

Grace Annalise Milne

Balancing public health and privacy: an exploration of citizen privacy attitudes towards governmental use of wearable technologies in public health crises

Master Thesis

at the Public Governance Institute
(KU Leuven)

Supervisor: Prof. Steven Van De Walle

Presented by: Grace Annalise Milne
Richard Sorge Strasse 36
10249 Berlin
+49 152 04863226
grace.milne@student.kuleuven.be

Date of Submission: 2021-05-28

Acknowledgements

As I submit this Master thesis, it's hard to believe that my PIONEER journey has just about come to an end. This thesis is the culmination of two years' hard work: it was a challenging and fulfilling experience, even though studying overseas in a global pandemic was not at all what I expected when I moved my life from Canberra to Europe. Nevertheless, it has always been a dream of mine to graduate from a European university, and I am profoundly grateful for being supported by so many people and institutions to achieve this. I feel fortunate and privileged to have been supported by KU Leuven, WWU Münster, TalTech, and the European Commission to achieve this Erasmus Mundus Masters degree.

Firstly, I want to express my sincere gratitude to my supervisor, Professor Steven Van De Walle. Your endless patience with all of my (many) questions and your honest advice with my research direction was enormously appreciated. I am lucky to have had a supervisor who showed interest in my work, took time out of your very busy schedule to critically review drafts, and to meet with me throughout the thesis process. I would also like to thank Dr. Noel Carroll for introducing me to the many possibilities of wearable technology.

I want to thank my family for their love and support throughout my time studying in Europe. To my parents, thank you for supporting and respecting my decision to stay in Europe and finish my Masters, despite the many struggles and challenges I experienced. I cannot even imagine how difficult and stressful it must have been to have me away from home for so long – especially in the midst of the pandemic. I will be forever grateful that you were just a phone call away whenever I needed you, and I am hopeful that we can meet again in Australia sooner rather than later. And thank you for sending so many pictures of our dog, Bowie, to remind me to relax a little bit!

Thank you to my friends – in Brisbane, Canberra, Melbourne, and throughout Europe – for both supporting me and distracting me whenever I needed it. I am lucky to be surrounded by such kind and interesting people. I also want to thank my fellow PIONEERs – you have become family, and I am happy and grateful that our paths crossed. We went through so much together – in three different countries, no less! – and I will always look back fondly on our times in Leuven (particularly De Vesten), Münster, and Tallinn. We have made many memories together, and I look forward to more adventures all over the world. Who knows when and where we will meet again? I'm excited to find out. I wish you all the best for the future and I know everyone will achieve wonderful things in their lives.

Finally, a huge thank you to the staff and professors involved in the PIONEER programme. Specifically, Professor Joep Crompvoets for his unparalleled passion for teaching, innovation, and eGovernance. To Joep and Steven – thank you for giving me this unique opportunity to be a part of PIONEER. And of course, a huge thank you to Lotte Laenan, who was just amazing in guiding and supporting the entire PIONEER cohort.

Abstract

The coronavirus disease (COVID-19) has pushed governments around the world to simultaneously address dynamics of public health and citizen privacy in unprecedented ways. Various mitigation measures such as lockdowns, quarantines, and social distancing have been used to slow the virus's spread, but at significant cost to the global economy, people's well-being, and their privacy. Wearable technology has been identified as having strong potential to keep infected or potentially infected individuals isolated, while allowing the rest of society to live a pre-pandemic lifestyle. However, there are strong privacy concerns with allowing governments to gather, access, and store data from citizen-worn wearable devices. Nevertheless, a select number of governments across the world have rolled out wearable technology as a tool to control the spread of COVID-19. Past studies have focused on the acceptance and adoption of wearable technology purely in a consumer context, and therefore these findings may not be applicable in a public sector context. Using Australia and Singapore as case studies, this study explores citizens' privacy attitudes towards governmental use of wearable technologies in public health crises, in the context of the COVID-19 pandemic, and with a focus on quarantine enforcement. The difference between data-first and privacy-first architectures are also explored, as well as citizens' preferences for the device to be mandatory or optional. Semi-structured qualitative interviews were conducted with wearable technology users in Australia and Singapore, and inductively coded to reveal exploratory insights. The findings indicate that there are seven themes that influence citizens' acceptance and adoption of wearable technology in a government context: perceived benefit, perceived privacy risk, context, time, choice, trust in government, and data access. Furthermore, there were cross-country differences in citizens' privacy attitudes. Future research ought to build on this study's findings by investigating these themes quantitatively with larger sample sizes and continue researching across countries and cultures to establish a research base that goes beyond the consumer perspective, and includes a public sector perspective. Governments considering to use wearable technology in public health crises should critically consider these themes in their roll out.

Content

Figures

Tables

Abbreviations

Apps	Applications
COVID-19	Coronavirus disease

Acronyms

4G	Fourth generation
5G	Fifth generation
FIP	Fair Information Practices
GPS	Global positioning system
IoT	Internet of Things
IT	Information technology
PIN	Personal identification number
SARS	Severe acute respiratory syndrome
TAM	Technology Acceptance Model
UAE	United Arab Emirates
UNDHR	United Nations Declaration of Human Rights
USA	United States of America
UTAUT	Unified Theory of Acceptance and Use of Technology
WHO	World Health Organisation

1 Introduction

The work of government is complicated by its need to effectively balance daily operations with being reactive to crises. In addition to business-as-usual activities to ensure that a country is running smoothly, governments are also responsible for reacting to more serious threats such as armed conflict, economic downfall, and life-threatening disease. Technology is often used in crisis responses, and while some governments may not be ready to implement such technologies, or the technology in question may not be fully developed, the risks and consequences of not using them may be far greater. Public health crises are serious societal events that not only threaten people's health, but their well-being, livelihoods, and overall way of life. The coronavirus disease (COVID-19) pandemic is a current and noteworthy example of a public health crisis that has interrupted people's lives across the world to an unprecedented extent, and that governments have had to react to at short notice. Key international organisations such as the International Labour Organisation and the World Health Organisation (WHO) have stated that COVID-19's global impacts have gone beyond the virus itself, with unprecedented consequences on poverty, unemployment, and social welfare (World Health Organisation, 2020). What was originally a public health crisis has transformed into a socio-economic disaster.

As at May 2021, approximately 165 million people globally have contacted COVID-19, with approximately 3.5 million deaths (World Health Organisation, 2021). Since the declaration of the pandemic in March 2020, governments around the world implemented lockdowns to control the spread of COVID-19, which gradually eased into strict social distancing measures and recommendations. As at May 2021, many countries around the world have continued to fluctuate between strict lockdowns and easing of restrictions. These measures have had severe impacts on the global economy and people's well-being: the economic consequences of lockdowns have resulted in intense declines in gross domestic product (König & Winkler, 2021) and have had a severe impact on people's mental health globally, with researchers finding a significant increase in online searches for loneliness, worry, and sadness (Brodeur et al., 2020).

