability, functionality, costs, etc. RTA states that there is a need for integrating social science and policy research with engineering investigations from the outset of any new technological innovation. This allows new technology to be considerably analysed, thereby maximizing its applications, minimizing its risks and ensuring responsiveness to public interests/ concerns. Within Europe, it is quite a strenuous process to follow such a method of technology assessment as various organizations have to work together to ensure proper analysis of new technology. For UWB, the official regulatory bodies include the Electronic Communications Committee (ECC), European Data Protection Board (EDPB), European Data Protection Supervisor (EDPS), ETSI, CEPT, individual data protection agencies and radio communications authorities of member states. Feedback from these different organisations can effectively push UWB through 'constructive criticism' and obtain a positive innovation.

Guston and Sarewitz, 2002 mentions a four step procedure to conduct an exhaustive TA:

1. **Analogical case studies** - Studying past examples of any similar type of technology, how it was presented and how it was accepted by the public and regulators alike. This means knowledge of who was responsible for an innovation in the past, how it was critiqued and thereby, the final release of the innovation to the public. In the case of radio technology such as UWB, the authorities mentioned above are the final ones responsible. Additionally, the author mentions that is a possibility to brainstorm some societal issues at this stage, that must be taken into account to present the iterative process of developing UWB.
2. **Research process mapping** - This step states that it is necessary to identify key RD trends, major participants in research and policy. A map is then made to link the different stakeholder groups responsible.
3. **Communication and early warning (CEW)** - The previous two steps have mentioned the 'back-end' impacts of new technology and have missed out the 'front-end.' This means that the public and media would shape the eventual release of the technology. CEW allows understanding how public perceptions are evolving and how they view the innovation with respect to similar technology and what issues they conceive. This effectively allows conversation between researchers and public thereby, leading to technology that is actually required by the common public.
4. **Technology assessment and choice (TAC)** - The final step has two main functions: assessing the improvements and future course of UWB through forecasting and experts elicitation, and curbing its potential impacts.

The four steps of the RTA process are moderately iterated with regard to this research to answer the three research sub-questions sufficiently. They are cross-referenced in a table to show which research question adheres to each step of the procedure. Moreover, it shows which chapter of the research corresponds to which stage of the RTA procedure. After the table, the data analysis methods employed for each of the research questions are explained in detail. RTA signifies that it is an internal process that needs to be kept in mind for

	RQ1	RQ2	RQ3
Chapter	Chapter 2: Technology and Regulatory Specifications Chapter 4: UWB Applications	Chapter 5: Privacy and radio technology Chapter 6: Expert Interviews Chapter 7: User Interviews	Chapter 8: Privacy mitigation strategies
Analogical cases studies	1. Comparison of UWB with BLE and Wi-Fi 2. Current applications of UWB from a research domain		
Research process mapping	Use cases envisioned by mobile phone companies	Policy regulations and general privacy concerns obtained from stakeholders	
Communication and early warning		1. Semi-structured interviews with users (and stakeholders) 2. Mapping privacy concerns of users and comparing with stakeholder input	
Technology assessment and choice			1. Privacy concerns of UWB vs BLE and Wi-Fi 2. Brief policy-based and technical approaches

Table 2.1: Revised RTA for this research

any new technology, which is why it has been iterated for this thesis. Analogical case studies are difficult as there are different regulations for different radio technology. This can be seen in various European Commission documents. This makes it difficult from an external thesis perspective as these documents can be quite extensive and include legal jargon. For this reason, research papers were the main data collection process. Further, there are various potential organisations responsible for the release and regulation of a new technology. In this research, it has been explicitly shown at the end of Chapter 3. This concludes the 'back-end' processes involved. For the 'front-end,' regulatory bodies usually have a public consultation prior to the release of any new technology. However for this research, one-on-one interviews are conducted as a substitute. This allows both privacy experts and users to voice their concerns which may not have been possible, otherwise. Finally, the technology is internally assessed and presented by regulatory bodies. This thesis seeks to iterate this process by including different privacy mitigation strategies so that user privacy can be protected properly in the future.

A literature review has been carried out to include different privacy concerns for incumbent radio technology. This firstly allows the user to make a comparison but also grounds the concept of privacy and help understand the evolution of privacy concerns. However, the biggest limitation is there is a lack of knowledge on whether all the research applications correspond to potential real world use cases. This is why it is difficult to understand what the actual privacy issues of UWB may be. Expert interviews are crucial for this purpose to highlight issues that may be overlooked by members who do not actively work in UWB. These interviews can be termed as the internal procedure of an RTA. Users are then interviewed to correspond to the idea of communication and early warning. A majority of users do not know about the existence of UWB and highlighting some use cases/ privacy concerns may help them provide their opinion. This provides another limitation as most users have lesser understanding of privacy. They need to be suitably informed and educated to ensure the interviews conducted with them are fruitful. This cross referencing of privacy issues between educated experts and users, help replicate an RTA while ensuring good privacy protection strategies are formulated.

2.1.1. Sub-questions breakdown

Before the table, the RTA process was introduced and the concepts of each row was explained. Below, the table is broken down by columns and individually, the methods to answer the three sub-questions is explained.

Q1. What are the possible applications of UWB within mobile phones?

Literature research is the main data collection method to answer this question. In chapter 4, the different applications of commercial UWB usage is introduced, both from research and mobile application perspectives. For the former, the data collection process is research papers on the potential applications. Since the European Union labels UWB usage in mobile phones as generic usage and limits frequency from 6-9 GHz, the extensive list of possible UWB applications are not all technically possible in mobile phones. In order to document use cases of mobile phones companies, a second literature review is conducted to gather patent papers and company statements from mobile phone companies such as Apple and Samsung.

Q2. What are potential privacy concerns associated with UWB?

The different privacy issues identified are categorised on the three paradigms mentioned in Gurses and Diaz, 2013 to help streamline the research and understand how stakeholders are envisioning UWB usage. This privacy methodology is discussed in section 2.2. Stakeholders working on UWB are interviewed to document their perceived value of UWB usage. To understand their perceptions, the main data collection technique is open-ended interviews. These provide a holistic understanding of why UWB is being introduced, what the use cases are and what potential privacy concerns could come up. For regulators, interview questions include – their understanding of UWB, what are the different regulations applied on comparable technology, how they plan to regulate the usage or if UWB proliferation will go unchecked. UWB privacy researchers' interviews include questions such as – if there are wide-spread ethical concerns, what use cases need to be regularly checked, what aspects regulators need to keep in mind. Their opinions and input is important in finding and highlighting any knowledge gaps that stakeholders such as mobile phone companies and regulators may have not considered.

Then, potential users are interviewed. Data obtained from stakeholders is compared with the statements received by users to see if privacy concerns from stakeholders and users are uniform. The interview structure for users is elucidated in detail in section 2.4. The data collected is then analysed. This is done with the use of thematic analysis which is visualised through mapping. The concept of thematic analysis is discussed in detail in section 2.5. Mapping as a technique states that the ideas, preferences and perceptions can be derived from users' speech acts and represented in visual and graphical form (Clarkson and Hodgkinson, 2005). The cognitive map would include the subject-verb-object construction such as 'x is a general benefit to society' or 'y marks a stark concern for privacy.' More specifically, a map is created to understand utility relationships, which can easily be derived from the answers to open-ended questions.

Q3. What are potential technical and societal approaches to address these concerns?

The main privacy concerns obtained from the stakeholder groups serve as an input for this sub-research question. A literature review will help uncover any technical and societal approaches to solving the problem of privacy. The final outcome is a list of privacy mitigation strategies that can solve the privacy issues of wide-scale and commercial UWB usage.

In the next four sub-sections, the methods employed to answer sub-research questions 2 and 3 are explained. This involves the privacy methodology employed to structure the interview questions for prospective interviewees, explained briefly in section 2.2. Section 2.3 explains the process of obtaining interviewees that are knowledgeable on the topic of UWB and fit within the stakeholder groups mentioned before. Section 2.4 includes the interview protocol for users. Finally, section 2.5 explains the concept of thematic analysis, its advantages and disadvantages to analysing replies to open-ended questions.

2.2. Privacy methodology

Privacy is defined as the state in which one is not observed by other people, which means that the number of potential privacy concerns may be endless. Different researchers have differing views on how privacy should be viewed and how to characterise such issues. This research, however, uses the concept of three paradigms of privacy, first mentioned in Gurses and Diaz, 2013. The general privacy problem is defined as being three dimensional: surveillance, social and institutional which are presented in the next few paragraphs. All the privacy issues mentioned in research, literature or in the interviews are categorised based on the three paradigms. The three paradigms of privacy are overarching and suitable for the assessment of technology. Gurses and Diaz, 2013 provided the framework from a technological perspective which is still quite holistic. It takes into account the use of technology, how it can inherently affect user privacy and finally, the institutional control users may have over data. It adheres to all procedures from the usage of technology to the eventual use of collected data. It is also quite simplified and easy to understand as other frameworks such as NIST and ISO are complex, comprehensive and suitable only for privacy experts.

The surveillance problem refers to the issues that arise from the personal information obtained from the activities of people as tracked by mobile phone companies. To specify it further, consider a scenario where two individuals are interacting with each other but the radio-waves which are being sent across, can be tracked by any party that is trying to listen in. The radio spectrum is regulated by official regulators whereas mobile services are provided by mobile phone companies or any third parties. Any relevant data can then be obtained by government authorities, intelligence agencies or law enforcement to keep track of the users. Mobile phone companies would be able to gather information and form customer profiles based on the information obtained because people use their technology. In other words, it refers to the confidentiality of the

information and how parties who are not involved get information about users because their technology is acting as the medium of communication.

The social privacy problem addresses the concerns that emerge through the boundaries of social interactions which are mediated by technology and in this case, mobile phones. Whether there are two users 'conversing' through the use of UWB or one user trying to locate another user without UWB, there is some information available. In the former, there may be circumstances where the other user may not want to be contacted or is seen on someone else's radar without consent. The second may be how someone without a UWB device may appear on the radar of someone with a UWB device. This paradigm largely refers to how social relations are disrupted and how privacy cannot be protected by technology but there is possibility for negotiation between people. This further includes the differences in understanding users have of technology and why they need to understand how privacy is being affected everyday. They need to understand how awareness of design can help improve their negotiating power while educating themselves about the issues of technology.

The final approach of institutional privacy refers to the problems related to users effectively not having control over the collection or processing of identifiable data. There are a number of official organisations responsible for regulating UWB and the General Data Protection Regulation (GDPR) for data collection and data usage which over time, has effectively removed a common user from the negotiation process. The GDPR was instated within the European Union to give citizens control over their data and ensuring transparency/accounting of organisations that collect their data. However, extensive privacy policies effectively make the user either agree to a 90 page document or forego their right to use a particular service. Many organisations or applications make use of third parties to process the data provided by users. While this may have been approved for collection to the main service provider, the third party also gets information, processes it and forms insights. This cross organisation information sharing essentially shows the lack of control citizens have over data and why this is an important privacy paradigm.

2.3. Interviewee selection

2.3.1. Expert Interviews

For the research, three main stakeholder groups were selected to gain a comprehensive overview of the technology and any risks it may bring up: privacy researchers, regulators and technology experts. Mobile phone companies seem to be an obvious stakeholder group that is missing in this data set, however online research has shown that they have always refused to comment on the applicability of UWB within their phones. They have also repeatedly stated that the use cases would try to maintain the privacy and location data of customers but their reputation with similar technology in the past, shows a different perspective. Stakeholder groups with knowledge on the topic were chosen and not groups that needed to be briefed on the concept of UWB. Technology experts further help highlight if there are more use cases of UWB that have not been mentioned by mobile phone companies. Independent researchers from technical institutions or privacy researchers were considered very important as their non-affiliation to mobile companies was a priority. The inclusion of relevant regulators is done to check if they are technically sound about newer technology and if proactive steps are being taken to ensure protection of civilian data. The different stakeholder groups help provide different perspectives and directions of consideration, whether it be technical, regulatory or economically. Finally, these different stakeholder groups were chosen to see if the privacy concerns across them would be similar or if there is a major difference in what they deem important when it comes to UWB technology.

The interviewees were acquired in two ways. In consultation with the supervisor for this research, the first set of privacy researchers and technology experts were enlisted. Secondly, the data protection authorities and privacy regulators within Europe were contacted through obtaining their information from the internet. This first network was asked if there were any additional relevant people that could be contacted from within their organisation or any acquaintances with relevant prior knowledge. This ensures that there was a diverse group of interviewees from all the relevant stakeholder groups. In total, six interviewees were interviewed for the research. The main criteria for selection was to ensure that the expert is currently working or conducting research on UWB. They would serve as the initial knowledge base for privacy concerns related to UWB. The interviewees were first sent an information sheet and a consent form which gave the researcher the permission to record the interview for any use in the research. This ensured that the research followed official GDPR guidelines and ethical guidelines of TU Delft (explained in detail in the appendix) and that interviewees knew

their position within the context of research. The time limit was informed in advance which varied between 45-60 minutes depending on the interviewee.

The interviews were conducted in an open-ended manner. The relevant background of the interviewee was taken into account. Questions were then adjusted and if the interviewee wanted to explore/ explain a certain issue with respect to UWB, questions were tailored so that the interviewee answered questions relevant to their knowledge domain. The results are extensively presented in chapter 6.

2.3.2. User Interviews

The users to be included in the research were obtained from technical backgrounds. The research was conducted in University of Technology Delft and the interviewees are also from the same institution. A broad diversity of interviewees from different faculties were sought to gain a varied overview on the privacy concerns that the public can see. It can be seen that the interviewees are all well educated, highly scientific individuals. This may, however, not be representative of the entire population. The interviewees have no business relation with any of the stakeholders responsible for UWB technology. But they have prior information on Wi-Fi, BLE and how location information is collected. This makes it easier for them to understand how UWB works and what technical gap it aims to cover. The interviewees have been selected from different faculties of the university which include management, computer science, policy analysis, electrical engineering, etc. These help provide a wide perspective of the possible issues. Some may see very surface level issues, whereas others may provide detailed insights.

The interviewees were acquired in different ways. Initially, the researcher's personal network was contacted to see if there were students willing to give their inputs. An announcement was also made on the student's notification board to obtain interested students. Secondly, the snowballing method was utilised where the network of the first students invited their friends to be included in the research. In total ten students were interviewed. The interviews were assured that their personal information would not be included in the research and for that reason, they are referred to as P1 to P10 in chapter 7. The number of interviews were conducted to reach the point of saturation until no new insights or answers were obtained. This helped conduct the analysis in a complete manner while taking into account all the possible issues that were apparent.

The interviews were conducted in a semi-structured way. All users were asked the same set of questions and if they presented something that needs more explanation, questions were slightly adjusted. This approach gives the respondent the ability to share his view without having to answer very objective questions. The goal is to get subjective answers so that their concerns could be highlighted. Prior to the interview, the interviewee was asked to fill in a questionnaire to get their basic information, contact details and area of study. After this, they were given a consent form that was GDPR compliant allowing the researcher to audio record them. A background information sheet was also provided explaining the basic information needed about UWB and its potential use cases. These helped the interviewees theoreticize some potential concerns prior the interview. The interviews lasted 20-35 minutes each.

2.4. Thematic analysis

The use of thematic analysis (TA) helps understand core differences, similarities and priorities between statements made by interviews (Nowell et al., 2017). It is a qualitative research process which is increasingly recognised nowadays. It is used for data analysis in this research to characterise similarities, differences and opinions of users within the context of privacy concerns. This helps highlight main points of interest of users that may present the most pressing issues. It also helps quantify the number of people that consider the same issues and how many have different opinions. A severe limitation of TA is that on increasing the number of participants, it becomes difficult to visualise the entire data set (Nowell et al., 2017). This thesis aims to use a circular method of visualisation for the statements made by interviewees. Elucidated below are the list of advantages and disadvantages of thematic analysis within the context of data collection for the thesis:

Advantages (Nowell et al., 2017):

1. Thematic analysis helps provide a very flexible approach that can be modified for the research in question, but still providing rich, detailed and complex bits of data. This includes providing far-reaching statements made by interviewees or even common ones.
2. Thematic analysis is a useful tool to examine perspectives and statements from different research participants, thereby generating unanticipated insights. There are some statements made by only one

individual. TA helps highlight this while quantifying the number of users that have the same opinion.

3. It helps summarize and structure key findings across data sets or statements, as it helps the researcher form a well-structured approach within different 'themes' in order to produce an organized final report. Since the concept of the three paradigms are used, TA helps structure the analysis into these three themes (or paradigms). It essentially eases the process of choosing themes amongst the various statements made by participants.

Disadvantages (Nowell et al., 2017):

1. There is a lack of substantial literature on thematic analysis as compared to other qualitative technological methods such as grounded theory and phenomenology, which may cause first time researchers unsure on how to conduct a rigorous analysis. The TA analysis used in this thesis went through an iterative process of first breaking down statements into actual themes and thereby then presenting them in the easiest way possible.
2. There are a number of themes that can be formed within a context of a single research. It comes down to the researcher to formulate their own themes and align the information gathered into these different groups. Thematic analysis does not have a certain criteria to help the distinction for groups.

Nowell et al., 2017 admits to the usage of TA in various aspects of technology management or assessment. This includes in the commercialization and adoption of any new technology. It helps support the strategies of a company which can then be traced to market requirements. Fittingly, this thesis uses TA to understand the perspectives of users and provide a starting point in theory (and industry) of privacy concerns to help the scientific community.

In order to adhere to the structure of TA, the interviews need to be processed and analysed. Processing includes interviews being recorded and then transcribed. From the transcripts, the data is structured by making use of the Atlas.ti software. Structuring helps highlight the most important statements made by different interviewees and possibly forming links between them. As users were all asked the same questions, the analysis was conducted uniformly. This was done in a step-wise process. In the first step, the most relevant parts of the interview are highlighted within each interviewee's transcript. Next, the answers are compared across interviewees to see if they share the same concerns or have differing views. This helps in the cognitive mapping of concerns within the three paradigms. If viewpoints are similar across participants, the participant 'bubble' is connected to the similar statement. This helps understand, highlight and report the different privacy concerns. The most referenced issues will have multiple participant bubbles connected to them, which may be representative of how the respondents view UWB. The presence of outliers with differing viewpoints is also very indicative. It helps present inconspicuous privacy issues of UWB that regular users may not see. Finally, these similarities and differences is used as input for visualisation on Gephi software.

3

Technology and Regulatory Specifications

This chapter introduces the technological perspective of the research which is UWB. In order for the reader to gain an understanding, the basic technological capabilities of UWB are introduced and how it differs from similar wireless technology. The last section of the chapter elaborates on the regulatory bodies in charge for radio technology in the European Union.

3.1. Ultra-Wideband Technology

Ultra-wideband wireless communication has become a revolutionary and novel way for transmitting large amounts of digital data over a wide frequency. UWB commonly refers to a signal that has either one of two: large relative bandwidth (BW) that exceeds 20% or a large absolute bandwidth of more than 500 Mhz (Kshetri-mayum, 2009). This allows for the transmission of a large amount of signal energy without interfering with conventional narrow-band and carrier wave transmission within the same frequency range. Thus, pulse-based systems where each transmitted pulse occupies the UWB bandwidth can access the UWB spectrum under the two aforementioned rules.

The precursor of UWB was referred to as a impulse and carrier-free technology. The US Department of Defense was the first to coin it 'ultra-wideband' (Alarifi et al., 2016) after which it was widely used. Recently, UWB has emerged to the forefront with great promise to satisfy a growing demand for low-cost, high data rate and short wireless range transmission (Zin and Hope, 2010). As mentioned before, it does this over a large portion of the radio spectrum. This means that is is able to operate as short range communication - like WiFi and Bluetooth - through radio waves.

The first basic concept of UWB is that frequency is relatively meaningless. UWB uses electromagnetic pulses and not short wave packets. These electromagnetic pulses could be declared as pulses repetition frequency (PRF). PRF is typically in the range of 1 to 50 MHz. However, with the pulse being rather narrow, in the order of hundreds of picoseconds, the spectrum widens up to a few gigahertz often without a clear peak. (Staderini, n.d.)

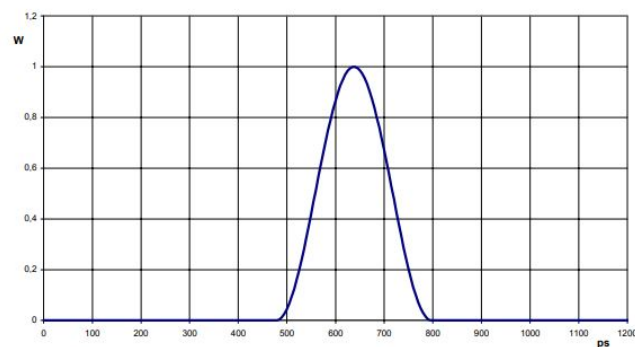


Figure 3.1: A sinusoidally shaped UWB pulse

The second basic concept of UWB communications which shows that they are fundamentally different from all other communication techniques, is that they use extremely narrow radio frequency pulses to communicate between transmitters and receivers. Utilizing short-duration pulses as the main constituent for communications pushes UWB to operate over a wide frequency. (Kshetrimayum, 2009)

A major difference between regular radio transmitters and UWB is that the former transmits information by varying power levels, frequency and/ or phase of a sinusoidal wave. UWB systems transmit information by generating radio energy at specific time intervals and simultaneously, occupying a large bandwidth, thus enabling pulse-position or time modulation. This means that UWB pulses can be sent sporadically at low pulse rates to support time or position modulation but can also be at rates up to the inverse of UWB pulse bandwidth. These pulse systems have been defined as channel pulse rates higher than 1.3 gigapulses per second (Kshetrimayum, 2009).

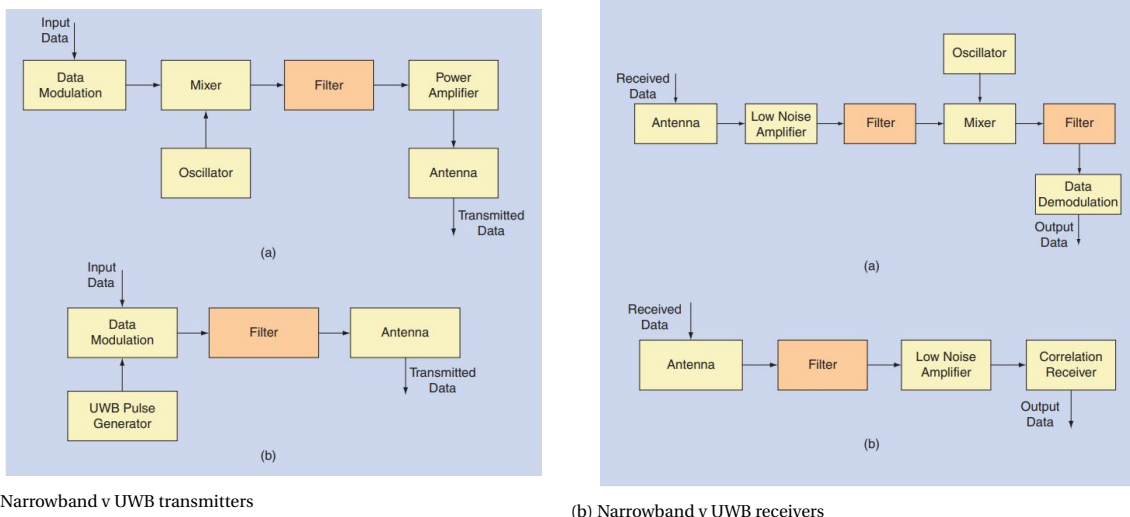


Figure 3.2: Difference between narrowband and UWB transceivers (Kshetrimayum, 2009)

As seen from the images, the UWB transmitter and receiver designs are considerably less complicated than those of other transceivers. The transmission of low-powered pulses reduce the need for power amplifiers in the UWB set-up. Additionally, since UWB transmission is carrier-less or does not need modulation, there are no oscillators and mixers to convert carrier frequency to the required frequency band. This also means that the reverse process will not need to be done at the receiver side of the signal.

Additionally, a third advantage of UWB is its multi-band capabilities. This means that in multi-band UWB systems, instead of using the entire 7.5 Ghz as a single band of propagation, it can be divided into multiple sub-bands of 500Mhz or more. This helps divide the communication channel in different paths, where people can avoid sending signals in those frequency regions where a radio communication device is already operating. However, using a multi-band UWB system involves sophisticated signal processing techniques and transceiver design which is much more complicated than shown in the two figures above. (Kshetrimayum, 2009) Given below are the main advantages and disadvantages of UWB technology.

Advantages (Kshetrimayum, 2009)

1. **High data rate and low power** - UWB systems have a high data rate for low signal to noise ratios, even in noisy environments. Due to the simpler transceiver architecture as compared to its counterparts, UWB devices make use of extremely low energy to transmit data or signals.
2. **Very low power secure communications** - The Federal Communications Commission specifies the use of Effective Isotropic Radiated Power (EIRP) for frequency transmission in UWB devices as it is defined as the highest signal strength measured in any direction. It helps limit lower than the noise floor level of -41.3 dBm/Mhz which allows UWB systems to coexist with other devices in the same frequency region. This low emission of UWB leads to higher communications security by reducing the probability of signal detection and jamming.

3. **Low cost and minimal hardware** - UWB is known to transmit short impulses at specific time intervals rather than continuously transmitting modulated waves. As mentioned above, they do not require oscillators, mixers or other filters, thereby reducing the cost of the entire device.
4. **Multiple access communications** - UWB-based multiple access communication is capable of handling many users at the same time. Direct sequence communication is one such technique where the transmitter information symbol is spread with a pseudo random sequence which the receiver needs to despread to understand the information. This does not have an upper limit meaning various users can gather this pseudo random sequence for final communication.
5. **Resolvable multipath components** - UWB pulses are short in space which comes up to about 60 cm for a 500 MHz pulse. This means that most signal reflections do not overlap with the original pulse and thus the problem of multipath fading in narrow-band transmissions does not exist. Since the transmissions are easily resolvable in UWB emissions, this makes them ideal for high resolution indoor applications.

