

***AN INVESTIGATION INTO THE ETHICAL CHALLENGES OF
THE INTERNET OF THINGS AMBIENT ASSISTED LIVING IN
IRELAND***



Michael O'Keeffe

The University of Dublin, Founded in 1592.

School of Computer Science and Statistics

Abstract

This research dissertation is the final part of a Master's Degree in the Management of Information Systems and will give a broad, but an informative view into the ethical challenges of the Internet of Things Ambient Assisted Living (IoT AAL) in Ireland from the perspective of six interviewee participants. The ethical challenges identified from the literature as part of this research are Privacy, Security, Social Isolation, Behaviour Modification, Roboethics and Regulation. Interview Participants ranged from Team leaders, Robotics Subject Matter Experts, Project Directors and Project owners, and all have a strong academic background with three having earned the title of Doctor in their chosen area.

These research participants were chosen from a carefully selected stakeholder membership; the reason for this was to capture a broad outlook of experience of ethics surrounding IoT Assisted technologies.

This research was a qualitative study; the design type was phenomenological using semi-structured interviews lasting forty minutes. Four out of the six interviews had eight main question and seven smaller questions to answer while two interviewees had specific question or questions relating to their subject matter.

The interviewees were also invited to give reflections of their experiences along with the questions asked. All interviews were digitally recorded with a manual analysis of the research findings using a qualitative approach.

This report will show that Ireland through work carried out in research institutes and through a charity working with elderly people are very much aware of the ethical challenges they face in Ireland. In addition to the ethical challenges identified in the literature, additional challenges of assessment, training, and safety emerged from the interviews. IoT AAL technology is still at an early stage in Ireland, and there is potential to expand into the community and become a significant technology in the self-management of older people in years to come.

Acknowledgements

There a lot of people I would personally like to thank for giving me their time, space, encouragement, support and direction over the two years of this Master's Degree and especially over the last nine months while writing this dissertation. Without these people in my life, this project would not be possible.

I would like to personally thank my wife Selene, for picking up the slack at home while I busied myself with the countless hours to see this project through. I also owe infinite gratitude to my beautiful daughter Emily who continues to be a shining light every day. This dissertation I dedicate to you both.

I own an incredible amount of gratitude to my academic supervisor, who for the past nine months has worked closely with me providing direction and wisdom as I attempted navigated the sometimes tepid waters of writing my first dissertation.

For my classmates, I thank you for the experiences, wisdom and high standards that set the bar to which I aimed to climb over the last two years. I hope I haven't disappointed. The friendships we have made over the last two year I hope will last forever.

To those participants who gave up their time to allow me to interview them, and share with this research their wisdom and experience, from the bottom of my heart I thank you.

Finally, to Sinead Impey from the O'Reilly Institute, who showed me how to carry out a qualitative analysis, when the books failed me, I thank you from the bottom of my heart and wish you the best in completing your PhD studies.

For anyone, I have left out, and there are a countless number of people that could be mentioned here, I apologise.

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: _____.

Date: _____.

Permission to lend and/or copy I agree that the School of Computer Science and Statistics, Trinity College Dublin (University of Dublin) may lend or copy this dissertation upon request.

Signed: _____.

Date: _____.

Table of Contents

ACKNOWLEDGEMENTS	III
DECLARATION	IV
LIST OF TABLES	VII
LIST OF FIGURES.....	VIII
GLOSSARY	IX
1. INTRODUCTION	1
1.1. THE CONTEXT OF THE STUDY	1
1.1.1. Terminology	1
1.2. GENERAL BACKGROUND	3
1.2.1. The problem.....	4
1.2.2. Who should benefit and why?	5
1.3. THE SCOPE OF THE STUDY.....	5
1.4. RESEARCH QUESTION, OBJECTIVES, TIMELINE AND ROADMAP	6
2. LITERATURE REVIEW.....	8
2.1. INTRODUCTION	8
2.2. PRIVACY.....	8
2.3. SECURITY.....	11
2.4. THE LAW	13
2.4.1. GDPR	13
2.4.2. A more in-depth look at some of the Articles of GDPR legislation	14
2.5. SOCIAL ISOLATION	16
2.6. ETHICAL CHALLENGES SURROUNDING HOMECARE ROBOTS.....	17
2.6.1. Deception.....	19
2.6.2. Dignity.....	19
2.6.3. Isolation	20
2.6.4. Privacy and Robots.....	20
2.6.5. Safety.....	21
2.7. CHANGE OF PHYSICIAN BEHAVIOUR TOWARDS PATIENTS	21
2.8. BEHAVIOUR MODIFICATION	22
2.9. CONCLUSION	24
3. STUDY DESIGN AND METHODOLOGY	25
3.1. INTRODUCTION	25
3.2. THE RATIONALE OF RESEARCH QUESTION	25
3.3. RESEARCH AIM.....	26
3.3.1. Interview Questions.....	27
3.4. RESEARCH APPROACH AND DESIGN	28
3.4.1. Literature Review	28
3.4.2. Qualitative Research.....	29
3.5. CHARACTERISTICS OF QUALITATIVE RESEARCH.....	29

3.5.1.	<i>'Researcher Key Instrument'</i>	29
3.5.2.	<i>'Participant's Meaning'</i>	30
3.5.3.	<i>'Emergent Design,'</i>	30
3.6.	THE RESEARCHERS ROLE	30
3.6.1.	<i>Ethics Approval</i>	31
3.7.	GRAND PHILOSOPHICAL APPROACH	31
3.8.	DATA RECORDING PROCEDURES	32
3.9.	DATA ANALYSIS AND INTERPRETATION	32
3.10.	VALIDITY AND RELIABILITY	33
3.11.	PARTICIPANTS – RECRUITMENT	34
3.12.	DEBRIEFING ARRANGEMENT	35
3.13.	LIMITATIONS OF THE RESEARCH	35
3.14.	CONCLUSION	36
4.	RESULTS	37
4.1.	INTRODUCTION	37
4.2.	RESULTING QUOTATIONS FROM RESULTS OF RESEARCH	38
5.	DISCUSSION, LIMITATIONS, RECOMMENDATIONS AND CONCLUSION	45
5.1.	INTRODUCTION	45
5.2.	THEMES EMERGING FROM THE INTERVIEWS	45
5.3.	DISCUSSION	48
5.3.1.	<i>Assessment</i>	48
5.3.2.	<i>Privacy</i>	49
5.3.3.	<i>Data Security</i>	51
5.3.4.	<i>Training</i>	52
5.3.5.	<i>Social Technology</i>	53
5.3.6.	<i>Roboethics</i>	53
5.3.6.1.	<i>Clear Distinction</i>	53
5.3.6.2.	<i>Safety</i>	54
5.3.7.	<i>Regulation</i>	56
5.4.	LIMITATIONS	57
5.5.	RECOMMENDATIONS	57
5.6.	CONCLUSION	58
REFERENCES		I
APPENDICES		1
APPENDIX A:		1
APPENDIX B:		3
APPENDIX C:		5
APPENDIX D:		7
APPENDIX E		9

List of Tables

Table 1.1, Summary of terminology for Connected Health and Related Technologies.....	2
Table 1.2, Status of themes in primary and secondary research.	6
Table 2. 1, Principals cited by (Mittelstadt, 2017) containing ethical principles based on Beauchamp and Childress and OECD.	10
Table 2. 2, Summary of GDPR Articles, and Subsections.	15
Table 3. 1, Question Type, Number and Subsection.	27
Table 3. 2, Database list and Search String.....	28
Table 3. 3, Coding Table Demo.....	33
Table 3. 4, Breakdown of Interviewees.....	35
Table 4. 1, Replica of Breakdown of Interviewees from Table 3.4 Above.	37
Table 5. 1, Themes that emerged in both Literature and Interviews.	46
Table 5. 2, Themes that emerged from Roboethics.....	47

List of Figures

Figure 2. 1, Simple Home Care System (HCS).....	12
Figure 2. 2, Frank's route to Jane's home.....	12
Figure 3. 1, Overview of the research process.	26
Figure 3. 2, Stakeholder Map.	34
Figure 5. 1, Example of a Telepresence.	54

Glossary

ACTUATOR: Device that reacts according to the information it receives from sensors. In the medical field, such a node can pump insulin, stimulate the brain or even pump the heart according to the specific application of its design.

AMBIENT INTELLIGENCE: Is multi-disciplinary, works at the intersection of several technologies including Artificial Intelligence, Big Data, Internet of Things (IoT), Pervasive-Ubiquitous Computing, Networks and Human Computer Interaction (HCI).

Ambient Intelligence (Aml) senses the environment and user context through various intelligent digital systems installed in our homes or workplaces, utilizing different IoT sensors and devices (Shyam, 2019).

CONNECTED HEALTH: A model for healthcare that uses technology to provide healthcare. People are increasingly using ambient and wearable sensors to generate continuous data through connected devices, whether that is blood pressure or distance walked. These personal devices are being used for medical applications too. Suitable data analytics methods and wireless technology to enable remote patient monitoring, point of care diagnostics, and self-care will transform healthcare. Encompassing mobile health (mHealth) through healthcare IT to telecare and telehealth (Varnai, 2015).

FRAILITY: More than three of the five criteria, including weakness, slowness, low level of physical activity, self-reported exhaustion and unintentional weight loss.

H-IOT: Health Internet of Things usually associated with IoT devices within hospitals or other health Centre's. IoT devices, however, for the purpose of this dissertation and according to Mittelstadt (A view of the abstract, introduction and footnote² of the paper (Mittelstadt and al., 2017) will reveal a crossover between the terminology and the functionality of Aml and H-IoT, ultimately meaning the same thing from a high level point of view and as expressed in relation to (Mittelstadt and al., 2017).

OBTRUSIVENESS: has been defined "as summary evaluation by a person based on characteristics or effects associated with the technology that is perceived as undesirable and physically and/or psychologically prominent" (Hensel, 2006).

1. Introduction

1.1. The context of the Study

The research area that this research is concerned with is “*An Investigate into Ethical Challenges of the Internet of Things Ambient Assisted Living (IoT AAL) in Ireland.*” However, before presenting the need, motivation, background and scope of this research it is necessary to present the often confusing and cross over terminology, between Internet of Things (IoT) health-related technologies, and IoT Ambient Assisted Living itself. This terminology is presented in section 1.1. There is also a need to understand that this technology isn’t all that new; this understanding will give us a sense of the depth and character to the technology.

When environmental support or assisted sensor devices (ambient devices) and subsequent monitoring are combined with IoT technology, this is known as the Internet of Things Ambient Assisted Living (IoT AAL).

When the terms, IoT AAL are seen in the literature, one cannot help but think that the conversation is about relatively new technology. The earliest reference for environmental support or assisted devices that have been found in the literature to date on this project goes back as far as 1986, and 1999 (Craig, 1986, Mann, 1999). Equally, it is important not to forget Kevin Ashton (Executive Director Auto-ID centre MIT), who coined the phrase “*The Internet of Things*” in 1999 (Ashton, 2019).

IoT AAL data like any other form of IoT application data can be subject to analysis, or it can be used in binary (alert or no alert, such as a fall monitor) or continuous monitoring (chronic illness monitoring over time) only applications. Data captured from sensor technology may generate data in the form of standard biomedical test or investigations, subjective reports of symptoms or even feelings. A key feature or desirable outcome of using these technologies is the self-management of the patient or users own health through feedback and follow on improvement in lifestyle changes (Caulfield, 2013).

1.1.1. Terminology

The terms described in table 1.1 are related to IoT AAL and rightly or wrongly are used interchangeably in the literature and include Connected Health, Health Internet of Things (HIoT), Medical Internet of Things (MIoT) or (IoTM), Ambient Intelligence (Aml), Assisted Technology (AT) and Mobile Health (mHealth), These terms HIoT, MIoT and Aml are very similar in principle to the monitoring of users in the IoT AAL environments, and monitoring of sometimes similar parameters, such as heart rate, diabetes and other environmental parameters. The four HIoT, MIoT and IoT AAL can get crossed over by many authors in the literature. The term connected health is used to describe technology that is used to deliver healthcare, and according to (Caulfield, 2013, Varnai, 2015), connected health comprises the use of wireless, digital, electronic, mobile devices, healthcare applications and other related mobile technologies. When connected

health solutions are combined with modern ICT solutions, the term is further enhanced giving rise to Mobile Health (mHealth). mHealth includes sensor technology for both ambient and wearable technologies (Varnai, 2015).

At a high level, one may be able to use these terms interchangeably. However, at the lower granular level, these term branch off into particular areas of their own and interchanging these terms can cause confusion. While it is understood at a granular level that the terms differ for this research, these terms will be used interchangeably at a high level. This allows the reader to quickly refer back to cited references in this research and use the term as the authors do.

Table 1.1, Summary of terminology for Connected Health and Related Technologies.

Terminology	Technology	Application
Connected Health	Wireless. Digital. Electronic. Mobile Devices (mHealth). Healthcare Applications.	Technology that is used to deliver healthcare. Connected health comprises the use of wireless, digital, electronic, mobile devices, healthcare applications and other related mobile technologies. (Caulfield, 2013, Varnai, 2015).
Combined Connected Health and ICT	Same as above, and including MHealth. Sensor Technology such as blood pressure monitors or pedometers for example. (Varnai, 2015).	Healthcare model that uses technology to provide healthcare. Especially relevant to older people, who more than likely have chronic health conditions and need health services more. They are using ambient and wearable sensors to generate continuous data. These devices are being used more for medical applications including mobile health (mHealth) through healthcare IT. Suitable data analytics methods and wireless technology to enable remote patient monitoring, the point of care diagnostics, and self-care (Varnai, 2015).
IoT AAL	Ambient Sensors, Binary Applications including environmental sensors and Body Area Networks just to name a few.	Assistance systems and services which support people in life. Intelligent devices and tools are connected to each other and/or to the healthcare centres. Devices have sensors to observe the health state of people and forward such information to the

		responsible healthcare person. Mostly in homes, residential care, used with elderly, young kids and cognitive impaired. Can cross over into HIoT and MIoT applications (Hail. Admed, 2015).
HIoT	<i>“Smart medical devices”</i> in a hospital or other health centre setting that can monitor in real-time the condition of a patient.	(Patel Nasrullah. No Date), the real-time monitoring of patients via connected devices that measure heart failures, diabetes, asthma attacks and more. Can also monitor the daily condition of users or patients. Data stored in a Cloud, with real-time monitoring of conditions taking place with usually with the aid of smartphone apps. To inform physicians, and other medical professionals, of the health state of the patient.
MIoT	Devices include heart rate monitors, hospital beds and even pills just to name a few.	(Martin, 2018), enables virtually any medical device to collect, analyse and send data back to the cloud. Data can be analysed by authorized personnel.
AMI	Sensors or devices that are context-aware Achieved through analytics. Machine learning is also a crucial part of Aml environments.	(Rouse, 2017), Aml as a form of a smart pervasive computing environment that enable sensors to interact with and respond to humans in the environment.

1.2. General Background

(Hayutin, 2007) in the following journal article *“Older Adult’s Attitudes to Self-Management of Health and Wellness through Smart Home Data”* written by (Doyle et al., 2015) makes a point that *“Globally, human populations are ageing and there is a significant cost element to the health care of older adults.”*

Other authors inclusive of (Doyle, 2016) and many more have also made the same point about the rising global ageing population, highlighting the growing population trend of ageing people, (Novitzky, 2015, Patrice, 2016).

The outcome of this phenomenon of a global ageing population is of growing interest in relation to the factors that can support older people for longer in their own homes or in smart homes. Projects such as the Great Northern Haven or GNH project (Great Northern Haven. No Date) are of pivotal importance because

they are the lead projects in Ireland in relation to the advancement of IoT AAL and other related technologies for the benefit of older users in their homes and residence of care.

When one reads more in-depth into the GNH project, you come to realise computers, mobile devices, and the IoT AAL technology all play a crucial role in allowing older people to stay at home for longer.

Staying at home for longer is known, according to (Doyle et al., 2015), as “*ageing-in-place*” and is personal or patient (user) centric care. In the case of IoT AAL technology, this allows carers, both professional or non-professional, to detect acute health problems (such as falls or anxiety), and health professionals to detect behaviour or pattern changes of a user’s routine over time (deterioration) due to the binary and continuous monitoring capabilities of IoT AAL technology. Patients can also receive their own data in order to see for themselves their own health state, and this can lead to an improvement in their own health and self-management.

Due to a lack of facilities at home or in the community that is readily available to support them, patients have an increased length of hospital stay. ‘*Bed-blocking*’ is an unfortunate and often frowned upon term used in relation to his situation. In Ireland, this delay on care packages or a place in a community setting can be up to 80% of the waiting time for discharge (O'Regan, 2015). A benefit of the use of IoT AAL technology is the potential reduction of cost and the freeing up of beds as patients leave the hospital.

By providing a tailored IoT AAL solution in the community and indeed in users own homes, this could prevent the readmission to hospital for repeat issues according to (Couturier et al., 2012, Doyle, 2016) and (Siddique, 2017). This strategic approach could also allow for a reorganisation of the healthcare system, potentially reduced costs in some areas of our health services, and broad autonomy and independent living for older users of IoT AAL technology (Couturier et al., 2012).

1.2.1. The problem

However, despite all of these described benefits, there are, however, challenges with IoT AAL, some of these challenges are technology-related while others are related to ethical issues of IoT AAL (Patrice, 2016, Novitzky, 2015, Mittelstadt, 2017) and (Marcello, 2018).

Marcello goes on to say “*Our screening shows that a significant portion of current IAT’s (Intelligent Assistive Technology) is designed in the absence of explicit ethical considerations.*”

The objective of this research is to interview a number of key informants who work with the implementation of IoT AAL technology concerning ethical challenges found in the literature. The intention is to bring siloed information surrounding ethics to the surface and add it to the current literature. This is so that the research can help in some small way, to highlight to current and future academics, engineers and project managers of private companies and charitable enterprises. Thereby making a contribution to the acceptance of IoT AAL.

1.2.2. Who should benefit and why?

The importance of highlighting these ethical issues is to facilitate more widespread acceptance of this technology for the benefit of users. For instance, in a study as far back as 2007, (Tomita, 2007) pointed out that, forty-six elderly users compared to a control group of sixty-seven over a two year period did not decline at nearly the same rate as the control group. In fact, the control group declined significantly over the same period. (Christian, 2014) also goes on to say *“AAL solutions can enable people to live a self-determined life if the systems are adjusted to their needs and seek to compensate their problems.”*

Another study by (Vincent, 2006) showed similar outcomes. In the latter case, results showed no overall decline over a six months period and also showed a reduced number of hospital visits for the users of IoT AAL. Both studies used standard clinical measurements. (Dupuy et al., 2017), however, points out the latter study by Vincent did not have a control group. The reduced number of hospital visits over the same period and a lack of decline shown in Vincent’s study would indicate the importance of AAL solutions.

(Christian, 2014) points out that, it will become necessary for the development of technology solutions to facilitate social support, enable workforce availability and make the care of older people more effective in relation to our healthcare systems. However, it is not only users or care receivers who will benefit, but caregivers can also benefit. (Christian, 2014) again goes on to make the point that, caregivers available resources to take care of elderly people can be optimised based on the presence of monitoring systems (IoT AAL). In the case of cognitively impaired people, family caregivers or relatives can even gain additional spare time; this can have a positive impact on their own mental health.

1.3. The Scope of the Study

The ethical challenges discussed in this research included a number of themes which were found in the literature review. These were the most prominent areas discussed in the literature, and include Privacy, Security, Social Isolation and Behaviour Modification, and these are also included in Table 1.2 below.

There are other headings, including *“The Law”*, *“Ethical Challenges Surrounding Homecare Robots”*, and *“Change of Physician Behaviour towards Patients”*. However, due to the scope of this project, these themes were included in the literature review but not necessarily in the primary research. They remain in the text of this dissertation, however, to try and inform both the author and reader alike of the broader ecosystem in which the subject of this dissertation finds itself.

In the case of *“The Law”*, and *“GDPR”* as a subsection, these are included to inform the reader of privacy rights in relation to their data under European law. It was, for this reason, given a separate section and included as part of one of the questions from the interviews. The following table 1.2 below highlights areas included in the primary research and areas that were not.

In the case of “*Ethical Challenges Surrounding Homecare Robots*”, this was included in the literature, but only one question was asked in the primary research. Although Homecare Robots are “*things*” in the context of IoT and AAL, the subject quite quickly branches off into its own discipline. The question asked in the interview was a broad question to capture a general view on the application of such devices in Ireland from our key informants.

The theme, “*Change of Physician Behaviour towards Patients*”, was included in the literature review but not in the primary research. Like previous themes, talked about such as “*The Law*” this theme was to inform both reader and author alike. However, due to the scope of this project, Physician’s as a stakeholder group were outside the remit of this project.

The final area mentioned here is Regulation. It was mentioned briefly in the final chapter under section 5.2.7 and had a dedicated set of questions to a specific stakeholder in the primary research phase. It is an important theme, however, and is intended for the readers to know about some of the challenges surrounding the ethics of regulation. This is in order to have a more rounded view of our research question and study conducted in this dissertation.

Table 1.2, Status of themes in primary and secondary research.