As the COVID-19 vaccine rollout continues, there is an urgent need to understand what can be done to mitigate the negative economic and social effects of public health measures such as lockdowns. Furthermore, governments need a strong evidence-base on what measures can be taken to prevent and respond to future pandemics. To date, governmental measures to control the spread of COVID-19 have been inconsistent both domestically and internationally, and have been implemented with a limited evidence-base. Past public health crises such as the severe acute respiratory syndrome (SARS) outbreak and the

Ebola outbreak have provided precedents for quarantine and lockdown measures (Brooks et al., 2020). However, these measures have never taken place on such a large scale as has been required for COVID-19.

The purpose of having strong digital technologies to support lockdown and quarantine measures is not just to identify and isolate infected or potentially infected people from the rest of society, but to ensure that non-infected people are impacted to the lowest possible degree (Colizza et al., 2021). To date, this is not the case in many countries throughout the world: governments have increased their surveillance of citizens and restrictions on freedom of movement have been implemented in various degrees. Furthermore, many of these measures have been implemented hastily and are accompanied by significant losses in privacy (Rodriguez et al., 2020). Citizens may not understand what information the government is collecting about them, and may have limited choice in participating in surveillance activities (Rodriguez et al., 2020). These governmental surveillance tools include digital contact tracing technologies (hereafter referred to as apps) (Wiggins & Carrick, 2020); wearable devices for people under quarantine obligations (Wiggins & Carrick, 2020); and drones ensuring that individuals are staying at home (Krauss, 2020). Some countries have implemented government-run quarantine facilities for travellers and unwell people (Murphy, 2020). These facilities are expensive to run, and have negative financial and psychological effects on those required to use them (Brooks et al., 2020).

Considering these negative impacts, it is important for governments to consider the role of innovative technology to facilitate alternative approaches in public health management. Sun et al. (2020) recommend that wearable technology is a viable tool for governments to use to complement or replace lockdowns, quarantines, and social distancing, at a reduced disruption to non-infected individuals. However, noting Rodriguez et al.'s (2020) privacy concerns, any governmental use of wearable technology must take citizen privacy into account. This thesis's motivation is therefore rooted in the need to understand citizen privacy attitudes towards wearable technology in a government context. These insights have important implications for the growing debate surrounding public health and privacy.

However, there is a significant gap in academic literature on governmental use of wearable technology, and as result, very little is known about how citizens may respond to governments rolling out this type of technology. Wearable technology adoption factors – as well as privacy factors – are a developing research area in a consumer context, but have never been researched in a public sector context. In the context of the COVID-19 pandemic, this is problematic because governments around the world have started

implementing wearable technology as a pandemic management tool and they have very weak understandings of what may be required to ensure citizen acceptance and adoption. Without theoretical understandings in this area, governments will not be aware of what conditions ought to be met to enable device uptake. Harari (2020) writes that while wearable technology has the capacity to shorten infection chains very quickly and ultimately reduce the length and impact of pandemics, such uses of innovative technology foster a new surveillance system for governments to monitor their citizens. Therefore, while the technology itself has been identified as having strong capabilities as a pandemic management tool, the privacy implications are significant (Harari, 2020; Sun et al., 2020). Therefore, this study seeks to answer the following research question: *what are the privacy attitudes of citizens towards adopting wearable technology as a tool for the government to enforce quarantine obligations during public health crises?*

There are different ways that governments can manage the collection, storage, and access of data collected by their state-implemented wearable technology. The device can have a data-first approach, whereby the information collected through the wearable technology is gathered in large quantities and public authorities have full access to it (Fahey & Hino, 2020). Alternatively, the device can have a privacy-first approach, whereby the data is protected through encryption and public authorities have limited access to the collected data (Fahey & Hino, 2020)[1]. It is important to consider the way the government manages data collection, storage, and access because it has a strong impact on privacy and effectiveness: the former approach facilitates easier and quicker government responses to quarantine breaches, but at the cost of citizen privacy, whereas the latter approach enables stronger privacy protections for citizens at the cost of the government's ability to quickly respond to quarantine breaches. Additionally, governments are faced with a choice of whether to make wearable technology as a quarantine enforcement tool mandatory or optional. Therefore, this paper seeks to address the following two research sub-questions: *do citizen attitudes differ in relation to whether the wearable technology operates as data-first or privacy first? Do citizen attitudes differ in relation to whether a government makes wearable technology mandatory or optional?*

To answer these research questions, this thesis adopts an exploratory multiple-case study research design and uses semi-structured qualitative interviews with citizens from Australia and Singapore. The research background provides depth to the research problem by outlining essential insights on wearable technology, privacy, and governmental technological responses to the COVID-19 pandemic. The literature review provides a

[1] The distinction between data-first and privacy first architecture approaches is discussed in greater detail in the Research Background.

comprehensive overview of known wearable technology adoption factors in a consumer context, to demonstrate that public sector use may be subject to different factors. The methodology outlines the exploratory multiple case-study research design and provides a strong justification for the selection of Australia and Singapore as case studies. A cross-country approach was selected to add breadth to the research findings. The results present a full summary of interviewees' responses and their privacy attitudes, structured by inductive themes and country responses. Finally, the discussion analyses these findings and answers the research questions, as well as indicating the theoretical and practical implications of this study.

2 Research Background

2.1 Wearable technology

Wearable technology has permeated many areas of people's everyday lives throughout the world. It has a wide range of different applications, such as in healthcare, sports and fitness, gaming, lifestyle and fashion, and security (Berglund et al., 2016). From people who want to track their daily steps, to people who need remotely facilitated doctor consultations to monitor health conditions, this technology has a broad societal reach. The form of these devices is also broad, ranging from wrist-worn to head-mounted (Mewara et al., 2016). However, the most popular from of wearable technology to date has been the wrist-worn device, more commonly known as the smartwatch (Berglund et al., 2016). Hiremath et al. (2014, p. 305) provides a wearable technology architecture that visually displays the ecosystem that facilitates their functionalities (see

Figure **1**). Wearable technology is made up of a combination of wearable body sensors, Internet-connected gateways, and a cloud, that each enable the collection, processing, and storage of user data (Hiremath et al., 2014).