Disadvantages (Kshetrimayum, 2009)

1. **Interference** - UWB devices occupy a large portion of the frequency spectrum, there is a possibility of interference with existing devices or users. Existing devices include WLAN devices (operating at 5.150-5.825 GHz) and 2.4 GHz industrial, scientific and medical band devices which are used by personal area networks such as Bluetooth.
2. **Complex Signal processing** - For carrier-less transmitting devices, sophisticated signal processing methods are needed to recover data from noisy environment. This is because every narrowband signal in the vicinity is a potential interferer and of course, every other carrier-less device. This would mean that, in order to specify which signal you want to receive, this signal processing is crucial.
3. **Bit synchronization time** - Pulses with picoseconds precision are used in UWB, which means that the time needed for a transmitter and receiver to achieve bit synchronization could be as high as a few milliseconds. Channel acquisition time thus becomes higher which can significantly affect performance.

UWB has similar properties to Bluetooth and Wi-Fi. The functions that each carries out is not the same but on a higher level, they are all used to connect different consumer electronics technology to each other. The UWB Alliance categorically proved that UWB has taken the shortest amount of time for integration into consumer electronics compared to the other two. It took about 13-15 years for UWB bandwidth to become unlicensed and their subsequent inclusion into mobile phones or other handheld devices. This is about 2 years faster than Bluetooth and 7 years faster than Wi-Fi (Alliance, 2020). This shows that UWB is progressing at a fast rate and seems to be the future of connectivity. The global UWB market is expected to grow from 1.1 billion USD in 2020 to 2.7 billion in 2025 with a compound annual growth rate of 19.6% which is extremely high for any industry. This shows that this is an exponentially improving industry that will only attract more competition as its functionality is improved. In the last year, the market has been predominantly dominated by Decawave (US), Apple (US), 5D Robotics (US), Pulse LINK (US), BeSpoon (France), Zebra Technologies (US), NXP Semiconductors (Netherlands), Texas Instruments (US), Johanson Technology (US), Alereon (US), LitePoint (US), Fractus Antennas (Spain), Nanotron Technologies (Germany), Samsung Electronics (South Korea), Sony (Japan), Ubisense (UK), Alteros (Ohio), and Starix Technology (US). A significant amount of these companies are located in the North American region which makes it the centre for UWB research, but these companies are looking to gain ground within the European markets as well by company acquisitions or collaborations (Bridge, 2020). A major portion of the market is believed to be in the smartphone industry, views which are shared by the UWB Alliance. For this to be technically beneficial, it needs to function alongside Bluetooth and WiFi, which is the basis for the next section.

3.2. Comparison with other wireless technology

UWB operates in the almost the same frequency spectrum as Bluetooth and WiFi. This section will look at the similarities and differences of UWB with the other two and compare it on some criteria such as accuracy, power, cost, etc.

3.2.1. Bluetooth

Bluetooth is based on a wireless radio system that is usually important for short range communication to replace cables for peripherals such as earphones, mice, keyboards, printers, etc. The range for these applications is known as wireless personal area network (WPAN) (Basiri et al., 2015). In a conventional Bluetooth connection, one device serves as the master whereas one or more Bluetooth devices serve as slaves. The devices termed as slaves communicate with the master in a point-to-point fashion whereas masters communicate in either a point-to-point method or multi-point method. This allows a singular master device to connect to many at the same time (J. S. Lee et al., 2007). The low power consumption of some applications of Bluetooth allow for extended periods of several months without needing to be recharged (Basiri et al., 2015). Due to its low power and efficiency, BLE is used in various tags in indoor areas to increase the possibilities for indoor positioning solutions. Ideally, there is no upper limit on the operating range for Bluetooth but above 60m, it may become a problem (J. S. Lee et al., 2007).

3.2.2. Wireless Fidelity (Wi-Fi)

Wi-Fi includes standards for wireless local area networks (WLAN). It allows people to access the internet at broadband speed and fast connection rates when they are connected to an access point (J. S. Lee et al., 2007). The basic component of a Wi-Fi connection is a central device that other devices within a certain 'local area' can connect to. If a device leaves this area, then it can no longer communicate with other members in that area over the local network. There is a massive infrastructure created to make Wi-Fi globally available as a majority of smaller devices need Wi-Fi to function effectively (J. S. Lee et al., 2007). However, the issues with Wi-Fi are its channel effects such as multipath and shadowing which can severely affect signal strength if a user is trying to connect a device to the network (Basiri et al., 2015). This shows that estimated position error is found to be of a few metres as strength of the connection reduces.

UWB will first be compared to these wireless technologies over four technical characteristics such as radio channels, coexistence mechanism, transmission time and security protocol. Secondly, it will be compared across five functional characteristics that include accuracy, cost, availability, price and privacy.

3.2.3. Technical characteristics comparison

1. **Radio channels** - Bluetooth and Wi-Fi have spread spectrum techniques in the 2.4 GHz range. This is more generally known as the industrial, scientific and medical band and is unlicensed in most countries. Bluetooth has the capabilities of 79 channels whereas Wi-Fi uses about 14 RF channels. UWB, on the other hand, uses the 3.1-10.6 GHz specified range, at least in phones. (J. S. Lee et al., 2007)
2. **Coexistence Mechanism** - Bluetooth and UWB devices avoid collision by providing adaptive frequency hopping. Depending on any interference within the channel, the device will choose a freer one to communicate through. Wi-Fi uses dynamic frequency selection. Usually, the entire spectrum is allowed for Wi-Fi communication except for a few bands which are used for radar and military applications. These are licensed or disallowed in a number of countries. To ensure there is no interference, 60 seconds or so must be spent listening to the channel to see if it is free and indeed usable. (J. S. Lee et al., 2007)
3. **Transmission Time** - Transmission time depends on a number of factors including data rate, size of the message and the distance between the two communicating devices. If all of these are kept constant for all three wireless technologies, Bluetooth has a maximum data rate of 0.72 Mbits/s, UWB of 110 Mbits/s and Wi-Fi of 54 Mbits/s. Additionally, UWB takes the least amount of transmission time, with Wi-Fi being marginally slower and Bluetooth taking almost double the amount of time as Wi-Fi.
4. **Security** - All three technologies have relatively comparable encryption and authentication mechanisms. (J. S. Lee et al., 2007)

3.2.4. Functionality comparison

Basiri et al., 2015 uses an analytical hierarchy process (AHP) to compare these technologies. The priority of each of these factors is concluded from interviewing or surveying relevant parties which include users, manufacturers, policy makers, etc. From this, depending on the technical protocols of all three technologies, a final technology priority matrix is made which shows the ranking of each across five functionalities (Saaty, 2005).

The results of the study conducted in Basiri et al., 2015 show that UWB ranks highest in accuracy, followed by

Bluetooth and Wi-Fi. This means that it is able to locate another communicating device quite easily. Secondly, Wi-Fi ranks highest in availability followed by Bluetooth and UWB. This is due to the fact that UWB is an upcoming technology, there aren't nearly enough communicating devices for it to be available in every single country or location. Thirdly, Bluetooth ranks the best in power consumption, followed by UWB and Wi-Fi. As previously mentioned, Bluetooth is capable of being used uncharged for several days. Fourth, UWB ranks as the costliest amongst the three. UWB is still not a widespread technology and is definitely touted to become cheaper as more manufacturers build UWB devices. Finally, UWB and Bluetooth rank equally higher than Wi-Fi under the privacy criteria.

The initial literature review conducted on UWB gives the reader a brief introduction to UWB and its functionality. The subsequent literature review conducted on incumbent radio technology is relevant in understanding the technical differences between the different types of radio technology and which technical gap UWB is trying to fulfill. It also provides a ranking system on the basis of different functional and technical characteristics which highlight the potential advantages of UWB over these pre-existing technologies. These help the researcher streamline and ask potential interviewees the right questions. Radio technology and privacy are both inexhaustible domains, which the preceding sections try to bound to certain functionalities. The next subsection looks at the regulatory bodies in charge of radio technology in the EU.

3.3. Radio technology regulatory bodies

There are two main organisations responsible for radio technology regulation: CEPT - European Conference of Postal and Telecommunications Authority and ETSI - European Telecommunications Standards Institute. The CEPT is a voluntary regulatory organisation where policy makers and regulators of 48 countries discuss policies regarding telecommunications and the radio spectrum. The CEPT has a number of working groups and project teams which conduct various technical and regulatory studies for any new radio technology that might be put on the market (CEPT website). It ensures that this new technology complies with the radio spectrum and ensures there is no interference with any incumbent technology. Main outputs from the CEPT are 'Decisions' and 'Recommendations' on major harmonization issues. These inform the Decisions of the European Commission, which are then binding on the Member States.

The CEPT formed the ETSI under the recommendation of the European Commission (EC). Its main responsibility is the standardization of Information and Communication Technologies (ICT). It is one of three bodies which is formally recognized as a European Standards Organization. These were made to support the European Commission with regulations and policies surrounding telecommunications and the radio spectrum, much like the CEPT. This means that they work together to ensure the final policies are binding, well researched, tested and only then released for public consultation (ETSI website). ETSI has more than 900 member organizations from 62 countries and 5 continents which include companies, regulators, academia, government, public bodies and even observers. This is to ensure every single perspective is taken into account to formulate all-inclusive recommendations. ETSI works alongside the CEPT in conducting technical tests and formulating recommendations for the European Commission. They also work alongside national governments or National Standards Organizations (NSO), which presents the final stakeholder responsible for conducting technical tests within each member state.

This research is being conducted within the Netherlands and the NSO in charge is the Radiocommunications Agency (RCA) (Agentschap Telecom in Dutch). They are responsible for obtaining and allocating frequency space and monitoring usage (RCA website). They ensure every company, individual and organisation within the country follows the guidelines and regulations of the European Commission based on the recommendations made by the ETSI and CEPT. Additionally, they are in charge of all wireless and radio communications within the country of Netherlands. If any organisation within the country wants to use the radio spectrum, they need to get a license for usage or ensure they adhere to all the regulations made by the EC. If any technology is found to be in violation of the directives of the EU, the RCA holds them accountable. The penalty may differ based on the violation. The different stakeholders in charge for widespread UWB usage are given in the figure below.

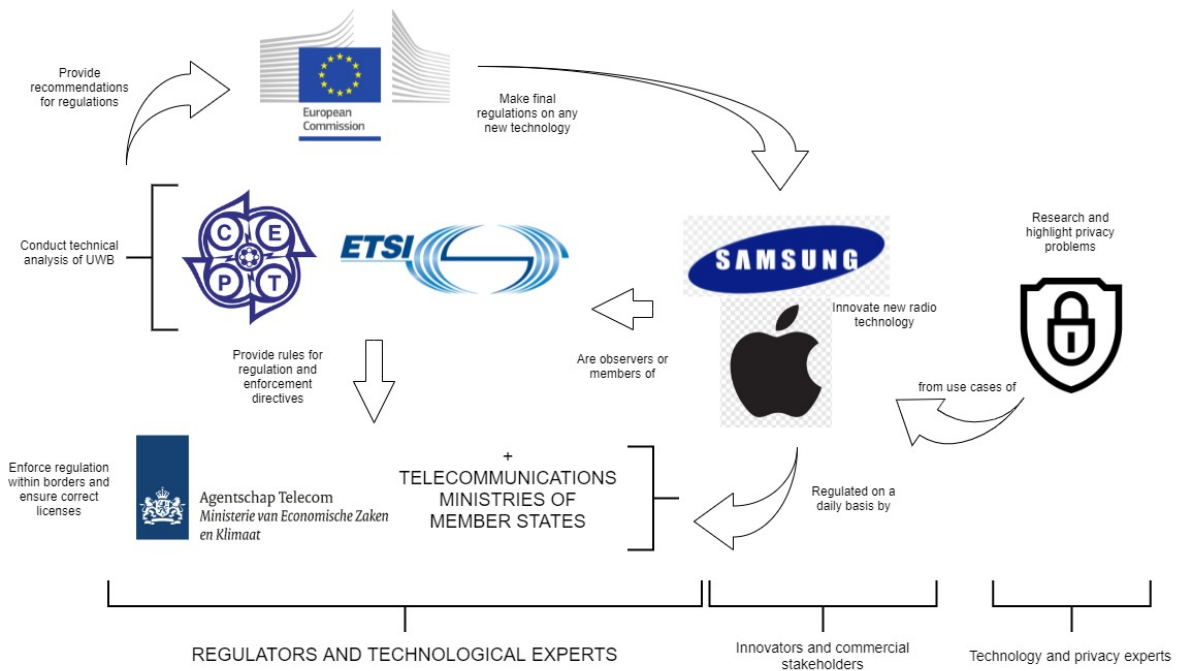


Figure 3.3: Stakeholders responsible for UWB usage

The figure shows how the different, relevant stakeholders are related to each other. In this research, the stakeholders labeled as 'Regulators and technological experts' and 'Technology and privacy experts' are interviewed. They are relevant to provide an outside and unbiased perspective to the commercial usage and potential privacy concerns of UWB. The commercial stakeholders such as Samsung, Apple, the UWB Alliance, etc are not considered because they have a business allegiance to commercial UWB usage. They need the incorporation of UWB in mobile phones, which may lead to biased statements and misaligned data. Regulators are important to provide an overview on their daily functioning and their insight in privacy issues. Privacy experts actively research new innovations and list potential privacy concerns which are unbiased and based on findings. This helps in providing a wider knowledge base for user interviews and also for any future research in the field of UWB.

4

UWB Applications

UWB was first discovered in the 20th century when G. Marconi built spark gap transmitters for transatlantic communications (Kshetrimayum, 2009). During the mid 20th century, the technology evolved considerably in the United States and was used for radar and communications applications (Fowler et al., 2017). However, this was strictly restricted to military applications till the beginning of the 21st century. This was because UWB devices operate in the same frequency range as other radio-band technology.

Eventually, the United States gave unlicensed access for UWB usage in 2002 (Fowler et al., 2017) whereas Europe allowed unregulated access in 2007 (Wilzeck et al., 2010). This was after considerable development in UWB allowed it to co-exist with other radio-band technology. In order to ensure that this remained the case, both continents decided to continue regulating parts of its widespread usage. In the United States, special rules were placed on Indoor UWB systems, handheld UWB systems, wall-penetrating radars, surveillance systems and medical imaging systems. Similarly, European regulation placed special rules for the following categories of location tracking systems, vehicular UWB devices, material sensing devices and generic UWB usage. These rules mainly governed the bandwidth requirement and emissions limit (Wilzeck et al., 2010). The former refers to the frequency range that the application-specific devices are allowed to operate in and the latter refers to the power output from a singular device (Ministry of Economic Development, 2005).

The European Commission considers devices with a minimum bandwidth of only 50 MHz as UWB devices whereas for the United States, the minimum requirement is 500 MHz (Ministry of Economic Development, 2005). Additionally, the specific time requirement for when the device occupies the minimum bandwidth has not been mentioned in the EU UWB regulation. This allows for a workaround as devices that are capable of operating above the 500 MHz requirement can usually operate below it if they choose to do so. This can go largely unnoticed if not checked regularly.

The unregulated and unlicensed use of UWB allowed a number of applications to be considered viable for research. A literature review done on research articles from the last 10 years classified different application on the basis of five different domains: medicine, localization, penetrability, connectivity and crowd-sourcing. It is important to keep in mind that these are not mutually exclusive domains and that some applications will overlap in their functionality. Given below is a table with different research articles and some details about the research.

Paper name	Application Domain	Research Application
Sen Yan et al (2018)	Medicine	Wireless body area networks (WBAN) being able to monitor health for emergency rescue services or care for children and the elderly
Fowler et al (2017)	Localization and penetrability	Terrain profiling, imaging tactical targets and foliage penetration
Feng et al (2018)	Localization and connectivity	Human and robot tracking
Zhang et al (2019)	Localization and connectivity	Locating pedestrians if their location is unknown; possibly locate vehicles that the owner may have forgotten the location of
Vishwesh & Raviraj (2018)	Connectivity and medicine	WBAN applications; imaging within the medical domain
Zhang et al (2018)	Localization	Precise positioning in a ship interior
Ullah et al (2009)	Connectivity and Medicine	WBAN applications; Connecting various multimedia devices in a wireless personal area network
Kim et al (2012)	Localization	Child-care and safety localization service for children who may be in danger
Yang et al (2018)	Crowd-sourcing and localization	Counting the number of people in a dense environment
Sadrezami et al (2019)	Penetrability and medicine	Standing, walking and fall detection for the elderly through walls
Kim (2012)	Crowd-sourcing and localization	Ability to detect/ count steps of a person and also which direction he/ she is walking in
Choi et al (2018)	Crowd-sourcing	Counting number of people walking through gates, escalators in dense environment; direction detection
Cheng et al (2017)	Localization	Gait recognition and path followed by a person within a confined space
Brilakis et al (2011)	Localization and connectivity	2D and 3D precise localization for assets, equipment and people
Mavridis et al (2015)	Localization and connectivity	Usage of a dual antenna system to locate/ count people and devices inside a building
Wu et al (2019)	Medicine	Calculation of heartbeat
Pelka and Helbruck (2020)	Localization	Locating and following moving nodes in open and closed environments
Rana et al (2019)	Localization and medicine	Usage of a singular UWB device to locate and track people within a single household
Singh et al (2011)	Penetrability	Motion/ person detection across different wall types
Cheng & Shu (2020)	Localization	Usage of four devices to locate something underwater
Pochanin et al (2016)	Penetrability	Detection of buried items and impurities in historic artwork
Kolakowski (2019)	Localization	Hybrid UWB and BLE device for map formation and low power localization
Shi et al (2020)	Crowd-sourcing and localization	Using various UWB devices within a certain known area to locate all existing nodes or devices
Lee et al (2018)	Medicine	Heart beat and respiratory characteristics detection with a UWB device

Figure 4.1: Application domains

The rest of this chapter will briefly introduce and summarise different applications mentioned in the papers.

4.1. UWB research use cases

Ullah et al., 2009 mentions the use of a wireless body area network (WBAN) to provide smart or adaptable healthcare. A WBAN has wireless biosensors and is placed on or planted in a human body. Each biosensor is capable of processing a task given to it such as respiratory measurement or heart rate monitor and communicates this information to a network coordinator (Wu et al., 2019). This coordinator then accumulates a patient's information and sends it across to the right organisation for diagnosis. The paper further states that the power consumption of a WBAN extremely minimal which forces the network coordinator (such as a computer) do most of the analysis and thus serves only as a measurement device. Since UWB devices work based on pulses, the power consumption can be kept marginal while measurement is done periodically as pulses are sent and received.

Yan et al., 2018 builds on this experiment by analysing the time behaviour of the received pulses from a UWB device for different respiration phases. The results were positive in detecting any respiratory problems while being completely contact-less. Alternatively, Y. Lee et al., 2018 designed an experiment that compares the functionality of a UWB device with electrocardiography (ECG) to measure heart rate of people. The heart rate of six volunteers and sixteen patients was recorded and compared across the data acquired from the two devices. ECG devices are currently used to record heart beat of people which means that an accurate return from the UWB sensor would be a huge breakthrough for the industry. The results showed a percentage mean error of lesser than 3%. However, a major controlled element within the experiment was to make sure subjects held their breath through the measurement process. This was done to reduce the post-processing time which would be required if respiratory effects were captured in the UWB signals.

UWB is acclaimed to be very advantageous in heart and obstetrics imaging (Vishwesh and Raviraj, 2018). For the former, a UWB transmitter emits discrete pulses towards a body and receives reflected pulses from the heart. This could be used as a radar stethoscope by showing the exact heartbeat on a nearby screen. For the latter, a similar idea is used where the pulses are emitted to and returned from a mother's womb to check

on the well-being of a child. These two applications help in reducing contact with the patient (if necessary), remote operation, increased hygiene and easier use.

Brilakis et al., 2011 mentions the use of UWB systems to track and locate certain equipment and assets within a certain area. The experiment conducted in the paper looks at using UWB devices on trucks, tractors and some basic building materials. This helps provide accurate 3D locations in real-time, thereby increasing active zone work safety. However, a major drawback is that for higher accuracy, every asset must be tagged with a UWB device. Feng et al., 2018 furthered this possibility by making use of a UWB system for human and robot tracking. The experimental setup was the usage of a UWB system on a robot to continuously track a human in real time, for any integrated function. The results proved that robot could accurately track a specific human without showing the same errors as that of vision tracking which is vulnerable to glare. Additionally, UWB devices which are soon to be incorporated within cars (Alliance, 2020) have led to the possibility of infrastructure free localization. Any device capable of locating a UWB transmission such as a mobile phone can be used to locate the exact position of a car, if the owner has forgotten where he parked it (R. Zhang et al., 2019). The research article further states that the usage of dual UWB sensors on an autonomous vehicle helps in pedestrian detection around the vehicle. Results show that pedestrians are detected immediately and help reduce the speed of autonomous vehicles when there is driver error.

Singh et al., 2011 introduces the concept of wall-penetrating applications with respect to UWB. UWB radars can use a large spectrum in combination with lower frequency, hence making them suitable for ground penetration and object detection. The research conducted in this article tries to detect basic movements of a person through four types of walls which include: wooden, gypsum, brick and thick concrete. The possibility to detect a heartbeat or breathing movements is possible for the first three wall types but not for a thick concrete wall. However, received signal amplitude is affected if a person is bent down or continuously doing some activity.

It is common for mobile operators in Korea and Seoul to provide child-care services which help locate a particular child based on their GPS location, in case they are in danger (Kim et al., 2012). The research article introduces a model where the UWB device in the possession of the child is linked to location provider service such as Google Maps. In case there is some reason to suspect that the child is in danger, the end users can contact the mobile operators to provide a location of the child. Since, UWB provides location within 10 cm of the device in outdoor environments (Colmer, 2019), this makes it a very accurate option as compared to BLE or Global Positioning System (GPS).

Schindhelm, 2012 hints at the possibility of using UWB devices for activity recognition and step detection. The paper mentions the use of multiple sensors within a closed environment such as library or a train station. Once a person's initial position is located, all subsequent positions can be calculated through a plethora of sensors on a smartphone such as compasses, accelerometers, gyroscopes, etc which are combined to provide maximum functionality. Additionally, the steps taken in a direction can be measured and consequently, the path can be tracked.

Sadrezami et al., 2019 builds on this application domain by utilising UWB devices for activity detection in a room but mainly focused on fall detection for the elderly. A UWB sensor was placed 1.5m high in a room and sends periodic pulses every 15 seconds within the room and immediately digitized on a computer. The subjects in the experiment were asked to stand, lie down and fall over. The data received from these actions were fed into a convolutional neural network (CNN) to teach an AI how to differentiate different activities. The eventual classification was accurate to make distinctions between different body movement and applicable for the elderly who didn't want to move to an old-age home but still required medical assistance.

UWB radars can be used to count the number of people in a dense environment (Yang et al., 2018). Research shows that it can be done by using a single UWB device to capture the number of people within certain degrees or curvature. The number of people within that space is known to the researcher and compared with the final output after regular pulses are transmitted and received. The overall accuracy reaches up to 97%, which shows that UWB devices are viable options for dense environment counting without the use of physical architecture such as doors and gates. Choi et al., 2018 further elaborate on this research by placing UWB transceivers in one subway station in Seoul. The number of people passing through escalators or elevators were counted through UWB sensors for various time periods within a week. Consequently, the number of people actually using these amenities were manually counted for comparison. The results of the experiment showed that the errors obtained were lesser than 10%. It is also effective of being used in instances of fire, smokey and light-less conditions.

Furthermore, UWB devices have the capabilities of connecting several devices in a smart environment (Mavridis et al., 2015). The cited research articles makes use of a dual antenna system to reduce the noise in the environment while focusing the energy in multiple directions, thereby increasing the area of connectable devices. This connectivity increase allows all devices in the area to improve data transfer rates and improve wireless connectivity, which subsequently reduces the need for cables in a living room setting. This allows for information sharing in a wider area such as business meetings, without having to share the data with each person individually.

Pochanin et al., 2016 introduces and highlights UWB's capability for ground and wall penetration. This is being employed in humanitarian efforts of detecting Improvised explosive devices (IEDs) in the Donetsk and Luhansk regions, which are post-conflict areas. This is done by equipping a miniature robot with a UWB device, which is connected to a controller. The robot, on finding any hidden IEDs will notify the controller and they can then disarm them. Fowler et al., 2017 mentions a crucial military application of foliage penetration. By sending out pulses in an open environment, any tactical targets hidden behind shrubs, trees or camouflaged can be picked up by the receiver to provide their exact locations. Additionally, UWB's tetrahertz imaging can help detect the internal structure of paintings or mosaics that have cultural significance (Pochanin et al., 2016). This provides in-depth information about highly absorptive organic compound which cannot be visualized in other parts of the electromagnetic spectrum.

It is known fact that about 80-90% human activities occur indoors (Chen et al., 2017). Which means that there is high possibility of commercial value for indoor location information of crowds. The experimental setup mentioned in the research article uses a combination of inertial sensors and UWB transceivers. This was tested on a person who was made to walk on a predetermined course and the results showed that the average accuracy of positioning can reach 10-15 cm in static and dynamic conditions.

Furthermore, K. Zhang et al., 2018 introduces the concept of indoor positioning within an enclosed space such as a ship or submarine. This is done by using anchors or nodes in a network whose location is known. Pulses sent out from a UWB device help triangulate the position of any person in the vicinity of the anchor node without needed to actively find the position of a person. Additionally, the time difference taken for the outgoing signal to be received help map out a general floor plan of the ship and exact position of any individual or object.

Rana et al., 2019 took this one step further by using a singular UWB device in a four-room ground floor apartment, for home monitoring. The monostatic UWB device was placed in one of the extremities so that the pulses could be sent outwards through all the other rooms. The experimental setup was connected via an Internet of things (IoT) platform from where information could be sent to a server. From the server, the signal data could be analysed for pattern analysis. Different body movements such as fluffing pillows, opening the refrigerator door, walking, lying down, etc were recorded and saved for analysis. After the pulses generated by the UWB device were received and compared to the time stamp of the aforementioned activities, a timeline of activities was made. If those body movements were repeated a second time, the computer instantly knew what the action was. Some issues occurred beyond 10m coverage as this was the specified possibility for the UWB device but it could be improved with better antennas for signal transmission. The experiment resulted in a 90% testing accuracy in a real-time scenario.