Included in Primary Research (Interviews)	Included in Primary Research (Interviews), only as part of a question.	Not included in Primary Research (Interviews)
Privacy	GDPR	Change of Physician Behaviour Towards Patients
Security	Social Care Robots	
Social Isolation	Regulation of IoT AAL in Ireland (Not included in the literature review)	
User Behaviour Modification		

Ireland was chosen as the location for our research, due in part to the time frame, the geographical scope of this project and the availability of key informants locally.

1.4. Research Question, Objectives, Timeline and Roadmap

When the pre-literature review of the project started, it became apparent that there is no shortage of literature surrounding the devices and even applications of IoT AAL, and other related technologies such as HIoT and MIoT. However, there wasn’t nearly as much literature surrounding the ethics of these technologies, and especially specific detailed information relating to the use of these technologies in Ireland.

With the growth of IoT set to increase at a pace and this includes health and medical related IoT (Martin, 2018), it was felt that this study would begin to investigate some of the critical problems of ethics in this area. This way engineers, academics and managers could lay the groundwork for a healthy, and ethically sound approach to the application IoT AAL in Ireland.

There was a need to first establish the situation on the ground in relation to Ethics of the IoT AAL in Ireland before there could be an engagement in discussion or conclusion drawn.

The research area that this research is concerned with is “*An Investigation into the Ethical Challenges of the Internet of Things Ambient Assisted Living (IoT AAL) in Ireland.*”

The roadmap for the rest of this dissertation includes a literature review which will determine the most common found using the research methods discussed in chapter three.

Chapter three, Study Design and Methodology, will be a discussion about the research design, approach and the grand philosophy.

Chapter four is the Results chapter, Tables and a flavour of some of the sample responses to questions from the primary research of the study (Qualitative Interviews) will be presented.

The project will conclude with a final chapter, Discussion, Limitations, Recommendations and Conclusion, where all the different parts of this research will come to together to create the grand picture of the ethics surrounding the IoT AAL situation in Ireland.

The time frame for this entire project, from start to finish was nine months. This project started in September two thousand and eighteen and finish on the week of the first of May two thousand and nineteen.

2. Literature Review

2.1. Introduction

In this chapter, a closer look at a number of themes that are directly related to the ethics of the IoT AAL technology and that frequently featured in the literature review will take place. These themes were Privacy, Security, Social Isolation, and Behaviour Modification. These four themes are presented below and were included in the primary research phase of the project. However, other themes presented below such as, *“The Law”*, *“Ethics Surrounding Home Care Robots”*, were included only as part of other questions. In the case of *“Change of Physician Behaviour towards Patients,”* this is not included in the primary research but is included in the literature to give the reader a rounded and informed view of the ethics of IoT AAL.

2.2. Privacy

According to (Patrice, 2016) finding a solid consensus definition surrounding privacy can be challenging, this can be a problem, and definitions range from *“a right to be left alone”* to privacy actually being a commodity that can be bought and sold, and not always in monetary terms. For example (Brey, 2005) points out, AAL or Aml tends to make the user's environments more responsive, therefore making their lives easier by trading customisation information, and gaining cognitive and physical effort reduction in the meantime. Users trade their privacy through customisation information by delegating a certain amount of control to machines; in this way, users lose control to gain control. (Bohn, 2005) goes on to say *“the walls have ears”* and *“if these walls could talk”* are both phrases that now have a disturbing reality or prominence to them.

Another problem apart from definition mentioned above in relation to privacy, is one that comes with IoT AAL and similar related health products, is the capture of medical or health data by what is otherwise called consumer, wellness or medical health products.

(Mittelstadt, 2017) mentions new challenges that exist which include the grey area of the so-called *‘health-related data.’* To what extent will *‘health-related devices’* be classed as *‘medical devices,’* which enjoy more stringent data protection measure? Traditionally medical devices adhered to more stringent data protection legislation such as Article 4 section (15) and (9) of the relatively new GDPR. However, on the other hand, data captured in IoT AAL devices or *‘health-related devices’* which may contain elements of physiological, psychological and even behavioural measures, and may not have that same stringent data protection.

Mittelstadt goes on to say in his papers H-IoT, which is the same as IoT AAL for the purpose of this dissertation, are designed to operate in both public and private spaces. As a consequence of this and owing to the fact that older users are already vulnerable (Pellegrino, 1993, Edgar, 2005), a private window can be opened up into the lives of the users of such devices (Mittelstadt and al., 2017). There is always a

risk under these circumstances of personal data being collected; analytics can then be carried out by third parties in order to socially categorise individuals. (Lyon, 2003).

However, there is the counter-argument, here again (Mittelstadt, 2017) goes on to say health-related data is defined as data relating to the person's physical or mental health and is in fact '*health data*' once it reveals information about their health. This implies the purpose of what processing the data is subject to and not the source that defines the status of the data as '*health data*.' This is covered in more detail in (Recital 35) Article 4(15) of the GDPR according to (Mittelstadt, 2017).

This can only be good news for the user, as it further implies that health-related inferences surrounding data captured appear to fall into the category 'health data' or 'special category of personal data' (Article 9 GDPR) thus extending the legislative reach of protection over IoT AAL data to the same protections as medical data.

Data that is captured with the use of IoT AAL devices and the inference surrounding the user or patient's health data make IoT AAL devices very invasive. This is particularly true when it comes to Big Data analytics of IoT AAL (H-IoT) data (Mittelstadt, 2016). Protection of this data is in fact, equated to the control of the privacy of the individual's personal identity (Garcia-Morchon. O, 2013). However, techniques such as anonymisation and aggregation are suggested to reduce this risk of re-identification of the user, this according to (Hayden, 2012, McGuire, 2012, Joly, 2012) and (Choudhury, 2014), should provide some guarantee of privacy.

With Big Data, one must remember data captured today, no longer has the limitations of memory that existed in the past, data captured nowadays can, in theory, be presumed to exist for years to come in the same condition it was first stored, making it accessible for much longer than first anticipated. This phenomenon increases the risk of privacy violations due in part to the longevity existence of the data, or in other words, the longer that data is stored, the more significant the risk of privacy violations (Mittelstadt, 2017).

Legislation (GDPR) is there in principle to ensure trust between users and service providers. However, one must be equally aware of situations when commercial actors are involved in the IoT AAL data capture and storage. Commercial databases may not be subject to the same stringent data protection laws, unlike medical or academic medical research repositories, (Mittelstadt, 2017).

One area of privacy that may not seem so obvious is Group Privacy, even though anonymisation may be successful on the individual level of preventing the re-identification of that individual. The grouping together of geographical, socioeconomic or ethnic characteristics, just to name a few categories of data, can be used to discriminate or stigmatise against the group as a whole, and is a risk even in anonymised datasets (Docherty, 2014). In fact, this discrimination or stigmatisation may reach beyond those that gave consent in the group or community to those that didn't even give consent (Fairfield, 2014).

(Mittelstadt, 2017) makes the important point that we should all consider, data minimisation may exist in our data protection laws, (GDPR Articles 6-7) (2017). However, a culture of hoarding in relation to data exists in practice. People must be conscious of the potential risk to the users in these circumstances. Health, well-

being and other information pertaining to the user's lives are being digitised, and therefore, there is a need to ensure we only capture the minimal data required.

It is paramount that the design choices and approaches to system design of IoT AAL devices include ethical considerations; this is key to a positive perception by users, and caregivers. Trustworthiness and privacy-enhancing should be front and centre in the design, as IoT AAL devices can create both a granular and longitudinal record of health and activity that can be highly invasive (Mittelstadt, 2017).

In a paper given by (Mittelstadt, 2017), which lists ethical principles based on Beauchamp and Childress (Beauchamp, 2009), and the Organisation for Economic Co-operation and Development's (OECD) Privacy Framework (Woodward, 2009), These principles are listed in table 2.1 below and some can be found in the newest data protection laws (GDPR).

Table 2. 1, Principals cited by (Mittelstadt, 2017) containing ethical principles based on Beauchamp and Childress and OECD.

1.	Facilitate public health actions and user engagement with research via the H-IoT.
2.	Non-maleficence and beneficence.
3.	Respect the autonomy and avoid subtle nudging of user behaviour.
4.	Respect individual privacy.
5.	Respect group privacy.
6.	Embed inclusiveness and diversity in design.
7.	Collect the minimal data required.
8.	Establish and maintain trust and confidentiality between H-IoT users and providers.
9.	Ensure data processing protocols are transparent and accountable.

So far there has been literature and examples of privacy surrounded individuals. However, there is another side to all this, as expressed in the following quotation,

"The value of advancing medical and public health knowledge through secondary analysis of H-IoT (also applies to IoT AAL) must be taken seriously" (IoT AAL) (Schaefer, 2009).

There are those in society who would argue that yes, individual privacy is paramount; however, should it always trump the greater good of societal interests? These arguments can cause conflicts, (Schaefer, 2009); however, would argue the value that can be extracted from IoT AAL data should be taken seriously in the design of data sharing protocols. (Dove, 2014) goes on to say, IoT AAL providers may have a duty of care to the user, informing them of the potential risks of data sharing for research purposes, and organisations who participate in such research should be vetted prior to conducting research.

Therefore, a balance needs to be struck between the rights of the individual and the collective good of society in relation to medical research, for example, disease outbreak tracking as put forward by (Mittelstadt, 2017). Another example (Doyle et al., 2015, Mittelstadt, 2017) puts forward is that of the insight gleaned into the health and behaviours of the user, this can be generated alongside other biomedical data or research to give a more holistic view surrounding public health and epidemiology.

2.3. Security

When people talk about security in the context of IoT AAL, the actions described below as examples can include people and organisations that either act in a deliberate or malicious manner or are unaware of their actions, and are found throughout the literature.

One of the examples put forward by (M. Schukat, 2016) for example, includes Insurance companies and even governments which may be very interested in data pertaining to lifestyle, for instance, obesity or diabetes. In this scenario, a patient may or may not receive discounted insurance or a premium depending on whether they keep themselves active or not. Governments too could offer tax breaks or even tax hikes depending on lifestyle choice or presence of an illness. This could be achieved in a very unethical way by associating a customer and a wireless sensor, thereby indicating the presence of chronic disease.

Another scenario which will go into more detail later includes a user called '*Frank*', due to privacy issues with Radio Frequency Identification (RFID) tags and data stored on Home Care System (HCS), data can be obtained both legally and illegally. Someone may know that '*Frank*' lives alone and knows that '*Frank*' is currently out, or in the hospital for a few days due to data leakage from RFID tags or hacked HSC's. They could break into Frank's house while he is not there (G. Bleser, 2013).

They are also less dangerous scenarios as well, in which both security and privacy is breached by knowing the whereabouts and habits of '*Frank*'; this information can be used for marketing and even surveillance reasons, again this information can be obtained from RFID tags and wearable sensors (G. Bleser, 2013).

(Hensel, 2006, Nefti, 2010) both mention a psychological disturbance called Obtrusiveness (a feeling of 'being watched'), other authors expand on obtrusiveness by mentioning an example of extreme violations including the use of cameras (Caine, 2006). However, it should be pointed out that once IoT AAL is introduced a gradual loss of personal privacy can nearly always be expected (Steele, 2009).

It is because of these actions mentioned above that vulnerabilities can be categorised in two ways according to (M. Schukat, 2016).

- As with most IoT devices, wearable sensors are prone to accidental or deliberate data breaches which expose the patient's information and privacy.
- Users and patients become trusting of sensors, the data they produce and such technologies, leave the patient or user vulnerable.

However, (Mittelstadt and al., 2017) goes one step further and categorises the IoT AAL devices, into three categories explicitly relating to the device, data and practical level implication in terms of ethics.

IoT AAL devices can both violate personal privacy and security while at the same time provide safety to the user of such devices. Sometimes there is a need for the presence of devices in cases where a patient or user can have an intellectual impairment or disability, or where the patient is so frail (see Abbreviations and Acronyms above) that they have to be monitored. This tradeoff can sometimes be justified as there is a need for technology. In fact, the alternative to having in-person care assisted can be more intrusive according to, (Melenhorst, 2004, Steele, 2009) and (Ojasalo, 2010).

One area that hasn't been touched on yet is the application of a physical attack on a user or patient of IoT AAL devices in order to cause the patient harm or worse. When there is such mention of that type of attack, the reference is in relation to Glucose Monitors, however, that is just one example. Actuators explained in Abbreviations and Acronyms, can be used to administrate both the correct (under normal operations) and the incorrect amount of insulin to the patient in the case of hacking with malware or other means.

Another scenario involves violations of both privacy and security, and is put forward by (Patrice, 2016) in their paper *"Privacy Challenges in Ambient Intelligence Systems."* In this scenario, our user 'Frank', mentioned earlier, who is seventy years old has Alzheimer's and lives alone. 'Frank' has an HCS installed which helps him in critical situations such as medical emergencies and stressful events. 'Frank' also wears a health bracelet, which measures things like heart-beat, body temperature and even daily distance travelled while out exercising, usually on a call to his daughter 'Jane' who lives close by. However, this closeness to relatives might not always be the case, and this must be stressed in our explanation of the scenario here.

This bracelet communicates via a smartphone and app back to the HCS mentioned above which includes GPS coordinates of the current location. The bracelet itself might give personal details such as the user's name, address, age and even the user's medical profile including emergency contact details (Patrice, 2016).

In this scenario, 'Frank' also has a Radio Frequency Identification (RFID) reader in both his own house and Jane's house; when 'Frank' is close to Jane's house, the RFID reader lets 'Jane' know 'Frank' is close by. See Figure 2.1 and Figure 2.2 below, simple home care system, and the route 'Frank' take, which may help with the explanation.

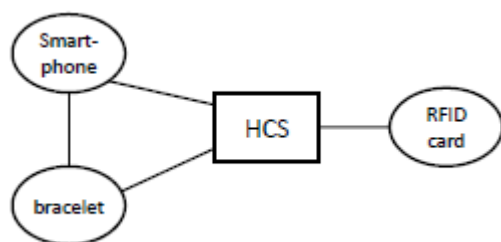


Figure 2. 1, Simple Home Care System (HCS).

(Patrice, 2016)

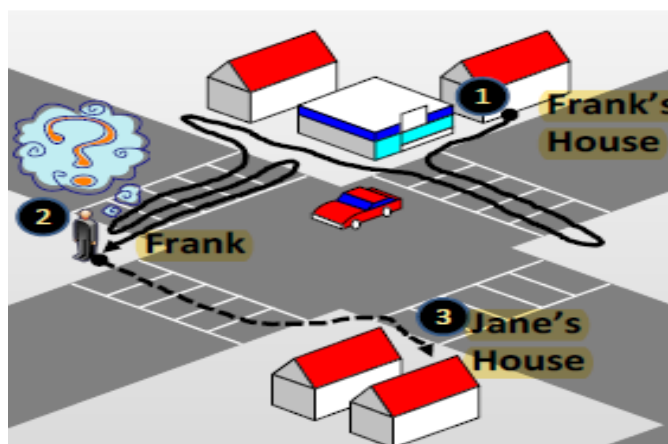


Figure 2. 2, Frank's route to Jane's home.

The problem with this situation surrounding the RFID tag is anyone with an RFID reader or in fact, multiple RFID readers spread over a geographical location can pick up on Frank's location as he passed by their reader. They then know that Frank is out of the house and could break into his house, this could also be a valid scenario if, for instance, the perpetrators of this type of crime knew that 'Frank' is away in a hospital for a number of days (Patrice, 2016).

It is therefore imperative that the devices should be tested to prove functionality and long-term assurances related to the security, reliability, and safety of the device prior to entering the market. Safety and therefore security is of particular importance when taken into account the use of devices with actuators or location information, imagine a glucose pump failing or giving the wrong dose to a diabetes patient?

It is paramount that it is not forgotten the lessons about securing the physical device along with its information privacy needs as well, according to (Langheinrich, 2001), privacy by design principles should be used by default. In relation to security profiles on devices such as HCS's, the maximum privacy first setting should be the default configuration on devices, and it's up to users when the system is being installed to select what best suits them in the potential privacy and security trade-off. Failure to have robust privacy and security practices in place will continue the mistrust amongst IoT AAL devices; trust should be a prerequisite for any IoT AAL device (Bagués, 2010, Huckvale, 2015, Sajid, 2016).

2.4. The Law

2.4.1. GDPR

Before jumping straight into a General Data Protection Regulation (GDPR) discussion, there is a need to address the definition of consent, which is at the core of GDPR. Article 4(11) addresses this theme with the following definition.

"Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Mira, 2016).

One of the core concepts of GDPR is to increase the digital rights of the EU citizen in relation to decisions surrounding consent, processing of their data and use of that same data. However, it does not stop there, developers of IoT products and services and by extension IoT AAL "things," also need to have permissions to access user data. So it's not only people who need permission to access other user's data but also devices which carry out services and functions (Wachter, 2018).

One example given by (Wachter, 2018) is the use of Biometric authentication methods which has grown in popularity in the last number of years (Khodadadi, 2013). Input from such Biometric devices includes activity, and behavioural modelling (S. Batool, 2017), accelerometer data, Electrocardiogram (ECG), Vein recognition and Iris recognition that can be used as an authentication method (N. Karimian, 2016).

However, this type of authentication can leave an exact fingerprint of the individual, and inferences surrounding their health (Brent, 2016). In addition to this fingerprint, both (S. R, 2014, Mahmoud, 2012) go on to say, multiple streams of data relating to user health combined with geographical data can be used to violate the privacy of users of IoT further and by extension IoT AAL by more in-depth inferences surrounding individuals.

These examples serve as a reminder of the importance of consent from both human data controller and control over machines. Following on from our consent and introduction paragraphs GDPR, we will now have a look at GDPR with a limited view, as a detailed discussion is beyond the scope of this thesis.

GDPR is a piece of legislation brought into focus a number of years ago on April 2016 but only really came into effect two years later on the 25th of May 2018. It contains ninety-one articles and over thirty thousand words (Radiology, 2017). GDPR deals with a whole host of data issues including transparency, storage, access, rectification, deletion (Article 5) and informed consent mentioned above (Article's 4 and 7) just to name a few (Wachter, 2018). The problem for organisations and service providers is that if they fail to comply with the legislation, they could be in for stiff financial and reputational penalties (Neame, 2014).

2.4.2. A more in-depth look at some of the Articles of GDPR legislation

Let's begin with our first article, Article 8 of the GDPR. In Europe, the fundamental human rights to private life, family life, and personal data protection fall in under Article 8 of the Council of Europe's convention on human rights (Mira, 2016). Article 17 which in some ways leads on from article 8, gives the consumer or user the right of erasure of data, and no longer subject to processing when the reason for the capture of the original data is no longer valid.

In fact, this article 17(1) also extends to situations where consent has been withdrawn, or an objection has been raised by the patient or user in relation to the processing of their own data. However, exemptions exist, Article 17(3) Recital 66 and 67, in this instance, data can be kept for health and scientific research (Mira, 2016).

Staying on article 17, another extension of this article is in section (2), which deals with the '*Right to be forgotten*', this means if a user or patient requests to be forgotten. All links, copies or replications of their data needs to be erased, and this request also needs to be passed onto other data controllers who may have a copy of the user or patients data through the first data controller from which the request to be forgotten has come. However, the legislation also mentions the term '*Reasonable steps*' which implies the technology availability and technical procedural skill needs to be there to carry out the task (Mira, 2016).

Like the previous legislation that GDPR is replacing, access to personal information or data is also a right. Articles 13, 14 and 15 cover this right, in the case of Article 15, this leads on from Article 5, transparency mentioned above. However, Article 15 (4) Recital 63, restricts access to data where there is a risk of trade secrets being leaked. While article 12 and 20 cover the right to transparent information and data portability

respectively. Data portability is the data subject, patient or user's right to take a copy of their own data and give it to another data controller even if that is in a different EU country (Wachter, 2018).

While Article 16 deals with the right to rectification of their own data, that is when there are mistakes in the data, and the user or patient wants these mistakes corrected (rectified). Adding to this list of articles is the '*Right to Object*' in relation to data held on patients or users, and this is covered under articles 21 and 22 (Mira, 2016).

One of the up and coming trends with IoT and therefore, IoT AAL is the issues of 'Big Data.' An issue that is addressed under GDPR which will most certainly be of interest to IoT AAL. Big Data privacy is the problem of decisions being made in relation to people by means of algorithms and automatic processing or profiling. These are covered in Article 13 (2)(f), Article 14 (2)(g), and (Article 29), (Wachter, 2018). This issue is especially important in the context of IoT AAL because of the failing health that is expected with the ageing process, and this could affect the users understanding the importance surrounding such matters. Everything from health insurances, to insurances in general, of vulnerable people in our community is at stake (Saurwein, 2015).

The last article we are going to cover here is article 13. This article pertains to the right to know who is processing your personal data and will it be revealed to third parties? If your data is to be revealed to third parties, you have the right to know under what circumstances, will this be the case. Finally, you also have the right to know how to withdraw consent and even how to have the data in question, erased (Wachter, 2018). In summary, then, the following table 2.2, will hopefully categorise at least some of the different articles that we have felt is specific to IoT AAL in Ireland as a member of the EU.