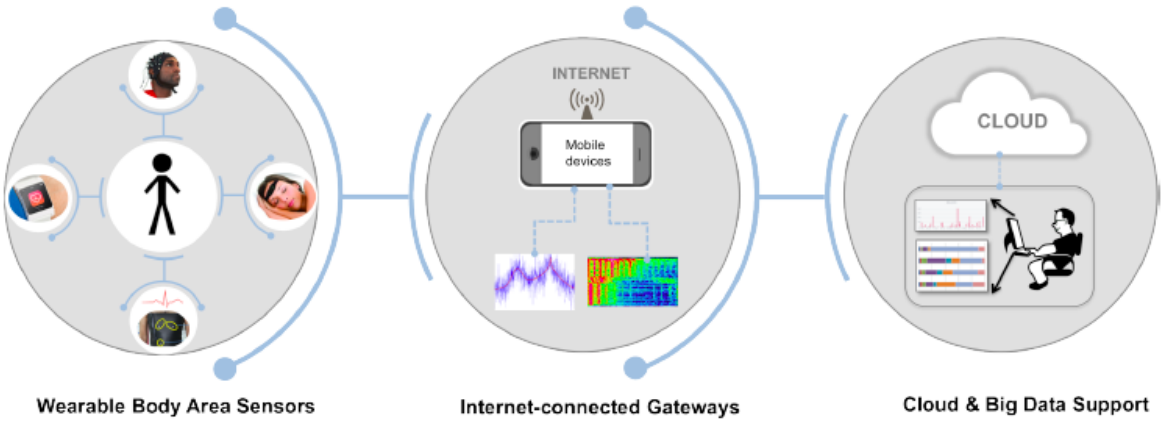

Figure 1: Wearable technology architecture (adapted from Hiremath et al., 2014, p. 305)

It is also necessary to emphasise the nascency of the wearable technology industry. The sector's growth is rapid and vast: in 2020, the industry was valued at US$27.9 billion and is predicted to reach US$74 billion by 2026 (Mordor Intelligence, 2020). This fiscal growth has been accompanied by growing interest from academia. Wearable technology research has increased immensely in recent years, alongside growth in sensor technologies, fifth generation (5G) cellular network technology, and the proliferation of cloud architectures and big data (Loncar-Turukalo et al., 2019). To understand the role of

wearable technology in government settings, it is first necessary to outline a brief history and establish a common definition of this technological development.

2.1.1 A brief history

Wearing technology on one's body has been a science fiction dream for some time: for example, Isaac Asimov's canonical *I, Robot* depicts a future where human life is dominated by wearables (Asimov, 1950, as cited in Winchester, 2015). At the time of Asimov's writing, wearing technology on or close to one's body was enormously futuristic. However, humans altering or adding accessories to their bodies is not new: tattoos and piercings have existed for millennia (Winchester, 2015). These close-to-body accessories represent the imbrication of the human body and wearable items. However, tattoos and piercings do not serve functional purposes, while modern wearable technologies are characterised by the functions they perform (S. Park et al., 2014). A brief history of wearable technology highlights the overwhelming absence of government in the field to date. Early examples of wearable technologies include abacus rings from 17th century China, and of course the wristwatch (Winchester, 2015). In a modern context, Mewara et al. (2016) describes the 1960s and 1970s as the embryonic phase of wearable technology development, where devices were largely experimental and non-commercial. One of the most notable modern wearable technology developments occurred in 1961, where a number of professors from the United States of America (U.S.A.) developed a pair of shoes that enabled the user to cheat when playing roulette (Mewara et al., 2016; Winchester, 2015).

Following this, the 1980s and 1990s were entirely technology-driven, with not yet much thought for user friendliness nor for introducing these devices to the economy (Berglund et al., 2016). For example, in 1981, the photographer Steve Mann developed an early version of the Google glasses concept, which was a head-mounted device that photographed the wearer's everyday surroundings (Mewara et al., 2016). This device was never made commercial by Mann and was not practical to wear. Developments in the early 2000s focused on integrating smart clothing into the economy, and to date this has had limited success (Berglund et al., 2016). Furthermore, the proliferation of smartphones during this time slowed the popularity of wearable technology as these mobile devices are highly functional without having to be worn directly on one's body (Winchester, 2015). In recent years, wearable technologies have achieved huge levels of growth and the emergence of companies such as Fitbit and Garmin – and the development of products such as Google glasses – have brought wearable technologies into the mainstream (Mewara et al., 2016). It is estimated that by 2022, one billion people worldwide will own a wearable device (Statista, 2021).

The technological advancements that have aided the growth of wearable technologies have given rise to a generation of tiny computers that are simultaneously easily transportable and yet very powerful machines. The most important technological development that has aided the proliferation of wearable technology is the Internet of Things (IoT) (Malmivaara, 2009; Swan, 2012). The European Commission (2019) defines IoT as a phenomenon that "…merges physical and virtual worlds, creating smart environments". Governments in the U.S.A. and Australia have simpler definitions, proclaiming that IoT can refer to any object or device with an Internet connection (Australian Signals Directorate, 2020; U.S. Department of Commerce, 2019). While computers were once huge objects that took up entire rooms and were unimaginably slow compared to today's standards, over the years they have both shrunk in size and increased in speed (Chatterjee et al., 2016). So much so, that the technology in today's smartwatches is faster and more advanced than the computers that were once as big as the rooms that housed them (Chatterjee et al., 2016).

2.1.2 What is wearable technology?

In academic literature, there is little debate over what is meant when referring to 'wearable technology'. Malmivaara (2009) differentiates between wearable computers and wearable technologies: on one hand, a wearable computer is "…a computing device assembled in a way which allows it to be worn or carried on the body while still having the user interface ready for use at all times" (Malmivaara, 2009, p. 4); on the other hand, wearable technologies are more targeted versions of wearable computers, as they are "…constructed with set tasks to fulfill one or more needs of a specific target group." (Malmivaara, 2009, p. 5). In this sense, wearable technologies are a subset of wearable computers that do not have universal applications and are instead targeted towards specific functions. Meanwhile, Mewara et al. (2016, p. 62) state that wearable technology, wearable devices, and wearables are interchangeable terms that "…refer to electronic technologies or computers that are incorporated into items of clothing and accessories that can comfortably be worn on the body". This definition is supported by Wright and Keith (2014) and Alrige and Chatterjee (2015), but they add more depth to Mewara et al.'s (2016) definition by noting that wearable technologies can also be represented through more invasive items than glasses and wrist-watches, such as technologies that are either implanted into the body or are edible (Alrige & Chatterjee, 2015; Wright & Keith, 2014). Acknowledging the absence of controversy when defining wearable technology, this thesis will adopt Mewara et al.'s (2016) definition and similarly use the phrases 'wearable technology', 'wearable devices', and 'wearables' interchangeably.

2.1.3 Classification

But while the definition of wearable technology is not contested, there are different layers of complexity in their classification. There are very few wearable technology taxonomies, and therefore there is some difficulty in classifying wearables into different categories. Park et al. (2014) developed a wearable taxonomy to assist industry professionals in designing and developing new wearables. According to this taxonomy, there are six different classification dimensions of wearables: functionality, type, deployment mode, communication mode, disposability/reusability, and field of use (Park et al., 2014). Later taxonomies are less detailed: Alrige and Chatterjee (2015) propose a wearable technology taxonomy with three dimensions:

1. **Application:** which refers to the purpose of the wearable technology. They subdivide this dimension into monitoring, prevention, assistive, and communication.

2. **Form:** which refers to the physical form the wearable takes. They subdivide this dimension into accessory, garment, implantable, and portable.

3. **Functionality:** which refers to what function/s the wearable is able to perform. They subdivide this into single sensor and multi-sensor.