The biggest advantages of UWB are location accuracy and monitoring as seen from the infrastructure-free localization and indoor positioning experiments mentioned briefly above. Pelka and Hellbruck, 2016 uses two characteristics of UWB devices to accurately locate and track other devices based on the timestamp of messages. The first is two way ranging which refers to two way communication needed and the second is time distance of arrival which is the phenomenon of calculating distance based on the time difference of messages received. For the experimental setup, three anchor nodes were used whose locations were known and recorded. A fourth node which is called a tag, was to be located. The usage of two way metering by consistent pulses or messages was used to initially locate the location and movement path of the tag. The time distance of arrival method helps improve the accuracy through each anchor node recording the absolute time of the received pulse and time difference to the other anchors. This accuracy of this experiment was approximately 1 metre. This system works efficiently for underwater localization as well (Cheng et al., 2020).

Building on this experiment, Kolakowski, 2019 introduces the integration of a UWB and BLE device for localization purposes. The proposed application is infrastructure free but crowd-sourced where multiple anchor nodes are used for the purpose. Initially, the integrated UWB and BLE device on people are used to mark their approximate location within a known area such as a building. The device transmits both BLE and UWB packets concurrently. The marked points are then sent to the system server to understand the topography of

the building and where every individual is. After a basic map was created, the devices turned off the UWB capability and worked only on BLE packets. The entire system showed considerable accuracy in tracking user movements with a trajectory error of less than 65 cm. For the entirety of the experiment, four anchor nodes were used to initially locate the people. Additionally, Shi et al., 2020 mentions that if additional devices were added to the system, their location could also be obtained without considerable difficulty. The new devices added to the infrastructure would communicate with the existing ones to provide an approximate location on an arc around the existing devices. Thus, the crowd-sourcing capabilities of UWB devices are tested, where only a small number of UWB anchors are required to provide accurate positioning.

As shown above, a significant amount of research conducted on UWB applications is based on location accuracy and monitoring. Based on this applicability, parallels can be drawn across the functionality of UWB and BLE with respect to accurate localization (Colmer, 2019). However, UWB is the far superior technology in this regard as it can provide accurate location with the error of centimetres compared to BLE which provides an error up to 10 metres or so (Gezici et al., 2005). Both of them are affected by obstacles however, UWB significantly outperforms BLE, where the former gives a 1% error and the latter gives a 500% error (Colmer, 2019). UWB devices are also capable of transmitting data at a speed of over 20 Mbps which is touted to increase over time. This data transfer rate sufficiently enhances all the applications mentioned in this chapter.

4.2. Mobile phone companies use cases

As of 2019, UWB has been added to mobile phones such as the iPhone 11 from Apple and various flagship phone models of Samsung (Shi et al., 2020). Apple has included the MKA75 Ultra Wideband chip which is manufactured in-house compared to Samsung using a third party NXP's SR100T chipset. Both these chips have integrated functionality of UWB and near field communication (NFC). They have a range of 80-100 metres for transmitting and receiving pulses/ messages from other UWB devices. Apple has stated that its UWB-equipped devices are capable of only communicating with fellow Apple devices but with the UWB standardization wave that is estimated in the near future, it will be able to make further connections (Shankland, 2021). Apple's incorporation of UWB is on the back of the UWB Alliance's agenda for unlicensed and unregulated UWB proliferation (Alliance, 2020). This sections looks at the business case from the mobile phone companies' perspectives.

Apple and Samsung have both stated that UWB technology provides unprotected accuracy for both line-of-sight and non-line-of-sight localisation which include crowded environments through walls, people and other obstacles (Evans, 2021; Clark, 2020). Additionally, with the use its angle-of-arrival characteristic to indicate the direction of a signal helps locate and identify objects at centimetre level. This works by one device sending a packet of data to a second device and it then reciprocating the response. The times of transmission and receiving are then recorded. The first device then sends a third packet which includes the device ID, timestamps for the first two packets of data. These three packets are then capable of determining the accurate location of both devices (Owen, 2020).

Apple has stated that the reason for including a UWB chip in it's phone is strictly "spatial awareness" which helps your phone precisely locate other mobile phones portraying the image of a GPS at the scale of your living room. The Apple website states that this enables faster localization and sharing files through the usage of AirDrop. AirDrop is a proprietary ad-hoc service which allows sharing of files across all Apple devices without the use of emails or mass storage devices. Literature research suggested that there a few additional services that will be introduced by mobile phone companies in the near future.

The first major application that Apple is looking at, is CarKey. Being a member of the Car Connectivity Consortium (CCC), Apple plans on using UWB to help open car doors as a user approaches them (Evans, 2021). By extension, they expect this model to extend towards any other gates or needs that need authorization to open. Right now, for authorization, Apple products need the iPhone to be moved closer to the sensor to be detected but UWB helps speed up the process dramatically.

Apple has also filed a patent for a smart home system that can configure itself. It is inherently tough for different smart components such as televisions, smart light switches, etc to be connected seamlessly together due to differing wireless protocols and connector types (Peters, 2020). This smart home system would detect a new smart device in the vicinity and automatically add it to your iPhone home screen. Additionally, with the use of the UWB, the system could detect other units around a house to auto-generate a floor plan and detect regular objects like a furniture table to know their exact location. This integrated system would make use of the iPhone's time-of-flight camera and UWB sensors to get 3D depth data or the room and help connect all

the devices together. This system is capable of knowing when you are walking around your house (Evans, 2021). Consequently, Apple has patented their iBeacon technology for UWB transceivers, shifting over from BLE technology (Purcher, 2019). In addition to increasing the functionality of the applications mentioned above, UWB is better suited than BLE technology to accurately map out geographic locations in an indoor environment. This allows newer models of the iPhone to communicate with other users, items in a store, pet leashes and entry transponder devices seamlessly.

Apple has looked into the development of some non-iPhone UWB usage with the introduction of AirTags. These are devices that resemble a bottle cap and can be connected to anything a person considers valuable, which include briefcases, laptop bags, etc. The idea is that the AirTag will repeatedly ping out using UWB which can be picked up nearby iPhones (Owen, 2020). To locate the missing items, AirTags would be able to provide location with Augmented Reality (guidance). In the case it is in a floor above or below you, UWB devices would be able to measure distances and not just measure signal strength as done for BLE devices. AirTags could be used in big retail stores to provide directions to various departments, current sale items or emergency exits to customers (Truly, 2020). It could be used in tourism industries by helping tourists locate points of interest such as historical sites, museums, restaurants, etc. Additionally, UWB is being considered to unlock personal computers by merely approaching them (Truly, 2020). They wouldn't require passwords or any additional information if the person without a specific tag did not approach them. Recently, Apple announced that it would allow third-party finding experiences. This allows companies such as Belkin and VanMoof integrate their technology to allow Apple users to track their products which include electric bikes, earphones, etc (AppleUpdate, 2021). This has forwarded the timeline now providing location information to third parties, as well.

The idea of location, proximity and connectivity ties in quite well with Apple's concept of AppClips. AppClips allows users to partially use sections of an app without actually downloading it (Evans, 2021). This could be used for renting out scooters/ electric bikes or for non-contact shopping which allows pay and collect. The concept fits adheres to tourists who want to quickly sight-see but may not want to download all the local applications for their journey.

Three patents filed by Apple all regarding location accuracy were found with dates ranging from 2007 to 2017 (Forbes, 2019). These include something termed as 'time instant reference' which allows UWB devices to use pulses to improve ranging accuracy. This improves the possibility of timestamp localization. Another concept of 'beacon triggering processes' states that a singular beacon can be set up in a room for communication. It consistently tries to communicate with mobile devices in its immediate range. This may be for transaction purposes or merely broadcasting messages. On receiving a message which may include questions such as 'Where can I find t-shirts' or 'I need help from an employee,' these beacons can help shoppers or merely direct people to areas of interest. Given below is an image with an overview of all the applications Apple has in mind for the near future.

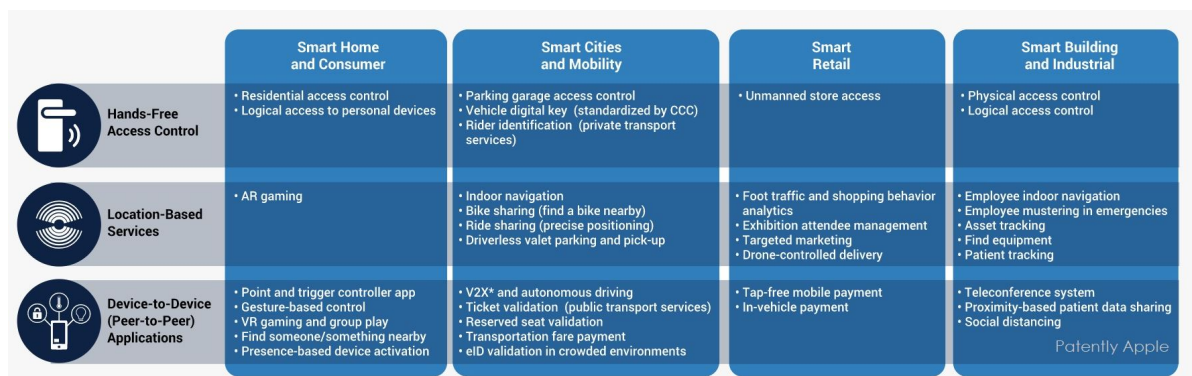


Figure 4.2: Use cases for Apple's UWB devices (Evans, 2021)

4.3. Discussion

The biggest similarity between applications from literature and use cases of mobile phones is the overlap of three domains: localization, crowdsourced and connectivity (peer-to-peer). While the actual applications are starkly different, this overlap shows that public research has a possibility of eventually reaching consumer

devices. Mobile phones equipped with UWB in the future, may have the possibility to increase health applications such as heartbeat or fall detection.

Indoor navigation and localization is a major domain that is showing promise. While this may not be completely effective in current generation mobile phones, research has shown that the accuracy is there and will become better as similar phones becomes widespread. It is just a matter of time before infrastructure localization of cars, people, shops and interest points becomes common. It further goes to show, just from cross-referencing applications, that the ability to measure location with centimetre-level accuracy is the biggest advantage. Mobile phone companies want to use it for asset tracking, equipment finding and patient localization. Literature has shown that robot and asset tracking are already big applications that have interest.

Another common and interesting application is the teleconference system. Research shows that as the number of UWB equipped devices increase, the seamless experience of entering or exiting a particular ecosystem increases. This means that a person could simultaneously enter a shop and its UWB ecosystem, thereby being given directions to potential items that interest them. Mobile use cases include the idea of shopping analytics and attendee management which shows a clear overlap. This can also include the teleconference system where if someone enters a meeting room, their mobile phone is connected to a 'host' device that sends relevant documents across.

A rather novel application from the use cases is the concept of AirTags. They are small devices with no operating system and settings that can be changed. But, they are still UWB equipped. It will be interesting to see how these devices weave themselves into the mobile ecosystem and operate as merely location providers to mobile phone companies. While they are operated by the owner of an AirTag, the possible third-party information that can be gathered seems like an endless list.

A glaring similarity between the two sections is that none of the articles referenced have considered privacy concerns. These are all applications researched with results posted. As previously mentioned, there is a big knowledge gap when it comes to juxtaposing UWB applications to privacy. Subsequent chapters aim to do that as comprehensively as possible.

The biggest similarity is the overarching idea that the number of potential applications, both from research and mobile phone companies, will keep increasing. The boundaries have not been defined yet. Figures 4.1 and 4.2 aim to highlight as many applications as possible but as the regulated UWB power in mobile phones increase, the applications may also exponentially increase. While this may seem advantageous, the potential privacy concerns may also increase. This thesis aims to get ahead of the curve but it is set in the current regulatory context of UWB and as it evolves, applications and privacy issues alike will increase.

It will be wise to note that the applications mentioned in research papers alone have UWB devices of different frequency ranges, even higher than the generic UWB bandwidth of 3-9 GHz. The use cases of mobiles are only possible within the generic UWB usage bandwidth. There is a chance that the higher frequency applications are partially possible on mobile phones. The interviews with experts will help highlight the actual possibility.

5

Privacy and radio technology

From academic research and phone companies use cases, it is easy to recognise that the potential for UWB is significant. It also shows us that UWB in mobile phones is privacy neglecting. Xia and McKernan, 2020 mentions that it is quite characteristic of researchers and innovators alike, to forget about the issues of privacy new technology may bring. In order to conduct a suitable technology assessment from a privacy perspective, the three privacy paradigms structure will be followed.

In the next section, the use cases of UWB will be categorised into two main domains. In section 5.2, these domains are cross referenced across the three different privacy perspectives mentioned in Gurses and Diaz, 2013 to inform the reader what potential privacy concerns are present. It formulates a structure to fully comprehend and analyse data obtained from interviews.

5.1. Potential privacy issues of UWB integration in mobile phones

Initially, when the iPhone 11 was released, Krebs, 2019 stated that the location tracking icon would show up on the top right of your mobile screen, even when all location services were turned off. This went against Apple's privacy policy which stated that a user can turn off all location monitoring services by deselecting the location services option in the settings menu. On questioning Apple why this icon remained, they gave two reasons: first, that this icon remained for some services that did not have a switch within the settings option (Krebs, 2019) which is gross customer misinformation; second, that UWB is not licensed for use in some countries (which is approximately 5 out of all the countries in the world) (Apple website). Apple have subsequently stated that they would add an off switch for the UWB functionality and have finally done it (Krebs, 2019). However, there are some privacy concerns that arise because of this. If indeed, there are some countries that do not license UWB usage, what is to stop users from turning them on within the geographical borders of that country and how will Apple handle that? Additionally, Josephson, 2019 state that the UWB technology within phones could function very similar to how phones use Wi-Fi. Wi-Fi tracking is possible even if a device is not associated with a network because Wi-Fi chips periodically send out packets to discover the available networks nearby. This would enable more periodic and accurate tracking of devices.

From different use cases shown by researchers and mobile phones companies, these can be divided into two main categories: 1. UWB as a personal device and 2. UWB as an infrastructure. Given below are the applications of UWB within these domains and what additional information UWB gives as opposed to BLE and Wi-Fi.

1. UWB as a personal device - Research shows that there are two main applications when talking about UWB used for personal reasons. The first is the connection of WBAN devices to help with affordable healthcare. With the use of UWB, the ability to synchronise your WBAN, which are UWB chips that can be placed or underneath your skin, is easier and helps provide live-data at all times. This can be used for heartbeat monitoring, breathing analysis, or remote care for the elderly. However, the UWB device would not operate by itself and would need to be connected to a smartphone or personal computer. Nowadays, there are a number of applications developed for providing and analysing health related data. The integration of UWB makes it easier to calculate required information, however, the same information could be gathered by a third-party. It is not new that various companies hire third parties

to analyse customer data to help provide personalised tips and suggestions to customers (Karim, 2004). The second application is related to locating and unlocking personal belongings such as laptops or cars. Mobile phone companies state that UWB pings will be able to successfully locate someone that you want to transmit data or merely locate something you have misplaced. The drawback is the fact that any other person with a UWB equipped device may be able to infiltrate this ecosystem.

Personal use cases of UWB also include connecting and data transfer between smart components in a room. It is a well-known property of BLE connections cutting out when there is an interruption in the signal, something UWB is touted to overcome. Additionally, the possibility of forming a 3D image of the room and efficiently locating each smart component is a unique selling point. This would mean that anyone who enters the room with such a device can be added into this connectivity 'bubble' or see all the available devices. Martin et al., 2019 has shown that the connectivity of different BLE devices is powered by a concept known as 'continuity.' The author states that this continued continuity leads to leaking of sensitive information which can be tracked by an onlooker. UWB connection are less affected by walls than BLE or WiFi which means the signals could be detected across them, further increasing the chances of information leakage. This essentially amplifies the concerns of UWB versus other incumbent radio technology. This must be taken into account when Apple decides to introduce this technology on a large scale.

2. UWB as an infrastructure - The main application Apple indicates is that UWB operates as a radar and provides 'spatial awareness' to the user. This presents a number of applications as mentioned in the previous chapter which include dense people counting, number of people within a room, localization of unknown nodes, etc. This seems to operate similarly to Wi-Fi and BLE as every mobile phone with UWB capabilities can scan for nearby devices. Further post processing of signals could reveal higher level information such as where people without UWB devices are located or the orientation of a room. However, the scanning capability for mobile phones is done by governments for natural disaster detection and communication. While this seems like a major advantage, there are some privacy concerns which rise. If UWB infrastructure is installed within a public building, the number of people that regularly visit the same place can be recorded. Additionally, their patterns of movement over time can be recorded thereby enabling the ability to profile the person. This is all possible with centimetre level accuracy if UWB operates similar to WiFi. Finally, UWB capability on mobile phones would present a bigger threat if they operate the same way as a radar with signals that only need post-processing. This would mean that people with malicious intent can operate similar to UWB devices mentioned in academic experiments by using multiple phones in a public space.

More importantly, the possibility of proliferation of UWB devices in the near future, is imminent. It essentially seems like an infrastructure is being introduced where every UWB device would be part of a network. This may put the user in a position where he might not have any power. This would allow for more devices to be connected to each other but it also means that there is a possibility of more personal information being at risk. If it is incorporated into buildings such as malls or shopping stores, there is a chance for consistent localization of a person throughout the length of their visit. If it is incorporated into workplaces, consistent monitoring of employees would be quite possible. Finally, UWB is touted to be integrated into the 5G mobile network due to its high data transfer rate. This means that the user may need to keep his/ her UWB capabilities on the phone turned on at all times to get these data rates, leading to the possibility of the user being consistently tracked and/ or not giving them the choice to turn off their phone's UWB function.

There are two main inferences that can be drawn from the aforementioned domains. The first indicator is that these issues would not be a major problem if mobile phone companies or carriers securely protected data. However, Apple has had a number of allegations for storing user location data without their consent in the early parts of the 2010s. Their response was that the location information obtained on phones are private and can be only seen by the owner of the phone. Additionally, service providers such as ATT, Verizon, Sprint and T-Mobile were found guilty of selling user location to third-parties as recently as 2018 (Herbert, 2020). The second observation is that the catalyst for a majority of these applications is UWB's ability to track users' location very accurately. Mobile phone companies have termed this as advantageous for their users. Privacy issues of knowing customers' locations were initially transcribed when the global positioning system (GPS) was introduced. GPS was introduced to help map out the world, help in providing directions and direct users to important places. More location privacy issues were introduced as Wi-Fi and BLE became the norm within

mobile phones. BLE was initially introduced to inter-connect people when it comes to data transfer or sending messages. As UWB gets integrated within mobile phones alongside these incumbent technologies, the same functionalities may be possible with increased accuracy, indoors (Wang and Loui, 2009).

The discussion in the next section seeks to document the overarching privacy issues of location tracking made possible by GPS, Wi-Fi and BLE. Since UWB is a newer type of radio technology, it also allows a comparison into the potential privacy concerns that expert interviews may magnify. It provides the reader an insight into the current dynamics of privacy and how technology, which has been on the market for years, still has pressing concerns. It also juxtaposes onto the biggest advantage of UWB which is increase in location accuracy. There is a possibility that these issues re-emerge in chapters 6 and 7 from statements made by interviewees.

5.2. Privacy issues of location monitoring capabilities of radio technology

This section will separate the privacy issues into the three aforementioned paradigms of surveillance, social and institutional. These concerns obtained from research will help structure and formulate relevant questions for the interviewees.

5.2.1. Social privacy concerns-

Social issues arise from the social interactions between users or the inherent use of the technology. Becker et al., 2019 recently discovered a very insecure characteristic of BLE devices. They use public (non-encrypted) advertising channels to announce presence to other devices. BLE devices, as advertised by various technology companies, periodically change or randomize their MAC addresses in cycles. However, Becker et al., 2019 shows that there is a vulnerability in this technology that allows passive tracking well beyond the randomization cycles. The use of an address-carryover algorithm exploits this randomization to achieve tracking across the duration of a day (Vanhoef et al., 2016). This confirms MAC address randomization is not as secure as the public assumes or technology experts portray. It is further highlighted in Martin et al., 2019's research of Apple's BLE continuity protocol. This protocol is designed to support interoperability between various devices such as laptops, iPads, iPhones, etc without any connectivity delay. Continuity messages are broadcast over BLE for actions such as locking and unlocking a device's screen, making and receiving phone calls and even tapping the screen when it is unlocked. The format and content of continuity messages can be used to replicate the operating system version of a device and behaviourally profile users (Becker et al., 2019). The predictable sequence in the numbers makes MAC address randomization obsolete. Further, devices constantly transmit and receive information while not in use and this makes a device more vulnerable.

Gasson et al., 2011 conducted research on a set of European participants merely with their GPS data. On analysing the information and making informed guesses, the research was able to present how much time the user spent at work, at home, for travel, at a friend's place, in a public mall, at their doctors', at a park, etc. This information was further analysed to understand personal indicators of the person such as their gender, social status, religion of choice, sexual life, potential health issues and inadvertent commission of offences. A similar research was conducted by Iqbal and Lim, 2010 where information was obtained for cars' GPS systems. Analysis showed an 80% success rate in identifying user's work address and home address. Moreover, travel insights could be obtained such as whether they take a certain route, how long they are away from home, how fast they drive and the type of vehicle they own. The author predicts that insurance companies could make use of this hyperlocalised data to accurately reflect the risks of a specific user.

Users are increasingly being introduced to smart products and Internet-of-Things, essentially inanimate satellites. These include refrigerators, cleaning robots, bikes, cars, thermostats, etc. These all have an online presence, are connected to the internet and to personal mobile phones as well (Georgiadou et al., 2019). These devices are capable of informing third parties of location, presence and absence. The data security on these devices are alarmingly low which could lead to the revelation of personal data. Furthermore, with the proliferation of these smart devices, there is potential for increased granularity of location information. The smart devices and their potential continuous link to mobile phones could reveal two types of location data. The first is the whereabouts of an entity with contextual information such as the kitchen or living, etc. The second is timed location which references the location with time. This could mean exactly when the entity was close to a smart device and at what time (Georgiadou et al., 2019).

Ajam, 2010 states the location information does not have to be obtained because of a specific individual's negligence. The author makes mention of two scenarios. The first is when a friend of a privacy protecting individual has their own location services on for a particular reason. The circumstance in which both of their

phones are connected to the same public access point or while sharing data through BLE, may make it easier to locate the individual who wants to keep their privacy safe from abusive partners or parents. Secondly, consider the scenario of families that share cell phone plans. The main subscriber has the ability to access location information relating to all other phones in the plan. This is possible due to the pinpoint location tracking services provided by different tracking services.

Wang and Loui, 2009 argues that from the outlook, location information is not very obtrusive or indicative of the person using a particular device. In fact it certainly helps people triangulate the position of nearby restaurants, ATM machines, shops, etc depending on their needs and requests. However, as the aggregated information of where a certain customer enters and shops provides a composite portrait of a person's shopping identity making him more susceptible to targeted ads. The same paper further argues that when a customer is walking in a public space such as a mall or museum, it is not completely a violation of privacy to track that person and help direct them, after understanding their wishes, to places that they may find of interest. Privacy in public is a complex topic and questions keep arising whether the right services can be provided without getting usable information from people. However, if data is collected about what the person does in many different places to either actively influence the person or form an entire identity, that is a violation of privacy. This certainly forms a balancing act between the privacy rights of human beings and the rights of entities to conduct business.

Personal locators on mobile phones have always been able to generate huge amounts of data about the location of a person, which may be done from their inherent internet searches or messages sent to other people. A major example of this is Niantic, the company that created Pokemon Go which collects location information whenever a user uses the app or it is running in the background (D'Anastasio and Mehrotra, 2019). This particular detail has allowed the concept of 'geoconquesting' to grow. This term refers to advertisers gathering data about users related to their online purchases and map it out to what they believe the person will like when they visit a public space (D'Anastasio and Mehrotra, 2019). Facebook, a major social media website, has been involved in allegations for the past few years in relation to user data. A number of documents from within the company showed that Facebook shares data with other third party websites such as Netflix, Amazon, Spotify, etc (Madrigal, 2018).

5.2.2. Surveillance privacy concerns-

Heinrich et al., 2021 mentions how Apple has converted all their devices into the world's largest crowdsourced location tracking network called offline finding. It can be used to detect the presence of any missing offline device using BLE. While Apple has strongly committed to privacy goals, the aforementioned research experimentally shows otherwise. Unauthorized access to the location reports helps in accurate device tracking and retrieving user's top locations with an error of just 10 meters in urban areas. This data was available for a period of seven days from a location correlation attack. This is possible from a malicious application which effectively bypasses the phone's location API to retrieve their location.

Government institutions are often known to cooperate with private corporations. The National Security Agency (NSA) in USA obtained direct access to the systems of Google, Facebook, Apple and other big tech companies (Georgiadou et al., 2019). This has allowed them to collect material such as search history, content of emails, file transfers and location information. Europeans may consider this unrelated however, a significant number of European States are allies of the US. Moreover, a majority of consumers of these big tech companies reside in European States as well. The Snowden revelations have shown that citizens in the EU states are not completely protected by the GDPR because of their data being collected and analysed by companies in the USA.

Data Protection Working Party, 2010 highlights a technical characteristic of Wi-Fi which is passive scanning. It is defined as the "recording of periodic beacon frames transmitted by every access point (usually 10 times per second)." This type of scanning leads to the collection of data exchanged between the access points and devices connected to them. Additionally, phones may request to be geolocated without their owners knowing because this is how Wi-Fi access points operate. This allows the Wi-Fi provider to calculate the position of potential new Wi-Fi access points and/or improve the locations of the ones in the database. This way Wi-Fi location data is decentralised in a very efficient way. This information obtained from Wi-Fi access points is intrusive as they give marketers, service providers and advertisers private details about their life.