Table 2. 2, Summary of GDPR Articles, and Subsections.

GDPR		
Articles	Sections	Relates to:
4	(11)	Consent.
8		Private life, family life, and personal data.
5, 12		Transparent information.
13		Right to know who is looking after your data.
13, 14, 15	Article 13 2(f), Article 14 2(g)	Access to personal information.
16		Data Rectification.
17		Erasure, where data is no longer subject to processing once data is no longer relevant.

17	(1)	Consent was withdrawn, or objectives raised to use of personal data, by the data subject.
17	(2)	The right to be forgotten.
17	(3)	Exemptions such as health and scientific research.
20		Data portability.
21, 22, 29		Automatic Processing of decision making based on Algorithms and Profiling.
25		Privacy by design & default.
33, 34		Cybersecurity.
35. 36		Data Protection Impact Assessment.

2.5. Social Isolation

One area in need of a discussion is Social Isolation, caused by the convenience of the IoT AAL technology applications. For example, (Chan, 2008) goes on to say, studies have shown concern surrounding older people and the use of IoT AAL technology, the technology was never meant as a replacement instead of an augmentative tool to existing practices (Percival, 2006).

In fact, (Redmond, 2014) raises a critical point in a scene in the paper *“Unintended Consequences of Wearable Sensor Use in Healthcare”* by (M. Schukat, 2016), which goes on to describe a situation where an older relative is using an automatic fall detection pendant. The family, of course, feel relieved that the burden of care has been somewhat reduced if the relative falls, the device will work a hundred per cent of the time (in theory), and they don't have to call as much. However, for any of us who have worked with technology know, even the best-laid plans and theory can fail for the unlikeliest of reasons.

What has happened in this scenario is the device failed due to inadequate detection sensitivity, resulting in a failure to notify anyone that the user has in fact fallen. The result is the user or patient has been left for hours in a situation in which they can't move. This is just one example where a unique device needs to be backed up with more than one sensor device in order to ensure a more complete *‘picture’* of the scenario with the patient or user is obtained (M. Schukat, 2016).

For instance, a movement sensor to detect prolonged periods of time where a patient hasn't moved, alerting the relevant people that something may have gone wrong. With the right multisensory environment, a phone

call would be being made to the user to ascertain if everything is all right, the alert would have been put out then when the realisation that everything was in fact, not all right.

Are we engineering new problems for ourselves by designing systems that give the impression of substitution rather than augmentative towards existing procedures and practices? (M. Schukat, 2016)

Another author can be referred to in order to take a slightly different angle to answer this question, (Wallace, 2010), who goes on to say in the case of mild cognitive impairment (MCI) patients or users, special needs and requirements may not be apparent to the development and researching teams. In fact, (Wallace, 2010) also goes on to emphasise a need for feedback from the user or patient in the design process in order to reduce errors and prevent technology rejection.

One example of rejection may be a system that has a high learning requirement; this combined with diminished capabilities of the user has a higher likelihood of failure. To elaborate on this, for example, blinking LED's, many vibrating sounds and even screw heads that look like a button or some other anonymous object and cabling can cause confusion leading to frustration will most likely lead to a reject of the technology (O'Neill and al., 2011a).

(Abascal, 2007) and (Francis and al., 2009) both mention the need for customisation and adaptability in high-quality products in order to stimulate acceptance of the technology. (Decker, 2012) recommends a *'titration'* approach to define the needs of a user; this can take the form of self-reporting to find standardisations and personalisation for the various participants.

2.6. Ethical challenges surrounding Homecare Robots

Homecare Robots which can also be called Social Care Robots and sometimes Social Service Robots (SSR), will be abbreviated to the word robot for the convenience of writing this section. The author (Kortner, 2016) uses the same terminology (robot) from which a lot of the literature from this chapter comes from. When we mention ethics and robots, which is also known as Roboethics, and key to our discussion in this section, we are referring to the content of the Universal Declaration of Human Rights under the framework of the Treaty of Lisbon (2000). This applies according to (Kortner, 2016), to the identity and application of ethics toward issues that may arise *"from both current and upcoming robotics applications."*

Such issues should be coherent with Human rights and dignity as we have come to expect (Kortner, 2016).

However, situations can occur quite readily when we fail to meet these strict requirements as laid out in the Lisbon Treaty mention above. For example, in the following paper written by (Kortner, 2016) called *"Ethical Challenge in the use of social service robots for elderly people"*, a social robot called Henry is not tested for all situations, and therefore may not meet all the requirement or situations that it will encounter, even with the best of intentions of its designers.

In this situation put forward by (Kortner, 2016), Henry has a touch screen that is more suitable for people who are standing. However, people in wheelchairs, therefore, cannot access the touch screen. Is this

situation fair to all people that may use the robot? Unfortunately no, and therefore, as you can see, situations involving ethics can quickly arise, and this example is one such case. (Kortner, 2016) does not offer an explanation of why Henry was designed this way. However, he does go on to say

“In order to know what users regard as helpful and how they can operate the robot, prototypes have to be tested with (sometimes) vulnerable groups.”

These robots, social robots were designed around providing support for older people in their place of residence, and a tool to go some way towards addressing the Social Isolation issue. These objectives were meant to be achieved by displaying what can be called human-like interactions with their users (Misselhorn, 2013). For instance, (Hegel, 2009) states,

“...it implies the robot to behave (function) socially within a context and second, it implies the robot to have an appearance (form) that explicitly expresses to be social in specific respect to any user.”

(Saito, 2002), go on to state that, the results of residents showed improvement during and afterwards in feeling, laughter, depression levels, group participation and activities, from interactions with a robot seal called Paro. These findings were observed through facial expressions, reactions of vital organs in residences, and urine samples. However, (Klein, 2009, Shibata, 2011) make the point that a similar finding of physical and psychological effects can be found using an animal companion.

However, (Klein, 2011) points out these finding mentioned above are relevant in group therapy, while the use of robots in the one-to-one bases can actually lead to introverted, almost sedate and withdrawal type behaviour.

(Prince, 2015) expresses the following point, given the ratio of carers to user's or patients, robotics in assisted care could complement the current provision of care, and therefore reduce the burden on unpaid carers and maybe even improve the quality of care (Bharucha, 2009). Robots and the combination of IoT AAL can help older adults, especially those with Dementia achieve greater independence and autonomy by carrying out what to the rest of us are otherwise routine tasks or activities (Rashidi, 2013). Robots according to (Mordoch, 2013), can even assist in the emotional dimension of patients or users, alleviate agitation, loneliness and social isolation. They can also improve the emotional wellbeing of the user or patient.

However, (Decker, 2012) makes the point that one customisation that is needed is a veto function to stop robots carrying out its actions. (Portet, 2011) mentions in field trials the fear by individual users that technologies (robots) have a life of their own. With cognitively impaired individuals, however, this function may need to be withdrawn. Robots like any technology need to be considered in the context of sufficiently replacing some of the interactions between users and human carers or visitors. However, it must be pointed out; these interactions won't entirely replace face-to-face interactions, as they contribute to the patient's mental health and well-being.

When ethics is explicitly looked into in relation to social care robots, the heading that materialises is related to both the ethics of IoT AAL in general and robotics specifically. For instance, Privacy, and by extension Data Protection and Isolation appear both in the literature of IoT AAL and social care robotics. However, there are a number of headings that are specific to social care robots as well; these include, Dignity,

Deception, Safety and vulnerability. It is beyond the scope of this dissertation to give a fully comprehensive literature review of ethics surrounding social care robots. However, as robots are moving into the area of IoT AAL through continues testing and exploration, and therefore, are considered a subsection of IoT AAL “Things,” More detail surrounding the Roboethics headings mentioned above starting with our first heading, Deception will start below.

2.6.1. Deception

The appearance of a robot is quite essential in the expectations of what the functionality or even its perceived level of “*Intelligence*” is (Kanda, 2004). Speech is another factor that is considered quite important, robots can be machine-like or even polite and according to (Panek, 2015), depending on whether a robot can produce (preprogrammed) or recognise human speech, can give the robot its “*personality*.”

One type of robot that can be found in care situations are robots designed to exhibited emotional responses. According to (Broekens, 2009), the more free and intricate the design, including the behaviour of the robot, the more blurred the lines become between machine and living person become (Kortner, 2016).

Children and older persons according to (Kortner, 2016), may project emotions into the robots that are not truly there. (Turtle, 2006) goes further and says observations that they were involved in showed older people forming an emotional attachment with robots, which led to participants worrying about the robot missing them when they were not there, for instance, when they left the house. This according to (Sparrow, 2006) leads to the question of whether robots can be seen as devices of deception.

This situation, however, is unethical. Robots are known as not having conscious or emotion. Despite the unethical nature of this situation, everyone has the capability of anthropomorphising objects. Everything from dolls to motorcars can be anthropomorphised according to (Epley, 2007). The problem for older people, however, is false hope or trust in machine objects (robots), this according to (Kortner, 2016) can cause stress in relation to deception and expectations management surrounding older people.

2.6.2. Dignity

The object of the exercise according to (Wada, 2005) when dealing with emotionally related robots, is to engage the user (usually a dementia patient) in interaction and activation behaviour, thus motivating them. However, Infantilisation and patronising occur with older adults in dementia situations. The infantilization of this older group violates the human rights of users or patients and therefore is considered morally wrong in geriatrics according to (Fruhwald, 2012). Another factor (Fruhwald, 2012) points out that is easily overlooked is a group activity, which could account for some of the improvements apparently seen in the use of robots.

(Kortner, 2016) points out, Henry our robot introduced above, had patients from a physiotherapy walking group following him around whilst he played traditional music, in this case, up and down the corridors of the

residence where the patients were living. This behaviour according to (Kortner, 2016), asks the reader, is this Infantilisation of the patient or is there a real benefit in terms of emotions and activity?

2.6.3. Isolation

One of the main reasons put forward by (Parks, 2010) for resisting the introduction of robots into social care, is the idea of isolation that robots would cause. Another author (Von Stosser, 2011) explains that the use of robots in institutions could minimise contact from human carers, and therefore deprive them of genuine emotional contact. (Von Stosser, 2011), however, highlights the following situation in institutional care which may be seen as siding with robots,

“Even without robots, today’s operations in care institutions come down to mere handling of patients which reduces the human being to an object” (Von Stosser, 2011).

(Sharkey, 2012) then goes on to say, the more people communicate with robots, the less likely they are to communicate with their human counterparts, this may be especially true with senior citizens who may be cognitively impaired. Evidence exists that indicates the more people communicate with other people in social networks, the longer the period before the onset of dementia.

However, such evidence is lacking in relation to robotics. Therefore, the potential danger exists in communication with robots as a replacement for human communications, and where this outweighs the objective of increasing independence, the use of robotics become an ethical issue according to (Sparrow, 2006).

However, (Borenstein, 2009) goes on to say, other developers and engineers would argue that the possibilities of robotics and even other assistive technologies could actually promote or improve communications between humans.

2.6.4. Privacy and Robots

It has been found according to (Beach, 2009), that people with a greater need for care are most likely the same people who are willing to give up their privacy. This is including very personal situations such as recording vital signs and even toiletry behaviours with the use of camera technology. However, these situations involving toiletry situations are the least desirable. Therefore, a basic understanding of the risks associated with autonomy gain versus personal data management should be pointed out to users prior to using the technology (Wagner, 2010).

Privacy does not stop with the primary user or patient, other people in the same environment as the user can also be affected by robotic technology. For instance, in the case of our robot Henry, introduced above, care staff in the institute where Henry was deployed could also have felt monitored as well.

(Denning, 2009) goes on to say, simple domestic robots could easily be located, hacked and even controlled by remote parties. However, it does not stop with small domestic robots; bigger more complex machines can also be subjected to the same risks. This can result in data loss for users which can lead to a loss of control and autonomy resulting in the feeling of objectification (Sharkey, 2012). It's for this reason that the importance of being in control of the robot and not the other way around is crucial. Two tools that are useful according to (Kortner, 2016) is informed consent to address privacy issues. However, another tool is the registration of the robot with the data protection agency in charge; this then ensures compliance with the laws surrounding the use of robots in care situations.

2.6.5. Safety

Robots no doubt can cause damage when accidents occur; however, this is not intended, at least not in the social care setting. The risk, however, cannot be ruled out, and especially when robots are still in the prototype stage. For instance, if we refer back to our robot called Henry, mentioned above, Henry has been known to bump into people who were assisting patients in wheelchairs as they and Henry met on a corner of the corridor. In another instance, Henry fell down a set of stairs. The question that arises, who is liable in this situation? Is it the engineer, designer, company or even the user themselves? (Kortner, 2016).

People when they first encounter a robot, may not feel safe; this is despite the robot meeting the safety requirements laid out in standards or legislation. An example (Kortner, 2016) uses, a person in a wheelchair may feel endangered as a robot moves past them. Therefore, space between the robot and the wheelchair user is essential in this instance.

2.7. Change of Physician behaviour towards patients

One risk associated with IoT AAL is that of the simplification of the output of sensors to parameters, and their follow-on processes. If people allow IoT AAL devices to do this contextually, it means this could bias the results towards an overly optimistic prediction (Mittelstadt and al., 2017). A key challenge for the physician is to ensure their view of the patient's case isn't altered unnecessarily and incorrectly by filtration of data through interpretive frameworks built into the monitoring systems (Lyon, 2003, Hildebrandt, 2008). Monitoring data supplied to the team and patients due to summarising and simplification can vary in the degree of complexity and completeness, and this can lead to value-laden data (Gadamer, 1976).

The risk here of objectifying measurements of health and well-being through monitoring and summarising data means human and the social embodiment of the person's contextual factors along with the data collection context, may not be taken into account leading to a '*veneer of certainty*' (Haggerty, 2000). This may all lead to the quality of care provided be of a lesser standard because it undermines clinical and benevolent care.

It is therefore essential to understand that IoT AAL data is complementary rather than a replacement for traditional physical examinations. Things like social, mental and even emotional state can be missed if examinations are relied upon entirely by the sensor and remote monitoring data. The relationship therefore between Patients, Medical staff and Manufactures of IoT AAL devices and services need to be developed further in order to build trust and norms in the governance of IoT AAL devices (Mittelstadt and al., 2017).

2.8. Behaviour Modification

The explanation given by (Hensel, 2006) in the Abbreviations and Acronyms section surrounding the definition of Obtrusiveness will be repeated here for our convenience, and is just one aspect that can cause behaviour modification :

“a summary evaluation by a person based on characteristics or effects associated with the technology that are perceived as undesirable and physically and/or psychologically prominent” (Hensel, 2006).

A discussion will take place about more behaviour modification below starting with (Courtney, 2008), who goes on to say, behaviour can include walking around pressure sensors or even disabling the systems of AAL altogether. After some time such devices in the environment that the user is living with are forgotten about, as consent can be seen as a once off event.

Therefore it is essential for patients or users to be reminded that monitoring is still going on for validity and purposes. Cognitively impaired persons also need to be reminded that the technology is still there as well, as they may not be able to give consent themselves (Kenner, 2008) and (Bowes, 2012). Outside of this circle, guests of users can be inadvertently monitored using IoT AAL while visiting loved ones.

Another aspect worth noting that may have both positive and negative changes on user behaviour is nudging. Behaviour nudging can be easily overlooked; however, it can be used in several ways to change user behaviour. An example given by (Mittelstadt, 2017) shows that providing personal feedback on health or activities can help by nudging the user towards a goal set out by a device, care team, service provider or public health promotion. Nullifying can be enhanced by the design of the device where emotion can be attached to the device due to its aesthetic looks. However, on the downside care needs to be taken to ensure the autonomy of the user is not undermined by pushing the user towards an institutional goal, or promoted third-party interests rather their own preferences (Johnson, 2013). It's essential, therefore, to design acceptability of nudging around promoted interests that are beneficial towards the user rather than third parties or commercial parties.

As is known Visibility in terms of IoT AAL devices is the noticeable presence of such devices in the environment. Unlike Obtrusiveness, Visibility is the aesthetic aspects of the device which impacts the perceptions of users which can include ease of use, size and even the weight of the devices (Landau, 2010).

Both Obtrusiveness and Visibility can cause a user to change their normal behaviour, or daily routine, decision making, personal identity and even cause stigma associated with their illness, and cause the patient or user to take risks in order to assert their independence (Percival, 2006, Courtney, 2008, Essén, 2008, Tiwari, 2010), and (Remmers, 2010),.

(M. Schukat, 2016) also goes on to make the following point, if sensors are visible to other people, this can bring personal, social, positive and negative feedback not to mention whether such feedback is even wanted or not. For example, in a positive light other people may see such devices as positive self-control, while negative feedback may erode the wearer's privacy.

Sensory devices can also be used to give feedback on physiological parameters in order to motivate them to change their behaviour. As (M. Schukat, 2016) goes on to say, some wearable sensors are used to track a patient's physical activity or medication regime, Adherence Management System or AMS for example sometimes uses a patch on the belly to check pills have been taken.

However, sometimes these AMS systems can lead user or patients being "*coached too intensively*", and when the device or technology is no longer available, the user or patient cannot adhere to the regimes without the device (M. Schukat, 2016). Another more complex scenario with medication and monitoring devices is a polypharmacy situation, Users who are sometimes required to take large amounts of drugs may modify their regime against their doctor's wishes to avoid the side effects of their medication.

They may even avoid taking certain drugs altogether. However, once a drug monitoring regime is introduced this can trigger the very side effects they were avoiding or even cause the user to withdraw from the regime altogether. This may result in a visit to their doctor or an unscheduled hospital visit resulting in the user being put on a regime that actually works for them. One could view this as both a positive and negative issue as a result of medication monitoring devices (M. Schukat, 2016).

When a patient is introduced to a medical monitoring device, one behaviour that can happen is they become anxious or "*Hypochondria*" surrounding their health situation.

The widespread problems of addiction to smartphones is already known (Stone, 2014, Deb, 2015), while (M. Schukat, 2016) goes on to point out, wearable medical monitoring devices are not as pervasive as standard smartphones. However, this addiction can be experienced in wearable health technology as well when patients become obsessed with self-monitoring (Smith, 2015).

The problem here is because these devices and methodologies (before and after paradigms) often target the actual outcomes of the behaviour modification such as physical activity, blood pressure, and adherence to set lifestyle or disease management programs. The user can often change their behaviour for the worst.

In fact, according to (Maguire, 2011) and (M. Schukat, 2016) patients may decrease their physical activity because the device has indicated the user has reached their goal, while before the use of the device they may have done more exercise because they didn't know precisely how much activity they had done.

This type of behaviour modification is sometimes referred to as "*trained helplessness*" (M. Schukat, 2016). After a period of time, the support of the technology has led the user relying on the device. (Kosta, 2010) also points out that users of IoT AAL technologies can become prisoners in their own homes due to over-

reliance on the technology. Thus when the device is removed the patient, or user reverts to a level below that of the required standard, they would achieve with the device.

For example, (Van Hoof and al, 2011, Portet, 2011) make the point that there is a particular fear that exists surrounding the failure of the device, in this instance, to power cuts or a breakdown in the technology itself. This is especially important when taken in the context of life, and health logging sensors are at play, or when an annoyance is being caused in some users, partially because of the volume of false alarms that need to be investigated to rule out real alarms (Van Hoof and al, 2011).

(Van Hoof and al, 2011) mentions the failure of automatic beds that have deflated during such examples as a blackout. Similar battery-driven devices, sensors and even external devices should avoid causing problems for people with mobility problems when installing in their homes.

Moreover, caregivers themselves have been known to show over protectionism in relation to care receivers (users) in their charge, this over protectionism in question usually relates to privacy issues and can result in IoT AAL or ICT devices, in general, being brushed aside regardless of the needs of the or user. Caregivers in this case often rely on previous or more traditional methods of caregiving (Sponselee, 2008, Robinson, 2009). This is another reason why the design of such devices should be very much user-centric.

2.9. Conclusion

In this chapter, a number of themes were included in our literature review such as Privacy, Security, Social Isolation, and Behaviour Modification. However, there was also included a number of other themes that were not in the primary research to give a more informed and rounded view of the subject that is the Ethical Challenges of IoT AAL. These included Changes of Physician Behaviour towards Patients, Ethics Surrounding Home Care Robots, and The Law. The object of the literature review was to give the reader a broad but somewhat detailed view of the situation surrounding the ethics of the IoT AAL. Equally, where there was an opposing view, an effort to include both sides was made.

3. Study Design and Methodology

3.1. Introduction

This chapter covers the research methodologies, key informants recruitment and identification, ethics approval process, why the use of qualitative research and why specific qualitative methods were used. Also included in this chapter, is the approach to data collection and analysis.

A new theme that was included in the list below was, the Regulation of the Internet of Things Ambient Assisted Living in Ireland to give a more rounded view of the ethics of IoT AAL.

Social Care Robots was another theme or heading that didn't dominate but more on the fringes of the literature review. However, a research question was included in relation to this theme. The reason for a limit coverage of this theme was mostly to do with the scope of this project. The study of robotics would in itself require an entirely separate study.