Similarly, Mewara et al. (2016) propose a two-fold classification standard for wearable technologies, which matches Alrige and Chatterjee's (2015) taxonomy but omits the wearable technology application dimension. Their form dimension is instead subdivided into head-mounted, body-dressed, hand-worn, and foot-worn devices (Mewara et al., 2016). Finally, Kirby et al. (2016, p. 1) propose four dimensions of wearable technologies (see Table 1).

Level	Boundary	Example
Embedded	Implanted within the body	Pacemaker
Intimate	Attached to the body in such a way that it could be deemed indistinguishable	Contact lens, prosthesis
Mounted	Attached to the body	Smart watch, head-mounted display

Carried	A device that is carried and used close to the body	Smart phone

Table 1: Wearable technology classification (adapted from Kirby et al., 2016, p. 1)

These different wearable technology taxonomies are useful to disaggregate the term 'wearable technology' into distinct categories. Information systems research has established that technology's emergence and usage is hugely context dependent (see Orlikowski & Iacono, 2001). Wearable technology is no exception, as different types of wearables have different usages: for example, wearables used in healthcare tend to require full skin contact to work effectively (Malmivaara, 2009). Meanwhile, wearables used for gaming purposes tend to be head-mounted devices that use augmented/virtual reality technology (Winchester, 2015). Having a solid understanding of wearable technology classification is therefore relevant for the context of wearable technology emergence and usage. For this study, this refers to public sector usage of wearables.

2.1.4 How do they collect data?

Because wearable technologies sit on or close to the human body, the data they gather is extremely personal. This data may be biometric, but also has the potential to be geographical or social (Kirby et al., 2016). Basic wearable technology functions include sensing, computing, and communication (Hiremath et al., 2014): using sensors, wearables gather information on the wearer such as their physical activity, their vital signs, and their location (Chatterjee et al., 2016). Some argue that smartphones are a type of wearable device because they are so often close to their owner's body, and have the capacity to collect personal information such as their location and movement (Godfrey et al., 2018; Kirby et al., 2016). However, wearable technologies differ from smartphones because they are able to gather more detailed data through continuous skin-placed sensors (Hiremath et al., 2014). While a smartphone can easily gather personal data such as the information the user inputs to the device, and their location, they do not have the capability to gather information from within the user's body. There are a range of advantages and disadvantages to the level of data collection enabled by wearable technology. Firstly, the pros of wearable technology data collection include the facilitation of remote healthcare monitoring and users having increased understandings of their bodies, which can be used to foster healthier lifestyle choices (Godfrey et al., 2018). However, these affordances are also accompanied by a range of security and privacy concerns.

2.1.5 Security and privacy issues in wearable technology

Wearable technology security concerns relate to the safety of the systems that data is stored in, whereas wearable technology privacy concerns relate to the safety of the gathered data itself. Hiremath et al. (2014) argues that each layer of wearable technology architecture – the body sensors, Internet-connected gateways, and the cloud storage – must all be protected if the data is to be kept safe from prying eyes. Because there are these multiple layers of vulnerability, there is the risk of unauthorised parties accessing wearable users' personal data by attacking various levels of the wearable technology architecture.

Goyal et al. (2016) and Cusack et al. (2017) investigated possible security vulnerabilities in wearable technologies, and found that while wearable manufacturers have invested considerable effort into data security, there are still a range of potential security breaches. Consistent with Hiremath et al.'s (2014) findings, they found that this can occur at different architectural layers and can give hackers the capacity to access personal data and potentially misuse it (Cusack et al., 2017; Goyal et al., 2016). Yaqoob et al. (2019) conducted a comprehensive study of the various attacks that wearable devices are vulnerable to, with a focus on healthcare devices. They found a wide range of susceptibilities, including a lack of encryption, weak authentication mechanisms, and the potential for reverse engineering (Yaqoob et al., 2019). Camara et al. (2015) note that security precautions must be developed with the constraints of wearable devices in mind, particularly their small size, computing power, and battery capacities. Designers and developers need to balance user privacy and security alongside the limitations of these devices (Camara et al., 2015).

Wearable technologies face a number of privacy issues alongside these security issues. Raij et al. (2011) discuss how the sensors embedded in wearables have the ability to gather information that their user may not be aware of, and therefore did not intend to share: this can have both positive and negative consequences. For example, they refer to wearables detecting medical conditions that the user may or may not know about, and while this can be beneficial, the user may have sensitivities as to who this information is shared with (Raij et al., 2011). Other privacy issues associated with wearable technology include video and audio recordings being made without user consent, unauthorised tracking of eye movement, location tracking, and third party data access – all of which can be done continuously and discretely by the wearable (Ching & Singh, 2016; Kapoor et al., 2020). Location tracking has had a strong research focus in the context of privacy. While it is possible to de-identify the data, having identified datasets is sometimes necessary for these datasets to be fit for purpose and the data subject can experience

financial, psychological, and/or physical threats as a result (Raij et al., 2011). In relation to location tracking, Xu et al. (2009) state that a one-size-fits-all approach is not suitable because different people have different privacy needs. As with any technology, there is the potential for wearable devices to be used in ways that their creators did not intend. Wang et al. (2016) found that wrist-worn wearables can be hacked to reveal their user's personal identification number (PIN), such as when a someone wearing a smartwatch types in their PIN to an automatic teller machine keypad or computer keyboard. Therefore, in addition to wearable technology being subject to serious data security and privacy threats, these threats are not the same across societal groups and devices can be used in unintended ways.

2.2 Privacy

This thesis will focus on the privacy element of wearable technology adoption: therefore, it is necessary to establish a solid understanding of what is meant by privacy. This is an area of academia which is subject to extensive and ongoing debate. More than 2,000 years ago, Aristotle distinguished between the polis and the oikos, or the public and the private realm of existence (DeCew, 2018). According to him, the polis was a place for government and official proceedings, whereas the oikos revolved around family life and as such, it was desirable to limit government authority on the oikos by separating the two spheres as much as possible (DeCew, 2018).

In modern times, conceptions of privacy have become more complex than simply separating public and private spheres. To date, there is no universally accepted definition of privacy (Solove, 2008). Traditionally, privacy has been considered as a person's right to be left alone (Langheinrich, 2001). Solove (2004) adds greater depth to this perception and categorises privacy into four main conceptions: as protection from Big Brother, as secrecy, as non-invasion, and as control over the use of information. Similarly, Tavani (2007) categorises established privacy theories into four distinct categories: non-intrusion, seclusion, limitation, and control. These categories respectively divide conceptions of privacy into a person being free from intrusion, being left alone, being able to restrict access to their personal information, and being able to control their personal information (Tavani, 2007). While Tavani (2007) argues that these categories alone are insufficient to create an all-encompassing theory of privacy, this categorisation demonstrates that privacy has multiple dimensions beyond a person being able to keep their information to themselves. These categorisations by Solove (2004) and Tavani (2007) demonstrate privacy's complexity, and that it certainly goes beyond Aristotle's separation of the public and private spheres. A canonical definition of privacy is provided by Westin (1967, p. 7): "…the claim of individuals, groups and institutions to determine

for themselves when, how, and to what extent information about them is communicated to others". In later years, he also argues that understandings of privacy must be informed by situational, political, socio-cultural, and personal factors (Westin, 2003).