Kostakos, 2008 conducted research into the main privacy implications of BLE devices and how similar they may be to RFID devices. He considers three main threats which could translate into UWB. The first is association: buyers of different Bluetooth devices can be linked to BLE unique identifier of their devices. With

the number of banking apps allowing users to directly pay from their phone, each sale can be linked to this unique identifier of the purchaser. While such a database does not exist in the public eye, there is a possibility for it to be monetised in the future. The second is preference threat: the accurate indoor localization of a user can detect if they like a particular store and how many times they visit it. If this were converted into understanding exactly which medicine the person uses, they can infer the specific disease they have. Such techniques could be enabled to derive estimates of the monetary values of commercial products and also the willingness-to-pay of each customer. The final issue is called the constellation threat. Every BLE device such as a mobile phone, headset or satellite navigator creates a 'digital' shadow of all the locations it has been. If this is tracked, information such as associations between people, their regular visits and type of relationships can be derived. This is termed as a social graph (Data Protection Working Party, 2010). From a pattern of activity, inactivity and travel, mutual relationships can be obtained. These types of behavioural patterns can reveal visits to certain departments within hospitals, presence at political demonstrations, etc. Data about the former could push insurance companies into increasing their premium, whereas data about the latter could help the government identify individuals who do not approve of their governing methods.

Phillips, 2003 and Karim, 2004 argue that the data collected about users is useful for law enforcement agencies to have an overview of the public and potentially investigate any threats that they see. Law enforcement agencies have found use by monitoring people on the messages they send and the locations they visit to rank how much of a terrorist threat they are (Phillips, 2003). This was seen to be an advantage from the perspective of governance but it further reduces the control individuals have over their privacy. It also helps governments govern societies from an authoritarian perspective (Karim, 2004). Iqbal and Lim, 2010 argues that law enforcement officials remotely activate mobile phones for audio surveillance and couple it with pinpoint location accuracy, making it an ubiquitous surveillance methodology. This does not only lead to privacy concerns but questions about ethics as well. These include who is responsible for the protecting a user's data if authorities have access to it as well, how long are they allowed to have this data, how much of this data is used to racially segregate and target people. The increase of personally identifying data enables these situations quite rapidly.

5.2.3. Institutional privacy concerns-

Any software related technology in the modern era including mobile phones, network providers or applications collect, retain, use and (possibly) disclose data collected from users. The first of this is easily enhanced with the capabilities of radio technology within mobile phones. It is wise to note that these mobile phones only act as receivers, which means location determination is done independently which can then be seen by the user, if needed (Minch, 2006). This section aims to understand how regulatory authorities view privacy and whether users have any control over their data.

"Location data" is described as any data processed in an electronic communications network by an electronic communications service, indicating the geographic position of the equipment of a user of a publicly available device (Data Protection Working Party, 2010). The hybrid geolocation services provided by Wi-Fi, BLE and GPS are all constituents of this. The European Commission states that the party responsible must obtain prior consent before it is shared with a third party. However, there are a number of companies purely responsible for analysing this data, who operate in a loophole to this particular regulation (Ajam, 2010). Typically, companies that provide services based on location information are termed as information society services. While GDPR has clamped down on these types of companies using location data, the regulations aren't completely stringent (Georgiadou et al., 2019). Such services do not just include one party but twelve others: the mobile device, the hardware manufacturer (same for Apple but different for Samsung), the operating system, the operating system manufacturer (same for Apple), the specific application, the application developer, the core application, the third party software, the third party software developer, the location based service (GPS/ Wi-Fi/ BLE), the network operator and possibly, the government (Georgiadou et al., 2019). These different parties are not all regulated and since many of them may work together, they have found a loophole to use customer data while bending the regulations.

According to the GDPR, Article 4(1), personal data is "any information relating to an identified or identifiable natural person." These could be distinguished between three types of data: volunteered - handed over by the person as 'part of a deal', observed - continuously monitoring a person and inferred - created beyond the person's natural cognitive horizon or through context such as friends. However, this distinction has not been made in the GDPR. Most of this is spatial data based on map or GPS coordinated made possible by the integration of radio technology. While companies say this data is anonymised, the increasing granularity of

information is rendering anonymization futile (Georgiadou et al., 2019). The typical business model of a service includes: a small, fixed fee seen as transaction cost to buy the application, subscription fee for a time period or completely free, in exchange for receiving advertisement or sharing data. It is third business model which the public needs to be mindful of (Georgiadou et al., 2019). Users have to scrutinise end-user agreements to see which parties gain knowledge of this information, much like cookies on an internet browser. Ghezzi et al., 2010 states that as the amount of time and effort increases in navigating settings to protect privacy, the common individual chooses not to do so. This is the strategy that current applications and location based services (LBS) have adopted.

Madge, 2017 highlighted some potential loopholes in the GDPR. The first is that of post processed data. While the GDPR ensures that the personal data processed in the EU is covered by the GDPR, there is no article concerning the sharing of this post-processed data extraterritorially. The GDPR puts limitations of data sharing but there needs to be an equivalent legal protection. While people may argue EU data is essentially useless elsewhere, it could give potential market entrants the ability to target customers. The second issue is termed as the 'invisible data chain.' While the GDPR gives users the chance to specifically ask for deletion or collection of their personal information from any company, internal data or cookies are shared with various third-parties mentioned in a privacy statement. It seems impossible that a user will be able to demand all their data from the plethora of companies that their data is shared with.

With the advent and integration of UWB into mobile phones, the above mentioned concerns may amplify. Previously, devices were able to gather location data when a user is outside with an accuracy of roughly 15 metres, whereas with the integration of UWB, the accuracy drastically improves to the scale of 2 centimetres, even indoors. Mobiles phones are devices which contain critical information which include personally identifiable data, crucial documents, shopping habits, location data, all of which need to be protected more but have become more susceptible due to UWB. Additionally, the accuracy increases the possibility of coercing people on a consistent basis. This may be done by providing personalised ads when walking down a public street or giving a group of friends the exact some vouchers for shopping. Further, UWB signals have the possibility of passing through walls, which means the accuracy of tracking people across rooms increases when they enter a building. However, the biggest inference that can be drawn is the number of pressing privacy issues that remain with current incumbent technology. BLE and Wi-Fi have been on the market for a significant amount of time, yet the number of privacy issues seem to remain stagnant with no major steps being taken to reduce them. GDPR is a big step in the right direction for the EU, but the US is still lacking federal laws on privacy. UWB is more accurate, touted to become cheap very soon, requires low power and has a high possibility of fast proliferation. The aforementioned issues amplifying and potentially getting out of hand, seems like a real possibility.

6

Expert Interviews

This chapter focuses on understanding privacy concerns from expert interviews. It is broken down section-wise into: 6.1 focuses on the demographics of the experts, their organisations, their relevance to the topic and the results of interviews. Section 6.2 explains UWB regulation within the EU and the Netherlands as explained by experts. Section 6.3 compares, contrasts and presents the different privacy concerns of stakeholders broken down into sub-questions. Section 6.4 presents the analysis of the interviews.

6.1. Expert Interviewees

Prior research about the privacy issues on UWB is scarce. As mentioned in chapter 1, this is the knowledge gap the thesis seeks to fill. In order to document potential privacy issues, interviews were the chosen data gathering procedure. They allow an in-depth discussion and expert analysis of potential privacy concerns. The data collected helps form the first singular knowledge base for any future research in the field of UWB and privacy. Additionally, the experts interviewed have experience with both real-world solutions and actively work within the context of UWB. They have the capacity to explain the characteristics, functioning and capabilities of UWB extensively.

The interviews were completely open-ended. Each interview started with the interviewee explaining their field of work within the context of UWB. The following question explored their area of expertise. If the interviewee mentioned an interesting application, a thorough discussion followed on the privacy issues. Additionally, if the interviewee felt there were unexplored issues that needed to be discussed, they would then lead the conversation. This allowed the data obtained from the interviews to be relevant to the thesis but also as exhaustive as possible. It also ensured that the most effective analysis could be conducted. The biggest talking points from expert interviews were used to formulate questions for users (chapter 7). The table below provides the details of the interviewees which includes their organisation, code name as they will be referred to in forthcoming sections and which stakeholder group they adhere to.

Code name	Organisation type	Stakeholder group
PR1	Regulatory authority in Europe	Regulator and Technology expert
PR2	Regulatory authority in Europe	Regulator and Technology expert
PR3	Regulatory authority for a European country	Regulator and Technology expert
PE1	Privacy group based in USA	Privacy expert
PE2	Public University in Canada	Privacy expert
PE3	Private University in USA	Privacy and Technology expert

Table 6.1: Expert Interviewee details

PR1 through PR3 are all regulators within the EU with extensive knowledge on radio technology, short range devices and UWB. PR1 and PR2 have been employed by regulatory authorities for most of their professional career and have regularly worked on technical analyses and drafting final decisions for the EC. PR1 is currently in charge of managing the entire radio spectrum when it comes to newer applications such as UWB.

PR2 is the head of UWB technical testing and applications discovery for the EU. Finally, PR3 is in charge of technical testing within a national telecommunications authority. They work in conjunction with the two organisations that employ PR1 and PR2. It is safe to assume that there is significant knowledge sharing between the three institutions and that the process of UWB regulation in EU, is managed by all three individuals.

PE1 through PE3 are well-known privacy experts within the USA. PE1 is the head of a privacy based group that researches and releases reports on newer types of technology and how it affects personal privacy. They have extensive technical knowledge and their input helped bridge the gap between the research applications and mobile use cases of UWB. PE2 is a privacy expert within the domain of contextual integrity. PE3 is a privacy expert who has conducted extensive technical research into UWB. They initially discovered UWB through research into soil structure. The accuracy and potential of UWB lead to their research into the technical characteristics which were subsequently presented at international conferences and consortiums. Usable data gathered from the interviewees is presented from section 6.2 onwards.

6.2. UWB regulation within the EU

It is important to call back on the regulation of UWB within the EU, where CEPT and ETSI are the premier organisations for UWB regulation. They report to the EU but also assist national telecommunications authorities provide the correct licenses to individual companies within specific member state borders. PR1 and PR2 initially stated that their roles within these two organisations are to protect the radio frequency spectrum from interference across applications or apparatus. This means that they technically test to see if newer applications interfere with incumbent radio uses. Further, they term themselves as "innovation progressive" bodies that allow innovators to innovate while ensuring the radio spectrum is harmonised across the 48 countries they are in charge of. However, PR3, member of a regulatory body for an EU member state mentioned they were the premier authority to sanction any private company within their country border.

PR1 stated that UWB is one of many short range devices communication technology that is authorised within the EU. It has been in use in Europe for quite some time however, the name UWB was coined when the FCC and USA required that a standard regularization was needed. From 2007, when UWB first became 'unregulated,' consistent technical analyses and regulations are needed and being conducted. All three interviewees PR1, PR2 and PR3 agree that:

"UWB is a difficult technology to understand. Within the EU, organizations were using this type of radio technology across the spectrum prior to 2007, without knowing it was actually UWB. Pulse-like, multi-band signals are not the norm for radio technology."

Further, they stated that the industry strive for innovation brings about regulation needed for UWB. PR1 explained the concept of regulation when it comes to short range communication. It is actually 'de-regulation' where no apparatus can use a certain bandwidth and frequency unless the lawful authorities regulate it for usage. PR1 stated that various apparatuses were initially made for the American market but there was no lawful administration within Europe. This led to the 'Systems Reference Document' which documents the use cases that industry incumbents envisioned. Some parts of the UWB spectrum became liberalised and broken down into different spectrum frequencies where 3-9GHz is largely known as the generic UWB range. PR3 clarifies by saying that:

"3-9 Ghz is the generic UWB range, however, for mobile phones the operating range is from 6-9 as mentioned by different mobile phone companies"

This would mean that they are classified into the generic UWB range. All three interviewees state that any new application from UWB devices introduced into the market fall into this particular category. As frequency increases beyond 10 GHz, there are specific applications such as level probing radars, material sensing technology, wall penetration, wall material sensing application, ground penetration radars, etc. These have different regulations as they have much higher frequencies, higher possibility to interfere with regular radio signals and can only be used in special circumstances. There is a possibility of these uses being applicable in the generic frequency range with lesser effectiveness but this needs more research. Furthermore, PR3 stated that the power limit for the generic UWB applications base is around -41 dBm which is quite low and highly advantageous for its day to day operations. PR1 further elaborated on the differences between the European

and American market by stating that the regulations in America have a minimum field strength and power below which they are not interested. In Europe, the entire power limit and field strength is regulated throughout and apparatus cannot be put on the market unless it fulfills all the requirements.

PR2 and PR3 describe the European procedure of ensuring an apparatus is within the regulation for any industry innovation. If an apparatus is designed, firstly, all the tests must be conducted to ensure they adhere to regulations. This is done by going through a checklist and ensuring the application fulfills all the criteria in that frequency range. If manufacturers think that they can forego or ignore the regulations, PR3 mentions the existence of a subgroup under the RCA in charge of enforcement.

"This enforcement group goes to product websites or stores to check the working conditions of the product. If they find any issue, there are no negotiations but rather the product must be corrected or pulled off the market."

From a mobile perspective, tests are currently being conducted on the electromagnetic field exposure on people and whether there is any signal overlap with BLE and Wi-Fi. As UWB becomes more common in mobile phones, there will be more tests for any potential issues.

PR2 provided us with a brief insight into the standardization across application types. UWB has four different standards based on applications: generic usage (connectivity applications), location tracking, ground based vehicles and material sensing. These are standards not based on the regular distinction of frequency range such 3-9 GHz or above. These directives are based on applications. Technical studies for these lead to updates to specific technical documents which are internally debated and then released for public consultation. The public consultation, from the European Commission is an open platform where the public can share its views on the decision to provide their input. This is an iterative process where standards, technical reports and regulations are consistently updated for newer technology. PR2 affirmed that:

"The number of applications for UWB are consistently increasing making it difficult to have individual regulations for all different application domains."

Some use cases may never be covered, whereas some newer use cases will be given more priority. Since the technology is proliferating, manufacturers have to have presumption of conformity, where the individual RCA will ensure that the technology meets the criteria.

PR3 and PR2 asserted that UWB has quite a prominent market potential for a few reasons. Technically, it operates across a wide frequency range making it easier to use the spectrum. PR3 says that within the generic frequency range, it is largely unregulated which means the number of applications can grow exponentially. From an application perspective, PR2 stated that the main focus nowadays is on automotive radar ranging, sleep apnea monitoring, material exploration, fall monitoring, gesture detection, professional audio, entry keys for houses/vehicles, fitness trackers, smartphone ecosystems, etc. Some applications require more power and a higher frequency range to operate whereas others do not. UWB allows for the manufacturer and application to determine which range is the best and subsequently adjust. In cases where privacy of civilians comes into question, Article 3.3 of the Radio Equipment Directives comes into effect.

6.3. Privacy concerns

The expert interviews conducted included a section of questions for potential privacy concerns. It was conducted in two ways, first by getting a bird's eye view on the potential issues but also deep diving into some use cases and seeing if any potential privacy issues were relevant. However, as mentioned previously, the experts are quite different in their expertise and it is difficult to obtain relevant information if the exact same questions were asked. This is why, as the interviews progressed, the open-ended interview evolved into a discussion on the interviewee's expertise, what applications they feel are more relevant to UWB and what potential concerns are there. In order to provide a streamlined results section below, the answers were broken down and categorised into eight questions.

6.3.1. How does UWB differ from other incumbent radio frequency technology?

Wi-Fi and BLE operate near the 2.4-5 GHz range whereas UWB in mobile phones operates in the 6-9 GHz range for mobile phones. PE3 says that the Wi-Fi channel is only about 20 MHz whereas the wide-band nature of UWB gives it more frequency to work with. PR1 and PR3 agree by saying that the Wi-Fi and BLE channels are usually very crowded while the UWB spectrum has much more 'free' bandwidth to work with, making it a better communication and data transfer platform. PR3 further states:

"The distance of communication increases while using a UWB device. BLE allows for a communication distance of 20 metres while the UWB chips in mobile phones allows for communication across 80-100 metres."

From a technical perspective, PE3 explains that ranging is one of the biggest advantages of UWB, which is like echolocation. It measures the time of flight between when your phone emits a ping and it arrives at a receiver. Additionally, the high bandwidth fights multi-path interference. A multi-path is when the signal bounces off lots of surfaces in the environment and give duplicate copies to the receiver. This makes it difficult to get clean, noisy data. UWB transmits really short impulses, making it less likely for these multi-path signals to collide. Complicated environments include streets, supermarket aisles, crowded places or within households. PE3 states:

"UWB chips reduce the location tracking uncertainty to a circle of few centimetres, whereas it was about 20 metres for BLE devices indoors."

They further say that in the near future, it may be the norm that big places such as supermarkets and offices upgrade their access points to integrate UWB to increase location accuracy while possibly increasing data speeds of all users within the premises.

PR2 believes that the biggest defining factor of UWB is its operating power of -41 dBm thereby reducing chances of other devices interfering with respect to the frequency spectrum. Further, the higher bandwidth of operation gives UWB devices more security as a potential spoof would need to test out various frequencies to find the corresponding one. This means that the applications such as keyless entries to cars, houses or unlocking laptops become more secure.

6.3.2. What are the major issues seen with AirTags (and Android equivalent)?

AirTags are a use case specified by Apple that allows for a user to buy a UWB equipped device which is the size of a bottlecap. The user can place this 'AirTag' in any of his/ her personal belongings which sends out pings at regular intervals to the user's phone, allowing him/ her to track their belongings at all times, with an accuracy of 2 cms. In order to do this, PR3 explained the semantics of the technology. It fits into Apple's idea of the Find My network ecosystem where if a person loses his phone, he can check its location with the help of GPS and BLE localization. The phone that is lost pings out pulses through UWB, which then ping off of other users and eventually show up to the user when he logs into the Find My network. Apple aims to incorporate AirTags into the network where at any time, various users can be localized because they have their UWB capabilities on. PE3 assumes that the localized data of users would be saved on Apple's servers.

From the interviews conducted, there are very different views on the privacy issues of the meshed network. PE1 has some reservations about the actual issues. Since this is an incumbent technology, they expect that the network is pretty attenuated by the number of people in the network which means that no onlooker would be able to actually localise a specific individual from the Find My UWB ecosystem. But they agree that the idea of opting in and opting out is needed. The user should have the opportunity to choose whether he wants to be a part of this network and there should be a certain setting to toggle it. PR3 further builds on this by saying that:

"The members of the chain must be made certain that their location is not made explicit. From a security perspective, if a repeater knows which part of the chain he is in, he would be able to locate the AirTag by himself."

PE2 explains the concerns with the backdrop of contextual integrity, where people need to know who is in charge of this information, whose information is being stored, how it is collected and the flow of information. For AirTags, they believe a majority of people are not aware about the inner working of the Find My network which means that they do not know they are repeaters.

However, PR3 does not see this meshed network as all disadvantageous. It could help with disaster relief and ensuring public safety if timely notifications are sent to people who live near a possible natural disaster site. Further, they propose the solution to the mobile company to remove any type of identifier of devices within the network. This means that instead of the AirTag showing up as an AirTag, it should be a regular 'device' on the network.

6.3.3. What are the concerns with 5G UWB being introduced?

PE3 categorically denies that 5G and UWB are being interlinked to get 'faster data rates' as advertised by Verizon. It seems that Verizon is one of the first network providers to obtain frequency bandwidths in the

30GHz range for faster transmission rates. They are planning to build infrastructures in certain hot spots such as offices, malls and stadiums where users will get fast mobile data rates indoors. These are called micro cells where the concept of beam steering is used to create point to point high data rate transmission.

However, the concept of UWB in phones gives mobile phone companies the chance to improve something known as ad hoc or meshed networking. This is when users with UWB near a cell tower can help users who are not in the vicinity of a tower get faster data rates by 'latching on to' the former. This still requires research as technically, a mobile phone will spend a lot of time trying to communicate with another device rather than actually 'sending' any data speed. If the research turns out to be fruitful, PE1 and PE2 have some concerns. The latter states that this may coerce people into having to keep their phone's UWB capabilities on at all times. This would mean an increase in location accuracy at all times. They further state that this allows for mobile phone companies to track people at all times. While testing the technology, P2 claims that UWB occasionally turns on when other functions such as Wi-Fi and BLE are turned on. This is counter intuitive because people do not expect it. There might be a duality where people are okay with being tracked but if their location gives up aggregated information such as where they were, what they spent their money on and what they lingered in front of, it may raise more concerns.

6.3.4. What might be some security concerns?

UWB is rated high amongst other incumbent RF technology based on security. But with the issues of accurate localization and high number of people/ products interconnected at all times, interviewees were asked their opinion on the matter. While a majority of them agreed that UWB is quite a secure technology with regard to the radio spectrum, two of the interviewees shared their thoughts in detail.

PR3 picks one side of the coin by reinstating the security of UWB. Since UWB has multiple bands of operation, there is additional security as any infiltrator will have to scan across multiple frequencies and codes to find the correct transmission. Since UWB pulses are transmitted in intervals, the timing to scan also needs to be coordinated which is quite difficult to do. However, PR3 also states that they would not like the mobile phone company to collect their data when it comes to applications such as keyless entry. This would give insights of when one leaves his house or enters his car which is saved on company servers thereby increasing the possibility of revealing information such as when one leaves the house, walks his dog, etc.

Oppositely, PE1 says that:

"The security claims of UWB 'gives flashbacks to the BLE and Wi-Fi standards that first came out. But eventually people found out security issues, one of which is the issue related to MAC address randomization..... This leads me to believe that it is a matter of time before someone realises how the security of UWB can be infiltrated."

PR3 sees a stark contrast in the way security is handled for consumer applications. They state that the cyber-security for military and medical equipment follows technical rules and specifications, whereas for consumer applications it lags behind.

6.3.5. What are some surveillance privacy concerns?

This question was the biggest talking point for all of the interviewees. UWB is not only seen as a positive change for mobile phones but as a way of interlocking users with their surroundings. The main contributors to the discussion were interviewees PE2 and PE3.

PE3 claims that from an economic perspective, UWB's location data is exactly what advertisers have been waiting for. Google experimented with Wi-Fi for indoor localization but it wasn't fruitful. With the advent of UWB, their hopes are renewed and it seems to be a matter of time till infrastructure catches up. Which means that UWB may become the standard for access points in stores, hospitals, warehouses or offices. PE2 furthers this claim by saying:

"Implementing UWB in public access points is highly possible. This may give stores information such as which shop you visited, exactly which product you looked at for a long time, sent to advertisers and then you would get personalized ads."

From a technical perspective, PE3 explains that its not your phone doing this but just the inherent functioning of Wi-Fi and possibly UWB in the future. Your mobile would send out signals, the store would have access points waiting to listen. You could possibly take this into the context of a hospital and see which person is regularly visited by another individual, making social connections purely based on proximity. This could also

be translated in trying to identify one person who has a 9-5 job because they spend a significant amount of time at one place which has UWB access points and then go home. Over time it can be inferred who this person is, thus creating a customer profile. Since most people may not knowingly allow location permissions, this happening behind the scenes needs more recognition.

PE3 tries to further explain the technical possibility of tracking people purely based on the UWB integration in mobile phones. Something that differentiates GPS and UWB localization is the lack of context in the latter. GPS may be able to locate the number of people in an environment and place them in a physical location in the world like a museum or park. However, turning on only UWB localization, there is most likely a lack of context. In simpler terms, UWB can only provide relative location without placing someone in a certain location, whereas GPS localization provides absolute locations. However, permissions or settings will make a big difference in the instance. If UWB works in conjunction with BLE or Wi-Fi in the settings then there would be a continuous gleaning of information with context, with an accuracy of centimetres. This means that people would be tracked in their offices, stores, malls, etc unless they make sure they turn off each location setting every time they leave the house.

PE2 feels that with the advent of UWB, the opportunity to collect fine-grained information is higher. They think that as a user, you should be informed exactly how UWB works and the granularity of information it provides. Users may not expect to be tracked indoors because it hasn't been technically possible till now. PE1 argues along a parallel route where:

"UWB is being introduced to interconnect a lot of IoT devices such as a smart TV, headphones, smartwatches, phones, etc in an ecosystem. Since they are all connected at all times, there is free flow on information between them leading to data collection such as dog walk timings, TV schedule, grocery shopping, etc."

PE3 brings up another issue with the example of a company called Five Tier that updates ads in Times Square in real time based off of the information from nearby cell phones. UWB integration has the potential to make this a reality in most city squares.

This essentially puts us under a microscope, where we are tracked at all times or data is being collected of us. PE2 argues that these location based services will help notify users during natural disasters. However, certain questions persist of how the information is used after this period, how long it is saved and whether there is a possibility of using it for unexplained reasons. PR3 says that the idea of data collection goes against what the public agrees to. If the idea is just to count the number of people in the vicinity or the number of visitors, then absolutely minimal identifiable information is needed. PE3 argues against this from a company perspective saying that Apple does not need to leverage customer data for additional income. Browsing the mobile phone market shows that they have costly devices which is their main source of income and it would be a deviation from the norm if they did that. However, Android phones have more reason to do this as they are linked to Google, a company which has historically wanted to use customer information to increase ads and provide personalised services.

6.3.6. What are some social privacy concerns?

PE1 says that a major social concern is if UWB operates similar to BLE's beacon mode, which is of course co-opted by the police during times of emergency or when information is needed about a suspect. At the moment, there are strict guidelines for this. UWB and its ability to triangulate people through using access point or known locations of a few nodes really amplifies concerns. It would enable the access point owner to see how many people visit a certain place at a certain time only because one person may have forgotten to turn off their UWB services. UWB may enable the mapping of hyper localised information which may be hard to comprehend at first but may later on turn into a salient feature that becomes the norm.

PE3 highlighted a major concern of how there is a transfer of data across applications, something users may not know of. Apple, as a company, may not see the need for collecting information as stated before. However, they are making it possible for third party applications to collect data, use it or sell it on to another company. PE2 gives the example of a weather app which may have been made for noble intentions. But after a certain time, your current location or information can be shared to other developers because it is seen as a source of income/ revenue. This seems to be the biggest issue from a contextual integrity standpoint, as PE says:

"The fact that the five independent parameters of: data subject, sender, recipient, information type and transmission principle are made not made explicit throughout the usage of a technology or application. Users

need to be made aware of how they are monitored, how a service is provided to them and what type of information is being obtained from them."