3.2. The Rationale of Research Question

As discussed in the literature, one of the critical barriers to acceptance of IoT AAL technology amongst users is the existence of ethical challenges. If the central issues of ethics surrounding the technology of IoT AAL can be brought into one location, coupled with the views of key informants who work with Assisted Living technology, then maybe the ethical issues can be tackled by highlighting these issues more clearly for engineers, manufacturers, managers and academics alike.

Finally, the name or word Ireland in our research question is a boundary defining word or name. It deliberately limits our project scope to Ireland. Otherwise, the project would become too big for the time frame and resource limits, which include financial constraints (travel costs) in which the project has to work.

3.3. Research Aim

Just to remind ourselves, our research area is:

“An Investigation into the Ethical Challenges of the IoT Ambient Assisted Living in Ireland.”

What was to be achieved, is the capture of key informants professional views on the ethics surrounding IoT AAL in Ireland under a number of headings or themes that were discovered in the literature review, including:

- Privacy.
- Security.
- Social Isolation.
- Behaviour Modification.
- Regulation of the Internet of Things Ambient Assisted Living in Ireland.

These themes were the most dominant (apart from Regulation) to emerge from the literature. An effort was made to try to make sense of the ethics in the literature review (Secondary Research) and possibly discover new material (themes) that may emerge in participant organisations by interviewing key informants (Primary Research) and hopefully adding this back to the current literature.

The following diagram, Figure 3.1 below, is an overview of the research process, the big white arrow at the bottom of the diagram illustrates the process of adding back to the literature review, any possible findings that come from both the Results and Discussion, Limitations, Recommendations and Conclusion chapter.

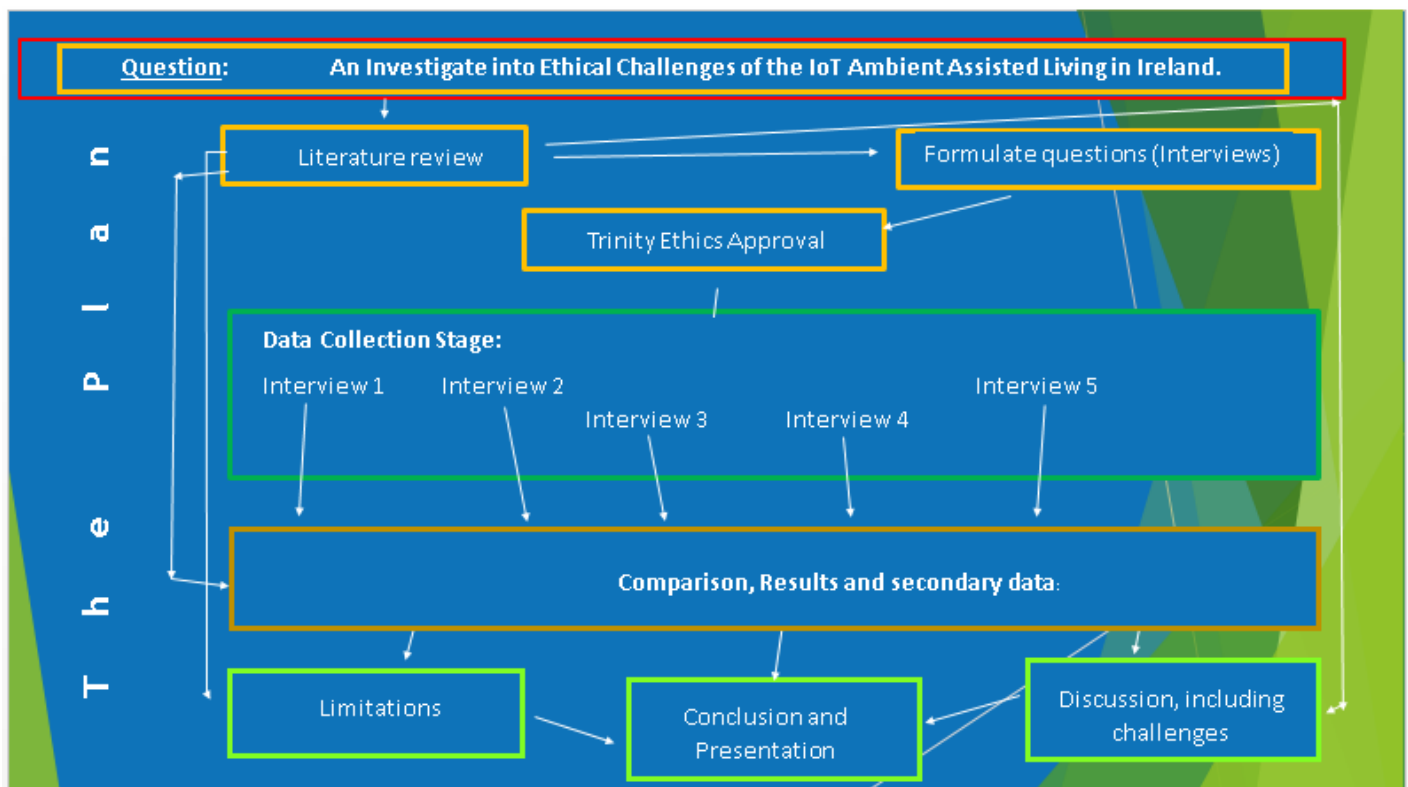


Figure 3. 1, Overview of the research process.

3.3.1. Interview Questions

Interviews were conducted with participants coming from a charity organisation, two project leads, linked to different parts of the overall (Project noted) portfolio in (Location 1 noted) and (Location 2 noted). One Robotic Engineer who is also an academic with a background in assisted technologies and robotics, and who also provided essential insight into the application of robots and social care. Another academic who works with the regulation of medical devices, which includes IoT AAL technology. It was hoped that by including a person from regulation, this study would have a more rounded view of the ethical situation involving IoT AAL in Ireland.

Participants were chosen because it would give the study a broad spectrum of people that work with the IoT AAL and other related technologies, and therefore have plenty of working and academic experience that they could share with the research. By selecting a broad spectrum of people with these skills and knowledge, it was hoped that this initial investigation would capture a diversity of views.

There were eight major questions, and seven minor questions created based on the literature review's themes, see table 3.1 below. The use of terminology surrounding the words major or minor was an attempt to structure the interview within a forty-minute timeslot.

Each theme emerged out of the literature review had a number of questions and sub-questions in relation to its subject matter, and these were grouped in order of importance from the top down on our questionnaire sheet found in Annex C.

Table 3. 1, Question Type, Number and Subsection.

Question Type, Number and Subsection		
Subsection	Major	Minor
<i>Privacy</i>	1	1
<i>Security</i>	0	2
<i>Social Isolation</i>	2	0
<i>User Behaviour Modification</i>	1	2
<i>*Regulation of the IoT AAL Technology</i>	4	2
<i>Total Question Types</i>	8	7

***Note:** Questions for regulators only.

3.4. Research Approach and Design

Two methods were employed in the research, which is presented below; these are Literature Review and Qualitative Research.

3.4.1. Literature Review

The literature review involved searches across seven different databases that were available to the University of Dublin at the time of writing this dissertation. The search string that had been developed was manipulated according to each database, the reason for this is because each database has a particular way of searching with the use of special characters, commonly referred to as ASCII (American Standard Code Information Interchange) characters. In this case, these characters were brackets around particular groups of text and inverted commas to encapsulate phrases. Some databases also have a controlled vocabulary; therefore, we included as many possible words and phrases as we could to ensure nothing was left out.

The following table 3.2 below is the list of databases that we used in the literature review and the search string on the right of the table is the general format that was used:

Table 3. 2, Database list and Search String.

Database Name	Search String
• ACM Digital Library	(("internet of things" OR IoT OR "ubiquitous computing" OR "pervasive computing") AND ("ambient assisted living" OR "assisted technology" OR "intelligent assistive technology" OR AAL OR Aml) AND (ethics OR "ethical challenges"))
• EMBASE	
• IEEE Xplore Digital Library	
• JSTOR	
• PubMed	
• Science Direct	
• Web of Science (all databases)	

The overwhelming majority of documents we ended up with were PDF documents, and from here these were filtered down. This was done by reading the Abstract, Conclusion, and Introduction to test the relevance of the document to the research.

Documents that were borderline were downloaded, and an internal search of the document with the words privacy, security, ambient assisted living amongst other words or phrases using the Find function was carried out. If such words were found, reading around the location in the document where the word was

found to indicate relevance, taking note of the frequency of relevant words found, helped to make a decision whether a document was dropped or included in the shortlist.

Relevance was determined by the research question, which set the boundary or scope constraints of our research. No preconceived ideas were brought into the literature review, so no expectations surrounding what the literature review would give was imagined. Equally, there was no bias or previous experience in the area of IoT AAL, and more specifically the ethics surrounding this area. Therefore, the available literature shaped the research themes which were used to develop the strategy for the primary research stage (interviews).

3.4.2. Qualitative Research

A qualitative research approach was chosen to try to bring forward information if it existed with the stakeholders and make sense of it. The objective wasn't to try to solve a hypothesis or theory, therefore, unlike quantitative research methods, which deals with measuring numbers and variables. Qualitative methods were deemed more suitable; this is a human problem rather than a problem of numbers or variables. As (J, 2014) p. 4 goes on to describe qualitative research as "*an approach for exploring and understanding the meaning individuals or groups ascribe to a social or human problem.*"

The particular type of research that was being conducted in terms of actual design falls under what is described as phenomenological research, an inquiry or investigation into the experiences of our key informants. The participant's or critical informants in the research are the members of the stakeholder map, Figure 3.2 below. (J, 2014) p. 14.

3.5. Characteristics of Qualitative Research

The following three characteristics of qualitative research as defined by Creswell, (J, 2014) have been used in this dissertation.

3.5.1. 'Researcher Key Instrument' (J, 2014), p. 185.

Data has been collected through semi-structured interviews carried out using key informant participants from organisations that represent some of the stakeholder membership, see Figure 3.2, Stakeholder Map below, around three to six interviews, but no more than ten. Interviewing the participants at their own work locations, or alternatively somewhere close, which is both comfortable and devoid of distractions was thought to be the best approach. Semi-structured interviews were chosen, as this would allow participants

every chance to express their professional and experienced point of view without the rigidity of a Quantitative investigation.

3.5.2. *'Participant's Meaning'* (J, 2014), p. 186.

The attempt was to learn the meaning that participants hold about the problems of ethics in IoT AAL, and try to bring these meanings to the forefront.

However, at the same time, there was a need to steer the participant towards a number of questions in order to discover information surrounding a small number of key themes that came out of the literature. Discovery of a number of new heading not in the literature may occur, so the open-minded approach is needed.

There was a need to avoid a situation where the participant felt this was an opportunity to get *"issues off their chest,"* open, unstructured interviews we felt, wouldn't be of much use to in the investigation.

3.5.3. *'Emergent Design,'* (J, 2014) p. 186.

As the literature review evolved, there have already been some changes since this project was first conceived, and small changes were to be expected, as is the case in any project. However, the objective was to gain insight into the ethics of IoT AAL from our participants. A certain amount of flexibility was expected, but as the researcher, there was a needed to stay focused on the investigation of ethics surrounding IoT AAL in Ireland.

3.6. The Researchers Role

"The Inquirer is typically involved in a sustained and intensive experience with participants. This introduces a range of strategic, ethical, and personal issues into the qualitative research process" (Locke, 2013).

However, from a research point of view, there are no known ethics issues directly related to the researcher. Equally, there were no known biases from the researcher's point of view. The reason for this is because no previous experience existed while working with IoT AAL from a professional or private point of view. Therefore, no inferences could be brought into the interviews or shape the outcome of the literature review. Organisations were contacted for recruitment purposes, by their publicly available contact details to request participation in this project.

3.6.1. *Ethics Approval*

Ethics approval was sought and approved through the School of Computer Science and Statistics in Trinity College Dublin (TCD) in February 2019. Following on from the guidelines developed in the ethics application the participants were emailed three documents which were the Information Sheet for Prospective Participants, Informed Consent Form, and finally the Research Interview Questions. These forms and interview questions can be found in the Appendices (A, B, C). Information in the consent form included the right to withdraw from the research process at any time up to submission date (May 1st 2019), the voluntary nature of the research, and the research given to us through the interview process was the interviewee's own personal point of view and not the view of their employers. A fully comprehensive list of themes can be found in the consent form.

3.7. **Grand Philosophical Approach**

In this dissertation, 'The Constructivist Worldview' (J, 2014) p. 8 was used. However, there may also have been elements of 'The Pragmatic Worldview' in our methods (J, 2014) p. 9. The reasoning for the choices, starting with the constructive worldview were:

- 3.7.1. There was a need to understand the Ethics of IoT AAL in Ireland which people experience through working with users and caregivers in their daily lives. It was through these key participant informants we would gain a greater understanding of the Ethical challenges of IoT AAL in Ireland.
- 3.7.2. Pragmatism isn't at least from our high-level viewpoint of Qualitative Design, that much different to constructivism. In fact, the focused was on understanding the ethics of IoT AAL through constructivism. Therefore, at the same time bringing to the foreground information regarding the needs to solve some of the ethics problems by virtue of understanding those same problems.
- 3.7.3. It is not realistic to talk about constructivism without realising; Problems were being solved (Pragmatism). Adding to this, questions were asked, not only to understand ethics but also how participants were solving some of the ethics problems mentioned in the literature review. The literature may grow through gaining insight into problems and solution that may not be in the literature, thus adding to the existing literature.

3.8. Data Recording Procedures

An Interview Protocol described by (J, 2014) p. 194 was used and contained the following components:

- A heading (date, time, location, interviewer, and interviewee) for each interview to aid administration of a number of interviews would be carried out, to help with data processing, and analytics.
- A set of standard instructions followed for each interviewee; these were the same for each participant. Training for conducting interviews was carried out with student services.
- A list of questions including an ice-breaker and a concluding question was put together. The list of questions was no more than eight main questions with a number of sub-questions for each interview and set a limit of twelve questions in total for both the main questions and sub-questions.
- Time was allocated between the questions to record responses were used.
- The handwritten pages for the interview were set up to have the main area and an area to the side for comments, personal hunches, feelings, problems, ideas, impressions, and even prejudices if they existed.
- A recording device was used for the convenience of transcription and to reflect back on the interview; Interviewees were informed in advance of this procedure when they received the list of questions in advance.
- Interviews were also voluntary, and the participants were made aware of that fact in the Participants Information Sheet.
- Participants can request debriefs that will take place with participants at the end of their participation or at a later stage.
- A final thank you statement to acknowledge their time given to us for the interview and any follow-up that may have occurred.

3.9. Data Analysis and Interpretation

While the data collection process (interviews) will be taking place, analytics on the data will be taking place and a write up of the finding between interviews.

In relation to the analysis, a certain amount of filtering will be expected; this is to ensure only relevant data will be allowed. Here are the following steps involved in relation to data analysis and interpretation cited in (J, 2014) p. 197.

- Organise and prepare data for analysis, and this will involve transcribing the interviews (handwritten notes, and audio to text).
- Have a read through the data; this will give a general meaning or sense of the information and an opportunity to reflect on the themes in the data. It will also allow an acknowledgement of what participants are saying, the tone of the ideas, the overall depth, credibility and even the use of the

information. As the researcher we can also at this stage, make sure there are no glaring mistakes in the transcripts.

- Then the coding will start on the data by picking the most interesting interview, and asking what this is about? This will continue for the rest of the interview transcripts, while making a list of the themes as the process move along, then clustering them based on similarity. Once this is done, the themes will be put into columns as shown in the following table 3.3.

Table 3. 3, Coding Table Demo.

Put Heading Here		
Major	Unique	Leftover Theme
Major Theme	Unique Theme	Not So Significant

- The table above will be brought back to the data with the list that has been created in the table and abbreviated the themes as codes, and write the codes next to the appropriate segments of text. The reason for this is to figure out if new categories and codes emerge. This is to ensure there is no drift in the definition of codes (a shift in the meaning of the codes as we code), this can be achieved by continually comparing the data with the codes and writing memos about the codes and their definitions.
- A process of describing the themes with the most meaningful words will take place; this is to ensure the categorisation of the data can take place. There a may need at this stage to reduce the complete list of categories by grouping themes that relate to each other. A map will be drawn from the relationship between these categories. This should allow any new categories or code to emerge.
- A final decision is needed then to abbreviate for each category and finally alphabetise these codes.
- Assemble the data belonging to each category in one place and perform a preliminary analysis.
- If there is a need to recode existing data, it will be done at this stage.

Common sense, reader's expectations, and past literature will define to a large extent the themes that will emerge from the data. However, there is a need to be open-minded about surprising and unanticipated codes or themes that may emerge. A good recommended number of themes according to (J, 2014) pp. 199 – 200 is around five to seven themes. Appendix E, at the back of this dissertation, will contain a snapshot of the results of this process.

3.10. Validity and Reliability

Employing more than one technique or approach will allow an assurance to the reader of the accuracy and validity of the finding in this dissertation.

Some of the approaches will include:

- Triangulation, by interviewing participants from different stakeholder memberships as shown in Figure 3.2, Stakeholder Map below. A comparison of different perspectives from three different stakeholders may add validity to our study (J, 2014) p.201.
- Member checking, I will take specific parts or even the complete report, finished or semi-finished, back to the participants to ensure they feel their account is accurately portrayed in the thesis.
- Peer debriefing, with the supervisor, will continue as she has throughout this project to ask questions surrounding the qualitative study set out in this dissertation, and ensure it resonates not only with the researcher but also with the reader. This strategy hopefully will add validity to the research.

3.10.1. Use of a dedicated book for reference called “Cite Them Right”. This book contains all the major reference styles from around the world. The style that most interests this research is, in fact, the Harvard style, and ironically I used this very book to cite itself (Pears, 2016).

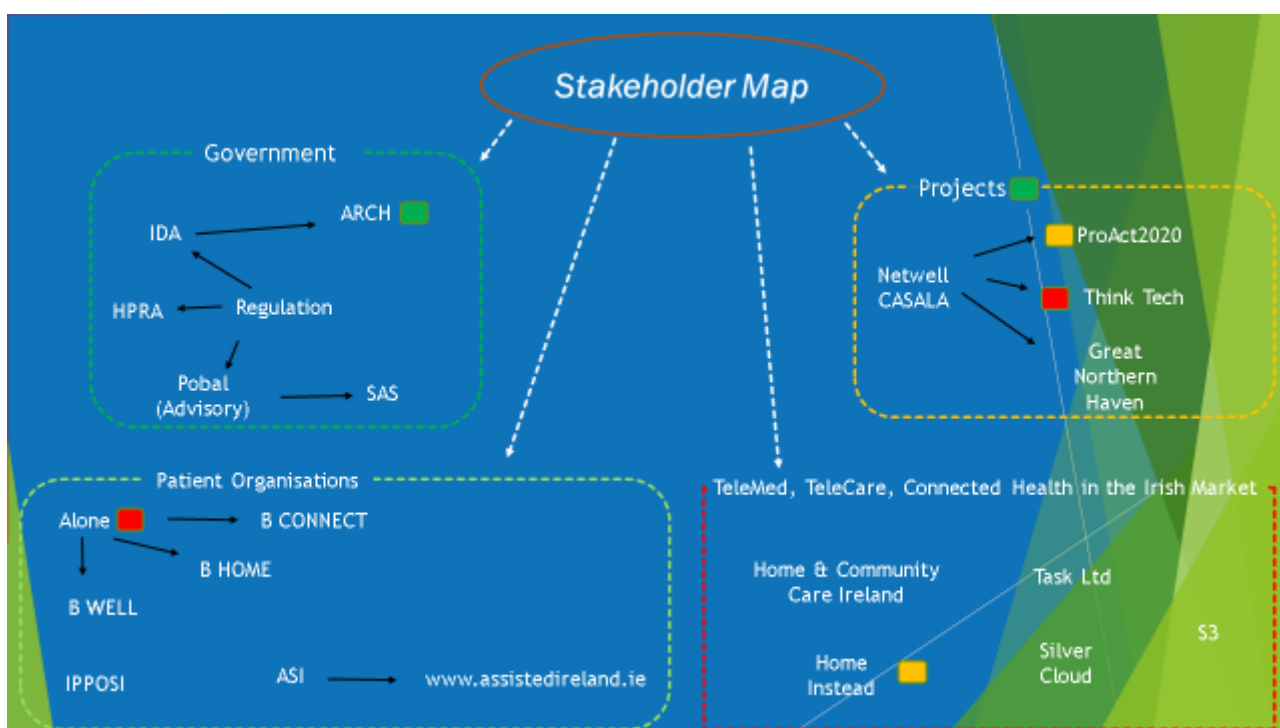


Figure 3. 2, Stakeholder Map.

3.11. Participants – Recruitment

- There was an objective to recruit between three and six people, one or more from each of the stakeholder memberships where possible and the duration of each interview was around forty minutes. However, no one of the commercial markets came forward for an interview.
- Organisations were selected from the Irish Medtech website and a search on the Google search engine.
- Publicly available contact details for participants during recruitment were used.
- Once contact was made, a switched to email for all correspondence thereafter was sought.
- In regards to gender or age, no preference was introduced. Therefore no exclusion or inclusion preference existed.