In addition to there being no universally accepted definition of privacy, scholars are unable to agree on whether it is a right or an interest. The United Nations recognises privacy as a fundamental human right, with the United Nations Declaration of Human Rights (UNDHR) 1948 stating: "No one shall be subjected to arbitrary interference with his [sic] privacy, family, home or correspondence, nor to attacks upon his [sic] honor and reputation" (United Nations, n.d.). While the UNDHR still carries enormous weight in the present day, there have been debates over whether privacy is indeed a right or an interest. This debate is relevant to this thesis's research question because it sheds light on whether citizens are entitled to privacy, or if they simply desire it. Smith et al. (2011) describe the privacy paradox, whereby in spite of people stating they are concerned about their privacy, they nonetheless provide their personal information in exchange for benefits. This contributes to discussions over whether privacy is a right or an interest, and scholars of the latter argue that privacy is indeed an important individual and societal phenomenon, but it is also subject to cost-benefit analyses (Bennett, 1995). By sacrificing privacy through information disclosure, individuals can attain benefits such as financial rewards and service personalisation. Furthermore, the expansion of IoT technologies has facilitated an enormous shift in people's privacy perceptions versus their desired level of service personalisation (Kim et al., 2019). This cost-benefit analysis that people perform is explained by the privacy calculus theory. Laufer and Wolfe (1977) created this theory, and it refers to individuals weighing up the benefits of what they will obtain from sacrificing their privacy with the possible negative effects of this disclosure. Therefore, the debate around whether privacy is a right or an interest is ongoing and subjective, for while people desire privacy, some are also willing to give it up in order to get something in return.

The proliferation of information technology (IT) plays a huge role in the growing complexity of privacy. Contemporary conversations about privacy tend to circle around information privacy as opposed to physical privacy (Smith et al., 2011). Information privacy can be defined as people wanting to control or have influence over their personal data (Bélanger & Crossler, 2011). Westin's (2003) evolution of information privacy demonstrates how as IT has evolved, so have conceptions of privacy (see Table 2).

Period	Characteristics
Privacy Baseline 1945-1960	Limited information technology developments, high public trust in government and business sector, and general comfort with the information collection.
First Era of Contemporary Privacy Development 1961-1979	Rise of information privacy as an explicit social, political, and legal issue. Early recognition of potential dark sides of the new technologies (Brenton, 1964, as cited in Westin, 2003), formulation of the Fair Information Practices (FIP) Framework and establishing government regulatory mechanisms established such as the Privacy Act of 1974.
Second Era of Privacy Development 1980-1989	Rise of computer and network systems, database capabilities, federal legislation designed to channel the new technologies into FIP, including the Privacy Protection Act of 1984. European nations move to national database protection laws for both the private and public sectors.
Third Era of Privacy Development 1990-present	Rise of the Internet, Web 2.0 and the terrorist attack of 9/11/2001 dramatically changed the landscape of information exchange. Reported privacy concerns rose to new highs.

Table 2: Westin's (2003) evolution of information privacy (adapted in entirety from Smith et al., 2011, p. 991)

This table demonstrates that information privacy conceptions are heavily influenced by IT. In this sense, information privacy conceptions can be thought of as socio-technical systems whereby IT and information privacy mutually shape and react to each other.

The usefulness of IT is context dependent, particularly in relation to privacy: in a healthcare context, IT enables more effective care and treatment and is held in high regard by many, whereas video surveillance in public spaces to enhance public safety is often met with suspicion and outcry of privacy violation (Nissenbaum, 2009). For example, Westin (2003, p. 451) writes that "…how well democracies balance the competing demands of privacy, disclosure, and surveillance will exert a major influence on the quality of civic life in the 21st century". Therefore, privacy and technology share a mutually shaping relationship.

2.3 The COVID-19 pandemic

A public health crisis can be defined as a situation whose "…scaling, timing, or unpredictability threatens to overwhelm routine capabilities" (Nelson et al., 2007, p. S9). These types of crises can include anything from a terrorist attack to a pandemic (Nelson et al., 2007), and this thesis will use the COVID-19 pandemic as an empirical focus. COVID-19 – which originated in Wuhan, China as a cluster of unknown respiratory infections in December 2019 – is an infectious, airborne virus that is caused by a new strain of the coronavirus (World Health Organisation, 2021a). While initially countries throughout the world did very little in response to the virus, COVID-19 rapidly spread

internationally, and infection rates and morbidity soared globally (World Health Organisation, 2021a). Ultimately, the WHO declared COVID-19 a pandemic on 11 March 2020 (World Health Organisation, 2021a). Upon this declaration, most countries throughout the world closed their borders, suspended domestic and international travel, and imposed strict lockdowns and quarantines to slow COVID-19's spread. There is an important distinction between lockdowns and quarantine during COVID-19. Lockdowns refer to community-wide restrictions where activities such as freedom of movement and social interaction are strictly limited, whereas quarantine refers to this same restriction, but for specific people who may have or be at risk of contracting COVID-19 (Heffernan, 2021).

Many governments began using surveillance technologies to aid them in controlling the virus, and these technologies were harnessed to assist with contact tracing, and to enforce quarantine obligations and social distancing (Kitchin, 2020). Rothstein (2020) explains that while contact tracing procedures are not new – having been used in prior disease outbreaks and more commonly for sexually transmitted infections/diseases – they have never been used on such an enormous societal scale. Contact tracing government workers have traditionally used interviews to meet with infected people and trace back their movements in order to identify and isolate their past contacts, but the scale of the COVID-19 pandemic has grown such that contact tracing is beyond the capacity of humans to perform (Bhattacharya & Ramos, 2021). This has led to the proliferation of digital contact tracing applications (hereafter referred to as apps) on citizens' smartphones, developed and rolled out by governments. These apps use smartphone data to track people's interactions, and identify if and when an individual may have come into contact with an infected person (Kapa et al., 2020).

Since March 2020, there has been a growing quantity of literature reflecting on the relationship between the state, citizen privacy, and public health. Scholars have commented that standard approaches to citizen privacy are no longer appropriate in public health crises, including in the COVID-19 pandemic (Martinez-Martin et al., 2020; The Lancet Respiratory Medicine, 2016). Research into digital contact tracing technologies – such as COVID-19 apps – is applicable in this context. In particular, there is significant discourse surrounding whether or not citizen location and/or movement data can be used to replace lockdowns and quarantines (see Kapa et al., 2020; Simko et al., 2020; Sun et al., 2020). On this, Colizza et al. (2021) argue that the purpose of digital contact tracing apps should not be limited to quarantining individuals infected with COVID-19, but to minimise how much time non-infected people must experience lockdowns and quarantine. However, alongside this conversation have been musings over how to effectively balance achieving public health goals with individuals' personal privacy (see

Kapa et al., 2020; Martinez-Martin et al., 2020; Simko et al., 2020; Weizman et al., 2020). The lockdowns and quarantines imposed by the COVID-19 pandemic have restricted people's freedom and movement in unprecedented ways: Rowe (2020, p. 2) argues that: "while privacy is a fundamental human right, freedom to move and safety are also fundamental". He states that this comparison forces people to consider which they value more: their freedom or their privacy (Rowe, 2020).