PE2 further explains it from the perspective of AirTags where users only know about how well they can track their own belongings. But some users may not know that they are part of a Find My network or that they are a potential repeater through their personal device. This further begs the question of whether users are made aware what information is obtained from them in specific scenarios. It is safe bet to think that a user assumes it is only his location that is obtained when using a weather app but if they regularly go for bike rides during the sunny weather, this provides insights based on the context of weather and information.

PE3 argues that there is a lack of awareness in the common citizen when it comes to downloading free applications. Since there is no income from the consumer, their data then becomes the paramount trading commodity. The initial step would be educate themselves to understand that this is the business model for a lot of companies. Secondly, it would be to look at the settings, per application if necessary. If you do not understand why your gaming app has asked for your location, it would be wise to turn it off. PE2 consequently says that a lot of manufacturers try their best to ensure consumers do not worry about their privacy. This is done by providing them data collection 'levers' but it seems like a far fetched idea for a day-to-day consumer to navigate the landscape of settings that are either changed regularly or keep asking you to affirm your choices. This shows that the information is crucial to the receiving party.

6.3.7. What are some institutional privacy concerns?

PE2 believes that there is a major concern in the way UWB has been advertised to customers. They state:

"Apple and Samsung did not clearly mention the integration of a UWB chip in their newer models to the general public. Flashy scenarios of benefits to the customers were presented while hiding the other side of it. Only technology experts would be able to pick up on that from the keynote presentations that were made."

Advertisements only showed how people get better data rate and spatial awareness, whereas the increase in accuracy of localization is something that needs to be inferred from the regular public.

Secondly, PE2 believes that the information flow must be brought to the forefront of discussions. If technologies that are pervasive proliferate freely, regulators will have a tough time as they become the norm. They believe this comes on the back of the current ecosystem of applications, where the burden is on the user to take into account the information flow, in, between and through different applications on our phone. This is inherently hard because of the number of applications that are being used daily. There is quite a lot of data sharing between applications that need to be made clear to users. PE2 also mentions that:

"Mobile phone companies plays to the market and consumer knowledge very well. Users have very different views on the privacy of new technology, what should be available and what should be under their control. Apple knows that there are some technical gaps that their products fit into and this is where they operate."

For example, UWB is still an upcoming technology, the technical boundaries have not been discovered and complete analyses have not been conducted yet. This allows Apple to gain a stranglehold on the industry prior to the rest of it catching. PE3 shines some light on the public perspective: "People have gotten used to trading access to free things for being advertised at but are not aware what sort of sensitive information is going into serving these advertisements." Current business models revolve around providing the user something such as free coupons or additional functionalities. A rather unpleasant example presented by PE3 is Amazon Smile. It is a supplementary Amazon website that donates part of the money of your purchase to charity. However, to avail this 'functionality,' users had to agree to collection of their data and pop-up notifications.

Thirdly, PE2 believes that the GDPR is not as significant as the general public has made it out to be. GDPR allows the user to have control of his data but in a lot of situations, the user does not have complete information on the data being collected. The GDPR says that the collection of 'legitimate' data can be done. For a privacy adherent consumer, they will want to give up data that is only relevant to the service that is being provided to them. For example, for a food delivery app, your preferences of food and location seem to be the only data that is legitimate and the application should recognise that. However, the example of Facebook selling customer data to a long list of advertisers or influencers shows that there is a reason for customers to be concerned with what data is being collected and how it is being used, whether it be for information gathering or manipulation. Moreover, the issue of extraterritorial reach comes into the picture. It applies to all EU citizens wherever they are situated, which means that there are a number of liable organizations in different

parts of the world that do not know that they have to change their data collection procedures. There seems to be a gray area of operation here which affects users' privacy.

The two application domains of UWB are cross referenced against the broadly mentioned privacy concerns highlighted by experts in the table below.

	UWB as a personal device	UWB as an infrastructure
Surveillance	<ol style="list-style-type: none"> 1. UWB radar to map surroundings 2. UWB radar to locate users who may not want to be located 3. Ability to track and profile people based on UWB devices and usage 	<ol style="list-style-type: none"> 1. Track people based on location with multiple UWB sensors 2. Tracking a MAC address across time 3. Intrusive inquiry and targeted advertising 4. More devices naturally leading to easier surveillance 5. Social distancing surveillance
Social	<ol style="list-style-type: none"> 1. Data sharing in a confined space with unknown people 2. Use of UWB to locate other's belongings 3. Usage of UWB localization to follow/ track people with identifiable IDs 	<ol style="list-style-type: none"> 1. Stalking users 2. UWB inter-connected involving additional users within the mesh network 3. Social network analysis
Institutional	<ol style="list-style-type: none"> 1. Information on personal apps may be processed by third parties (health, online retail, etc) 2. Excessive data collection without a justifiable reason 3. Aggregation of data across applications 	<ol style="list-style-type: none"> 1. Excessive data collection without a justifiable reason 2. Aggregated data and customer profiling 3. Deliberate de-anonymization 4. Integration with 5G for faster data rates

Table 6.2: Different privacy concerns of UWB incorporation

6.3.8. What can be done to protect privacy?

The answers from the privacy researchers seemed to be most relevant in answering this question. PR1 and PR3 stated that Article 3.3, previously introduced, would come into play if there was any issue of users' privacy being affected. There is a sub department in every member states' telecommunications industry that works on a need-to-know basis. This means that any time a privacy neglecting technology is introduced to the market, this department tests the new technology and decides whether it complies to privacy standards. It can then suggest changes or take the product off the market.

PE1 says that mobile phone companies need to decouple services from UWB and the functionality it serves. This means that the number of applications that need UWB must not proliferate. BLE and Wi-Fi already serve a large amount of services without the need of centimetre level accuracy. There would be no need to couple these services and users need to be able to choose the level of functionality they want from an application without being coerced into turning on UWB obligatorily. They further say:

"Responsible organisations such as the CEPT, ETSI and RCA need to test applicability of UWB in individual cases faster than the applications come out to the market to ensure that mobile phone companies are kept in check. Or they would need to make extensive directives from the get-go that reign in the border of what can be called innovation."

PE2 states that privacy is not about secrecy or data minimization. It is about the appropriate information flow and the definition of appropriateness is defined by the societal norms in a particular context (Nissenbaum, 2004). This means that the data collected from a person should be based on the function a particular application solves but advertisers 'throw a cog in the works.' People want their data to be collected about their cooking habits when they visit a cooking site or their interests when they visit YouTube, for example. However, advertisements are everywhere which means data collected from your shopping patterns on one website can be used to advertise to you on another website. These two may not be related in their domains, however over time these websites collect information, aggregate the data and form customer profiles of everyone. Websites say they do not collect personal information but only public information. In the end, the locations people have been to explain everything about a person without the need for personal data to be collected (Thompson, 2019). The referenced article mentions how 50 billion location pings of 12 million people in America were tracked for several months. This gave information about the people such as which places they visited, what they did for hobbies, whether they were religious, exactly which stores they visited and the paths they took from home to work everyday. This dataset which was analysed helped identify celebrities and eventually track them across the country. The research also introduced 'inform analysis'. This is the method of analysing data of people after they have received or seen an advertisement and whether they visit the place or buy the product advertised. This tests the effectiveness of marketers.

PE2 mentions that if a person does not have an AirTag or UWB, he should not be included within the system unless there is an opt-in/ opt-out option. However, they believe that the company may consistently send notifications coercing the person into finally agreeing. They also state that the regular user needs to be properly informed by the companies: their marketing banners or keynotes. People did not know about UWB,

except as a U1 chip which wasn't explained properly by Apple. PE2 says that the public does not have the time to actively check for settings or make changes. They need phones to go about their daily lives and you cannot expect them to be knowledgeable about privacy. PE2 states that:

Users, regulators and companies need a coherent sense of privacy. What is meant by privacy from an industry perspective is different from what it means to every individual. What can then be termed as private information in this day of data collection needs a legal definition.

There needs to be communication between stakeholders and users so that there is an understanding of technology and improving technology in the right direction. Following these lines, PE2 supports the need for the right framework for software engineers and companies to design innovations properly so that privacy is taken into account effectively. This means that applications and technology are designed with how it affects society and if it is in line with human values rather than just filling a technological gap.

PE3 believes that the length of impenetrable license agreements is something regulators should look at. Of course, it is the users' responsibility to read these and ensure their data is protected. There are two big issues with this. The first is that there is always something known as 'mandatory' or 'functional' data that is always collected, which doesn't really give users an open choice. Secondly, this is asking a lot of people who are using multiple services a day and not technologically inept. People do not realise that they are giving away data but are repeatedly surprised when a cover up story is shown on the news. PE3 explicitly states:

"Right now, the legal system is not geared at looking at privacy from the users' perspective but the functionality of the service provider."

They subsequently explain why this data is even collected in the first place. For brands, getting this information is like following a 'customer's journey.' Since online activity is the future, location information provides a major advantage by seeing whether the adverts that were shown, were actually effective and whether the right people were shown it. Other domains have found use in it as well recently which include governments trying to find out who protesters are or political campaigns targeting potential voters. PE3 also mentions the example of South Korea where leaders did not delete the contract tracing data collected during a previous outbreak. UWB allows the accuracy to increase quite significantly, something regulations need to clamp down on.

PE3 believes that there is a need for industry wide policy or discussion before privacy is lost too far. Right now, location based data is being used by a lot of companies with privacy reports being published regularly. There is a possibility immediately to stop the use of centimeter level data before it becomes the norm. This can be done based on managing the expectations that customers have with the functionality that is provided to them. Engineers only test the positives of any innovation prior to introducing it to the market. They need to assume the worst of technology and ensure that it is taken into account when introducing new technology to the market. Governments and regulators need to ensure that privacy is given more importance as currently, it is not considered as damaging as the sale of toxic chemicals, for example. PE3 believes that Wi-Fi localization is a blind spot in the regulations and the possibility of this happening with UWB is increasing. They say:

"Nobody expects that your phone is giving out your exact information as you walk through a public space and there is no reasonable reason for that to happen. It seems like innovation is outrunning policy. It should be the industry's job to protect the general public's safety as they know the technology better."

Companies need to take the initiative first by agreeing to unified laws about data collection and sharing in consortiums. They need to internally agree to prioritise public safety and privacy over business goals.

6.4. Discussion

UWB, as a radio technology has a long list of possible regulators in Europe which include the CEPT, ETSI, RCA but also the individual telecommunications authorities of each country within the European region. There seems to be an overlap in the functions of these organisations in trying to understand the technical or regulatory aspects of UWB, whereas potential privacy concerns are not given priority. PR3 only briefly introduced a security based department that worked on a need-to-know basis which was mentioned in section 6.3.8. It seems that from the offset, privacy of users has not been given enough importance. There are analyses and tests of UWB geared towards understanding its location tracking abilities but it seems that they are failing to

understand the privacy concerns that comes with centimetre level accuracy. Regulatory bodies need to be more proactive to get ahead of innovation so that users are given more importance in the marketplace. However, a big advantage for users in the EU is that regulations protect them much more both from a technical perspective (multiple regulatory bodies) but also a privacy perspective (GDPR).

The three privacy experts repeatedly stated how users do not fully comprehend how much more impactful UWB location accuracy could be. As the use cases for it increase in a largely 'innovative' world, the reasons to monetise it will also increase. This would give companies lesser incentives to ensure security of the public's information. As PE3 mentioned, if the access points in public places start integrating UWB, people could be tracked inside buildings and across streets. AirTags further help the possibility of big tech companies getting sensitive data only because people use their technology. From an outside perspective, it does not seem to be a detrimental technology as it may help people track their belongings or governments track people for uses such as contract tracing or positional locations near natural disaster sites. But this also means that there is so much more information for mobile phone companies to collect while the amount of usable reasons are rare. From a user perspective, a major question should be asked on whether this technology was even required, since BLE or GPS historically worked well for the purpose of AirTags or locating personal objects.

While a significant number of people believe in the anonymisation of data, PE3 mentioned that is not hard to identify specific people from the data. All of this information is saved on the specific company's servers. A majority of these companies say that the information will not be shared with anyone else, but the presence of this information goes against the idea of privacy. People are tracked at all times, their information is saved for whatever activity they are doing and all of this occurs because users are using technology. As PE3 mentioned during their interview:

"People need to realise that their data is the currency for when they are using a free application or technology."

From user interviews, it will be interesting to understand what potential applications people assume companies have for their data and whether they realise 'free' services come at a cost (Barth et al., 2019). Further, mobile phones companies may not have significant need to use the data that can be potentially collected, but they are making it easier for third party companies to do so. This means that Apple and Samsung are just providing the means for other companies to collect aggregated information.

The biggest highlight however, is the similarities in privacy issues between incumbent radio technologies and UWB. BLE was initially introduced in order to increase data rates and from a phone perspective, increase accuracy in location data. Then Wi-Fi was incorporated for increasing internet connectivity and fast transfer rates. Slowly the concept of accurate localization was introduced with respect to Wi-Fi technical specifications. Now, mobile phone companies want to integrate UWB with almost the same characteristics and functionalities. This begs the question if there is any improvement of functionality for users or if this is just another innovative way of increasing location information accuracy. The experts interviews showed that the privacy issues are quite linear and repetitive across a significant time period, something regulators must inspect properly. It definitely seems like there is a sale of an infrastructure, where users may be locked into at all times and over time have the inability to opt-out of.

The easiest solution to solve the privacy issue may be educating users but considering the long list of privacy statements and nexus of settings that users have to navigate through, this may be a foregone solution. As PE2 clearly mentions, big tech companies, consortiums and governments need to take responsibility for their actions. They need to ensure that the users are the focus of the technology. They need to realise that the technology that they are providing to the world needs some sort of regulation and at some point, a line needs to be drawn to ensure users are still the focal point of society. Users need to be informed of all the possibilities; something that was not done with UWB integration in mobile phones. Mobile phone companies marketed UWB integration very vaguely. Apple and Samsung have a significant market share of users and need to realise the power they have over the general public and start taking responsibility.

7

User Interviews

This chapter highlights the third step of the RTA - Communication and early warning. Students of the University of Delft were interviewed in a semi-structured process to see if they share and validate the concerns of experts on UWB. Justification for the interview process and why it was conducted is highlighted in section 7.1. The interview questions are presented in section 7.2. The interviewee personal identifiers is discussed in section 7.3. Sections 7.4-7.6 elucidate on the different privacy concerns broken down into the three privacy paradigms.

7.1. Interview procedure

Users are important stakeholders in the context of new technology and its acceptance. This chapter seeks to understand how users view new technology, possibly understand the functionalities and identify privacy problems. Their input is specifically valuable because prior to this point, the thesis has highlighted privacy concerns from industry experts and research, whether it be BLE, Wi-Fi or UWB. This sections provides the opposing perspective of people who are not in the technology or regulatory domains of UWB, but rather use the technology daily. This helps understand whether users know such a technology exists, what its possible applications are and whether they believe they need it. All the interviewees are from Delft University of Technology in Delft, which means that they have relatively high knowledge about the functioning of their mobile phones. A comparison is made between the input from experts and users to check whether both groups identify the same issues or what their overall perspective on privacy is.

The biggest challenge of conducting user interviews was to provide suitable background information to user prior to the interview. Since UWB is a relatively new technology, the general consensus assumed was that users do not know a lot about it. For this reason, a background information document was sent to the interviewee at least 4 days before the interview day. This provided them enough time to get accustomed to the functions of UWB and its use cases in mobile phones. Secondly, obtaining users from different departments was considered of paramount importance. If interviewees were from a singular department, the potential for them to give similar answers was assumed to be high. For this reason, an announcement was made on the university notification board across different faculties. This ensured students with different expertise were obtained. Finally, user interviews required the researcher to provide direction. This meant that if at times users mentioned issues or applications that were not technically possible, the researcher had to intervene and direct the interviewee properly. Furthermore, the Human Research Ethics Committee was consulted to ensure the entire process was GDPR compliant. In order to accommodate this, the actual interview procedure for each participant took 15-20 days.

The interviews were semi structured. The questions in the next section were asked in the order specified but if at any point the interviewee felt they had more knowledge/ opinion about a question, more specific personalised questions followed. The actual interview was broken down into two sections: personal indicators and different use cases of UWB. The former allows the reader to identify the type of users that were interviewed and gain an insight into the type of technical information the individual possesses. The latter provides certain use cases to the user and helps reveal any privacy issues that they identify.

7.2. Interview questions

The interview questions are shown in the table below. The text in parenthesis is the explanation the interviewer provided to the interviewee.

Context	Question	
Personal Indicators	Do you know what UWB technology is? (If not, explain it and how it differs from BLE)	
	How do you imagine UWB would be used in a mobile phone? (explain some use cases if the answer doesn't include them)	
	What do you use your BLE for?	
	How often do you use BLE to transfer data? Or connect to other devices?	
	Do you ever worry about the privacy or safety of location information on your device?	
	Are you aware of MAC address randomization on your device?	
	What if this isn't as safe as you thought? (explain how there is leakage of information)	
	(explain AirDrop usage) Do you think there are any issues when people who do not want to be seen on a network are included?	
	Have you ever received targeted advertising? Or personalised ads based on where you've been?	
	What are your thoughts on analysis of foot traffic in crowded environments? With newer technology able to record and interpret it?	
Technology specific	(explain Wi-Fi packets sent for internal localization) What do you think the issues would be if it were with UWB?	
	Where do you think these could be used from a UWB perspective?	
	(explain AirTags and meshed network) How would you feel being part of a network that has nothing to do with your belongings?	
	What privacy concerns do you see with this?	
	(explain GDPR) What do you think constitutes 'legitimate' data collection?	
	How do you feel about public access points behind able to connect to your device and obtain legitimate data, in addition to location?	
	Conclusion	What are your thoughts on how privacy can be protected? Technically? Policy-based?

Table 7.1: Breakdown of interview questions

7.3. Personal identifiers

The interviewees will henceforth be referred to as P1 through P10. They are all from the Delft University of Technology. They are all doing their Master's in the University. All interviewees are between the ages of 22 and 28. They represent 5 different countries. They all own mobile phones and use it on a daily basis, extensively. They know the inner workings of location settings which is very relevant to this research. They are from different faculties which include aerospace, policy management, industrial design, mechanical, civil and computer science engineering. Different perspectives have been included which helps make the research as complete as possible.

This paragraph contains the results of the personal identifier questions mentioned in table 7.1. None of the interviewees had prior knowledge of UWB or its integration in mobile phones even though three of the users had UWB integrated phones. After introducing UWB to them, most of the users described UWB as a 'high frequency, high bandwidth technology that seems to work similar to Bluetooth and has largely the same features.' Some users imagined functions such as short range IoT connectivity, location based services such as automated lighting, key-less entries, foot traffic analysis and social connectivity at events. One of the users was particularly bothered by the wide array of potential applications as they seemed to be quite privacy intruding if they were possible within mobile phones. Seven of the interviewees could not imagine the added functionality UWB could provide over BLE or Wi-Fi. All of the interviewees used BLE on a daily basis, specifically for connection to their headphones or speakers. A solitary user kept their BLE on throughout the day as it was connected to their smartwatch whereas everyone else preferred to turn it off. Only two users used BLE for data transfer daily as the rest of them felt that data transfer through BLE is unreliable, slow and a functionality of the past.

Concerning location information, five interviewees were not worried about the privacy or safety of location information that was saved on their device. They provided some reasoning for this which can be categorised broadly into two categories. The first is that they realise that this is something that they have to give in order to receive full functionality of their device. This involves tracking running routes, Google map history which provides suggestions or merely location recommendations. They realise this information could be analysed by the mobile phone company or a specific app that they have downloaded and this is the choice they have to make in order to use technology. The second reason which was voiced by two users is that they felt they were not important enough to be personally tracked for any reason. From the other 5 users, one user gave some explanation on the concerns they had. P10 clearly stated that they had concerns with private companies owning their data (not only location data), a concern voiced by all the other users. P10 continued by saying that:

"These companies have power over the general public, something that is understated by a majority of the population. On a personal level, they could find out a singular person's location and understand his/ her

interests. On a social level, these companies could influence society in a deep way without being brought to the forefront."

Only one user, P5, clearly understood how MAC address randomization works. They defined it as the process of randomising the MAC address every time a mobile phone is connected to another device through Bluetooth, ensuring that you are not tracked through the hardware. Rest of the users did not understand how MAC address randomization worked. Additionally, four users stated that they knew about their location information being saved on company servers but being inaccessible by any mobile phone company employee. P1 and P4 stated that they believed in the security that was offered by the introduction of GDPR. Oppositely, user P7 stated that:

"Our data is not anonymised. There would be no reason to do that, at least within company servers. They may take away some sort of identification information from your data but at the end of the day, it is linked to your account whether it be an iCloud ID or Gmail ID."

The company may state that they have randomized this information but trying to identify someone from this is uncomplicated, which renders the entire meaning of anonymisation useless.

When questioned whether they research the privacy concerns of a device before buying, eight users said that they buy a product and then change the settings of the device to give them the most privacy. These users believe that functionality comes first and that the settings that involve how much data is collected about you can be changed. User P10 stated:

"There is no mobile at a competitive level that focuses on privacy. They do not have good operating systems and are very slow."

7.4. Surveillance privacy

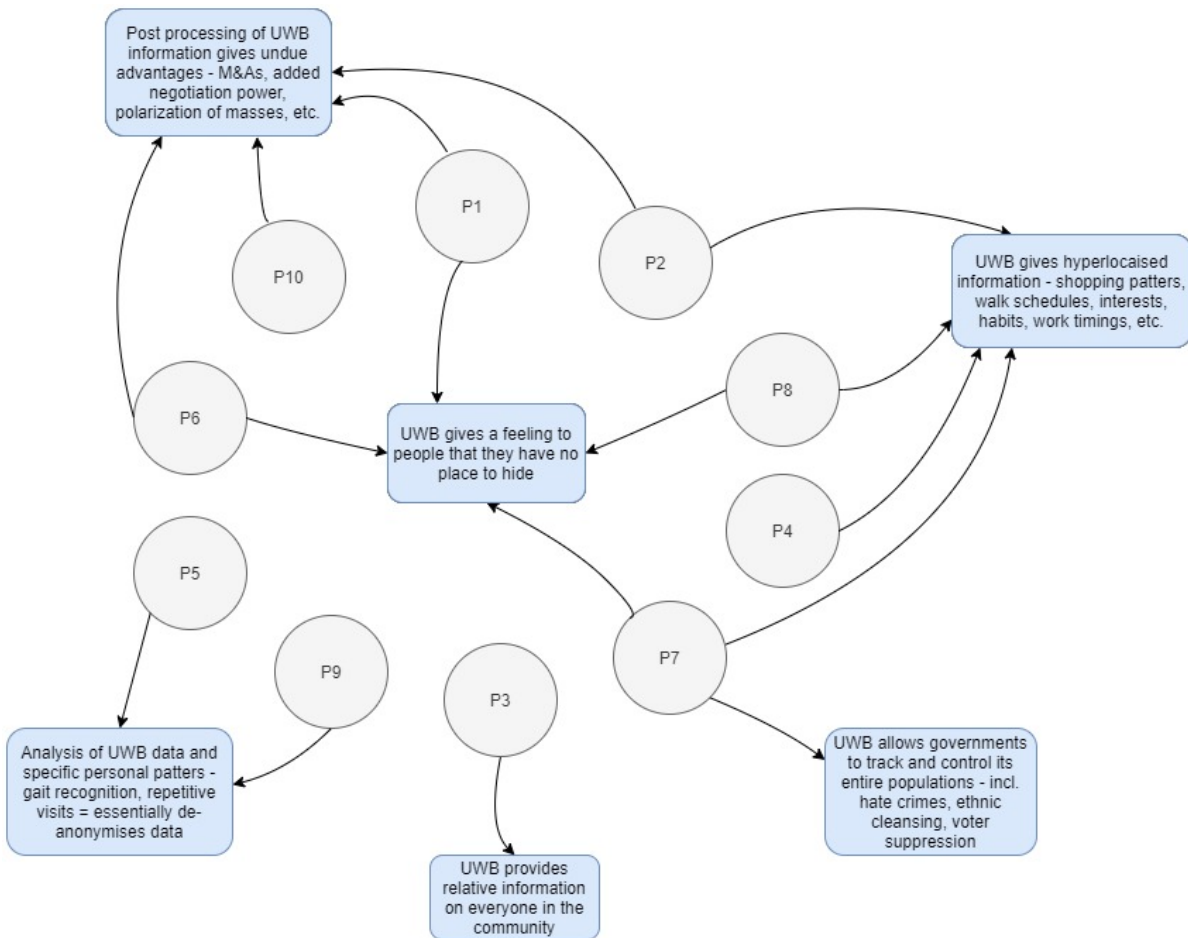


Figure 7.1: Surveillance privacy concerns thematic analysis

Surveillance privacy concerns were undoubtedly the biggest issues users saw with the integration of UWB. The foremost issue that was repeatedly mentioned through the interviews was the availability of hyper-localised data. Five users thought that Wi-Fi localization was very accurate inside buildings. They realised UWB incorporation further increases the possibility of this. All the users commented that:

This additional accuracy would increase the quality of services, but they did not understand why the increase in accuracy was required. Client information would not be anonymous anymore if such hyper-localisation becomes a reality.

P5 mentioned the possibility of gait recognition to identify the public. P2 mentions how this information could be used to piece together a complete client bio. This could involve the specific buildings that a person visits such as museums, libraries, stores, etc which could be used to provide personalised discounts and vouchers. These could firstly, push people into a specific interest while secondly, keep people within a social bubble. This would allow advertisers to learn if consumers react predictably. P6 believes that providing services based on location seems to cross a proverbial line and that services provided purely based on interests would help maintain trust in upcoming technology. Mobile phones companies have had chances to ensure customers do not lose faith in the product by making it even more invasive, but decided not to.