Below in table 3.4, is a description of the interview participants, this table is included to give the reader a flavour of the participant's areas of interest and Job Titles.

Table 3. 4, Breakdown of Interviewees.

Interviewee	Job Title	Area of Work	Interest Area
Interw1	Technology Group Manager	Charity	Helping older people live longer in their own homes using technology as a medium to achieve that.
Interw2	Technology Lead	Charity	Helping older people live longer in their own homes using technology as a medium to achieve that.
Interw3	Director at an Irish Research Institute, Leader and SME.	Health Informatics.	Human Computer Interaction in Health and Wellness technologies.
Interw4	Dr, Researcher, Leader and SME.	Health Informatics.	All things technology and Health-related.
Interw5	Lecturer and Researcher.	Research and Health Informatics.	EHealth, EHRs, Biomedical Engineering and much more.
Interw6	Assistant Professor	Research in Regulation.	Regulation of Health Apps and more.

3.12. Debriefing arrangement

A debrief of each participant using Member Checking mentioned earlier, was carried out and upon request, a brief explanation of the study was provided to participating members of the study.

3.13. Limitations of the Research

No commercial actors or interview participants accepted an interview. This meant the research had no input from the business community who would generate profit from IoT AAL or services. How would the ethics be affected when finance was the main business driver?

3.14. Conclusion

In this chapter, the headings covered were, rational of research, research aim, approach and design, characteristics of qualitative research, the researcher's role, grand philosophical approach, data recording procedures, analytics and interpretation, validity and reliability, participants, debriefing arrangements, and finally limitations of the research. There were also a number of subheading under most of these main headings as well.

4. Results

4.1. Introduction

In this chapter, the groundwork will be set for the discussion in chapter 5, Discussion, Limitations, Recommendations and Conclusion. Table 4.1 below, provides background information relating to interviewees. This will help in section 4.2, Resultant Quotations from Results of Research. This section will provide a flavour of some interview responses displayed under their relevant question.

There are subthemes under some of the main questions. For example, under the privacy question, the first question, GDPR and Group Stigma will be seen. These are subthemes of the main question that were expanded upon after the initial question was asked in the interviews. The checklist template, including themes, are subthemes, that was used in the interviews can be seen in Appendix D. This will help to create an understanding of the format of results displayed below in section 4.2.

Table 4. 1, Replica of Breakdown of Interviewees from Table 3.4 Above.

Interviewee	Job Title	Area of Work	Interest Area
Interw1	Technology Group Manager	Charity	Helping older people live longer in their own homes using technology as a medium to achieve that.
Interw2	Technology Lead	Charity	Helping older people live longer in their own homes using technology as a medium to achieve that.
Interw3	Director at an Irish Research Institute	Health Informatics.	Human Computer Interaction in Health and Wellness technologies.
Interw4	Dr, Researcher, Leader and SME (Health Informatics)	Health Informatics.	All things technology and Health-related.
Interw5	Lecturer and Researcher.	Research and Health Informatics.	EHealth, EHRs, Biomedical Engineering.
Interw6	Assistant Professor	Research in Regulation.	Regulation of Health Apps and more.

4.2. Resulting Quotations from Results of Research

Below you will find quotes from interviews divided up by regular interviewees. These were people other than the Robotics SME and the Regulation SME. These will be followed by interview quotes from the Robotics SME and the Regulation SME.

The format before will be the section heading followed by an explanation in the case of a main question, please see Appendix C for the main questions asked in the interviews. However, sub-themes will not have a question as it was expanded upon in the interview dialogue. An example of a sub-theme would be GDPR. The name of the theme itself will be the next line of text, followed by the quote, please see Privacy the first theme under Results from Regular Interviews.

Results from Regular Interviews

Explanation: Participants noted the ethics was quite complicated, involved a legal team and took considerable time to work out.

Privacy

Question: What is your approach to securing health-related data (for example AAL Sensors etc.) in the current GDPR climate, thus protecting vulnerable user's privacy and data?

Interviewee_4: "The ethics for (Project Noted) were quite complex, we had to go through (Organisation1 Noted), (Organisation2 Noted) and (Organisation3 Noted) ethics, so it was quite rigorous, and then the Data Protection Impact Assessment was separate..."

Explanation: GDPR is a complex set of laws that involve a lot of processes coming together in order to be compliant.

GDPR

Interviewee_1: "The whole process we have worked through our solicitors, to draft a consent form, and draft an information booklet that does meet the standards of GDPR..."

Explanation: Participants themselves don't carry out processes of ML and AI, however, they do share anonymised data with another company who do it on their behalf.

Big Data

Interview_3: "We don't ourselves but we collaborate with partners so one of the projects we're working on at the moment, which involves Interview_4, we work with (A big company, name withheld) on this, we would transfer anonymous data to their cloud servers, and they run algorithms, and they push it back to us..."

Explanation: Participants followed clear and transparent guidelines in compliance with GDPR. However, they do acknowledge that data may be inverting kept beyond the time frame.

Data Hoarding

Interviewee_1: "...we would store peoples information for maybe up to 7 years if they're no longer active with us, and then we would retain small pieces like even maybe the name and where the person lived...to have a record...in line with our legitimate interests for keeping that information to support our organisational statistics."

Explanation: There is an agreement, that research using medical data should be carried out, but only in the presence of consent and transparency.

Advancing Medical Science

Interviewee_4: "Absolutely, again I think its consent. I think when you are writing ethics, and you are asked to take part in a study, what would you be happy with..."

Explanation: The consensus is to treat both medical and health-related data with the same stringency.

The capture of Medical Data vs Health-Related Data

Interviewee_3: "I suppose we would treat it all the same and put the strictest handling of security on that we can..."

Explanation: The word anonymised was used regularly in interviewee text, but no notion of Hacking or Social Engineering.

Interviewee_3: “What we...have done is a quite detailed Data Protection Impact Session...highlighting what parts...the system was anonymised...what parts would have access to sensitive information...”

Security

Explanation: There wasn't much evidence of family or carers pushing technology onto older people, but it could be a problem if not monitored or recognised early on.

It's For Their Own Good

Question: Have you seen, experienced or are aware of situations prior to the implementation of the Co-Decision-Making Act (the week of the 14th of January) where IoT AAL was put in place as it was seen by caregivers as “It's for their own good” and what is/was your approach on this matter?

Interviewee_1: “Especially for us, it's always the old person's decision. At the end of the day, it's their home. I think if we were to notice something like that, we would need probable pull-out.”

Explanation: In the beginning of a project that one of our participants was involved in, there was some concern around being monitored continuously; however, over time this problem became less and less.

Obtrusiveness

Interviewee_3: “Yes, a little bit like, going back to smart homes that we had, I suppose at the start of that we would have a lot of questions from people...we know where the sensor and cameras are and are people going to watch us constantly?...”

Explanation: The literature was quite adamant that this was a problem with Social Isolation. However, participants mostly disagreed.

Social Isolation

Question: Have you seen, experienced or are aware of situations where after the introduction of IoT AAL technology, social Isolation become an issue? If yes, can you elaborate?

Interviewee_3: “No, I mean that is outlined in the literature quite a lot, and to be honest it's not something that we have experienced to date at all....families call into their loved ones for reasons other than for health and monitoring...I don't think it's an issue....”

Explanation: Participants report positive behaviour from the use of technology. There wasn't much indication of adverse effects despite the narrative from the literature.

Behaviour Modification

Question: Can you elaborate on examples of positive and / or negative behaviour changes in users in relation to IoT AAL technology?

Interviewee_3: “we have definitely seen positive behaviour changes in people...we always combine this feed from the sensors with education to help them change their behaviour and self-manage...”

Explanation: There is not a vast amount of evidence toward anyone that stigma is a significant problem; however, one participant was able to demonstrate through her experiences that it is definitely there.

Individual Stigma

Question: Have you seen, experienced or are aware of situations of social stigma or unwanted attention towards users due to the presence of IoT AAL? If yes, can you elaborate?

Interviewee_4: “...some people, nothing to do with stigma I think, it had a large face (a watch). Some of the women didn't think it went with their style or so not really stigma but more fashion I guess.”

Interviewee_3: “...people would put it upstairs rather than be on display where someone would see it downstairs...”

Explanation: There is no such evidence of resistance from carers or relatives. However, awareness and training are needed for staff reassurance.

Carer Resistance

Question: Have you experienced resistance to IoT AAL technology from users or their careers in relation to privacy or other issues? If yes, can you elaborate?

Interviewee_4: “So we have a home care organisation as a partner on the project....we recruited a lot of the formal carers to take part in these requirements, and some of the co-design sessions.....yes, people were really enthusiastic...”

Results from Robotics Related Questions and Specific Robot Related Interviews

Explanation: One of the critical items to come out of this section of the research is the need to keep robots looking and sounding like robots as opposed to humans, especially with cognitive-impaired people.

Deception

Robo_SME: “There should be a difference between robots and human-like robots. Because it can be a problem in terms of deception, it can also make people uncomfortable. People may feel that it is a bit creepy to have a robot so human-like. And that goes for voice as well.”

Explanation: This is something that can easily be overlooked. However, it is something that needs to be considered if deploying robots in a home environment with telepresence capability.

Dignity

Robo_SME: “Going back to the telepresence in relation to dignity. You are basically giving the relatively open access to the inside of your home, and they can move the robot around at any time in principal....you could ask....whether that is invasion...There is a dignity issue in terms of the state of the place like. If that is something that some care about....”

Explanation: Although this is a subject you wouldn't consider with older people as the expectation is that you may never be able to withdraw the technology due to the ageing process, however, this may be something worth considering if a person actually improves.

Fading

Robo_SME: "I know in work we did with (Organisation1 noted) and (Organisation 2 noted). They talk about this idea of fading that you get someone working with a piece of technology but not to the extent that it acts as a crutch...you can actually somehow carefully remove the support slowly over time."

Explanation: With robots moving around at ankle level off the ground this could be a real threat and one that needs to be taken seriously.

Safety and Changing the Environment

Robo_SME: "...like a lot of let's say the widely used domestic robots are very low profile. You think even like; we had one of the robot vacuum cleaners. I mean there is a trip hazard for sure. Somebody that doesn't have good hearing and the thing is under their feet; they could easily trip over and hit their head against something. Absolutely that is an issue, and how to deal with it."

Explanation: This is a significant issue with all IoT AAL technology. However, due to the volume of information that needs to be collected for an audit, it's an even bigger problem for robots.

Privacy

Robo_SME: "you have to have a very detail audit of someone's home. And that an awful lot of very personal information, like if you're recording that with cameras and video and stuff like that... stuff is written on the wall, and you know like there is intensively private information being gathered up and stored in a cloud to facilitate something like a safety audit..."

Explanation: This is an interesting application of robotics in a nursing home situation and one that could reassure both residents and relatives alike.

Robot as Police

Robo_SME: “One of the things we thought about in a nursing home situation, that something like that could go into a room and noticing stress in a room, by noticing the heart rates are elevated, and pulses are elevated...group stress, not even individual...all these scandals...people being abused in the home like older people being treated poorly,...they wouldn't have actually to take pulses they could just use video magnification...”

Results from Regulation Related Interviews

Explanation: Some of the results from the regulation of IoT AAL in Ireland are quite surprising, no one appears to be looking at the big picture, the societal ethics, and resources are minimal.

Question: How has your experience to date been in relation to this situation in Ireland?

Regulation_SME: “They're usual regulated as regard to their functionality that they do function correctly.”

5. Discussion, Limitations, Recommendations and Conclusion

5.1. Introduction

Below in table 5.1, the reader will find the themes discovered after analysis in both the literature review and the regular interviews (non-Roboethics and non-Regulation). The themes with a hyphen did not come up in the interviews or were very weak but exist in the literature review. While themes without a tick under the literature column are the new themes from the interviews, and these are number 21-25 below. The name of which were chosen by the researcher at the final stages of analysis. Table 5.2 below, shows the themes that emerged from the interview with the Robotics SME, again the theme names were chosen by the researcher.

One thing that needs explaining, if you compare the quotes from the Results chapter in section 4.2 to the analysis table found in Appendix E, and the order of the discussion in chapter 5, they are not presented in the same order. This is because each question was asked in the interviews in a linear fashion, question one, two, and so on and was displayed in that same order in the Results chapter.

When the analysis was carried out, the themes formed into existing and new themes based on the similarity of content rather than numerical order of question.

5.2. Themes Emerging from the Interviews

During the qualitative analysis a number of themes emerged, these were Assessment, Privacy, Data Security, Training, and Social Technology.

In the case of Privacy and Data Security these are existing themes in the literature, in the case of Data Security, this is the same as Security in the literature review. However, in the interview data, it was felt that there was a need to be more specific in the actual type of security, Data Security. Whereas in the literature review the finding from secondary research was a broader sense of security due to a shortcoming in IoT AAL technology in general, but for the purpose of comparisons here they both mean the same thing.

Assessment emerged as a new theme from the interviews. As a theme, it is relatively unusual in that it comprises a number of different actions as opposed to static concepts. Such actions include seeking legal advice, assessing system requirements, and creating Data Protection Impact Assessments or Data Protection Assessments for short (DPIA's or DPA's) just to name a few. The latter process of creating DPA's is covered under Articles 36-36 of the GDPR legislation.

Table 5. 1, Themes that emerged in both Literature and Interviews.

Themes that emerged in the Interviews and / or Literature			
#	Theme / Subthemes	Appeared in Literature	Appeared in Interviews
1	Privacy	✓	✓
2	GDPR	✓	✓
3	Big Data	✓	✓
4	Data Hoarding	✓	✓
5	Group Stigma	✓	✓
6	The capture of Medical data vs Health-related data	✓	✓
7	Advancing Medical Science	✓	✓
8	Security	✓	✓
9	Obtrusiveness	✓	✓
10	For their own good	✓	✓
11	Social Isolation	✓	✓
12	Roboethics	✓	✓
13	Behaviour Modification	✓	-
14	AMS	✓	-
15	Coaching people too intensively	✓	-
16	Hypochondria	✓	-
17	Trained helplessness	✓	-
18	Addition to Devices	✓	-
19	Individual Stigma	✓	✓
20	Career Resistance	✓	✓
21	Assessment		✓
22	Training		✓
23	Technology Acceptance		✓

24	Discrete Device		✓
25	Social Technology		✓

Table 5. 2, Themes that emerged from Roboethics.

Themes from Literature and Interviews that Emerged from the SME for Robotics	
Literature	Interviews Only
Deception	Clear Distinction
Dignity	Privacy
Isolation	Safety
Privacy	
Safety	
Vulnerability	
Autonomy	

5.3. Discussion

5.3.1. Assessment

Throughout the literature review stages and during the interviews, one theme that was quite prominent was GDPR. The phrase GDPR itself may not have been mentioned many times. However, the words consent, assessment and phrases like Data Protection Impact Assessment (DPIA or DPA) just to name a few, all have strong underpinnings associated with GDPR compliance. For example, Interw1, our first interviewee goes on to say *“The whole process we have worked through our solicitors, to draft a consent form....”* and *“...in terms of privacy everything is quite clearly laid out to the person when we meet them first in the home....”*

In order to be compliant with GDPR a great deal of work had to be done in order to know what the requirements were. This work and subsequent learning that followed took the form of the DPA. In our second example, our third interviewee, Interw3, went on to say,

“What we have done is a quite detailed data protection impact session highlighting which parts...the system was anonymised...what parts would have access to sensitive information...”

Interw4 equally mentioned the fact they too carried out a DPA with the resident Data Protection Officer at the time (DPO) at the time.

DPA's will feature quite readily in the practices of organisations who deal with user data in this area of monitoring users or patients using IoT AAL technology and other related technologies.

This DPA is essential in terms of user data, especially sensitive data such as health-related data or medical data. If you recall from our literature review earlier, (Mittelstadt, 2017) went on to mention the grey area of so-called health-related data being captured by health-related devices versus medical devices, the latter, enjoy more stringent data protection. Interw3 again goes on to say

“...we would treat it all the same and put the strictest handling of security on that we can...the...data we are collecting is not medical health records as such...it would be things like blood pressure...which would be considered medical type data or health type data.”

This practice by Interw3's organisation is in fact in line with what (Mittelstadt, 2017) expresses in the literature review when it is said that health data once it reveals information about one's health should be treated as a 'special category' under Article 9 of GDPR.

Interw4 follows on from Interw3 by saying *“...some of the data was being sent out to a triage nurse. The triage nurses were logging in to the system in (Location noted) so that the data didn't go anywhere, but they were presented with it.”*

So as you can see, actual monitoring of the data does occur by medical professionals in Ireland even if it is in a project base scenario, and by treating both sets of data with the highest standards of data protection, provides the best approach used by Irish organisations on the frontline of IoT AAL technologies in the

community. The importance of this approach can be further highlighted when you consider (Mittelstadt, 2016) from the literature makes the point that data captured by IoT AAL style devices which infer the user's health, can be very invasive. Further to this point (Garcia-Morchon. O, 2013) make an additional point that protection of this data is in fact, equated to the control of the individual's personal identity.

An aspect that is worth noting here is an external audit. This gives the team a second opinion to ensure compliance. Interw3 goes on to say, *"The other part is making sure the system is technically robust enough and is compliant...We have passed a data protection impact assessment person who would sign off on that."*

When Interw3 talks about the robustness of the system, they are talking about not only storing data in server farms but also storing data on external devices such as laptops and even paper copies of data. They had to review procedures involving storing of such data, to make sure they were in line with GDPR and their own ethical procedures. (Mittelstadt, 2017) in the literature mentions the point of data minimisation, this, of course, is said in the context of big data and holding on to information in data centres and in server farms.

When people talk about the storage of data, data types such as medical vs health-related, and even the DPA, they are trying to making plans about what they are going to do and why it's important. For example, Interw4 make the following point, *"...the procedures that we needed from the ethics side of the trial was all about consent, so it's all about transparency with the participant, so they know what happens to their data."* This is known to be quite complex, especially when a project is subscribing to multiple participants. A project that Interw4 was involved in made the point that they had to seek ethics applications from no less than three institutes and a separate DPA.

Assessment then as the reader may see and has been pointed out in the introduction to this chapter, is not a static concept. It is a number of actions that need to be carried out in order to ensure compliance, appropriate data handling, and ethics surrounding the user's data.

5.3.2. Privacy

In the introduction above I made the point that the concept of privacy in both the literature review and interviews was the same. That is the right to have information about yourself kept away from anyone you don't want to have access to it. As (Brey, 2005) from the literature points out, users trade customisation information in order to gain cognitive and physical effort reduction. It can also be the right to be left alone according to (Patrice, 2016), again from the literature. A disturbing reality that (Bohn, 2005) points out that further enhances what Patrice has said about being left alone, includes two phases cited in the literature above *"the walls have ears"* and *"if these walls could talk."*

The interviewees of this project also had a similar experience, as Interw4 points out, *"...so in terms of the approach for (Project name noted) if you were going to sum it up, or in terms of running a trial, the most important thing is consent."* Equally, Interw3 talks about when GDPR came in, it gave them the opportunity

to review the physical and electronic data associated with their policies to ensure compliance. GDPR is known to deal with everything from privacy, data security to who handles our data.

This leads us on to Big Data and Data Hoarding, which is what happens when our data is stored for long periods of time, and put through Artificial Intelligence (AI) and Machine Learning (ML) algorithms in order to gain an insight into trends within user's data, this is Big Data. As (Mittelstadt, 2017) points out, data captured today no longer has the limitations of memory that existed in the past. Therefore, data captured today can be held for more extended periods of time in the same state it was captured.

However, our interview participants follow quite closely, policies set through a combination of legal advice, and best practices through partnerships. For instance, Interw1 goes on to say *"We do follow our Data Protection Policy...we would store peoples information for...up to 7 years, if they are no longer active with us...we would be very clear on what we collect and why..."* Again this is in line with what (Mittelstadt, 2017) narrates; data minimisation may exist in our data protection laws (GDPR Articles 6-7) (2017).

In terms of Big Data and the use of algorithms mentioned earlier, this was one of the critical features in GDPR legislation, and is used to profile and automatically process user's data, Articles 13 (2)(f), Article 14 (2)(g) under GDPR cover this, (Wachter, 2018) cited in the literature. This is particularly important with IoT AAL, and similar technologies as older people through failing health may not understand some of the issues as pointed out by (Saurwein, 2015), also cited in the literature.

However, despite the extensive use of ML and AI in other industries, our interview participants, have limited exposure themselves to the use of algorithms. Interw2 for instance, points out *"We hope in the future to machine learning and AI to make a smarter system that indicates where activity was present."* While Interw3 makes the following point in relation to their approach to algorithms, *"...we work with (Company noted) on this, we would transfer anonymous data to their cloud...and they would run algorithms and...push it back to us."* So it looks like it depends on the resources of the organisation itself and the level of experience of working with specific technologies, whether they can utilise that technology (AI or ML in this case) or deploy anonymised (Privatised) data to a partner organisation for processing.

One last item that needs to be discussed under the theme Privacy is the Advance of Medical Science. (Schaefer, 2009) from the literature, if one may recall, makes the following point. *"The value of advancing medical and public health knowledge through secondary analysis of H-IoT must be taken seriously."* IoT AAL as is known captures similar types of data and measurements over a more prolonged and sustained way, and so this quote is quite relevant to IoT AAL.