2.4 Digital contact tracing applications

Digital contact-tracing apps have been implemented in more than 30 countries throughout the world (Weizman et al., 2020). While these apps have stronger contact tracing capabilities than traditional human contact tracers (Bhattacharya & Ramos, 2021), they must be downloaded and actively used by a significant proportion of a country's population in order to be effective (Martinez-Martin et al., 2020). To date, these apps have had remarkably low download rates throughout the world: even though governments have been urging their citizens to download and use the apps, the vast majority of countries have had a penetration rate of less than 5% of their population (Elkhodr et al., 2021). Bhattacharya and Ramos (2021, p. 2016) state: "Individuals may be skeptical to use technology that allows for interactions or locations to be recorded due to a fear of government surveillance or data abuse". The enormity and severity of the COVID-19 pandemic has clearly been insufficient to urge citizens to sacrifice their privacy in the name of public health. These apps function using a range of different technologies, including Bluetooth, global positioning systems (GPS), and Google/Android operating systems (Elkhodr et al., 2021).

Their architecture can be centralised, decentralised, or a hybrid format: in centralised digital contact tracing apps, the data collected from individual smartphones is sent straight to a central authority and all users are identifiable and therefore able to be directly sought out by government authorities (Vaudenay, 2020). In decentralised digital contact tracing apps, the data collected from individual smartphones is fully de-identified before being sent to a central authority, and the data is only labelled in relation to whether an individual is at risk of COVID-19 or not (Vaudenay, 2020). Kapa et al. (2020) refer to centralised and decentralised contact tracing architectures respectively as non-privacy-enabled and privacy-enabled architectures (see Figure 2). Furthermore, they include other technologies such as financial transactions and wearable technologies in their architectures. Similarly, Fahey and Hino (2020) use the terms privacy-first and data-first approaches to describe government approaches to COVID-19 data collection from digital contact tracing technologies: privacy-first approaches correspond with Kapa et al.'s (2020) definition of privacy-enabled apps, where citizen data is protected (for example,

through encryption) and public authorities have limited data access; data-first approaches correspond with Kapa et al.'s (2020) definition of non-privacy-enabled apps, where large quantities of identifiable citizen data are gathered and stored, and public authorities have full access to individuals' current and past contact information.

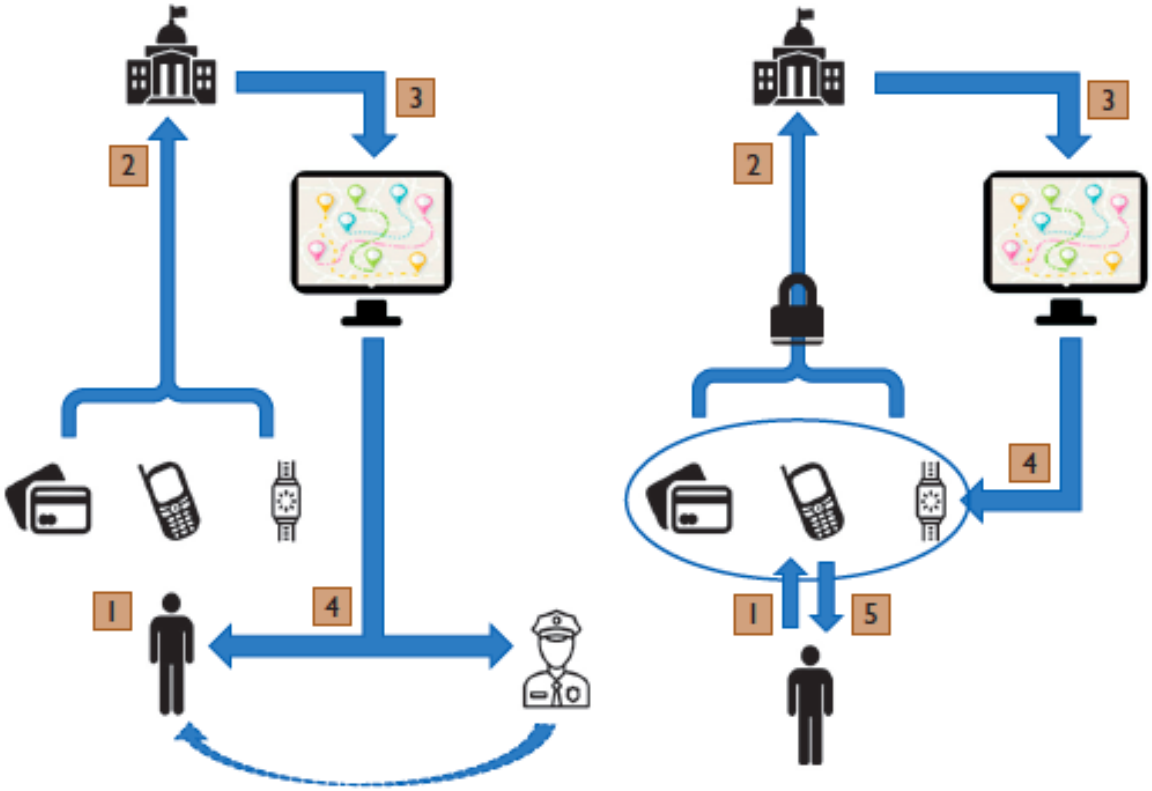

Figure 2: Centralised/non-privacy enabled architectures (left) vs decentralised/privacy-enabled architectures (right) (adapted from Kapa et al., 2020, p. 1321)

Once downloaded, these digital contact tracing apps track an individual's geographic location or their movements – depending on the privacy safeguards afforded by the government – and give users the ability to alert the app if they are infected with COVID-19 or if they are a close contact of someone who is (Rodriguez et al., 2020). Depending on whether the app is centralised or decentralised, the technology will identify which individuals have been in contact with an infected or at-risk individual and send them an alert to self-isolate and/or take a COVID-19 test (Elkhodr et al., 2021; Vaudenay, 2020). As previously discussed, this approach requires a high level of citizen uptake to be effective at reducing the spread of COVID-19 amongst the general public, and the majority of countries around the world have been unable to achieve the necessary levels of penetration (Elkhodr et al., 2021; Martinez-Martin et al., 2020). Some countries have moved beyond smartphone apps to mitigate the effects of the COVID-19 pandemic and

have either implemented or are considering using wearable technologies to slow community transmissions.