The second biggest issue that users highlighted was the fact that this would lead to consumers feeling that they were being watched at all times. P6 and P8 said:

"With the accuracy that current technology provides, no mobile phone user ever has privacy as there is always some setting that helps locate a person. Even though companies state that the information is secure, the very existence of this information is a loss of privacy."

Further, P10 believes that phones can be tracked even if the phone is switched off, something NSA of USA was rumoured to be able to do (Georgiadou et al., 2019). This may further increase the paranoia of people, making them feel like they have 'no place to hide.' P4 states that not all location information is the same. Location of how much time people spent within a store is acceptable but when it comes to public buildings or hospitals, the information becomes sensitive. People may forget to turn off their location based services which could reveal potential health issues people have based on which doctor they visit.

P1 and P9 further the concept of feeling conspicuous at all times by saying that they feel mobile phones can listen in on them. They provided particular examples of when they had conversations about a potential purchase, their search engines would subsequently show ads about similar products. This led them to theorize situations where the accurate location information and potential listening capability of their devices would be interlinked. They believed this is a big breach on privacy which on aggregation would provide an entire customer profile to mobile phone companies, government agencies and advertisers alike. P9 gives a conclusion by saying:

"At some point, nothing will be considered private the way technology is evolving."

P1 builds on this idea by saying that there are potential loopholes to regulations. Private and third party companies have several reasons to monetise our data in the future and just the presence of such accurate information makes it very probable. P3 worries that there is a possibility of someone getting all this information purely from the radio waves by standing in a crowded area with a frequency scanner.

P7 believes that the entire tracking of location information is society's way of keeping track of every single individual. UWB would allow government agencies to get information on people's location, the people they are in contact with, where they go everyday, whether they follow the norms of law-abiding citizens and of course, the relative distances between each other. This information is then shared with governments. This could then be shared amongst state allies and subsequently an entire network can be made on exactly where people are at what time and the granularity of UWB enables that. They believe that such information could be used to target people, citing examples of Uighurs in China or Palestinians in Palestine.

A relatively rare argument was made by P10 where they mention the manipulation of the public through location based services. They cite the example of the US and 'Cambridge Analytica which helped polarize an entire nation based on political ideas.' They believe that if companies only had to pay money to manipulate people, it would proliferate. They believe that the possible manipulation of the public is being understated right now and need to be kept in mind as newer technology comes to the fore.

7.5. Social privacy

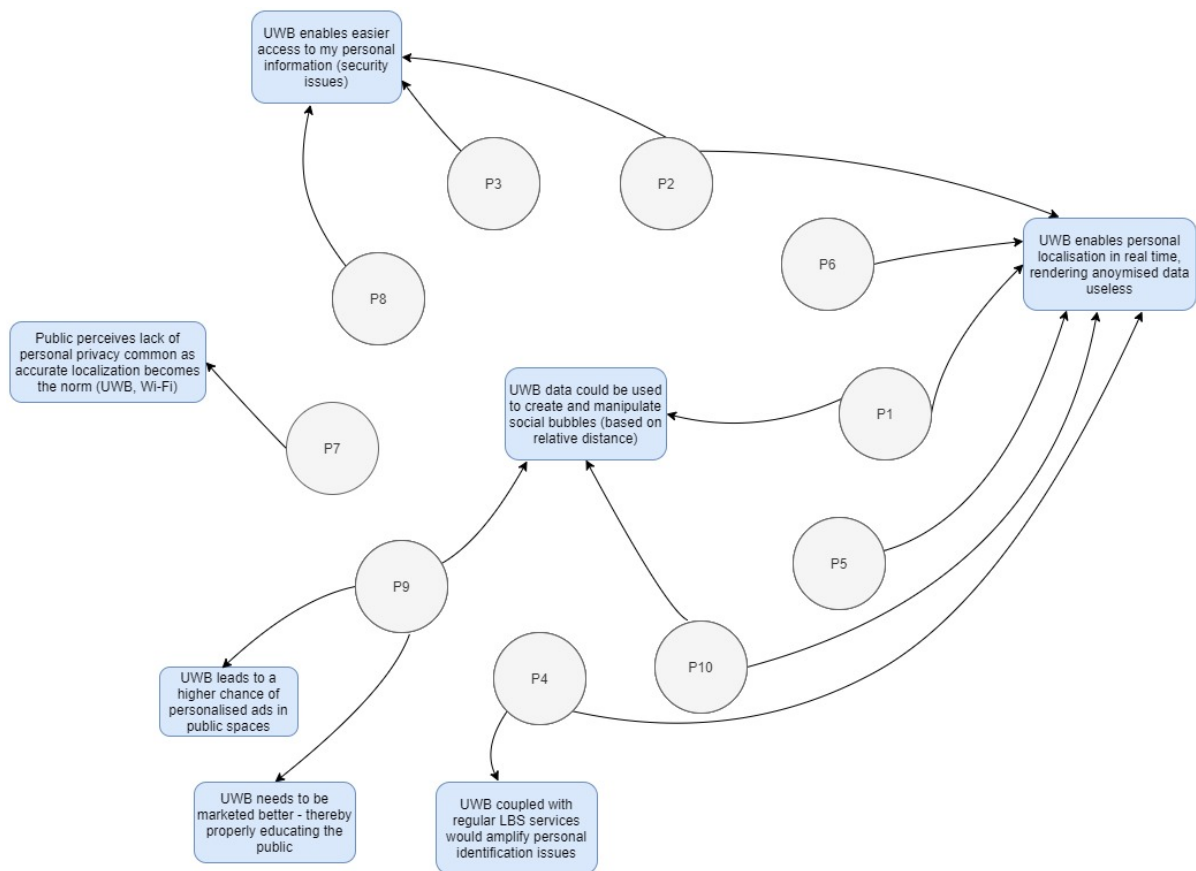


Figure 7.2: Social privacy concerns thematic analysis

The most pertinent issue when people were asked about social privacy lies within the 'Find My' network. Four of the users felt that their personal location would be easier to find out, either through other phones or through anyone with a frequency scanner. The second most pertinent issue brought up by three users was that the properties of AirTags and AirDrop allowed passers-by to retrieve personal information if they wanted to. P2 states that no technology 'cannot be hacked' and in the future the possibility of someone obtaining hyper-localised information about something is not a chance we should be taking. However, this seems to be more of a security issue than a privacy concern. P6 hypothesises that the 'spatial awareness' provided by AirDrop could be used by people with malicious intent such as pickpockets.

Four users further bring up the possible issue of companies using relative distance information to hypothesise potential characteristics of people by placing them in bubbles. Users P1, P9 and P10 feel that this can lead to targeted advertising which could happen in public places such as the 'Hague Centre' where there are big advertising screens. P5 believes there is a lot of trust being placed in companies to keep all this information private. There is a lot of potential usable information from passive information that the 'Find My' network could provide. Users may not realise how harmful passive information could be to the general public and influencing public perspective.

User P10 believed that the possible influence that companies can have on the public needs to be highlighted more. The current generation is getting mobile phones earlier which means their entire location history is tracked ever since they are 10 or 11 years old. This is at a stage in their life where they are very impressionable. As mentioned before, user P10 believes that private companies are influencing politics and if they could influence the younger generation in any way, it would be detrimental. User P7 had the most to say on the lack of understanding users have on the technology and how this is the biggest issue. They mentioned how Wi-Fi localisation is becoming the norm and in the near future, UWB will. People will initially be asked to give permissions and as it becomes the norm, there is no going back. People will feel left out if they do not

accept. Secondly, they explicitly state:

"A small minority of people know privacy nomenclature or what cookies mean. Gaps such as this allow accurate personalisation of information across different websites and locations, rendering anonymised data illogical."

From a technical perspective, P4 feels that UWB localisation is not much different to Wi-Fi or GPS. People were located based through that and will still be able to. As long as companies decouple UWB functionality from other location based services, the onus would fall on the public to stay consistent with their settings. P9 feels that a functionality such as AirDrop should only show contacts in the nearby vicinity, thereby ensuring no stranger's MAC address shows up on your phone.

Of all the users questioned about social privacy and whether AirDrop/ AirTag leads to a loss of social privacy, only two said there is no inter-personal issue. They state that users have bought the phones and/ or the AirTags which means they consent to this increased functionality for their privacy loss.

7.6. Institutional Privacy

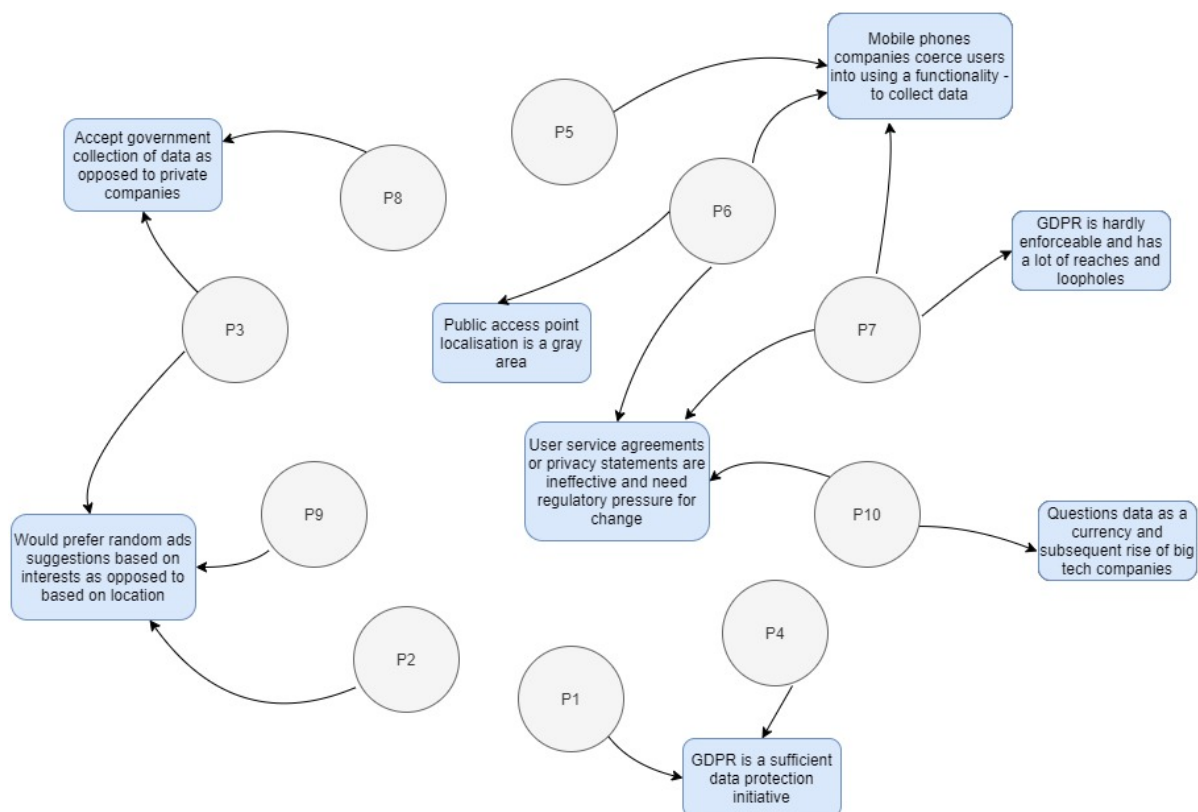


Figure 7.3: Institutional privacy concerns thematic analysis

When questioned about institutional privacy and GDPR, all the users agreed that the collection of information by private companies is a breach of privacy. Their main interests are monetary goals, which does not favour consumers. The biggest concern for users here, shared by four of them was the personalisation of advertisements or services. These users felt that suggestions made on interests such as which clothes store they preferred or which cuisine they prefer on their home delivery app are acceptable. They believe that stronger regulations are required for advertisements that are made based on location. Four interviewees also observed that some technologies are just forced onto people as they become the norm. P7 cited an example of how:

"All services on the Google Store can work without location information but the app repeatedly asks you to integrate location."

They feel that it is this coercion which need to be checked and possibly regulated.

P8 states that they appreciate the transparency that is given to the user when an app is downloaded of the Apple App store. It has a number of settings that allow the user to select what information is saved on them. They believe that this is a step in the right direction which they hope reduces the need for any background information to be collected without the users' knowledge. P6 however, believes that there is a possibility for UWB localization to work similarly to the loophole Wi-Fi localization fits into. If this done with UWB, it would allow companies pinpoint accuracy, something that they deemed unnecessary. They further state that the long list of agreements that a company makes a user read is counter-intuitive to actual privacy protection. Companies do this just to push users away from actually protecting their data by making them read long and incomprehensible service agreements.

The biggest two contributors to this question were interviewees P7 and P10. P7 states that cookies are an outdated service that help companies identify individuals from their online activity and that UWB may become the same for location information. They further believe that only 10% of the population actually understand what cookies are it is the 90% of population that the mobile phone companies are targeting. Further, P7 stated that it costs only 50 cents to get someone's location information from the black market so what is stopping mobile phone companies from using this easy to access information for their own personal gain? They further state that GDPR is a good sentiment for users, but it is 'hardly enforceable' which gives companies some leeway. Interviewee P10 voiced their concerns by asking:

"How is the general public is okay with giving up so much of their personal data without actually knowing what it is used for?"

Users may not have time to go through privacy options for every website or application which is leading to companies getting more power through loopholes or coercion. They believe that this is power that they have gained through their technology, through no one's approval and the only way to stop this is through proper regulation of data collection.

From all the interviewees, only two trusted the GDPR to keep their information safe. P4 cited the example of Gmail where users' emails are read to occasionally help provide predictive text. This is a very helpful feature where there is an algorithm that learns a personal mailing patters and helps improve the 'mailing experience.' UWB could be used for similar circumstances when it comes to locations. P1 cited the example of how CCTV camera footage cannot be seen by companies within the EU unless they had a reason to. They believed that this similar ideology would be carried out for location information collected by companies, which employ privacy officers to ensure the entire data collection is secure at all times. They believe in the validation process for collection, storage and usage of user data which enforces user privacy.

7.7. Privacy protection suggestions

Six interviewees lobbied for two big requirements to protect privacy: awareness among users and increased transparency by private companies. These users felt that there is not enough knowledge amongst users before they buy products. P2 feels this may be because some products are not marketed right because of which users do not understand the full functionality of new technology. Since none of the interviewees knew that UWB was incorporated into mobile phone, it seems a good hypothesis to make.

Additionally, interviewee P8 stated that these options should not be used to coerce people into accepting long unreadable privacy agreements. They believe that reduced functionality of services is a viable way of using new technology, if that is what the user wants. They should not be coerced into using something, if they feel that they are not being given an option. They cite the example of cookies when you visit a website:

"There is always one set of cookies that I cannot deselect, which further means I cannot use a service. Users need to be informed that their data is the price paid for any free content, whether it be personal interests or even data location."

A distinction needs to be made and regulators need to consider this. P5 further builds on this by saying companies need to invest in making data collection options as customizable as possible. This, they believe will not happen from the industry itself, but something regulators should consider proposing.

Consequently, P6 builds on this idea by stating that:

"I think ideally we should be owners of our own information. You have your own ledger of information, which is updated every time something significant happens like visiting a new location physically or even a website."

You own it locally and only when you accept to let someone see the ledger by sharing specific information, it would be okay. This effectively treats data as a currency that you can share the latest version of. Gener8 is UK based company looking into this idea where personal ledgers are made of a single user and if they want to share this data, the company would have to pay some amount for it.

Interviewees P9 and P10 chose more overarching perspectives to handle the issue of privacy. P9 stated that laws are being overridden when it comes to public privacy and this is a big concern. Regulators need to promote an ethical code of business for big tech companies. They believe that companies need to realise that they have immense power with huge amounts of data and it should be their responsibility to keep it safe. This would be an industry-wide ethical agreement or code, something that they should all aspire to uphold. P10 approaches the issue of privacy from a more holistic angle rather than just consider technical issues and forget the 'big umbrella' of social issues. They state:

"Any new technology should be evaluated from every possible perspective and in this case of accurate localisation by UWB - privacy, probability of psychological issues, political polarization, etc."

Interview P7, when questioned on their philosophy to increase privacy protection, provided a 4 step plan. Step 1 includes breaking up big tech companies such as Google, YouTube, Facebook. These companies have user data interlinked with a single account and if a company has made a profile about people, there is a high possibility it is one of these. Having smaller bits of information distributed amongst smaller companies would ensure no personalised profile is made about a singular user. Step 2 includes regulators forcing the public away from cookies as it is an outdated method of data collection. Step 3 involved regulators incentivising better systems of web-browsing or technology usage. P7 believes that there is too much the public needs to be informed about and that if it was left to them, big tech companies would always benefit. Regulators need to ensure they take the initiative by promoting authenticator apps, Brave browser which increases control over cookies or Nym network, a Virtual Private Network (VPN) that provides a full stack privacy solution.

7.8. Discussion

In this section, the similarities and differences between the statements given by users and experts is discussed. This provides the reader a comparative study on whether the public's views align with experts. Consequently, it tests whether users are technologically adept to understand the potential issues of a new technology.

As the interviews progressed, users deviated from privacy concerns strictly based on the technology. This can be seen in the difference of privacy concerns from the thematic analyses conducted for surveillance and social issues as compared to institutional issues. When talking about social/ surveillance issues, users mentioned issues based on how UWB can create social bubbles, profile customers, obtain hyper localised information, etc. However, when talking about institutional privacy issues, users brought examples from BLE/Wi-Fi but also issues with cookies and browser notifications. Users realised that the main selling point for mobile phone companies to integrate UWB would be data collection, which showed that users are interested in the kind of technology they consider. From the initial Google Form sent across, eight interviewees said they were interested in privacy and considered privacy a modern-day issue. The other interviewees claimed that the number of services that are present in the 21st century would only be possible if there was a reduction in user privacy. They agree with Mark Zuckerberg's statement: 'Privacy social norm is just something that has evolved over time as people tend to share more personal information with other people.' While this may be the case, people have to bear in mind there is difference between voluntary disclosure and information gathered from usage of services. Additionally, both groups considered surveillance issues to be of highest priority and most apparent.

The biggest similarity was that mobile phone companies can use UWB to personally identify specific people from their localised information. This stems from the surveillance concerns that both groups could identify. They felt that these concerns are of highest priority and an increase in accuracy of location information reinforces the idea of never being able 'to hide.' It makes it easier to build profiles of users, get their daily schedules and understand general characteristics of a person. Both groups questioned the need for the added granularity of UWB location information. They said that:

AirDrop, AirTags and GPS work well with the current hardware on the phones, with UWB trying to fill a functional gap that does not exist.

A more surface level discussion on mobile phone companies showed that both groups seemed to trust Apple more. Three users stated that the Apple ecosystem is quite secure for outsiders whereas PE3 stated that the general business model of Apple did not revolve around selling/ using customer location data. However, when discussing Android, both groups felt the link to Google gave them more reason to question the usage of their location data. Google has historically been a company that has a number of different services, where people use a singular email ID across all of these. This increases the granularity of information that Google can use. Additionally, discussions were held on the passive information available through AirTags or the Find My network. A majority of the users (50%) and the three privacy experts shared concerns on what passive information is available through this - relative distance or shared interests amongst users - and how granular this data was. They wanted to understand what type of information would be shared through the use of this new technology, where this was saved and how mobile phone companies handle this data.

Another major concern that was shared by both groups was the lack of knowledge of the regular user. All users agreed that they tried to keep themselves as educated as possible on potential privacy concerns but sometimes, they skip over cookie setting or privacy statements for lack of time. If this was translated to then general public, they believe about 75% of the population does not actively try to protect their privacy and these are the people companies are targeting. Further, a majority of users and privacy experts believed that users were eventually coerced into turning on a setting that they did not like. They cited examples from the weather app that worked as intended without turning on Wi-Fi localisation (PE3) or from the Google App Store that keeps repeatedly asking you to share your data every time you open the app (P7). They state that the probability of a user sharing all of this information is much higher than an individual actively changing his settings to protect his privacy as much as possible. Further, they believe not enough is being done from mobile phone companies to actively inform users. They cite examples of how UWB wasn't mentioned during the Apple keynote and that it is rarely mentioned on the website. This shows clear marketing issues that regulations need to tighten up.

The final concern that was shared by both groups was the coupling of UWB services with other location based services (LBS). PE2 and PE3 hypothesised scenarios where if GPS was linked with UWB, mobile phone companies would get contextual information of each device at all times. They would be able to locate them on the streets, where they are going, how fast they are traveling, information which would be readily available indoors as well. This functionality needs to be decoupled so that only very specific applications that require UWB, would ask for it turned on. PE3 already stated that there were some situations where UWB would be turned on when other LBS were turned on. This cannot be the norm in the future.

The biggest drawback amongst users was that they often mistook privacy concerns for security issues. Experts could make a clear distinction on how security refers to the defence of digital data/ information from malicious threats. These include being able to hack a phone from a public access point, people using frequency scanners to follow a phone user or sending malicious code to anyone within the Find My ecosystem. Users identified a number of security concerns as privacy concerns until the interviewer had to direct them. The lack of understanding of privacy from a user perspective is something companies and activist groups need to prioritise. Users need to be educated on the difference between privacy, security and what is classified as a loss of privacy versus a breach of security.

However, a rather positive difference that should be noted is the perspective users have toward protecting their data. When experts were questioned on how privacy can be protected, they gave options that were industry centered. These included a privacy framework for software designers, ethical codes for consortiums, technical clarification, user education or robust policies. Users comparatively, chose to give increased control of data to themselves. These involved the usage of a personal ledger of information that would be saved on a user's device and only shared when needed (P6), incorporating the idea of blockchain within the Find My ecosystem (P8) or the use of authenticator apps (P7). This shows that there is a stark difference in how industry experts and users view privacy. Regulators may benefit by allowing users higher integration into decision making processes. Additionally, users also presented social issues that arise due to the collection of personal data. They mentioned situations of manipulating the general public while citing examples of political radicalisation, psychological issues and generally pushing people into social bubbles. This shows how users realise that experts and regulators may not consider these problems when only technically testing a new technology. A more holistic approach is needed for new technology and some users think this should become the norm of policy regulation.

8

Privacy mitigation strategies

User and experts interviewees, at the end of each interview were asked if there should be more done to protect privacy and how. Different strategies and viewpoints were communicated across. The most significant suggestions are presented and grounded in literature in this chapter. Additional literature is used to provide any supplementary strategies that were not mentioned by either of the interview groups. These mitigation strategies will be broken down into two domains - technical and societal. Technical mitigation strategies involve any change in software or mobile design to protect the privacy of users. These involve changes in how users use specific applications or decide to use their mobile phones. Institutional mitigation strategies refer to any changes in the process by regulators or governments by keeping the users' best interests in mind. However, prior to this demarcation, there is an overarching strategy that cannot be distinguished into technical or societal but rather as a 'socio-technical' solution: privacy-by-design.

8.1. Privacy-by-design

A famous idea to preserve privacy adopted by the EU while drafting the GDPR was 'Privacy by Design (PBD).' While this may be incorporated from a software perspective, it may also make sense to include it from a hardware perspective. UWB is essentially the integration of hardware into a mobile phone which already included other technologies that provide locations. So the question remains as to why it needs to be integrated. PBD could be the approach that characterises proactive work rather than reactive measures (Cavoukian, 2011; Cavoukian and Dixon, 2013). There are seven foundational principles of PBD:

1. Proactive not reactive; preventative not remedial - PBD comes before any major privacy issue can be evaluated. It follows along the lines of GDPR where organisations are meant to be proactive when it comes to testing their hardware and any subsequent possible privacy issues. This would mean that while incorporating any new hardware or designing a new application, companies ensure that they think about the possible privacy issues and not just the advantages. This requires a change in enterprise 'state of mind' which includes the leadership and overall culture of the organisation.
2. Privacy as the default setting - Privacy should be automatically protected in any given IT system or business practice which involve mobile phone companies or any third parties making applications. No action must be required by the individual to protect their privacy, it is built in by default. This is something Apple may need to consider as when UWB was first introduced, users' locations were broadcasted by default before a change was made in the settings (Krebs, 2019). Examples of such policies include least privilege and need-to-know. Least privilege refers to the design principle of a system where minimum user data is required for the entity to perform its function. Need-to-know refers to the isolation of specific information of the data to use that resource and nothing more.
3. Privacy embedded into design - It is very similar to the previous principle where privacy is integral to the system without diminishing functionality. Privacy is not bolted as an add-on as an after thought, it is the primary value for designers and developers. While this may seem like a duplicate of the previous principle, this refers to software security assurance which seeks to decrease the risk of security vulnerabilities throughout the information system life-cycle. This means that throughout the life-cycle of a

user's input, their personal data collection to the query being handled/ service being offered, privacy is fundamental. This may mean regular code reviews to see if there are exploitable flaws, rigorous security testing through stress testing or comprehensive threat analysis.

4. Full Functionality - PBD seeks to accommodate all legitimate interests and objectives in a win win manner, not an approach which depends on trade-offs. Few examples of these are location information vs specific personalisation, convenience vs security, simplicity vs security. In order to overcome these issues, companies must ensure they seek to understand all the possible dichotomies, evaluate these conflicts, seek effective compromise, design create solutions that may involve restructuring the application architecture and finally, be willing to invest in these changes.
5. End to end security - PBD seeks to ensure security is embedded into the concept of privacy protection. They are a number of privacy breaches of big corporation, seen on the news every year. PBD seeks to ensure that all the data is securely detained and eventually destroyed at the end of the process, in the correct manner. Cavoukian and Dixon, 2013 mentions the concepts of database security and identity access management. The former refers to databases being protected where unauthorized entry and alteration is not allowed. The latter refers to the security discipline that enables the right individuals to access the right resources at the right time.
6. Visibility and transparency - This seeks to assure all the relevant stakeholders - users and employees - that the corporation is operating according to the stated promises and directives. It ensures that everything is transparent and visible to all parties involved. This can be done by disclosing security standards and possible issues that the company is facing. Additionally, external evaluation and validation of the security systems by regulators can help increase the trust users have.
7. Respect for User Privacy - PBD requires developers, designers, architects to maintain the interests of the individual by offering privacy defaults, obtaining prior consent and providing user-customisable options. While companies and employees may be tempted to monetise or post-process user data extensively, they should hold users' interests to the highest priority as for other services, they may be users themselves. They should ensure data minimization, effective flow of information and personal privacy upholding codes of conduct.