Equally, it has been found from the research here, that a similar attitude and belief exist with our interviewees. Interw3, for instance, has said *"Well I think research is definitely needed...once you're sharing data completely anonymised and can't be traced back to the individual..."* Interw1 who works with a non-research institute, but who has a partner relationship to research institutes, also makes the point.

"Unless explicitly stated in the consent form, or explicitly stated to the individual that this would be a trial...we would not share personal data." However, they do say that they do have consent to create reports and present data anonymously that could empower future learnings.

One final point needs to be made for the benefit of the reader, and that is an exemption that exists in Article 17 (3) Recital 66 and 67. This according to (Mira, 2016) from the literature, states that data can be kept for health and scientific research.

5.3.3. Data Security

The last section, the research has touched lightly on Data Security, with the use of words like anonymised, and consent. Data Security is the next theme presented.

Starting with (Hayden, 2012, McGuire, 2012, Joly, 2012) and (Choudhury, 2014) from the literature, all three narrate the point that the use of anonymisation and aggregation techniques reduce the risk of re-identification. While (G. Bleser, 2013) from the literature, highlights a scenario involving a character called '*Frank*', who is using RFID tags, a mainstay of IoT technology, that can be used to expose details about an individual's whereabouts. In this case, they know that '*Frank*' is out by using RFID readers scattered about the neighbourhood, and therefore, they can break into Frank's house while he is away.

The interviewees have not seen scenarios depicting the character '*Frank*' above. However, what they have to experience is the sharing of anonymisation data for the purposes of analysis using algorithms, and with health professionals to carry out a triage service.

For example, Interw4 made the point that a lot of time was spent in system design to make the system secure and allow only anonymised data to be sent out to the cloud that (Company noted) had set up. Interw3 went on to say that as part of their DPA, they needed to find out what parts of the system were anonymised, what part had sensitive information for input and output to healthcare professionals. Transparency was a cornerstone too, for example, who had access and to what data.

This anonymisation that occurred as Interw4 points out was an ingenious method of using two different sets of ID's, one on the resident computer network and an entirely different one in the cloud. This meant that data could not be traced back to individual end users without prior knowledge of the system. Interw4 points out that (Company noted) also stipulated that they didn't want any personal data, they were quite rigorous in their own DPA and ethics which formed the overall ethics and legal documents to the project.

However, it didn't stop there; the ID's were also used to set up third-party Apps and devices that were distributed to the individual end user. That way no personal information was held on the device, even if the device was kept in the user home and never brought outside.

Even though it is evident from the literature a considerable treat exists with the use of IoT technologies, our interviewees and their respective organisation have had little exposure to a malicious intent to date. However, procedures are in place, and tools such as anonymisation appear to be utilised in the frameworks set out by complex and rigorous ethics applications and DPA's. It is this planning and experience that no doubt will lead the way if a mainstream role out of these systems were to happen here in Ireland.

5.3.4. Training

Any DPA is only as good as the knowledge and training of staff that carry out daily operations in the shadow of the DPIA document itself. Interw1, for example, gives us the following insight, *“We are working with a research partner as well in (Location noted), and there in a research institute, so everything they do is in line with practices of a research institute.”* Interw3 who is part of the very research institute mention by Interw1 also goes on to say that they, in fact, carried out quite a big project to establish an understanding of the requirements particularly around health, and other sensitive data.

They did this by attending a number of GDPR related courses ran by the Health Research Board. This was a significant step taken by the team, to train up on data protection, (Mittelstadt and al., 2017) from the literature, expresses the idea of IoT Health, AAL and Medical devices are designed to operate in both public and private spaces. Medical, health-related, and IoT AAL devices which operate in both public and private space coupled with users that are already vulnerable (Pellegrino, 1993, Edgar, 2005) also from the literature, causes a window into the private lives of users to be opened up. Therefore, it is prudent that staff are trained up and are aware of the threats that exist for both their end users and their own systems.

However, the literature didn't mention anything about the training of staff and researchers in line with data protection. Therefore, one might assume or take a leap of faith and say that training and knowledge surrounding data protection is implied to exist in organisations as an automatic default and doesn't need mentioning or it's so non-existent it's not worth mentioning. However, there has been lots of advertisements about GDPR training. Maybe what is coming to the surface is that specific health GDPR training is not available.

This approach or ignoring training appears to be an unfortunate weakness in the current literature. On the other hand, research conducted in this dissertation shows that training and awareness for researcher, family, and end users alike is crucial for all involved if end users are going to get the most out of this technology. For example, Interw3 highlights the combined teaching and integration of technology for older people involved in their project.

“...this is more of the digital health technologies for chronic diseases management and...more ambient technologies...we always combine this feed from the sensors with education to help them change their behaviour and self-manage.”

Training end users to view their own data stream combined with education provides an opportunity for them to make informed discussions about their own health, and it also reduces the risks associated with the use of IoT AAL technologies discussed in the literature review by allowing staff to be more aware of risks.

5.3.5. Social Technology

This section looks at the potential problem of Social Isolation generated by the use of IoT AAL and associated technologies; it comprises two arguments both counter to each other. It is probably the smallest section in the entire Discussion section. However, it is a poignant section, and that's why it is included.

(Percival, 2006, Chan, 2008) in the literature stated that studies had shown concern surrounding older people and the use of IoT AAL technologies. The mainstay of the argument was that IoT AAL was never meant as a replacement tool, preferably an augmentative one. This argument is further enhanced when we take in the views of (Redmond, 2014) in a paper written by (M. Schukat, 2016) titled *"Unintended Consequences of Wearable Sensor Use in Healthcare"* also from the literature. Here Redmond raises a scenario where the family of a relative feel they do not have to come around as much due to the presence of the technology, as the relative is being monitored.

However, from our interviewees, in particular, Interw3, who make a very valid argument which can easily be overlooked.

"..., I mean that is outlined in the literature quite a lot, and to be honest it's not something that we have experience to date...families call into their loved one for reasons other than for health and monitoring...they would have called in the evening for the cup of tea or chat or at the weekend..."

This is a very valid counter-argument; it was felt that both prospective were valuable in the discussion.

5.3.6. Roboethics

5.3.6.1. Clear Distinction

(Kanda, 2004) from the literature makes a point about appearance surrounding robots being quite essential in the expectations of functionality or perceived intelligence, including speech. The more intricate and free the design, including behaviour the more the lines are blurred, according to (Broekens, 2009, Kortner, 2016).

However, this poses a problem according to Interw5 who goes on to say, *"There should be a difference between robots and human-like robot. Because it can cause a problem in terms of deception."* Interw5 further expands this point by saying, it can make people uncomfortable and that people may even feel creepy about a human-like robot, and this extends to voice as well.

It's not just Interw5 who expresses this view. However, Interw5 goes on to say that literature he or she has read, and from conversing with colleagues, the sense is that it makes for a more comfortable relationship with robots if there is a clear visible and vocal distinction. This appears to be especially poignant when you take into account cognitively impaired individuals, such as people suffering from dementia.

Both Interw3 and Interw4 have also expressed a personal disliking to the use of robots in social care settings. Interw3 saying, “...I wouldn’t be the biggest fan of robots let’s say...” and Interw4 also expressing the following point. *“I think from the group that we are working with; they would probably be quite suspicious of the idea.”*

One way around this problem of deception is to include the option of human occupation of the devices. Such a scenario exists in the Telepresence device. This is a robot on wheels that can be controlled over the Internet and allows the user to check in on people in what can be called a remote presence. See figure 5.1 below.



Figure 5. 1, Example of a Telepresence.

Both Interw3 and Interw4 can see the use of robots in a limited application of group therapy, for instance using the harrow seal, a cuddly robot or maybe in freeing up carers time by helping with remedial tasks. However, in Ireland, there doesn’t seem to be much rollout of care robots as there has been in other countries like Japan (Interw5, 2019).

5.3.6.2. Safety

In the literature, a robot called Henry depicted by (Kortner, 2016) has been known to bump into people and even take a tumble down a set of stairs. Unfortunately, testing for every scenario is a tremendous challenge. As Interw5 says *“Robots can’t possibly be tested for every situation, AI and ML need a lot of information in order to learn....How does it distinguish between boundaries without changing the environment?”*

However, surprisingly one solution is to change the environment, by setting a defined boundary. Interw5 gives the following example of how first-year robotic students in the class use a white line around the edge of a table that the robot can detect. By detecting this white line, the robot stays on the table rather than end

up on the floor. Although this is a rather simple solution, another scenario would be to use a dedicated sensor in the robot to detect a special type of carpet or the edge of the stairs.

Another problem with safety and domestic robots as expressed by Interw5 is the low profile; this isn't something that would ordinarily come to mind. However, imagine not having great hearing and a robot vacuum cleaner getting under the user's feet because you couldn't hear it coming. This could cause a trip or fall accident.

A similar scenario is a robot getting jammed behind a door, and the older person or user can't get into that room as the door is jammed. Safety is such a broad-ranging set of issues. One solution is to use AI or ML. This solution, however, leads to a requirement of a lot of environmental information that needs to be captured in a safety audit, the discussion around this theme leads into our next part the discussion, Privacy.

5.3.6.3. Privacy

As (Patrice, 2016) expressed at the beginning of the literature review, the idea that privacy was a commodity that can be bought and sold for reduced cognitive and physical effort. So too does (Beach, 2009) express a similar view; people with a greater need for care are most likely the same people who are willing to give up their privacy.

Our interviewee, Interw5 however, goes considerably further to express a big worry surround privacy and the use of Assisted Technologies in general including robots with the following quote:

“This is a huge issue overall...you have...a very detailed audit of someone's home...that corresponds to an awful lot of very personal information...with cameras and video...Who knows what stuff is written on the walls.”

The information captured all ends up in the cloud, and they don't always give you a clear idea of what the information is going to be used for. You may not want to share some of the things captured and saved to the cloud. Using basic cameras, such as night vision and infrared on a robot to learn the environment may not be enough as this may only give the user the basic structure of a building, not the tables, chairs and other objects (Interw5, 2019).

Finally, the last item to talk about under privacy is an unusual subject, which is the use of robots to monitor the wellbeing of residents in nursing home situations. When well been is expressed here in the discussion what is meant by this is to police any bullying or abuse that residents may suffer at the hands of staff or visitors. However, this may also apply to the end user own home. This can be achieved by using Eulerian Video Magnification, which can measure pulse by the changing capillaries in the face of residents thereby telling if there is stress in the room or not. The robot in this scenario can then take action based on predetermined instructions (Interw5, 2019).

5.3.7. Regulation

(M. Schukat, 2016) points out, regulatory authorities are struggling to keep up with the number of devices on the market. The majority of these devices are intended for the consumer market in an attempt to target interest and behaviour modification of their users, some manufacturers, however, are now jumping across to the medical device arena. Apart from Holter which has been around since the 1960s, manufacturers such as Nonin, Sotera, and even Samsung and Apple are encroaching into the field of medical wearables. A number of questions surrounding regulation need to be asked in order for the reader to have a comprehensive view of the Ethics of IoT in the AAL in Ireland, and it is for that reason we intend to include key informants of IoT AAL regulation in Ireland in our primary research.

Indeed, our only interviewee for regulation, Interw6 would agree with the sentiments expressed by Schukat above. For instance, Interw6 goes on to say, *“Well, it would be nice if they were all regulated, but they're not, that's the trouble.”* Following on from this direct quote, Interw6 also expresses the following view, *“There are lots of things developed for the home market and just put on the shelf without that CE certification.”*

When asked about the type of regulation the (regulatory organisation noted) is involved in, Interw6 say's *“Their usual regulated as regard to their functionally.”* However, the (regulatory organisation noted) are under pressure in terms of human resources in Ireland, for instance, Interw6 goes to say, *“...there is probably millions of devices out there, and you would need an absolute army to look at them all.”*

Interw6 was asked about the penalties surrounding breeches in regulation by organisations or people, Interw6 expresses the following procedural approach to enforcing the regulation.

“Well, it's usually with the withdrawal of the product, which means they're out of business if that was your only product. The (regulatory organisation noted) then has to trace everybody in the country who has got one or the other of those.”

How does the (regulatory organisation noted), find all those devices? Interw6 again informs the research by saying, the (regulatory organisation noted) would be able to contact the manufacturer about this and find out how many devices were sold. However, when asked about the regulation of residential care, and the home market type devices, the view expressed was that unless a complaint was received, there wouldn't be any regulation as such. However, every complaint would be followed up (Interw6, 2019).

One final question was asked surrounding the most usual, or out of the ordinary device or service allowed or disallowed, Interw6 talked about devices used to measure, saying that *“Certainly the measuring devices are the ones that are exploding at the moment. You can measure this; you can measure that...”* However, these according to Interw6 have non-existing ethics, and the calibration is in serious question, as highlighted in the following.

5.4. Limitations

- One limitation was the lack of response from a commercial venture who may use this technology in their daily encounters with elderly people. This could have provided a window into how they view things where finance is a key business driver. Commercial organisations were contacted and invited. However, those interviews never materialised.
- The next limitation is that another robotics subject matter expert (SME) was contacted as was the regulatory offices themselves; both engagements failed to produce an interview. Another view of the role of robotics and regulation from a more granular level within the regulatory organisation would have been welcomed.
- However, the input from Interw6 (regulation) has benefitted the research immensely, Interw6 as a reminder has oversight at a strategic level within the regulatory body as well as a solid academic background, for that input from Interw6 the research is much better off.
- Finally, the last limitation was the number of participants, the volume of research material and quality of the responses was incredible. However, as a study in itself, the number of participants is a limitation, and that has to be recognised even if the number of participants does fall within the recommended number for this size of this type of study.

5.5. Recommendations

There are a number of recommendations that need to be made, and these will be in bullet point below.

- Regulation: There is a considerable need for societal input and oversight into regulation as ethics is not clearly a part of the regulation of the technical health-related products.
- There is a need to regulate devices before they reach the market in the first place; this doesn't appear to be happening. However, one must remember that the regulator does not have an army of employees to carry out this essential work.
- A recommendation is that solutions surrounding AI and ML technologies be investigated if they haven't already, to aid in the struggle of regulation.
- Consumers themselves also need to be aware of the pitfalls of using devices and watch out for CE marks on packaging and devices. A small amount of research before deploying IoT AAL related devices is recommended.
- A more immediate recommendation is a possible increase in funding if it is deemed necessary to ensure an expansion of regulation surrounding health-related technologies.
- Expansion: One of the significant limitations of this study is that it doesn't involve Physicians in hospitals or General Practitioners (GP). However, for the scope of the project to extend this way

would require a prolonged ethics applications to the Health Service Executive (HSE) and GP practices thus expanding the scope of the project and increasing the risk to an unacceptable level, beyond timeframe allocated. By involving medical doctors, their professional and clinical experiences could be brought to bear in the research. This new primary material could then be used in the future to shape the outcome of a community-based roll out of IoT AAL and associated technologies with a link up to medical centres.

- **Terminology:** One of the significant issues with IoT related technology was terminology, and because this type of technology has a cross-disciplinary reach, this makes it even more challenging. The recommendation is to standardise terminology across ICT, Health Informatics and Medicine.
- **The rollout of existing projects:** There is an urgent need to expand the ongoing projects in which participants are involved in, into the community through the HSE's community care effort. This should alleviate some of the problems within the HSE, community and hospital themselves while serving the greater community.
- **Education:** There is a need for education and exposure for end users to this technology, and this has already been proven to be a viable strategy in the projects of many of the participants of this project.

5.6. Conclusion

All participants engaged in complex and rigorous legal, ethical and training sessions so as to ensure compliance with GDPR, this, as can be seen from the discussion above, was done through DPA's and an external audit. A vital feature of the DPA's was to treat all data regardless of whether it was classified as medical or health-related the same, with the strictest security settings. Participant of this research has demonstrated that this was the correct course of action to take on any future rollout of this technology in a community care setting.

While it has been shown that Irish medical organisations engage in viewing patient data through connected health and IoT AAL, coupled with external partnerships and strong ethics policies, what now needs to be done is to take connected health and IoT AAL to the next level for the benefit of older people in the community.

This research has shown that research institutes involved in this study have the legal, compliance and ethics in place, and tested to ensure a safe and secure roll-out of IoT technology. However, as a society, we have to ensure going forward that we adhere to the standards set by our participant organisations and the participants themselves.

One surprising realisation that emerged from the research was the contrast between training provided by participant organisations to both staff and end users and the lack of any mention of training in the literature.

This has been expressed as a weakness in the discussion, and it is hoped that the research conducted here will bring attention to this weakness. The training for the end user was particularly apparent as they were shown their own data and also received education to be able to make sense of the data, this led to the user being able to make an informed decision surrounding their health. This level of transparency and overall approach is a model to follow, set by our very own academia and charity organisations for any future roll out of IoT AAL and similar technologies.

Roboethics is an unusual subject to talk about as there appears to have to be very little in the way of applications of social care or home robots in Ireland to date. However, it is an application that has appeared on the horizon, and so it required our attention in the discussion section of this research. Distinction, Safety and Privacy were the main themes to emerge from that discussion.

Surprising regulation in this area of IoT AAL is particular light, considering health-related and medical data is being captured. The idea of a reactionary strategy, as opposed to a proactive one, may surprise most people. However, resources surrounding regulation is limited, especially in term of human resources in tackling the problem. There also appears to be a need of societal input in terms of the expectations of society towards the regulation of health-related and ambient technologies, especially surrounding the revelation of ethics not be playing a central role in regulation in Ireland. Instead, regulation focusing solely on functionality.

As this research has shown, there are many ethical challenges expressed in the literature review. However, interview participants and their respective organisations have shown they are well ahead in terms of ethics and GDPR compliance. The next steps are to amalgamate the hard work already done in charities, research institutes of education with community care based organisations including commercial ventures. By hopefully taking these lessons learned in relation to ethics, infrastructure and technical know-how, society as a whole can benefit from the massive potential that IoT AAL and its related technologies have to offer.

When a reflection of the literature is taken and compared to the primary research, one thing sticks out. The literature appears to have a lot of details that have not been reflected in the participants of this research yet. In other words, the research doesn't contradict the literature as a whole, maybe in parts. However, it does show that participants have not experienced yet, some of the findings in the literature. This is particularly true with care robotics. One conclusion that can be drawn is the youthfulness or level of exposure that Ireland has experienced through research participant's, which shows Ireland has not travelled far down the road on this journey that other countries have already begun, and maybe are further ahead.

However, there is an advantage; this allows Irish organisations of health, education, charity and others to learn without making the same mistakes that other countries may have made through research and reflection. This report indeed reflects the finding of authors, mostly from outside of Ireland, expressed through their own research papers, journals and conference proceedings in one location, this dissertation.

However, this report shows how far participants and their respective organisation have also come, from the early days of smart home sensor technology to the deployment of services in the community, and the recognition of problems that need to be tackled with safety and limitations surrounding robotics.

It is hoped that this research may complement or add to existing works of research carried out in institutes of education in Ireland as a reflection of the ethical challenges that exist. This research may even contribute to future projects such as an expansion of robotic applications to prevent abusive or bullying behaviour toward older people. To the increased use of ML and AI applications that may further enhance understanding and needs of end user both in their own homes and community care settings.

One may even question whether in some small way, the ethical challenges of Privacy, Security, Social Isolation, Behaviour Modification, Roboethics, Regulation, Assessment, Training, Data Security, Social Technology, Clear Distinction, and Safety presented in this report both from the interviewee participants and literature feed into a bigger plan for healthcare. This is an ideal application for IoT AAL. Will the ethical challenges presented here shape the path going forward; the answers to these questions remain to be seen.