2.4.1 Governmental use of wearable technology in COVID-19

There are a small number of governments using wearable technologies in the COVID-19 pandemic. The dialogue on public health versus privacy is just as applicable in wearable technologies as with digital contact tracing apps: however, because wearable technologies sit directly on the body for a prolonged period of time, there are greater concerns over what kind of data they may collect (Rodriguez et al., 2020). Governments are using wearable technologies for a range of COVID-19 mitigation measures, including social distancing, quarantine enforcement, and vital signs monitoring (Ding et al., 2021; Rodriguez et al., 2020). This thesis will concentrate on the role of wearable technologies in quarantine enforcement, and as such the other uses are out of scope. Nasajpour et al. (2020, p. 364) state that "IoT wearable bands have shown promising results to prevent patients from leaving quarantine areas". Whitelaw et al. (2020) describe the advantages and disadvantages of using wearable technology to enforce quarantine: on one hand, it can isolate individuals infected with COVID-19 and prevent them from moving around in the community; but on the other hand, it constitutes a severe violation of civil liberties and privacy, and may prevent some individuals from leaving their home for essential supplies. Privacy and security concerns are widespread in discussions of wearable technology adoption in the COVID-19 pandemic, as they can collect a huge quantity of personal data (Psychoula et al., 2020). Furthermore, the poor uptake rates of digital contact tracing apps and the associated privacy concerns do not indicate that there would be strong public or government support for wearable tracking technologies.

Some governments – such as Singapore, Hong Kong, the United Arab Emirates (U.A.E.), and Australia[2] - are currently using wearable technology to enforce quarantine obligations. The U.S.A. states of Kentucky, West Virginia, and Hawaii seriously considered rolling out these devices, but ultimately chose not to pursue the option due to privacy concerns (Rodriguez et al., 2020). The wearers' whereabouts are constantly monitored by authorities and in most of these countries, the wearable technology is paired with a smartphone app (Nasajpour et al., 2020). In Singapore, the government refers to its use of wearable technology as electronic monitoring devices and issues these devices to all people who are completing COVID-19 quarantine outside a government-run quarantine facility (Immigration and Checkpoints Authority Singapore, 2021). Government authorities assure citizens that the devices do not have any audio or video

[2] Only the state of Western Australia has pursued this, and it is reserved strictly for individuals who have a criminal record and/or have breached their hotel quarantine obligation (Perpitch, 2020).

recording capabilities and that their sole purpose is to ensure that wearers do not leave their home during the designated quarantine period; additionally, that authorities will be notified if the wearer tampers with their device or leaves their home (Immigration and Checkpoints Authority Singapore, 2021). To date, it has been an effective system: of the approximately 308,000 devices issued to Singaporeans, just over 300 breaches have been recorded (Judd, 2021; Min, 2021). This reinforces Rodriguez et al.'s (2020) point that wearable technologies are highly effective at stemming the flow of COVID-19, but at the cost of privacy.

The government of Hong Kong uses tracking bracelets paired with a smartphone app to enforce COVID-19 quarantine: individuals put on the wristband, set a perimeter of their home by walking around, and authorities will be alerted if they go outside this perimeter (The Government of the Hong Kong Special Administrative Region, 2021). In the U.A.E., quarantining individuals must use a government-issued smartwatch paired with a smartphone app – which requires access to their camera, media, location, audio, and calls – which tracks their geographic location (U.A.E. Government, n.d.). In Australia, there is considerable public support for innovative technologies such as wearable devices to enforce quarantine: a Guardian survey found that more than half of respondents supported compulsory tracking bracelets to enforce quarantine compliance (Murphy, 2020). The Australian Prime Minister has also indicated that he is open to innovative solutions, such as wearable tracking devices, to manage the COVID-19 pandemic (Karp, 2020). A wearable technology trial is currently underway in the Howard Springs quarantine facility in the Northern Territory, which monitors people's vital signs such as heart rate, oxygen level, and temperature (McDonald, 2020).

However, it is important to note that wearable technologies are strongly associated with criminality, and are also criticised for being uncomfortable and expensive (Schwartz, 2020). The Premier of Western Australia, Mark McGowan, has emphasised that wearable tracking devices are for extreme cases only, and is not yet considering wider government adoption (Perpitch, 2020). Therefore, while a limited number of countries have implemented wearable technologies into their COVID-19 quarantine management approach, there remain significant hesitations and privacy concerns to navigate.

2.4.2 Past government use of wearable technologies

Prior to the COVID-19 pandemic, there is little evidence to suggest that governments used wearable technology outside the criminal justice sector. It is outside the scope of this thesis to deliberate on how governments have used electronic monitoring in a criminality setting. While government electronic monitoring may be seen as an invasion of privacy, it is no greater an invasion than imprisonment (Bülow, 2014). In the context of COVID-

19 quarantine, it is necessary to consider the role of wearable technology with this point in mind. On one hand, while wearable tracking devices do invade people's privacy, it is no more an invasion than the government mandating people to complete the quarantine in the first place. It is also prudent to mention that studies on the acceptance of electronic monitoring indicate that culture and context are important acceptance indicators. Payne et al. (2009) found that people of colour are more likely to agree that electronic monitoring perpetuates inequalities and turns homes into prisons. Meanwhile, another study that compared U.S.A. students and Bosnian students' perceptions of electronic monitoring found that national affiliations influenced the respondents' views (Muftić et al., 2015). Therefore to date, governmental use of wearable technology has been limited and predominantly linked to home detention settings.

3 Literature Review

This section is a thematically structured literature review that assesses the research landscape for wearable technology adoption. Now that wearable technologies have been defined, and the delicate balance between privacy and public health has been established, the purpose of this literature review is to establish a thorough understanding on research conducted to-date on wearable technologies and how they have typically been adopted and accepted by their users. It is important to begin this section by noting that all wearable technology adoption studies to date have focused on acceptance and adoption from a consumer perspective. This means that voluntariness of use is a key assumption in the adoption factors outlined below. Furthermore, as established in the research background, governmental use of wearable technology has been centred in a criminal justice setting. There are very few studies on acceptance of this use, and adoption has never been researched. Therefore, before assessing the literature, it is already evident that wearable technology adoption factors in a public sector context are missing from existing research. As governments are beginning to use wearable technologies at a greater rate in the pandemic, it is important for research to develop an evidence base for adoption antecedents from a citizen perspective, beyond a consumer perspective. The outlined factors in this literature review are the predominant adoption antecedents from a consumer perspective that may be relevant when answering this study's research questions. The final section of this literature review is devoted to privacy, with a focus on what privacy elements shape people's attitudes to adopting wearable technology.

3.1 Technology acceptance theories

The majority of wearable technology adoption research[3] has been conducted using the technology acceptance model (TAM) (Davis, 1989), the unified theory of acceptance and use of technology (UTAUT) (Venkatesh et al., 2003), and the extended UTAUT model (UTAUT2) (Venkatesh et al., 2012) as theoretical frameworks. These theoretical frameworks have shaped the direction of this body of research by providing a set of consistent research factors, and have often been combined with each other or with other theories that are not necessarily focused on technology acceptance or adoption. This has created a highly fragmented field of research. Despite these technology acceptance models being widely used in technology adoption and acceptance studies, there are still limited conclusions as to why individuals adopt wearable technologies, and the factors and characteristics that influence this adoption (Chau et al., 2019; Jeong et al., 2017; Zhang et al., 2017). Kalantari (2017) notes that the consistent use of similar theories is a

[3] It is important to consider that acceptance and adoption are frequently used as interchangeable terms in this research area.

limitation of wearable technology adoption studies, as findings are constrained to a handful of variables and moderators. This following section will briefly discuss the main technology acceptance theories employed in the wearable technology adoption literature.