PBD essentially informs and tries to ensure developers include privacy in every stage of the development process. Developers here include app developers, mobile phone designers, website developers, etc. It can be assumed that the forthcoming technical and societal approaches to privacy mitigation stem from a PBD mindset.

8.2. Technical approaches

One of the most researched methods to hide a user's personal location is by incorporating the method of obfuscation. It is defined as the "degradation of quality of information being sent to the location based service, in order to protect the user's privacy" (Ajam, 2010; Gellersen et al., 2005). The type and accuracy of the location can be varied depending on the application as it may only need the city or postal code of the mobile, rather than centimetre accuracy. There are two ways to achieve this deliberate misinformation of location data: inaccuracies or imperfection. Given the example of a person whose current location is known, in the form of georeferenced x and y coordinates. With current technology, this is quite easy to obtain, more so with UWB. Using the concept of inaccuracy, the user may provide their wrong location information by changing the settings within the specific application. Imperfection is the concept where a higher level of location is provided rather than the exact point. The user can reveal that they are located in South Holland but not Delft exactly. Or they can say they are located in Delft, but not the exact street address. These scenarios involve downloading a separate application to do so, but it provides the user full control over their location rather than the application obtaining it. Gellersen et al., 2005 explains it in detail with the idea of proximity queries which correspond to searches such as 'where is the nearest sushi restaurant or where is the nearest football field.' While this may give away interests and location of the person, obfuscation can help the user retain control over their location. Therefore, the specific application can get one or the other - interests or location. However, the user can choose how much information they want to give based on how much of the service they want to receive. They can toggle their settings to also include street address if they are using their map application but the choice rests on the individual user.

The location anonymiser method or k -anonymiser aims to ensure that the third party providing location based service or any adversary that intercepts communication from a mobile cannot link this information to a specific user by masking the user's location (Huda et al., 2013; Ajam, 2010). For this, a trusted third party or software developer generates a cloaking region for a specific location, for example a hospital or particular mall. The cloaking region is then grouped with k number of requests from multiple users and sent to the LBS provider at the same time. There are two scenarios here where either there are actually k number of users in the vicinity using this cloaking application or just one user who can unilaterally change the value of k to create dummy requests and simulate users. The results from the LBS are then filtered by the k -anonymiser application and only the queried result is sent back to the user. However, there are two main issues with this method. The first is the k -anonymiser application itself. It can store a set of requests made by each mobile user and exploit this data (Ajam, 2010). A solution may be to ensure these applications are fully paid so that the company does not seek additional monetary gains by selling you data. The second is the dimensionality of data. High dimensionality such as time series data is very hard to anonymise as the person is continually providing identifiers or multiple data points (ND, 2017). Thus, user may want to use the anonymiser on a need-for basis and not all the time.

Integrating the concept of cryptographic techniques for storing and sending sensitive data may be an innovative approach to hiding identity. The concepts includes categorizing users' data into two terms: 'public' and 'private' data (Sujithra et al., 2015). The former includes information such as which applications are being used or user's current search or social media usernames. The latter can include information pertaining to location data, search history for a week or scheduled meetings. Essentially these are termed as a client's confidential information. Any time an LBS requires location information (or characterised private data), it must be transferred in an encrypted form. A secure hash is sent along with the user's request. The LBS has to process the request without having access to identifying personal information (Ajam, 2010). This means that the company providing the service receives the client request and only the public data that has been provides. An example could be a user searching for a coffee shop near the Rotterdam central station. Google Maps obtains information that a user whose name and place are unknown is asking for a coffee shop in Rotterdam. The answer is received without any personal information revealed. This is done by breaking down the search into the two aforementioned categories of private and public data. The former includes the device ID and location of the user whereas the latter includes their search query. Sujithra et al., 2015 states that the receiver shall only receive the decryption key for public data so that they can process the query. However, research show that low-powered mobile devices are incapable of doing this continuously which is why these techniques must be used only for highly sensitive search requests.

Dummy-based approaches generate dummies and send fake locations along with the user's real location to the service provider (Kang et al., 2020). The approach introduced by the author generates decoy trajectories that follow real-time road conditions such as traffic jams. It can prevent adversaries but also LBS from knowing which city or country by deploying various decoys at once. It also guarantees the user's experience and quality of search results without extra steps. The authors have designed an application called 'Move-WithMe.' It consists of five main components which preserve user privacy. the 'Decoy Simulator' which takes movement patterns and social profiles as inputs to generate real time trajectories of the decoys. These decoys are constantly running in the background even when the user is not using an LBS. 'Request interceptor' intercepts the request from the user, checks if it contains location information, generates several requests from the decoy and sends them to the LBS together. 'Service Monitor' keeps in check how often their location is needed by a certain LBS and notifies the user of its usage. 'Location recorder' is the component that keeps in charge the storage of both the dummy locations and actual location of the user. Finally, 'Trajectory display' is a function for the user that allows them to visual dummy trajectories and change them if they feel they are too repetitive. The application, on testing, introduces minimal overhead on the response time, data usage and battery consumption. However, users have to bear in mind that this application must be regulated as well, so that personal information isn't sold by the application owner.

The aforementioned application is designed for outdoor localization only. Subsequently, Zhao et al., 2020 designed a 'Location Preservation Algorithm with Plausible Dummies' which was the first successful attempt towards Wi-Fi localization privacy preserving using dummy approaches. They state that historically, dummy techniques are hard for Wi-Fi localization because they are susceptible to spatio-temporal correlation attacks. These attacks refer to how these Wi-Fi routers can first obtain the centers and radii of users in the vicinity. Depending on the time stamps and the overlapping of these centers, the final location of the user can be known.

Privacy can also be protected by traditional access control mechanisms triggered when certain conditions based on a user's physical location are satisfied or required to provide a service (Ajam, 2010). The access control matrix is a two dimensional matrix representing subjects on the rows and objects on columns (Tawfik et al., 2015). The access control paradigm seems most applicable is the "Access Control List." Here columns contain objects such as information shared, system time, control of information such as read-only or write-only and location coordinates. The rows contain the different users in the vicinity with identifiers such as device name or MAC address. The user's physical location has to be securely verified to meet certain criteria and access to a user's information can only be obtained when these criteria are met. Examples could be when the user allows information to be read-only or if the location coordinates correspond to a certain shopping mall. The access granted to the LBS can then be limited to only certain objects and controlled by privacy settings. Continuing the example of the shopping mall, the user may only want to receive advertisements related to women's clothing. They can set the preferences on the mobile device, only certain information is shared and if an LBS matches the criteria, they can push these advertisements across. If they do not meet the criteria, access is denied. However, this is unrealistic on a large scale.

Dwork and Roth, 2013 introduces the concept of 'Differential Privacy.' It states that: 'Differential privacy (DP) is a strong, mathematical definition of privacy in the context of statistical and machine learning analysis.' All big tech companies or service providers aggregate or need to aggregate data to get a more holistic understanding of a certain customer so that they correct services that can be provided to them. The working idea behind DP is that every company analyses or post processes the data that they receive. This includes shopping patterns, online purchases, interests, location information, device ID, etc. There is a certain overlap in what the researcher defines as 'general information' and 'private information.' The former relates to information of the general public when for example, a certain number of users enter a shopping mall every day. The latter relates to the information of a specific user based on his previous purchases and interests. DP states the information obtained from the people will be analysed as a whole rather than including users one by one. This guarantees that the analysis can be carried out for the general public, thereby improving their experience and quality of services. It ensures that a person's private information remains private and that they cannot be individually targeted based on their habits (Nguyen, 2019). However, it does have few drawbacks. The sharing of public information means certain insights can be drawn from the public as a whole. It also means that this public information is available to all the parties that want to process this data and while some users may not want this to be the case, they will have to agree with the approach.

Martin et al., 2019 and Becker et al., 2019 state that the inherent ideology of MAC address randomization may have issues but there seems to be a quick fix for it. In general the frequency of 15 minutes with which MAC addresses are rotated is the substantial flaw. If an adversary within the range of devices tries to keep track of a certain individual, it is not hard to see when a certain MAC address trails off and a new one starts. It is quite easy to link two subsequent randomized MAC addressed because the the rotation sequence is so infrequent. Additionally, it seems that it happens every 15 minutes so an adversary can predict it, almost like clockwork. The idea presented within the two research papers is one of two options. The first is that the every frame should have a new randomized MAC address. However, if this is too hard to calibrate or code, then devices should have a shorter period of rotation. The current rotation clock of 15 minutes is too predictable and hence, the new rotation should not have a fixed timer but rather be done randomly.

8.3. Societal approaches

There is a philosophy from individualists who frame data privacy as a commodity that can be exchanged on the market place for a fair price, that the person deems correct. Jaron Lanier, a famous computer philosophy writer believes that users should be incentivised into giving data away rather than hoping to lock it up. He states that: "I believe in markets. Taking data and using it to manipulate people is not a real market. Let's admit that data is valuable, pay people for it, motivate them to make it better. Let's get out of the manipulation business." These views have been shared by the Oxford-based Digital Rights to the City group who declared that "we will no longer let our information be produced and managed for us, we will produce and manage our information ourselves (Shaw and Graham, 2017)." This idea was further defined by French think-tank GenerationLibre who sought to extend the private property paradigm to personal data as well. They set out to give users (Landreau et al., 2018):

1. 'The possibility for e-citizens to negotiate and conclude contracts with platforms (possibly via intermediaries) regarding the use of their personal data, so that they can decide for themselves which use they

wish to make of them’

2. 'The ability to monetise these data according to the terms of the contract (which could include licensing, leasing, etc)
3. 'The ability, conversely, to pay the price of the service provided by the platforms without giving away our data’

This first point is shared by one of the users during their interview, with the idea of having a personal ledger and choosing to share parts of it whenever the user feels necessary. The ledger could be broken down into multiple categories such as clothing interests, sporting interests, vacation destinations, education, etc. Whenever the person visits a website or purchases a mobile phone, they can choose to give away a certain category that is most relevant to the website. This may seem time consuming but it is not very different from the current concept of cookies. Users can periodically revise what information is contained in each category. This helps them control what information they want to give away and restrict the rest.

The second point is shared by a company called Gener8 Ads which is revolutionizing the browser industry. It allows for users to choose which data they want to give and when. This allows for their ads to be personalised into what they actually want rather than suggestions which seem right. Finally, it rewards the user for any data that is shared about them (Gener8 Ads website). They can then redeem these points at online webshops. This idea of compensation is backed by research conducted in Xu et al., 2009. The author, in their findings, states that users perceive compensation as a reasonable input for sharing their data towards push-based advertisement methodologies. However, a major limitation is ensuring the contract between users and websites/ companies are legally binding. If any breach of contract is suspected, there needs to be suitable courts that users can take their claims to.

The third point seems to be the most controversial one as it essentially takes away the ability of private corporations to even access our data. The user pays a one time fee for an application or mobile phone, after which there is no transfer of data to the company to 'improve' user experience. Regulators need to ensure that if someone has paid for a service, the company or developer has been paid for their service and it is a breach of privacy if data is still collected without the user knowing. There needs to be stricter laws surrounding these types of business models.

The chairperson of the German Social Democratic Party framed the 21st century problem of big tech companies as: "Empires like Google and Amazon cannot be beaten from below. No start-up can compete with their data power and cash. If you are lucky, one of the big Internet whales will swallow your company. If you are unlucky, your ideas will be copied (Georgiadou et al., 2019)." Their solution is a Data-for-all law. The constituents would be that the dividends of the digital economy must benefit the whole society. As soon as an internet company achieves market share above a pre-defined threshold, it will be required to share representative, anonymised data sets with the public. Using these, smaller companies and start-ups can infer consumer behaviour and develop their own ideas for the marketplace. This essentially allows for there to be competition in the market but also allows for data to belong to the general public. There are a few drawbacks to this with the most prominent one being that data is still available for companies that want to target particular individuals. But this allows users to know that there are smaller companies benefiting from their data and there is a possibility for specialised services on the market. Another limitation that can be assumed is that there will be significant media and public backlash. The rules of engagement for effective data sharing must be defined under enforceable regulations. This way smaller companies that provide personalised services on the market increase while ensuring citizens know exactly how their data is being regulated and shared.

The sentiment of breaking up big tech companies stated by user P7 was shared by Warren, 2019. Companies such as Amazon, Google and Facebook, which operate majorly on user data share a monopoly in the market. The big tech companies have too much power in the economy, society and democracy as well. They do this by using private information for profit and thereby, have tilted the playing field against anyone else. They have broken down competition in any market they enter. They employ two main strategies to do this (Warren, 2019):

1. Using mergers to break competition: Facebook purchased fellow social media applications such as Instagram and WhatsApp, Google did so with a maps application called Waze and the ad company DoubleClick. This essentially blocks competition in the market which regulators have essentially allowed to pass through.

2. Using proprietary marketplaces: Examples of this include how Amazon crushes competition by copying goods of small business and selling them in an established market of the Amazon website. Google does this within its search engine by promoting its content in its algorithm, while simultaneously demoting results from competitors. An example includes how Google promotes its restaurant ratings over Yelp.

While the second point is not related to data usage, the first is heavily facilitated by collection of user personal interests. Once a big tech company realises that some services are preferred by users, they can essentially 'bully' smaller companies by buying them. This seems to be a repetitive cycle that seems to be possible by the collection of user data and their interests. Warren, 2019 has two potential solutions for this. The first is passing legislation that designates large tech companies to be designated as 'platform utilities' and broken apart from any participant on that platform. These companies essentially provide users with an online marketplace or a means to connect third parties. They should be unable to share data gathered from the marketplace with any third parties while structurally separating from other parties on the marketplace. This would mean, for Amazon, they would be unable to sell any products through the Amazon website but only become a logistics company. The second solution is to appoint regulators to reverse anti-competitive tech mergers. From a privacy protection standpoint, the increase in the number of mergers means there is facilitation to aggregate our data across services. From a business perspective, this would put pressure on big tech companies to be more responsive to user concerns as they would have various competitors to compete with.

Anti-trust laws have been drawn up to ensure no company gets big enough in the market that it essentially 'bullies' its competitors. However, Khan, 2017 argues that traditional anti-trust laws are not fit for today. These laws were primarily based on competitor price and output. Traditionally, monopolistic behaviour results in price increase however, the current generation of big tech companies have services that are free or cheaper than competitors. These companies are so much larger, employ bullish tactics as shown in the previous paragraph and essentially undercut competitors. Current doctrine fails to understand this type of predatory pricing and integration across distinct business lines (Khan, 2017). An example of this is how Amazon, which gained prominence and is now the global leader of online shopping, decided to start their streaming service called 'Amazon Prime' and gained a large market share of online audience instantly. Such issues are increased in the context of online platforms for two reasons.

1. The economics of online platforms allows companies to prioritise growth over profits. Under these conditions, predatory pricing becomes increasingly likely which eventually converts growth into actual profits, which current laws treats as implausible.
2. Online platforms control the essential infrastructure on which their rivals depend. This role allows these companies to exploit information collected on companies and users alike, which eventually undermines the former as competitors.

There are two possible solutions to these issues. The first involves governing online platforms through market share. This means that companies are evaluated based on the market share they possess, for example 40% and if in the future this translates into achieving scale economics by reducing prices, this should be regulated. Additionally, the author shares Warren, 2019's concept of preventing vertical integration of big companies buying out smaller competitors thereby obtaining huge amount of customer data and effectively controlling the entire market. The second solution is regulating monopolistic companies as such. With the assumption that some big tech companies have gained the biggest share of the market, the author proposes a non-discrimination policy similar to the early 1900s. This approach permits a company to maintain its multiple lines of business but not allowing them to discriminate against companies using their platform. This effectively translates into common carrier obligations - requiring platforms to ensure open and fair access to other businesses - thereby providing them competitive rivalry. Regulators should ensure Amazon cannot copy products on their websites or Facebook copying ideas from other social media applications.

Quest and Charrie, 2021 states that a national tech regulator that works alongside or incorporated into the data protection authority of each country, is needed. This could be not just to regulate anti-trust laws but understand how new technology/ innovations affect users from a privacy perspective. They can have a regulatory regime with nationwide statutes and clearly defined rules of engagement. Quest and Charrie, 2021 further defines the concept of tech regulators. They need to understand their regulatory scope by defining what is within the regulated perimeter, what is outside, what technology they would inspect and what industries they would operate in. For the EU, a new regulator working jointly with the CEPT or ETSI makes the

most sense. They would focus on three overarching objectives: safeguarding individuals and society from maltreatment; promoting responsible innovation and robust competition; and establishing understandable and consistent parameters for data privacy and monetization. These can be reinforced by metrics that are robust in the face of ever changing technology. They should not have any affiliation to any company and must be knowledgeable about industry tech standards. They must form statutes that individual companies have to comply to. Quest and Charrie, 2021 further mention two potential recommendations to facilitate proper functioning of these regulators. The first is prioritization of activities based on risk. Tech companies consistently introduce new apps, software and integrate newer hardware (such as UWB) consistently and there is a chance cash-strapped regulators do not have enough staffing to properly enforce regulations. The regulators should use a risk-based approach to rank the plethora of potential threats and prioritize the companies that put the most people at risk. The degree of intrusiveness should be commensurate with the potential threats a company poses. Therefore bigger companies may require dedicated in-house supervisory teams while smaller teams can oversee start-ups. The second recommendation is making supervision digital by default. Replacing quarterly reports with platforms that permit regulators to pull information related to key risk indications from companies' systems directly, regulators can monitor and regulate companies more efficiently.

A big concern among users was the length, content and reaffirmation of privacy statements when it came to applications or websites that required user data. Privacy policies usually write their policies in legal terms which the common user finds hard to comprehend (Nicole, 2021). Even though the GDPR and Privacy Directive prior explicitly mentioned that privacy policies need to reduce legal jargon and ensure the common public can fully understand what is asked of them, it remains a major issue. Transparency should remain the ultimate goal of privacy statements. Further, when it comes to the practice of data sharing, cookies that are shared with third parties are not explicitly mentioned to the user. Nicole, 2021 mentions that there needs to be a discontinuation of this practice where these third parties are hidden under 3 or 4 clicks. Next, the author makes mention of how large blocks of text essentially pushes the user away from reading what is considered 'irrelevant' information but rather important to users in the context of privacy. While companies are essentially following the regulations of GDPR, they are trying their hardest to find loopholes. Regulators need to enforce GDPR guidelines when it comes to privacy statements so that the average user can understand what they are getting into, know what they are opting out of and finally, reduce the number of websites/ applications that collect something termed as 'functional cookies' which does not allow the user to withhold their information.

9

Conclusion

The aim of this thesis is to highlight the potential privacy concerns that may arise with the integration of Ultra-Wideband technology in mobile phones. UWB has been utilised within the EU for a number of applications which include radars and communication devices. However, as of 2019, UWB has been integrated into mobile phones with the express idea of increasing data transfer rates, higher accuracy in localisation and inter-connectivity. Mobile phone companies have marketed UWB as technology that increases the aforementioned three characteristics. The flip side is that there are a number of potential privacy concerns that are brought up with the increase in functionality. Therefore, the main research question was introduced as **how do experts and users perceive privacy concerns of UWB usage in mobile phones; and how can they be mitigated?** This was divided into three sub-research questions that aimed at understanding how UWB can be used in a mobile phone, understanding potential privacy concerns from experts and users, and finally potential mitigation strategies. The rest of the chapter discusses the main findings from these three questions, the limitations of the research and future recommendations for research in the field.

9.1. Main findings

UWB is a relatively new technology and the amount of research on the topic is limited. There were multiple literature studies conducted through the duration of this research to understand the technology, place its relevance in the context of mobile phones, present potential concerns of incumbent radio technology and finally discuss relevant privacy mitigation strategies.

UWB commonly refers to a signal that operates at frequencies higher than 500 MHz. Comparable radio technology such as BLE and Wi-Fi operate in the 2.8 and 5 GHz range which shows that there is a big possibility of overlapping signals. Frequencies higher than 500 Mhz were all unanimously termed as 'ultra-wideband' by the US Department of Defence in the early 2000s. The EU decided to that as well to maintain equilibrium. UWB has a number of advantages such as low power, high transmission rates, secure communications channels and multipath components. After 2007, a number of potential applications from a research perspective came to the fore which include but are not limited to health monitoring, terrain profiling, foliage penetration, consistent localization, connecting multimedia devices in an ecosystem, activity recognition from distances and key-less entries for houses and vehicles. From the perspective of the mobile phone industry, use cases can be broadly categorised into location based services and peer-to-peer applications as shown in figure 4.2. On juxtaposing these domains, it can be seen that a majority of the applications mentioned in research are possible in mobile phones. It is not a matter of if but when these applications will become possible. This broadly answers the first sub-research question.

From a privacy perspective, the biggest issue with UWB was its ability to provide centimetre level accuracy of mobile phone users. Whether it be used as a personal device or part of infrastructure that communicates with people's devices, UWB seemed to have significant privacy concerns that were not documented or researched prior to this thesis. In order to do this in a structured manner, three paradigms were introduced: social, surveillance and institutional. Social privacy refers to issues that arise due to social interactions between people. Surveillance privacy refers to the issues that arise by users that essentially use a specific technology provided by a third party. Institutional privacy refers to the control users have over their data that is collected by the usage of certain service or applications. The possible privacy concerns were obtained through inter-

viewing experts in the UWB industry and also potential users. However prior to conducting interviews, a literature study was conducted to understand the different privacy concern of incumbent radio technology as a comparative study. Current technology has the ability to locate users throughout mobile usage activities. They enable profiling, locating and gathering insights about people from where they have been. This has lead to big tech companies using this data to push services towards people, manipulate them and gradually change the way services are provided to people. Almost every single service requires customer data and almost every application requires location information to work properly. While these may be viable business models, users' privacy is on the last rung of importance. The reasons to monetise users' data seem to keep increasing.

In the context of UWB, the data that was gathered from incumbent technology and potential applications helped structured interviews with experts and users. From the data analysed, it is easy to understand that the granularity of information provided by UWB is the biggest concern. It overtakes Wi-Fi, BLE and GPS localization to provide private corporations real time location information of every single individual. It enables information regarding relative distances, location history, profiles, behaviours and interests of people. People do not have a single place to hide purely by choosing to use a technology that is becoming the norm in the current world. A major concern that was shared amongst all the interviewees was that, without the public having a say in it, centimetre level accuracy may become a pre-requisite for any service. Both interviewee groups realised that the information that can be gathered from increased location accuracy is highly sought after and unless there are conversations about it, society will cross a line that it cannot come back from. A big inference that can be made from the data gathered is that privacy concerns of radio technology and localization has remained more or less the same as accuracy increased. However, there were a couple of stark differences between users and experts. The first is that users do not have a singular definition of privacy and oftentimes mistake security issues as privacy issues. The second biggest difference is that users choose user-centric methods for privacy protection. Experts chose to give statements such as 'regulators must...' and 'mobile phone companies should.....' whereas users want society to take control of their own data, their privacy and try to make change so that regulators can emulate them. They believe in more holistic approaches of introducing technology rather than pushing forth innovation and purely technical perspectives. They agree that while regulators need to be change-makers, user suggestions are not incentivised enough to become privacy protections norms. This shows that users are being coerced into living privacy neglecting lifestyles when they want to prioritise it instead. This answers the second sub-research question of how different stakeholders view potential privacy concerns of this new technology.

In order to protect privacy, two categories of privacy mitigation strategies were considered: technical and societal. There is however, the concept of privacy-by-design which cannot be included in either but is an overarching concept and thus termed as a socio-technical solution. The technical approaches seem effective and if they could become common among software developers, individual privacy could be protected. However, a significant issue was the need for third parties applications that could quite easily choose monetary gains over public privacy. This puts the user in the hands of another potential private organisation and on the back foot again. Therefore, it seems that the most effective ways of protecting privacy are through societal approaches. These include compensation models, differential privacy, enforcing anti-trust laws, tech regulatory bodies and revision of privacy policies. Users know that their data may be required to make use of certain services, however the lack of control is a major concern that needs revision. The aforementioned societal approaches help either give control of information to users or hold big companies responsible for their actions. These seem to be the best ways to protect user privacy as innovation/ technology keeps proliferating. This answers the third and last sub-research question.

9.2. Limitations

The research was carried out over the period of 5 months and has a few limitations that the reader needs to be aware of. The biggest limitation was the lack of time to gather more experts for interviews. Obtaining experts from various different organisations may have helped gather additional input on potential concerns. But it seems impossible to reach a saturation point in terms of experts as the concept of privacy is quite different depending on who is asked. Moreover, privacy researchers were mainly obtained from North America as opposed to the European region. European privacy researchers stated that the privacy concerns of UWB are quite similar to incumbent radio technology. This was largely true but their inclusion may have been able to provide a more region specific list of privacy concerns under the umbrella of GDPR. Within the EU, the GDPR protects citizens' right to privacy whereas in the US, there is no federal privacy law.

A similar limitation was noticed with respect to user interviews. If time permitted, the background of the users would be varied to include different ages, education levels, backgrounds and countries. The current user data only includes students from University of Technology Delft. Which means these are students who are technically adept and have enough background knowledge to understand privacy issues of any new technology. This also means that the thematic analysis conducted for users were skewed to only include highly knowledgeable individuals which may not be completely representative of the common public.

Furthermore, the degree of usable information gathered from interviews was a complex process that varied across interviews. Experts who were policy regulators could not completely shed light on possible privacy concerns as they did not either have enough technical knowledge or concepts about privacy. Coincidentally, experts who are not policy regulators shared recommendations to change policy but some of these were not institutionally possible. The technical, policy and business knowledge also varied across each individual. This meant that the interviewee would guide the interview to concepts that they were working on. This led to newer concepts being introduced in every expert interview with no pre-defined set of questions that were asked to each experts. It was a difficult task to obtain standardization across expert interviews.