References

- ABASCAL, J., & AZEVEDO, L 2007. 'Fundamentals of inclusive HCI design, In C. Stephanidis (Ed.)'. *Universal access in human computer interaction. Coping with diversity* pp. 3-9.
- ASHTON, K. 2019. *That 'Internet of Things' Thing* [Online]. Available: <https://www.rfidjournal.com/articles/view?4986> [Accessed 05 April 2019].
- BAGUÉS, S. A., ZEIDLER, A., KLEIN, C., VALDIVIELSO, F., & MATIAS, R 2010. 'Enabling personal privacy for pervasive computing environments'. *Journal of Universal Computer Science*, 16, pp. 341-371.
- BEACH, S. S., R. DOWNS, J. MATTHEWS, J. BARRON, B & SEELMAN, K 2009. 'Disability, age, and informational privacy attitudes in quality of life technology application: Results from a national web survey'. *ACM Trans Access Comput*, 2, pp. 1-21.
- BEAUCHAMP, T. L., CHILDRESS, J. F 2009. *Principals of Biomedical Ethics*, Oxford University Press, New York, NY, USA.
- BHARUCHA, A. J. A., V. FORLIZZI, J. DEW, M. A. REYNOLDS, C. F. III. STEVENS, S & WACTLAR, H 2009. 'Intelligent assistive technology applications to dementia care: current capabilities, limitations, and future challenges'. *American Journal of Geriatric Psychiatry*, 17, pp. 88-104.
- BOHN, J. C., M. LANGHEINRICH, F. MATTERN, M 2005. 'Social, economic, and ethical implications of ambient intelligence and ubiquitous computing'. *Ambient intelligence*, pp. 5-29.
- BORENSTEIN, J. H. M. R., H 2009. 'Assistive social robots in elderly care: a review'. *Gerontechnology*, 8, pp. 94-103.
- BOWES, A., DAWSON, A., & BELL A 2012. 'Ethical implications of lifestyle monitoring data in ageing research'. *Information Communications & Society*, 15, pp. 5-12.
- BRENT, M. L., FLORIDI 2016. 'The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts'.
- BREY, P. 2005. 'Freedom and privacy in ambient intelligence'. *Ethics and Information Technology*, 7, pp. 157-166.
- BROEKENS, J. H., M & ROSENDAL, H 2009. 'Assistive social robots in elderly care: a review'. *Gerontechnology*, 8, pp. 94-103.
- CAINE, K. E., FISK, A. D., & ROGERS, W. A. *Benefits and privacy concerns of a home equipped with a visual sensing system: A perspective from older adults*. 50th Annual Meeting of the Human Factors and Ergonomics Society, 2006 San Francisco. HFES, pp. 180-184.
- CAULFIELD, B. M. D., S. C 2013. 'What is Connected Health and why will it change your practices?'. *Q M Med*, 106, pp. 703-707.
- CHAN, M., ESTÉVE, D., ESCRIVA, C., & CAMPO, E 2008. 'A review of smart homes: Present state and future challenges'. *Computer Methods and Programs in Biomedicine*, 91, pp. 55-81.
- CHOUDHURY, S. F., J. R. MCGOWAN, M. L. JUENGST, E. T 2014. 'Big data, open science and the brain: Lessons learned from genomics'. *Front. Hum, Neurosci*, 8, pg. 239.
- CHRISTIAN, S. A., HOCHGATTERER & THOMAS, ERNST DORNER 2014. 'Contributions of ambient assisted living for health and quality of life in the elderly and care services - a qualitative analysis from the experts' perspective of care services professionals'. *BMC Geriatrics*, 14.
- COURTNEY, K. L. 2008. 'Privacy and senior willingness to adopt smart home information technology in residential care facilities'. *Methods of Information in Medicine*, 47, pp. 76-81.
- COUTURIER, J., SOLA, D., BORIOLO, G. S. & RAICIU, C. 2012. 'How Can the Internet of Things Help to Overcome Current Healthcare Challenges'. *Communications & Strategies*, 67-81,177-180.
- CRAIK, F. I. M. 1986. 'A functional account of age differences in memory'. *Human Memory and Cognitive Capabilities, Mechanisms, and Performance*, pp. 409-422.

- DEB, A. 2015. 'Phantom vibration and phantom ringing among mobile phone users: A systematic review of literature'. *Asia Pac Psychiatry*, 7, pp. 231-239.
- DECKER, M. 2012. 'Service robots in the mirror of reflection research'. *Poiesis & Praxis*, 9, pp. 181-200.
- DENNING, T. M., C. KOSCHER, K. SMITH, JR & KOHNO, T 2009. *A spotlight on security and privacy risks with future household robots: attacks and lesson. Proceedings of the 11th international conference on Ubiquitous computing.*
- DOCHERTY, A. 2014. 'Big data-ethical perspectives'. *Anaesthesia*, 69, pp. 390-391.
- DOVE, E. S. K., B. M. ZAWATI, M. H 2014. 'Towards an ethics safe harbour for global biomedical research'. *J. Law Biosci*, 1, pp. 3-51.
- DOYLE, J., CAPRANI, N. & BOND, R. "Older adults' attitudes to self-management of health and wellness through smart home data". 2015 9th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth), 20-23 May 2015. 129-136.
- DOYLE, J. C., N. KEALY, A. BOND, R. KOMABA, Y. INCOMATA, AKIHIRO. 'Healthcare Professionals Views on Technology to Support Older Adults Transitioning from Hospital to Home'. Proceedings of British HCI 2016 Conference Fusion, 2016 Bournemouth, UK. *BSC Learning and Development Ltd.*
- DUPUY, L., FROGER, C., CONSEL, C. & SAUZÉON, H. 2017. Everyday Functioning Benefits from an Assisted Living Platform amongst Frail Older Adults and Their Caregivers. *Frontiers in Aging Neuroscience*, 9.
- EDGAR, A. 2005. 'The expert patient: Illness as practice'. *Health Care Philos*, 8, pp 165-171.
- EPLEY, N. W., A & CACIOPPO. JT 2007. 'On seeing human: a three-factor theory of anthropomorphism'. *Psychol Rev*, 114, pp. 864-886.
- ESSÉN, A. 2008. 'The two facets of electronic care surveillance: An exploration of the views of older people who live with monitoring devices'. *Social Science & Medicine*, 67, pp. 128-136.
- FAIRFIELD, J. S., H 2014. 'Big data, big problems: Emerging issues in the ethics of data science and journalism'. *J. Mass Media Eth*, 29.
- FRANCIS, P. & AL., E. 2009. 'Towards co-design with users who have autism spectrum disorders'. *Universal Access in the Information Society*, 8, pp. 123-135.
- FRUHWALD, T. 2012. 'Ethik in der Geriatrie'. *Z. Gerontol Geriatr*, 45, pp. 545-557.
- G. BLESER, D. S., M. WEBER, G. HENDEBY, D. STRICKER, L. FRANDET, F. MARIN, N. VILLE, F. CARRÉ 2013. 'A personalised exercise trainer for elderly'. *Journal of Ambient Intelligence and Smart Environments*, 5, pp. 547-562.
- GADAMER, H. G. 1976. *The historicity of understanding*, Harmondsworth, Penguin Books Ltd.
- GARCIA-MORCHON. O, F. T., & WEHRLE. K 2013. 'Sensor network security for pervasive e-health'. *Security and Communication Networks*, 4, pp. 1257-1273.
- GREAT NORTHERN HAVEN. NO DATE. *Great Northern Haven* [Online]. Available: <https://www.netwellcasala.org/great-northern-haven/> [Accessed].
- HAGGERTY, K. D., ERICSON, R. V 2000. 'The surveillant assemblage'. *The British Journal of Sociology*, 51, pp. 605-622.
- HAIL. ADMED, M. F., STEFAN 2015. *IoT for AAL: An Architecture via Information-Centric Networking*. IEEE. San Diego, CA, USA.
- HAYDEN, E. C. 2012. 'A Broken Contract'. *Nature*, 486, pp. 312-314.
- HAYUTIN, A. M. 2007. *Graying of the global population*. Public Policy and Ageing Report.
- HEGEL, F. M., C. WREDE, B. HIELSCHER-FASTABEND, M & SAGERER, G. *Understanding social robots*. Second International Conferences on Advances in Computer-Human Interactions, 2009. pp. 169-174.
- HENSEL, B. K., DEMIRIS, G., & COURTNEY, K. L 2006. 'Defining obtrusiveness in home telehealth technologies: A conceptual framework'. *Journal of the American Medical Informatics Association*, 13, pp. 428-431.

- HILDEBRANDT, M. 2008. 'Defining profiling: A new type of knowledge? In M. Hildebrandt & S. Gutwirth (Eds) *Profiling the European citizen*. Dordrecht: Springer, pp. 17-45.
- HUCKVALE, K., PRIETO, J. T., TILNEY, M., BENGHOZI, P. J. AND CAR, J. 2015. 'Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment'. *BMC Medicine*, 13, pg. 214.
- J, C. W. 2014. *Research Design*, University of Nebraska, Lincoln, SAGE.
- JOHNSON, J. A. 2013. *Ethics of Data Mining and Predictive Analytics in Higher Education*, Rochester, NY, USA, Social Science Research Network.
- JOLY, Y. D., E.S, KNOPPERS, B. M. BOBROW, M. CHALMERS, D 2012. 'Data sharing in the post-genomic world: The experience of the International Cancer Genome Consortium (ICGC) Data Access Compliance Office (DACO)'. *Plos Comput. Biol.*, 8.
- KANDA, T. I., H. IMAI, M & ONO, T 2004. 'Development and evaluation of interactive humanoid robots'. *Proc IEEE*, 92, pp. 1839-1850.
- KENNER, A. M. 2008. 'Securing the elderly body: Dementia, surveillance, and the politics of "ageing in place"'. *Surveillance & Society*, 5, pp. 252-269.
- KHODADADI, D., BUYYA & F. GONCALVES 2013. *Security Architecture for Mobile E-Health Applications in Medication Control. International Conference on Software, Telecommunications and Computer Networks - (SoftCOM 2013)*.
- KLEIN, B. 2011. *Applications of emotional robots - First results from teaching/research projects at the Fachhochschule Frankfurt am Main. Ambient Assisted Living - AAL - 4th German Congress: Demographic Change - assistance-systems and their transfer from the lab to the market (AAL 2011)*. Berlin HVDC-Verlag.
- KLEIN, B. C., G 2009. 'Robotik in der Pflege - Entwicklungstendenzen und Potenziale'. *Public Health Forum*, 17.
- KORTNER, T. 2016. 'Ethical challenges in the use of social service robots for elderly people'. *Zeitschrift für Gerontologie und Geriatrie*, 4, pp. 303-307.
- KOSTA, E. P., O. NIEMELÄ, M & KAASINEN, E 2010. 'Mobile-centric ambient intelligence in health and homecare-anticipating ethical and legal challenges'. *Science and Engineering Ethics*, 16, pp. 303-323.
- LANDAU, R. W., S., AUSLANDER, G. K., SHOVAL, N., & HEINIK, J 2010. 'What do cognitively intact older people think about the use of electronic tracking devices for people with dementia? A preliminary analysis'. *International Psychogeriatrics*, 22, pp. 1301-1309.
- LANGHEINRICH, M. 2001. 'Privacy by design - principles of privacy aware ubiquitous systems'. *Ubicomp 2001: Ubiquitous Computing of Lecture Notes in Computer Science*, 2201, pp. 273-291.
- LOCKE, L. E. S., W. W. & SILVERMAN, S. J 2013. *Proposals that work: A guide for planning dissertations and grant proposals*, CA: Sage, Thousand Oaks.
- LYON, D. 2003. *Surveillance as social sorting: Privacy, risk, and digital discrimination*, London, Routledge.
- M. SCHUKAT, D. M., K. WANG, G. SCHREIER, N. H. LOVELL, M. MARSCHOLLEK, S. J. REDMOND 2016. *Unintended Consequences of Wearable Sensor Use in Healthcare*. IMIA Yearbook of Medical Informatics: IMIA and Schattauer GmbH.
- MAGUIRE, M., NICOLLE, C., MARSHALL, R., SIMS, R., LAWTON, C., PEACE, S., & PERCIVAL, J 2011. 'A study of user needs for the 'Techno Kitchen'. *HCI international 2011-Posters' extended abstracts*, pp. 66-71.
- MAHMOUD, E. S. S. H. C. 2012. *A Review of Mobile Location Privacy in the Internet of Things. ICT and Knowledge Engineering (ICT & Knowledge Engineering)*, 2012 10th International Conference on (IEEE 2012).
- MANN, W. C. O., K. J. FRAAS, L. TOMITA, M & GRANDER, C. V 1999. 'Effectiveness of assisted technology and environmental interventions in maintaining independence and reducing home care cost for frail elderly: a randomized controlled trial'. *Arch. Family Med*, 8.
- MARCELLO, I. T., WANGMO. FABRICE, JOTTERAND. RETO, W. KRESSIG & BERNICE, ELGER 2018. 'Ethical Design of Intelligent Assisted Technologies for Dementia: A Descriptive Review'. *Science and Engineering Ethics*, 24, pp. 1035-1055.
- MARTIN, R. 2018. *Internet of Medical things (IoMT) - The Future of Healthcare*.

- MCGUIRE, A. L. A., L. S. WHITNEY, S. N. SLASHINSKI, M. J. VERSALOVIC, J. KEITEL, W. A. MCCURDY, S. A. 2012. 'Perspectives on human microbiome research ethics'. *J. Empir. Res. Hum. Res. Eth. Int. J*, 7, pp. 1-14.
- MELENHORST, A.-S., ARTHUR, D. FISK., ELIZABETH, D. MYNATT., & WENDY, A. ROGERS. *Potential intrusiveness of aware home technology: perceptions of older adults*. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2004. pp. 266-270.
- MIRA, B. A. R. S. 2016. 'THE REFORM OF THE EU DATA PROTECTION FRAMEWORK: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy'. *Journal of Information Policy*, 6, pp. 479-511.
- MISSELHORN, C. U., POMPE & MOG, STAPLETON 2013. 'Ethical Considerations Regarding the Use of Social Robots in the Fourth Age'. *GeroPsych*, 26, pp. 121-133.
- MITTELSTADT, B. 2017. 'Designing the Health-Related Internet of Things: Ethical Principles and Guidelines'. *Information*.
- MITTELSTADT, B. & AL., E. 2017. 'Ethics of the health-related internet of things: a narrative review'. *Ethics and Information Technology*, 19, pp. 157-175.
- MITTELSTADT, B. F., L 2016. 'The ethics of big data: Current and foreseeable issues in biomedical contexts'. *Science Engineering Ethics*, 22, pp. 303-341.
- MORDOCH, E. O., A. GUSE, L. ROGER K & THOMPSON, G 2013. 'Use of social commitment robots in the care of elderly people with dementia: A literature review'. *Maturitas*, 74, pp. 14-20.
- N. KARIMIAN, P. A. W. F. T. 2016. Evolving Authentication Design Consideration for the Internet of Biometric Things (IoBT). *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*.
- NEAME, R. 2014. 'Privacy protection for personal health information and shared care records'. *Inform Prim Care*, 21, pp. 84-91.
- NEFTI, S., MANZOOR, U., & MANZOOR, S. *Cognitive agent based intelligent warning system to monitor patients suffering from dementia using ambient assisted living*. 2010 International Conference on Information Society, i-Society 2010, 2010 London. pp. 92-97.
- NOVITZKY, P., SMEATON, A. F., CHEN, C., IRVING, KATE., JACQUEMARD, T., O'BROLCHÁIN, F., O'MATHÚNA, D & GORDIJN, B 2015. 'A Review of Contemporary Work on the Ethics of Ambient Assisted Living Technologies for People with Dementia'. *Science Engineering Ethics*, 21, pp. 707-765.
- O'NEILL & AL., E. 2011a. 'Video reminders as cognitive prosthetics for people with dementia'. *Ageing International* 36.
- O'REGAN, E. 2015. Half of 'bed blockers' needing nursing home caught in HSE red tape. *Irish Examiner*.
- OJASALO, J., SEPPÁLÁ, H., SUOMALAINEN, N. & MOONEN, R. *Better technologies and services for smart homes of disabled people: Empirical findings from an explorative study among intellectually disabled*. 2nd International Conference on Software Technology and Engineering, ICSTE, 2010. San Juan, PR, pp. 1251-1259.
- PANEK, P. M., P. SCHULLER, F & ZAGLER, WL 2015. 'Beitrage zur Modellierung von "Personlichkeit" bei assistiven Robotern für alte Menschen zwecks besserer Mensch-Roboter Interaktion'. *AAL-Kongress*.
- PARKS, J. A. 2010. 'Lifting the burden of Women's Care Work: Should Robots Replace the "Human Touch"?''. *Hypatia*, 25, pp. 100-120.
- PARTY., D. P. W. 2017. *Article 29 Data Protection Working Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC*. 2014 [Online]. Available: <http://www.dataprotection.ro/servlet/ViewDocument?id=1086> [Accessed 22 January 2019].
- PATEL NASRULLAH. NO DATE. *Internet of things in healthcare: applications, benefits, and challenges* [Online]. Available: <https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html> [Accessed 21 March 2019].

- PATRICE, C. A., MOAWAD, VASILIS, EFTHYMIU. ANTONIS, BIKAKIS AND YVES, L. T 2016. 'Privacy Challenges in Ambient Intelligence Systems'. *Journal of Ambient Intelligence and Smart Environments*, pp. 1-27.
- PEARS, R. S., GRAHAM 2016. *Cite Them Right The Essential Referencing Guide*, London, PALGRAVE.
- PELLEGRINO, E. D. T., D. C. 1993. *The Virtues in Medical Practice*, New York, NY, USA, Oxford University Press.
- PERCIVAL, J., & HANSON, J 2006. 'Big brother or brave new world? Telecare and its implications for older people's independence and social inclusion'. *Critical Social Policy*, 26, pp. 888-909.
- PORTET, F., VACHER, M., GOLANSKI, C., ROUX, C., & MEILLON, B 2011. 'Design and evaluation of a smart home voice interface for the elderly: Acceptability and objection aspects'. *Personal and Ubiquitous Computing*, pp. 127-144.
- PRINCE, M. J. 2015. *World Alzheimer Report 2015: the global impact of dementia: an analysis of prevalence, incidence, cost and trends*.
- RADIOLOGY, E. S. O. 2017. 'The new EU General Data Protection Regulation: what the radiologist should know' *Insights Imaging*, 8, pp. 295-299.
- RASHIDI, P. M., A. 2013. 'A survey on ambient-assisted living tools for older adults'. *IEEE Journal of Biomedical and Health Informatics*, 17, pp. 579-590.
- REDMOND, S. J., LOVELL, N. H., YANG, G. Z., HORSCH, A., LUKOWICZ, P., MURRUGARRA, L 2014. 'What Does Big Data Mean for Wearable Sensor System?'. *Yearb Med Inform*, 9, pp. 135-142.
- REMMERS, H. 2010. 'Environments for ageing, assistive technology and self-determination: ethical perspectives'. *Informatics for Health and Social Care*, 35, pp. 200-210.
- ROBINSON, L., BRITAIN, K., LINDSAY, S., JACKSON, D., & OLIVIER, P 2009. 'Keeping In Touch Everyday (KITE) project: Developing assistive technologies with people with dementia and their carers to promote independence'. *International Psychogeriatrics*, 21, pp. 494-502.
- ROBOTS, T. 2016. Available: <https://www.telepresencerobots.com/robots/padbot-p1-inbot-technology> [Accessed 27 April 2019].
- ROUSE, M. 2017. *Ambient Intelligence (AmI)* [Online]. Available: <https://searchenterpriseai.techtarget.com/definition/ambient-intelligence-AmI> [Accessed].
- S. BATOOL, N. A. S. M. A. K. 2017. 'Internet of Things Data Analytics for User Authentication and Activity Recognition'. *Second International Conference on Fog and Mobile Edge Computing (FMEC)*.
- S. R, P. 2014. 'Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent'.
- SAITO, T. S., T. WADA, K & TANIE, K 2002. *Examination of change of stress reaction by urinary tests of the elderly before and after the introduction of mental commit robot to an elderly institution. Proceedings of the 7th International Symposium on Artificial Life and Robotics*, 1, pp. 316-319.
- SAJID, A., ABBAS, H 2016. 'Data privacy in cloud-assisted healthcare systems: state of the art and future challenges'. *Journal of Medical Systems*, 40, pg. 155.
- SAURWEIN, F., NATASCHA JUST AND MICHAEL LATZER 2015. 'Governance of Algorithms: Options and Limitations'. *Info* 17, 6, pp. 35-49.
- SCHAEFER, G. O. E., E. J AND WERTHEIMER, A. 2009. 'The obligation to participate in biomedical research'. *J. AM. Med. Assoc*, 302, pp. 67-72.
- SHARKEY, N. S., A. 2012. 'The eldercare factory'. *Gerontechnology*, 58, pp. 282-288.
- SHIBATA, T. W., K 2011. 'Robot therapy: A new approach for mental healthcare of the elderly - A mini review'. *Gerontology*, 57, pp. 378-386.
- SHYAM, D. K. 2019. *Living with Ambient Intelligence: So at Home with Technology* [Online]. Available: <https://www.infosys.com/insights/ai-automation/Pages/ambient-intelligence.aspx> [Accessed 05 of April 2019].