A significant limitation was the absence of experts from the mobile phone industry. Their inclusion would have helped provide an inside perspective on the privacy procedures that companies employ. They could further highlight any privacy concerns that these developers see and their strategies to mitigate them. When such potential interviewees were contacted, they declined by stating it was either against their interests or was internal information which led to their exclusion from the research.

9.3. Recommendations for future research

Over the course of the research, some changes were made that possibly excluded important research results. Below, recommendations are provided that can help improve any future research conducted within the same domain.

A major drawback of the research was the limited number of participants from both the expert and user stakeholder groups. This was due to the interview protocol taking longer than expected. Future research should try to include as many privacy researchers as possible where the interview results in section 6 can serve as an input to form suitable questions. The results of both the expert and user interviews will serve as a knowledge domain that any future research can build from as UWB becomes more prominent.

Secondly, the socio-demographic characteristics of the users can be expanded to include different universities, age groups and social statuses. This would help formulate a more representative knowledge base of how users view privacy concerns of a new technology and what ideas they have to mitigate it. Looking back at the results, users seemed to have better privacy mitigation strategies and incorporating more users would definitely benefit regulators in the long run.

A major insight that can be drawn from the research is that the privacy concerns of incumbent radio technology and UWB are roughly the same. Further research can distinguish itself by following one of two paths. The first is by comparing the privacy concerns of different radio technology on a like-for-like basis. The second can be by conducting research into understanding how much the privacy concerns multiply as UWB gets integrated into the Global System for Mobile Communications.

There seem to be significant societal approaches to protecting the privacy of users as presented in chapter 8. Further research should be conducted into how these mitigation strategies can be effectively implemented. These strategies can also be presented to regulators to gain their input. Depending on insights and iterations, these strategies can be integrated into official legislation/ regulation. Testing the effects on public privacy in small focus groups and how users accept them can help regulators become more user-centric.

A

Appendix

A.1. Ethics

This section of the appendix describes the ethical process of data collection as required by the Human Research Ethics Committee (HREC) of TU Delft and GDPR regulations. In order to conduct any research that involves humans, the HREC has a four step procedure to ensure the human subjects are comfortable and that the data collection process follows GDPR standards. It proceeds for this research, as:

1. The HREC uses a checklist to check whether the proposed research poses more than minimal risk. This involves questions such as if participants are dependents, if they are part of vulnerable groups, if it involves deceiving participants, if it involves collecting samples from participants or if it cause discomfort/ stress. Due to the fact that this research contains procedures that involve collecting and storing videos or other identifiable data of human subjects, it proceeds with step 2.
2. Suitable informed consent forms are needed to be sent across to potential participants prior to their interviews. However, the HREC needs to receive and approve these documents prior to contacting participants. The informed consent forms comprise of two parts: information sheet and consent form options. The former refers to suitably informing the participant of what the study is about, how long will it take, what interview questions can be expected and how their data will be analysed. Figure A.1 shows the information sheet for experts and A.3, for users. The latter contains the different options that the participants accepts to such as if they are okay being recorded, if they are voluntarily participating, if they understand the risks of their comments being anonymously included and if their data can be archived for future research. Figure A.2 shows the consent form for experts and A.4, for users. Additionally, a data management plan (DMP) needs to be sent across after being vetted by the Data Supervisor of the concerned faculty. The DMP includes details on how the data will be collected, whether it is stored on secure servers or in a secure location. The data collected for this research was saved on a TU Delft SURFdrive account and accessed every time it was necessary. This ensured the data was safe, not stored in an offline location and can only be accessed by the author of this thesis.
3. The checklist and consent forms have to be submitted to an online portal of the HREC. The committee meets once a week, debates on applications and either accepts an application or proposes changes. This research went through one revision which involved providing the exact details of the DMP. After the application was accepted, the interview process was started.
4. All potential interviewees were contacted through their emails and sent a consent form in the first two emails. This ensured that the participant knew this research was legit, conducted within TU Delft and had a concerned supervisor if they needed validation. After the interviewee sent across the signed consent form, meeting details such as day and date were finalised. This reassured interviewees that all the formalities were properly conducted and that the data will not be misused. They were also informed that they could change their viewpoints or delete them prior to the publishing of the final thesis.

Given below are the two consent forms as sent across to first (A.1, A.2) experts and then (A.3, A.4) users.

Informed consent form

INFORMATION SHEET

The research conducted is based on the up-and-coming UWB technology. Since its unlicensed usage since 2002 (in USA) or 2007 (in Europe), it has increased the possible number of applications. These include heart rate monitoring without contact, gait recognition, indoor localization, infrastructure-free localization, asset tracking and foliage penetration. Recently, Apple and Samsung have added UWB chips to their mobile phones. UWB has the possibility for high data rates, high connectivity and locational accuracy of 10 centimetres in most occasions. This research will seek to understand different privacy concerns that this may raise, something that research on the topic has not yet engaged.

As a technology expert, policy maker or privacy researcher, it is my hope that an interview with you will help me shed light on the topic of what the advantages or disadvantages of UWB are and what privacy concerns, if any, may arise from the integration of UWB within mobile phones. If we further have time, it would be beneficial for me to know what you think could be steps or directives relevant stakeholders/ organisations can take to curb any major privacy concerns that may arise. The answers to these questions will help fill a clear knowledge gap and help compare with some steps that may have been taken when BLE and GPS were first included in mobile phones. Additionally, our interview will help me understand what the widespread concerns are and form a knowledge base for any UWB enthusiast to start his/ her research from.

The formal interview that I would like to conduct will not take more than 45-60 minutes of your time. It will start off with a few questions related to you, your organization and line of work. From then on, the questions will strictly be related to UWB and its incorporation within mobile phones. I would like to audio record the meeting so that I can code it and use it for inclusion in my research. Your name and organizations will be anonymized throughout the duration of my research. Additionally, at any point prior to my final research submission, if you want to withdraw your viewpoints from my written document, you can mail and I will ensure that nothing that you have stated has been included in my research.

The answers provided by you during the interview will be used to compare and contrast viewpoints of other experts that take part in the study. This will firstly, help me form a knowledge base of viewpoints while secondly, allow me to highlight the most important characteristics of UWB. If, at any point you want to reiterate, affirm, request access to or rectify the data I have collected in our meeting, please feel free to let me know via e-mail and we can go through the information together and fulfil your specific request.

The data collected will be saved on a secure TU Delft SURFdrive server until it has been analyzed and included in my final document. It will be accessed by me alone and no one else can access the exact notes and recording made of our interview. After this, all the answers that I have collected from you will be deleted with only the analysis remaining in the final document.

Given below is the consent form which fulfils all the requirements under the GDPR and has been provided by my institution of TU Delft. Please tick the options you agree with.

Figure A.1: Information sheet for experts

Consent Form for “Privacy concerns related to UWB usage in mobile phones”

<i>Please tick the appropriate boxes</i>	Yes	No
Taking part in the study		
I have read and understood the study information dated [DD/MM/YYYY], or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.	<input type="radio"/>	<input type="radio"/>
I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.	<input type="radio"/>	<input type="radio"/>
I understand that taking part in the study involves an audio-recorded interview where my opinions are transcribed as text and used in the final research document. I accept that the information will be deleted upon the completion of the research.	<input type="radio"/>	<input type="radio"/>
Use of the information in the study		
I understand that information I provide will be used for forming a knowledge for UWB and its possible privacy concerns. I realize that the information provided by me may be compared with viewpoints of others to transcribe the differences and presented as research findings. I consent to it being included in the final research document.	<input type="radio"/>	<input type="radio"/>
I understand that personal information collected about me that can identify me, such as my name and organization, will not be shared beyond the study team or at all, if I request it.	<input type="radio"/>	<input type="radio"/>
Signatures		


Name of participant [printed]	Signature	Date
I have accurately read out the information sheet to the potential participant and, to the best of my ability, ensured that the participant understands to what they are freely consenting.		
Mohamed Adeeb Ahmed Researcher name	 Signature	12 th March 2021 Date
Study contact details for further information: Mohamed Adeeb Ahmed Number: +31 645251113 E-mail address: adeeb23ahmed@gmail.com		

Figure A.2: Consent form options for experts

Informed consent form

INFORMATION SHEET

The research conducted is based on the up-and-coming UWB technology. Since it's unlicensed usage since 2002 (in USA) or 2007 (in Europe), it has increased the possible number of applications. These include heart rate monitoring without contact, gait recognition, indoor localization, infrastructure-free localization, asset tracking and foliage penetration. Recently, Apple and Samsung have added UWB chips to their mobile phones. UWB has the possibility for high data rates, high connectivity and locational accuracy of 10 centimetres in most occasions. This research will seek to understand different privacy concerns that this raises, something that recent research has failed to highlight.

As a student or rather potential user, it is my hope that you will help me shed light on the topic of what you see as potential privacy concerns that may arise from the integration of UWB within mobile phones. It would be beneficial to know what steps or directives relevant stakeholders/ organisations can take to curb these privacy concerns that you see.

The formal interview that I would like to conduct will not take more than 25-35 minutes of your time. It will start off with a few questions related to your name, and area of research/ study. From then on, the questions will strictly be related to UWB and its incorporation within mobile phones. I would like to audio record the meeting so that I can code it and use it for inclusion in my research. Your name will be anonymized throughout the duration of my research and used only as a code. Additionally, at any point prior to my final research submission, if you want to withdraw your viewpoints from my written document, you can mail me any time and I will ensure that nothing that you have stated has been included in my research.

The answers provided by you during the interview will be used to compare and contrast viewpoints of other users. This will firstly, help me form a knowledge base of viewpoints while secondly, allow me to highlight the biggest issues that people see in UWB. If, at any point you want to reiterate, affirm, request access to or rectify the data I have collected in our meeting, please feel free to let me know via e-mail and we can go through the information together and fulfil your specific request.

The data will be accessed by me alone and no one else will look at the exact notes and recording made of our interview. Once the final thesis is written, your data will be deleted with only the analysis in the final document remaining, unless you state otherwise.

Given below is the consent form which fulfils all the requirements under the GDPR and has been provided by the institution of TU Delft. Please type in Y adjacent to the options you agree with. If you require more information about what UWB is and what the potential use cases of it are within mobile phones, I am attaching another document in the email for your reference. It will help introduce you to UWB, its integration in mobile phone, the three privacy paradigms and the potential use cases. This is not mandatory to read for the study but it would be appreciated.

Figure A.3: Information sheet for users

Consent Form for “Privacy concerns related to UWB usage in mobile phones”


<i>Please tick the appropriate boxes</i>	Yes	No
Taking part in the study		
I have read and understood the study information, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.	<input type="radio"/>	<input type="radio"/>
I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.	<input type="radio"/>	<input type="radio"/>
I understand that taking part in the study involves an audio-recorded interview where my opinions are transcribed as text and used in the final research document. I accept that the information will be deleted upon the completion of the research.	<input type="radio"/>	<input type="radio"/>
Use of the information in the study		
I understand that information I provide will be used for forming a knowledge for UWB and its possible privacy concerns. I realise that the information provided by me may be compared with viewpoints of others to transcribe the differences and presented as research findings. I consent to it being included in the final research document.	<input type="radio"/>	<input type="radio"/>
I understand that personal information collected about me that can identify me, such as my name and organization, will not be shared beyond the study team or at all, if I request it.	<input type="radio"/>	<input type="radio"/>
Signatures		
<p>_____</p> <p>Name of participant [printed]</p>	<p>_____</p> <p>Signature</p>	<p>_____</p> <p>Date</p>
I have accurately read out the information sheet to the potential participant and, to the best of my ability, ensured that the participant understands to what they are freely consenting.		
<p>Mohamed Adeeb Ahmed</p> <p>Researcher name</p>	 <p>Signature</p>	<p>10th May 2021</p> <p>Date</p>
<p>Study contact details for further information: Mohamed Adeeb Ahmed</p> <p>Number: +31 645251113</p> <p>E-mail address: m.ahmed-11@student.tudelft.nl</p>		

Figure A.4: Consent form options for users

- Gasson, M. N., Kosta, E., Royer, D., Meints, M., & Warwick, K. (2011). Normality mining: Privacy implications of behavioral profiles drawn from GPS enabled mobile phones. *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, 41(2), 251–261. <https://doi.org/10.1109/TSMCC.2010.2071381>
- Gellersen, H., Want, R., & Schmidt, A. (2005). *Pervasive Computing* (Third International Conference Munich, PERVASIVE, Vol. 3744 LNCS).
- Georgiadou, Y., De By, R. A., & Kounadi, O. (2019). Location privacy in the wake of the GDPR. *ISPRS International Journal of Geo-Information*, 8(3). <https://doi.org/10.3390/ijgi8030157>
- Gezici, S., Tian, Z., Giannakis, G. B., Kobayashi, H., Molisch, A. F., Poor, H. V., & Sahinoglu, Z. (2005). Localization via ultra-wideband radios: A look at positioning aspects of future sensor networks. *IEEE Signal Processing Magazine*, 22(4), 70–84. <https://doi.org/10.1109/MSP.2005.1458289>
- Ghezzi, A., Rangone, A., Balocco, R., & Renga, F. (2010). A Strategy-Technology-Regulation-User-Context model for Mobile Location-Based Services market activation analysis. *ICMB and GMR 2010 - 2010 9th International Conference on Mobile Business/2010 9th Global Mobility Roundtable*, 280–288. <https://doi.org/10.1109/ICMB-GMR.2010.49>
- Gurses, S., & Diaz, C. (2013). Two tales of privacy in online social networks. *IEEE Security and Privacy*, 11(3), 29–37. <https://doi.org/10.1109/MSP.2013.47>
- Guston, D. H., & Sarewitz, D. (2002). Real-time technology assessment. 24, 93–109.
- Heinrich, A., Stute, M., Kornhuber, T., & Hollick, M. (2021). Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System. *Proceedings on Privacy Enhancing Technologies*, 2021(3), 227–245. <https://doi.org/10.2478/popets-2021-0045>
- Herbert, G. (2020). Wireless Carriers Face 200M Dollar Fine for Selling Location Data.
- Huda, M. N., Yamada, S., & Sonehara, N. (2013). An Efficient k-Anonymization Algorithm with Low Information Loss BT. In F. L. Gaol (Ed.). Springer Berlin Heidelberg.
- Iqbal, M. U., & Lim, S. (2010). Normality Mining: Privacy Implications of Behavioral Profiles Drawn From GPS Enabled Mobile Phones, 39–46.
- Josephson, C. (2019). Every move you make, I'll be watching you: Privacy implications of the Apple U1 chip and ultra-wideband.
- Kang, J., Steiert, D., Lin, D., & Fu, Y. (2020). MoveWithMe: Location Privacy Preservation for Smartphone Users. *IEEE Transactions on Information Forensics and Security*, 15, 711–724. <https://doi.org/10.1109/TIFS.2019.2928205>
- Karanja, A., Engels, D. W., Zerouali, G., & Francisco, A. (2018). Unintended Consequences of Location Information: Privacy Implications of Location Information Used in Advertising and Social Media. *SMU Data Science Review*, 1(3), 13.
- Karim, W. (2004). The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring. *Washington University Journal of Law & Policy*, 14(January), 485–515.
- Khan, L. M. (2017). Amazon's antitrust paradox. *Yale Law Journal*, 126(3), 710–805.
- Kim, J., Kim, K., Park, J., & Shon, T. (2012). A scalable and privacy-preserving child-care and safety service in a ubiquitous computing environment. *Mathematical and Computer Modelling*, 55(1-2), 45–57. <https://doi.org/10.1016/j.mcm.2011.01.012>
- Kolakowski, M. (2019). A Hybrid BLE/UWB Localization Technique with Automatic Radio Map Creation. *13th European Conference on Antennas and Propagation, EuCAP 2019*, (EuCAP), 2019–2022.
- Kostakos, V. (2008). The privacy implications of Bluetooth. <http://arxiv.org/abs/0804.3752>
- Krebs, B. (2019). Apple Explains Mysterious iPhone 11 Location Requests.
- Kshetrimayum, R. S. (2009). An introduction to UWB communication systems. *IEEE Potentials*, 28(2), 9–13. <https://doi.org/10.1109/MPOT.2009.931847>
- Landreau, I., Peliks, G., Binctin, N., & Pez-Perard, V. (2018). My data are mine: Why we should have ownership rights. (April).
- Lee, J. S., Su, Y. W., & Shen, C. C. (2007). A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. *IECON Proceedings (Industrial Electronics Conference)*, 46–51. <https://doi.org/10.1109/IECON.2007.4460126>
- Lee, Y., Park, J. Y., Choi, Y. W., Park, H. K., Cho, S. H., Cho, S. H., & Lim, Y. H. (2018). A Novel Non-contact Heart Rate Monitor Using Impulse-Radio Ultra-Wideband (IR-UWB) Radar Technology. *Scientific Reports*, 8(1), 1–10. <https://doi.org/10.1038/s41598-018-31411-8>
- Madge, R. (2017). Five loopholes in the GDPR.

- Madrigal, A. (2018). Facebook Didn't Sell Your Data; It Gave It Away.
- Martin, J., Alpuche, D., Bodeman, K., Brown, L., Fenske, E., Foppe, L., Mayberry, T., Rye, E., Sipes, B., & Teplov, S. (2019). Handoff all your privacy - A review of apple's bluetooth low energy continuity protocol. *arXiv*, 1–20. <https://doi.org/10.2478/popets-2019-0057>
- Mavridis, T., Sarrazin, J., Petrillo, L., De Doncker, P., & Benlarbi-Delai, A. (2015). Information spatial focusing scheme for UWB wireless communications in smart environments. *IEEE Antennas and Wireless Propagation Letters*, 14, 20–23. <https://doi.org/10.1109/LAWP.2014.2354059>
- Michael, K., McNamee, A., & Michael, M. G. (2006). The emerging ethics of humancentric GPS tracking and monitoring. *International Conference on Mobile Business, ICMB 2006*, (July), 25–27. <https://doi.org/10.1109/ICMB.2006.43>
- Minch, R. P. (2006). Privacy issues in location-aware mobile devices. *37th Hawaii International Conference on System Sciences*, 00(100), 1–10.
- Ministry of Economic Development. (2005). An Engineering Discussion Paper on Spectrum Allocations for Ultra Wide Band Devices. (April), 1–31.
- ND. (2017). K-Anonymization: An Introduction.
- Nguyen, A. (2019). Understanding Differential Privacy.
- Nicole, O. (2021). 10 Common Issues with Privacy Policies.
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119–157.
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, 16(1), 1–13. <https://doi.org/10.1177/1609406917733847>
- Owen, M. (2020). Everything you need to know about Ultra Wideband in the iPhone 12 and HomePod mini.
- Pelka, M., & Hellbruck, H. (2016). S-TDoA-Sequential time difference of arrival-A scalable and synchronization free approach for Positioning. *IEEE Wireless Communications and Networking Conference, WCNC, 2016-Sept*(Wcnc). <https://doi.org/10.1109/WCNC.2016.7565024>
- Peters, J. (2020). Apple files patent for a smart home system that could configure itself.
- Phillips, D. J. (2003). Beyond Privacy: Confronting Locational Surveillance in Wireless Communication. *Communication Law and Policy*, 8(1), 1–23. https://doi.org/10.1207/s15326926clp0801_01
- Pochanin, G., Masalov, S., Pochanina, I., Capineri, L., Falorni, P., & Bechtel, T. (2016). Modern trends in development and application of the UWB radar systems. *2016 8th International Conference on Ultrawideband and Ultrashort Impulse Signals, UWBUSIS 2016*, 7–11. <https://doi.org/10.1109/UWBUSIS.2016.7724141>
- Purcher, J. (2019). Apple Invents iBeacon Version 2 using Ultra-Wide Band Radio Technology.
- Quest, L., & Charrie, A. (2021). The Right Way to Regulate The Tech Industry. *Oliver Wyman Insights*. <https://doi.org/10.2139/ssrn.986737>
- Rana, S. P., Dey, M., Ghavami, M., & Dudley, S. (2019). Signature inspired home environments monitoring system using IR-UWB technology. *Sensors (Switzerland)*, 19(2). <https://doi.org/10.3390/s19020385>
- Ruan, W., Sheng, Q. Z., Yao, L., Li, X., Falkner, N. J., & Yang, L. (2018). Device-free human localization and tracking with UHF passive RFID tags: A data-driven approach. *Journal of Network and Computer Applications*, 104(December 2016), 78–96. <https://doi.org/10.1016/j.jnca.2017.12.010>
- Saaty, T. (2005). Analytic Hierarchy Process. *Analytical hierarchy process*. <https://doi.org/10.1002/0470011815.b2a4a002>
- Sadrezami, H., Bolic, M., & Rajan, S. (2019). Capsfall: Fall detection using ultra-wideband radar and capsule network. *IEEE Access*, 7, 55336–55343. <https://doi.org/10.1109/ACCESS.2019.2907925>
- Schindhelm, C. K. (2012). Activity recognition and step detection with smartphones: Towards terminal based indoor positioning system. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, 2454–2459. <https://doi.org/10.1109/PIMRC.2012.6362769>
- Shankland, S. (2021). Galaxy S21 Ultra has UWB. Here's how ultra wideband tech will make your life easier.
- Shaw, J., & Graham, M. (2017). An Informational Right to the City- Code, Content, Control, and the Urbanization of Information. *Antipode*, 49(4), 907–927. <https://doi.org/10.1111/anti.12312>
- Shi, B., Hu, Y., Duan, Q., Han, L., & Ding, Y. (2020). A Crowdsourcing-based Localization Scheme with Ultra-Wideband Communication. *IECON Proceedings (Industrial Electronics Conference), 2020-Octob*, 4331–4336. <https://doi.org/10.1109/IECON43393.2020.9255352>
- Singh, S., Liang, Q., Chen, D., & Sheng, L. (2011). Sense through wall human detection using UWB radar. *Eurasip Journal on Wireless Communications and Networking*, 2011(1), 1–11. <https://doi.org/10.1186/1687-1499-2011-20>

- Staderini, E. M. (n.d.). Everything you always wanted to know about UWB radar . . . : a practical introduction to the ultra wideband. *Online Symposium for Electronics Engeneering*, 1–12.
- Sujithra, M., Padmavathi, G., & Narayanan, S. (2015). Mobile device data security: A cryptographic approach by outsourcing mobile data to cloud. *Procedia Computer Science*, 47(100), 480–485. <https://doi.org/10.1016/j.procs.2015.03.232>
- Tawfik, R., Samer, A.-R., & Samer, A. (2015). Security fundamentals: access control models. Interdisciplinarity in theory and practice. *International journal of interdisciplinarity in theory and practice*, (7), 259–262.
- Thompson, C., Stuart Warzel. (2019). Twelve Million Phones, One Dataset, Zero Privacy.
- Truly, A. (2020). Apple AirTag Patents Explain Location Tracking Navigation Potential.
- Ullah, S., Ali, M., Hussain, A., & Kwak, K. S. (2009). Applications of UWB Technology. <http://arxiv.org/abs/0911.1681>
- Vanhoef, M., Matte, C., Cunche, M., Cardoso, L., & Piessens, F. (2016). *Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms*. <https://doi.org/10.1145/2897845.2897883>
- Vishwesh, J., & Raviraj, P. (2018). Ultra Wide-band (UWB): Characteristics and Applications. *International Journal of Recent Trends in Engineering and Research*, 4(6), 45–52. <https://doi.org/10.23883/ijrter.2018.4315.vltok>
- Wang, J. L., & Loui, M. C. (2009). Privacy and ethical issues in location-based tracking systems. *International Symposium on Technology and Society, Proceedings*, 2–5. <https://doi.org/10.1109/ISTAS.2009.5155910>
- Warren, E. (2019). Here's how we can break up Big Tech.
- Wilzeck, A., Perez Guirao, M., & Dimitrov, E. (2010). *UWB Technology and Regulation* (tech. rep.).
- Wu, S., Sakamoto, T., Oishi, K., Sato, T., Inoue, K., Fukuda, T., Mizutani, K., & Sakai, H. (2019). Person-specific heart rate estimation with ultra-wideband radar using convolutional neural networks. *IEEE Access*, 7, 168484–168494. <https://doi.org/10.1109/ACCESS.2019.2954294>
- Xia, H., & McKernan, B. (2020). *Privacy in Crowdsourcing: a Review of the Threats and Challenges* (Vol. 29). Computer Supported Cooperative Work (CSCW). <https://doi.org/10.1007/s10606-020-09374-0>
- Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, 26(3), 135–174. <https://doi.org/10.2753/MIS0742-1222260305>
- Yan, S., Soh, P. J., & Vandenbosch, G. A. (2018). Wearable ultrawideband technology- A review of ultrawideband antennas, propagation channels, and applications in wireless body area networks. *IEEE Access*, 6, 42177–42185. <https://doi.org/10.1109/ACCESS.2018.2861704>
- Yang, X., Yin, W., Li, L., & Zhang, L. (2018). Dense people counting using IR-UWB radar with a hybrid feature extraction method. *arXiv*, 16(1), 30–34.
- Zhang, K., Shen, C., Gao, Q., Zheng, L., Wang, H., & Li, Z. (2018). Precise Positioning System of Ship Interior Based on UWB Ultra Wideband Technology. *Journal of Coastal Research*, 83, 908–912. <https://doi.org/10.2112/SI83-150.1>
- Zhang, R., Song, L., Jaiprakash, A., Talty, T., Alanazi, A., Alghafis, A., Biyabani, A. A., & Tonguz, O. (2019). Using ultra-wideband technology in vehicles for infrastructure-free localization. *arXiv*, 122–127.
- Zhao, P., Liu, W., Zhang, G., Li, Z., & Wang, L. (2020). Preserving Privacy in WiFi Localization with Plausible Dummy Locations. *IEEE Transactions on Vehicular Technology*, 69(10), 11909–11925. <https://doi.org/10.1109/TVT.2020.3006363>
- Zin, M. S. I. M., & Hope, M. (2010). A review of UWB MAC protocols. *6th Advanced International Conference on Telecommunications, AICT 2010*, (June 2010), 526–534. <https://doi.org/10.1109/AICT.2010.101>