- SIDDIQUE, L. J., QADIR; SHAHZAD, FAROOQ AND MUHAMMAD, ALI IMRAN 2017. "How 5G Wireless (and Concomitant Technologies) Will Revolutionize Healthcare?". *Future Internet: Basel*, 9.
- SMITH, M. 2015. A Fitbit fanatic's cry for help: I'm addicted to steps. Lessons from a year spent fully quantified. *Washington Post*.
- SPARROW, R. S., L 2006. 'In the hands of machines? The future of aged care'. *Minds Mach*, 16, pp. 141-161.
- SPONSELEE, A. M., SCHOUTEN, B., BOUWHUIS, D., & WILLEMS, C 2008. 'Smart home technology for the elderly: Perceptions of multidisciplinary stakeholders'. *Constructing ambient intelligence*, pp. 214-326.
- STEELE, R., LO, A., SECOMBE, C., & WONG, Y. K 2009. 'Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare'. *International Journal of Medical Informatics*, 78, pp. 788-801.
- STONE, M. 2014. 'Smart-phone addiction Now Has A Clinical Name'. *Business Insider Australia*.
- TIWARI, P., WARREN, J., DA, K. J., & MCDONALD, B 2010. 'Some non-technology implications for wider application of robots assisting older people'. *Health Care and Informatics Review Online*, 14.
- TOMITA, M. R., MANN, W. C, STANTON, K. TOMITA, A. D & SUNDAR, V 2007. 'Use of currently available smart home technology by frail elders: process and outcomes'. *Top. Geriatr. Rehabil*, 23, pp. 24-34.
- TURKLE, S. 2006. 'Relational artefacts with children and elders: The complexities of cyber companions'. *Connection Science*, 18, pp. 347-361.
- VAN HOOFF & AL, E. 2011. 'Ageing-in-place with the use of ambient intelligence technology: Perspectives of older users'. *International Journal of Medical Informatics*, 80, pp. 310-331.
- VARNAI, P. S., P. FARLA. K & SHARP. T. A 2015. *A Mapping of Smart Ageing Activity in Ireland and An Assessment of the Potential Smart Ageing Opportunity Areas*. In: (UK), T. G. (ed.) *A report to the Department of Jobs, Enterprise and Innovation of the Republic of Ireland*.
- VINCENT, C. R., D. DEAUDELIN, I. GARCEAU, M & TALBOT, L. R 2006. 'Public telesurveillance service for frail elderly living at home, outcomes and cost evolution: a quasi experimental design with two follow-ups'. *Health Qual. Life Outcomes*, 4.
- VON STOSSER, A. 2011. 'Robots as a solution to the care-dilemma? Ethical questions'. *Archive fur Wissenschaft und Praxis der sozialen Arbeit*, 3.
- WACHTER, S. 2018. 'Normative challenge of identification in the Internet of Things - Privacy, profiling, discrimination, and the GDPR'. *Computer Law & Security Review*, 34, pp. 436-449.
- WADA, K. S., T. SAITO, T. SAKAMOTO, K & TANIE, K 2005. *Psychological and social effects of one- year robot-assisted activity on elderly people at a health service facility for the aged*. *Proceeding of the 2005 IEEE International Conference on IEEE*. ICRA.
- WAGNER, I. 2010. *Forschungsethik in der Technikentwicklung*, New York, Springer.
- WALLACE, J., MULVENNA, M. D., MARTIN, S., STEPHENS., S., & BURNES, W 2010. 'ICT interface design for ageing people and people with dementia. In M. D. Mulvenna & C. D. Nugent (Eds.)'. *Supporting people with dementia using pervasive health technologies*, pp. 165-188.
- WOODWARD, R. 2009. *The OECD Privacy Framework; Organisation for Economic Co-operation and Development* [Online]. Routledge: Abingdon-on-Thames, UK. Available: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [Accessed 22/January/2019].

Appendices

Appendix A:

TRINITY COLLEGE DUBLIN

Participant Information Sheet

~ “An Investigation into the Ethical challenges of the Internet of Things Ambient Assisted Living (IoT AAL) in Ireland” ~

LEAD RESEARCHER: Michael O’Keeffe

Background

The purpose of this project is to investigate the ethical challenges of the Internet of Things Ambient Assisted Living (IoT AAL) in Ireland under a number of headings bullet-pointed below.

- Privacy.
- Security
- Social Isolation.
- User Behaviour modification.
- Regulation of the Internet of Things in Ambient Assisted Living technology in Ireland (IoT AAL technology).

This project will be used for the researcher to gain a Master’s Degree in the Management of Information System Strategy

PUBLICATION:

Individual results may be aggregated anonymously, and research reported on aggregated results. The results of this research will be published in a TCD MSc dissertation and may be published in scientific journals or at conferences.

PROCEDURES OF THIS STUDY

You are being asked to participate in this study based on your experience and interest in the use of technology to support ambient assisted living. I obtained your contact details via your organisation's website.

You are being asked to participate in an interview that will take about 40 minutes of your time. The interview can take place at a location that is convenient for you. The interview will involve questions concerning the ethical challenges of privacy, security, social isolation, and user behaviour modification.

Your participation in the study will be on an anonymous basis.

I will be using a recording device for the convenience of transcription and to reflect back on the interview. You can decline to be audio recorded.

On request, debriefs can take place with the participants at the end of their participation or at a later stage by contacting the researcher.

The entire transcript or parts of the interview including handwritten notes can be withdrawn from the research process at any stage without the need for explanation or penalty.

No risk is anticipated in relation to a participant in this study, and any material gathered is considered low risk.

I don't have any bias or conflict of interest with anyone or any entity in relation to this study.

Your interview will be recorded by voice recorder via a laptop, or smartphone or another dedicated device. The recording will be backed up to an encrypted ThinkPad external hard drive containing a Symantec encryption (password protected) and hardware coded pin number both known only to the researcher, and an encryption volume on the laptop for analytics at a later stage. The original recording will be password protected and kept in a secure location in work or secured at home. All copies of the recordings will be destroyed once the MSc study is complete. The recording may be transported on the secure hard drive mentioned above to Trinity College Dublin from home or work for analysis using specialist software (if required) or Microsoft Excel at home. Thematic Analysis may be required but is not expected to be required.

Appendix B:

TRINITY COLLEGE DUBLIN

Participant Information Sheet

~ “An Investigation into the Ethical challenges of the Internet of Things Ambient Assisted Living (IoT AAL) in Ireland” ~

LEAD RESEARCHER: Michael O’Keeffe

Background

The purpose of this project is to investigate the ethical challenges of the Internet of Things Ambient Assisted Living (IoT AAL) in Ireland under a number of headings bullet-pointed below.

- Privacy.
- Security
- Social Isolation.
- User Behaviour modification.
- Regulation of the Internet of Things in Ambient Assisted Living technology in Ireland (IoT AAL technology).

This project will be used for the researcher to gain a Master’s Degree in the Management of Information System Strategy

PUBLICATION:

Individual results may be aggregated anonymously, and research reported on aggregated results. The results of this research will be published in a TCD MSc dissertation and may be published in scientific journals or at conferences.

PROCEDURES OF THIS STUDY

You are being asked to participate in this study based on your experience and interest in the use of technology to support ambient assisted living. I obtained your contact details via your organisation's website.

You are being asked to participate in an interview that will take about 40 minutes of your time. The interview can take place at a location that is convenient for you. The interview will involve questions concerning the ethical challenges of privacy, security, social isolation, and user behaviour modification.

Your participation in the study will be on an anonymous basis.

I will be using a recording device for the convenience of transcription and to reflect back on the interview. You can decline to be audio recorded.

On request, debriefs can take place with the participants at the end of their participation or at a later stage by contacting the researcher.

The entire transcript or parts of the interview including handwritten notes can be withdrawn from the research process at any stage without the need for explanation or penalty.

No risk is anticipated in relation to a participant in this study, and any material gathered is considered low risk.

I don't have any bias or conflict of interest with anyone or any entity in relation to this study.

Your interview will be recorded by voice recorder via a laptop, or smartphone or another dedicated device. The recording will be backed up to an encrypted ThinkPad external hard drive containing a Symantec encryption (password protected) and hardware coded pin number both known only to the researcher, and an encryption volume on the laptop for analytics at a later stage. The original recording will be password protected and kept in a secure location in work or secured at home. All copies of the recordings will be destroyed once the MSc study is complete. The recording may be transported on the secure hard drive mentioned above to Trinity College Dublin from home or work for analysis using specialist software (if required) or Microsoft Excel at home. Thematic Analysis may be required but is not expected to be required.

DECLARATION:

- I am 18 years or older and am competent to provide consent.
- I have read or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions, and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I understand that I may stop electronic recordings at any time and that I may at any time, even subsequent to my participation have such recordings destroyed (except in situations such as above).
- I understand that subject to the constraints above; no recordings will be replayed in any public forum or made available to any audience other than the current researchers/research team.
- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.
- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I understand that my participation is entirely anonymous and that no personal details about me will be recorded.
- I have received a copy of this agreement.

PARTICIPANT'S NAME:

PARTICIPANT'S SIGNATURE:

DATE:

Statement of the investigator's responsibility: I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

RESEARCHERS CONTACT DETAILS:

Phone Number: 0879088522

Email: mokeeff6@tcd.ie

INVESTIGATOR'S SIGNATURE:

DATE:

Appendix C:

Sample Interview Questions:

Questions for providers of IoT AAL services other than for profit which may also include devices:

Privacy:

Major Question 1: What is your approach to securing health-related data (for example AAL sensors etc.) in the current GDPR climate, thus protecting vulnerable user's privacy and data?

Minor Question 1: Have you any experience in group privacy Stigma or unwanted behaviour toward groups of users in relation to IoT AAL technology? If yes, can you elaborate?

Security:

Minor Question 1: Can you give examples of security issues involving IoT AAL from your experience?

Minor Question 1: Have you seen, experienced or are aware of situations prior to the implementation of the Co-Decision-Making Act (the week of the 14th of January) where IoT AAL was put in place as it was seen by caregivers as *"It's for their own good"* and what is/was approached on this matter?

Social Isolation:

Major Question 1: Have you seen, experienced or are aware of situations where after the introduction of IoT AAL technology, social isolation becomes an issue? If yes, can you elaborate?

Major Question 1: Have you seen, experienced or are aware of the use of care-robots in use and what is your professional opinion of them to date?

Behaviour Modification:

Major Question 1: Can you elaborate on examples of positive and/or negative behavioural changes in users in relation to IoT AAL technology?

Minor Question 1: Have you seen, experienced or are aware of situations of social stigma or unwanted attention towards users due to the presence of IoT AAL? If yes, can you elaborate?

Minor Question 2: Have you experienced resistance to IoT AAL technology from users or their careers in relation to privacy or other issues? If yes, can you elaborate?

Questions for-profit organisations providing IoT AAL services which may include devices:

The questions from above, plus one more.

Minor Question 1: “Given you are an international organisation”.

Are elderly Irish people more cautious towards privacy and/in relation to IoT AAL than other peoples, from your experience or observations?

Questions for the regulator in the Irish Market:

“Regulation authorities around the world, such as the FDA and the EU are finding it challenging that more wellness and health-related devices are moving into the medical device field / IoT AAL”.

Major Question 1: How has your experience to date been in relation to this situation in Ireland?

Major Question 2: Do you generally regulate the services and devices of charities or companies that use IoT AAL technology and/or social care robotics? Can you elaborate?

Major Question 3: Have you seen, experienced or are aware of ethical issues that arise surrounding IoT for AAL?

Major Question 4: From your point of view as the regulator, what are the most concerning trends, devices or services of IoT for AAL either now or in the future that you are concerned about?

Minor Question 1: Is there anything that you would like to see as the regulator that you know about and haven't seen yet in relation to the ethics of IoT AAL?

Minor Question 2: What's the most unusual or out of the ordinary device or service you have allowed or disallowed and why?

Appendix D:

Interview Checklist

Interview Checklist						
Interviewee:						
Organisation Type:						
Theme and Question Category	Type	Question #	Subtheme	Left Over theme	In Interview	Not in Interview
Privacy	Major	1	The capture of Medical Data VS Health-Related Data	<u>Autonomy</u>		
			GDPR Compliance	Freedom		
			Big Data	Independence		
			Data Hoarding	Unwanted Sharing of Data		
	Minor	1	Group Privacy	Intrusions inhibiting decision making		
			Advancing Medical Science	Chronic Illness Management		
Security	Minor	1	Behaviour of Organisations			
			Behaviour of Individuals			
			Social Engineering			
			Hacking			
			Obtrusiveness			
			Physical Attack by altering equipment			
			Ease Dropping			
	Minor	2	Need for technology despite the risk to the individual			
Social Isolation	Major	1	Replacement VS Aggregation			
			The distance of relatives due to the presence of technology			
			Rejection of technology			
	Major	2	Deception			
			Dignity			
			Isolation			
			Privacy			
			Safety			

			Vulnerability		
			Autonomy		
<i>Behaviour Modification</i>	<i>Major</i>	1	Avoiding sensors etc		
			Altering devices (e.g. Switching them off)		
			Adherence Management System		
			Coached too intensively		
			Hypochondria		
			Trained Helplessness		
			Addition to Devices		
	<i>Minor (1)</i>	2	Negative Feedback		
	<i>Minor (2)</i>	3	Caregiving rejection of devices		

Appendix E Resultant Procedure and results of the Qualitative Analysis

Below shows some of the qualitative analysis procedure and results that were carried out. Starting from left to right, the first column is the interviewee or participants quote; this was taken from the interview transcripts themselves. The second column contains the quote from the first column written in the researcher's own words.

An extract theme was the product of the first two columns which ended up in the third column, followed by a subtheme, which is at a more granular level. In the second last column or second, from the right, a theme emerged. However, these themes were many, and further analysis was needed in order to widdle them down. That was the function of the last column on the right; this was the high-level theme.

It was these themes that emerged from the interview research. A quite scan through the literature revealed if the narrative from both literature review and interview data was the same. This is what was done for all themes that emerged from the interviews; this final step was carried out. One final note, in the far left column, you will see the interviewee in brackets abbreviated to (Interw1), just as an example, this means the first interviewee. This will be followed by Line 1-2, again this is an example. That means line 1 to 2 in the interview transcript and is for the benefit of the researcher who is carrying out the analysis as the reader won't actually see the interview transcripts themselves.

Theme: Privacy Question 1: Major

What is your approach to securing health-related data (for example AAL sensors etc.) in the current GDPR climate, thus protecting vulnerable user's privacy and data?

Participant Quote	Description	Extract theme	Sub-Theme	Theme	High-level theme
(Interw1) Line 1-2 "The whole process we have worked through our solicitors, to draft a consent form kinda".	Working with legal experts to create a consent form.	Get legal advice, to minimise risk.	Seek legal advice.	Legal Advice	Assessment.
(Interw1) Line 2 "Draft an information booklet that meets the standards of GDPR."	Working with experts to provide a booklet for transparency.	Get legal advice to provide transparency.	Seek legal advice.	Legal Advice	Assessment.
(Interw1) Line 2-4 "We are working with a research partner as well in Dundalk and there in a research institute, so	Seek a knowledgeable partner that is in line with best practices.	Seek knowledge for best practices.	Seek knowledge and training.	Training.	Training.

everything they do is in line with practices of a research institute.”					
(Interw1) Line 6-9 “In terms of consent... in terms of privacy, everything is quite clearly laid out to the person when we meet them first in the home...the technology engagement officers would go out to the home and explain the booklet to them; they would obviously leave the booklet.”	Privacy and consent are clearly laid out and explained by the technology engagement officer; the booklet is left to read and to make an informed decision.	Create user booklet with staff training.	Create a booklet and training.	Training.	Assessment.
(Interw3) Line 7-9 “we have to do a substantial piece of work...to understand what the requirement was, and particularly for health data, sensitive type data, we would have attended a lot of GDPR type courses and information sessions, and ones that were run by the health research board.”	Attend courses, and information sessions, run by the health board to understand system requirements, especially for sensitive data types and GDPR compliance.	Training on GDPR, system requirements and handling of sensitive data.	Training on system design and sensitive data handling.	Training	Training.
(Interw3) Line 11-17 “what we...have done is a quite detailed data protection impact session...highlighting what parts...the system was anonymised...what parts would have access to sensitive information...for example with our system we would...bring data into the system but also put data out of the system to let a healthcare professional, we would have to say this is “John’s” data or “Mary’s” data we can’t hide it behind...a pseudo name in that case. Part of it is being very transparent about where data is flowing and who has	Detailed Protection Impact Session to find what parts of the system were anonymised, what parts have access to sensitive information for input, and output to a healthcare professional. Transparency is key to who has access and where data is going.	Detailed Protection Impact assessment, for anonymised, sensitivity and access control.	Carryout Detailed Data Protection Impact assessment.	DPIA	Data Security.

access, and who can see identifiable information.”					
(Interw3) Line 18-20 “The other part is making sure the system is technically robust enough and is compliant...We have passed a data protection impact assessment person who would sign off on that”	Ensure the system is compliant and technically robust enough, external audit signed off.	Proper testing, compliance and external audit sign off.	Robust Testing and external audit.	Testing and Audit.	Assessment.
(Interw3) Line 21-23 “Collecting questionnaires...interview data and storing data on laptops and paper copies...reviewing our procedures to ensure we are in line with GDPR and ethical procedures, that we are compliant with them.”	Ensure the understanding of compliance, and ethical procedures in line with storing data on laptops and in paper form.	Create Compliance procedure for storage of electronic and paper data.	Create data storage compliance procedures.	Training.	Assessment.
(Interw4) Line 3-4 “...we undertook quite a rigorous Data Protection Impact Assessment (DPA)... So we worked with the Data Protection officer here,”	Undertook rigorous DPIA with oversight from the DPO.	Oversight of DPO in DPA.	Seek advice from DPO.	DPIA	Assessment.
(Interw4) Line 4-5 “...so in terms of the approach for (Project) if you were going to sum it up, or in terms of running a trial, the most important thing is consent.”	The essential item in running a trial or project is consent.	Consent is the most important.	Implement a consent policy.	Consent Policy	Privacy.
(Interw4) Line 5-7 “...in terms of GDPR, as far as I am concerned, the consent that was needed was always needed...there just implementing the data protection procedures that were always there.”	Consent was always needed despite GDPR, their just implementing data protection procedures as expected.	Implementing Consent as expected.	Implement a consent policy.	Consent Policy	Privacy.
(Interw4) Line 7-8 “But now there is a heavier fine because there are really implementing it.”	Taking compliance seriously because of Heavy fine’s,	Financial risk due to compliance issues.	Enforce compliance policy.	Data compliance	Legal.

(Interw4) Line 8-11 “The ethics for the project were quite complex, we had to go through HSE, TCD and DKIT ethics, so it was quite rigorous, and then the Data Protection Impact Assessment was separate. Now from my understanding, they're trying to merge the DPA more with the ethics procedures. But we got our ethics, and after that, we did the DPA.”	Ethics for the project were quite complex and rigorous which came from three institutes. DPA was separate, but in future will be merged with ethics.	Ethics from all stakeholders, and DPA from the lead institute.	Seek stakeholder ethics and DPA.	Ethics and DPA.	Assessment.
(Interw4) Line 15-17 “...the procedures that we needed from the ethics side on trial was all about consent, so it's all about transparency with the participant, so they know what happens to their data.”	The ethical procedures from the trial were all about consent and transparency of what happens participant's data.	Create Ethical procedures for consent, and transparency of participant data.	Create ethics surrounding privacy and transparency.	Ethics	Assessment.
(Interw4) Line 17-21 “And then for (Project), there was a lot of time spend in the system design to make sure it was secure. The main data is stored in DKIT, and only anonymised data is sent to the cloud that IBM use. But all the security is really designed in Netwell CASALA because personal information is only stored there. Anything that is sent to IBM is anonymised.”	For the project, a lot of time was spent in the system design making it secure. All the security was really designed in (location noted) because the personal information was stored there and anonymised data sent to (Company X cloud).	System designed, data security and the cloud.	Design system and Anonymisation for the cloud.	On-Premises and Cloud operations	Assessment + Data Security.

Subtheme: Big Data

Participant Quote	Description	Extract theme	Sub-Theme	Theme	High-level theme
(Interw2) Line 25-30 "We hope to in the future use like machine learning and AI to make a smarter system that indicates where activity was present. To react to that but at the moment the processing is really done manually and sort of identifying if there is a sort of trend that is not healthy and also the fact that if there is then like temperature going below a certain level. Sort of then cause an alert, and we will receive those alerts and react accordingly so if there were things like motion in the bathroom for over an hour, but no other room maybe they're having a fall in the bathroom for example, or in the hall, that's another one."	At the moment they don't use AI or ML to analysis the presence of activity. Processing of presence activity and alert data is done manually. For example, an activity that is not healthy such as being in the bathroom for an hour or hall and nowhere else could suggest a fall. Other alerts can be the temperature for example. They will react accordingly to alerts.	Room for future growth in AI and ML integration into the system for alert profiles and appropriate action.	AI and ML integration.	Future Development	Future developments.
(Interw3) Line 46-51 "we collaborate with partners so one of the projects	We work with a particular company, where we transfer	Third party cloud, for analytics, data compliance.	Cloud analytics and compliance.	Cloud operations.	Data Security.

<p>we're working on at the moment, which involves Interw4, we work with (company noted) on this, we would transfer anonymous data to their cloud servers, and they run algorithms, and they push it back to us. So they are never aware of the identity of data when it passed into their system and get a different ID, and it can't be traced back basically to the person, yes. (company noted) themselves would also be very strict with their compliance."</p>	<p>anonymised data over to their cloud, and they give up back the results after running algorithms. They never know the ID of the person as the ID they use is different from the original one assigned to the uses data. That same specific company has strict compliance conditions.</p>				
<p>(Interw4) Line 23-25 "From there perspective, there were quite strict in the kind of data, they didn't want any kind of personal data. So that was really set up from the beginning, I suppose the other thing about GDPR, the definitions, anonymised and sudo-</p>	<p>(Company noted) were quite strict, no personal data. It was set up that way from the start. With GDPR the definitions of anonymised and sudo-anonymised were more precise.</p>	<p>Strict policy on personal data, clear definitions.</p>	<p>Create clear data protection policy.</p>	<p>Data Protection policy.</p>	<p>Data Security.</p>

anonymised are probably more clear than they were previously."					
--	--	--	--	--	--