3.1.1 Technology acceptance model

Davis (1989) created TAM based on the expectancy value theory and the theory of reasoned action. While these two theories aim to explain individual behaviour in general, TAM is specific to individual behaviour in relation to technology. There are two variables in TAM: perceived usefulness and perceived ease of use (Davis, 1989). Perceived usefulness refers to how much an individual believes that using the technology will be useful to them, and perceived ease of use refers to how much an individual perceives the technology to be easy to use (Davis, 1989). However, because TAM was developed to be used for voluntary usages of technology (Davis, 1989), it cannot be used in situations where use is non-voluntary.

3.1.2 Unified theory of acceptance and use of technology

UTAUT was created by Venkatesh et al. (2003) by combining eight different models. There are four variables in UTAUT: performance expectancy (equivalent to TAM's perceived usefulness), effort expectancy (equivalent to TAM's perceived ease of use), social influence, and facilitating conditions (Venkatesh et al., 2003). These variables are moderated by age, gender, experience, and voluntariness of use and the framework is typically used to understand organisational uses of technology (Venkatesh et al., 2003).

3.1.3 Unified theory of acceptance and use of technology 2

In 2012, researchers altered UTAUT to create an extended version called UTAUT2. This variation focuses on the consumer use instead of organisational use, and adds hedonic motivation, cost, and habit as explanatory factors to the model (Venkatesh et al., 2012). Additionally, it removes the moderator addressing voluntariness of use (Venkatesh et al., 2012).

3.2 Adoption factors

Bagozzi (2007, p. 245) notes that the "study of technology adoption/acceptance/rejection is reaching a stage of chaos, and knowledge is becoming increasingly fragmented with little coherent integration". This aptly reflects the state of wearable technology adoption literature. The field is messy and inconsistent, with each study investigating wearable technology adoption in different contexts, countries, and user focus groups. There is only

one comprehensive literature review that clearly identifies adoption antecedents of wearable technologies (see Kalantari, 2017). Consequently, this study's literature review structure will be selectively based on Kalantari's (2017, p. 299) summary of wearable technology adoption factors (see Figure 3). She categorises the adoption factors into five categories: perceived benefits, individual characteristics, perceived risks, technology characteristics, and social factors (Kalantari, 2017, p. 299). A table summary of wearable technology adoption studies included in this literature review can be found in Table 5.

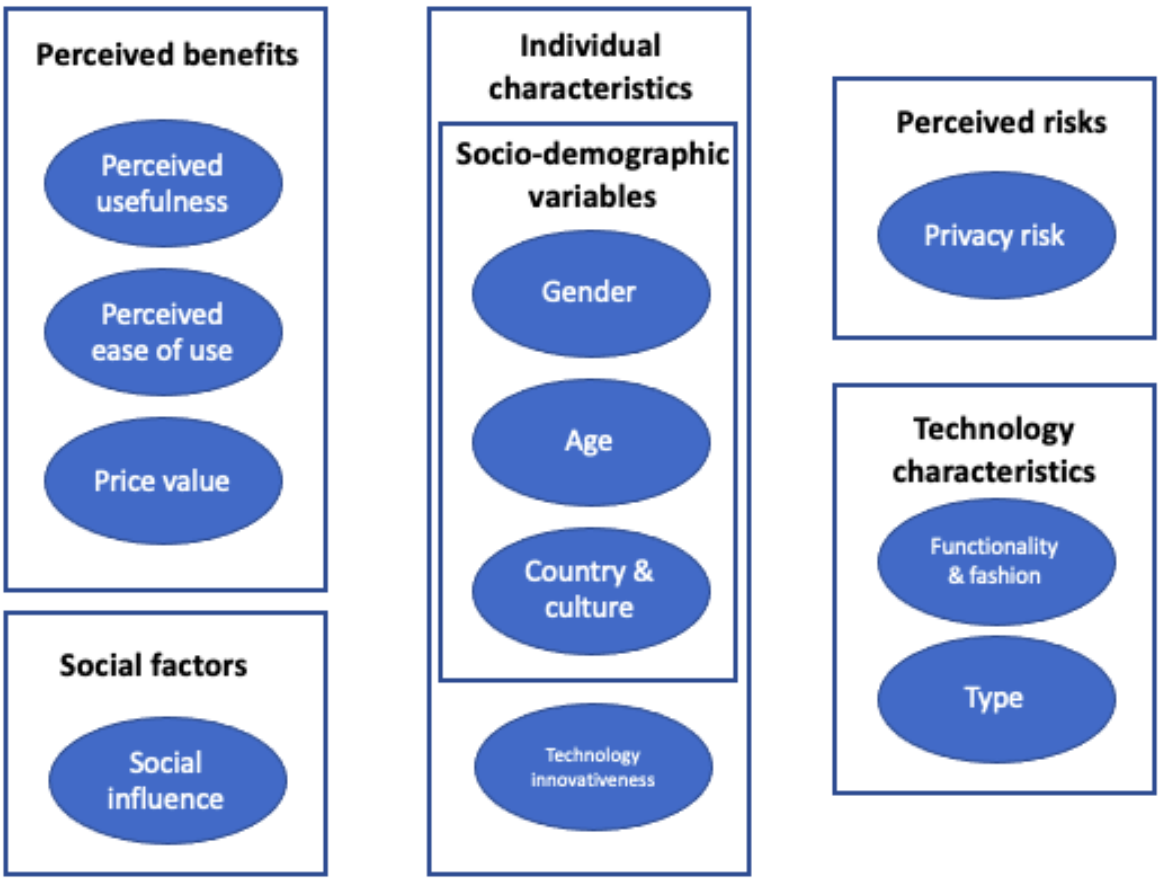

Figure 3: Summary of wearable technology adoption factors (adapted from Kalantari, 2017, p. 299)

3.2.1 Perceived benefits

Here, Kalantari (2017) lists perceived usefulness, perceived ease of use, and price value as key wearable technology adoption factors. Each of these factors may be extrapolated to a public sector context.

3.2.1.1 Perceived usefulness

Perceived usefulness has been identified as a huge adoption antecedent by a range of researchers. Adapa et al. (2018), Gao et al. (2015), and Talukder et al. (2019) each find that performance expectancy significantly affects wearable technology adoption. In relation to perceived usefulness, Kim and Shin (2015) find that affective quality (to what degree a wearable technology can change a user's lifestyle) and relative advantage (when a wearable technology gives the user an advantage compared to other available ideas or products) have a positive association. This means that if a wearable technology user believes that using these technologies will positively change their lifestyle and give them an advantage over non-users, they are likely to adopt the technology. This is reinforced by Rauschnabel and Ro (2016), who find that smart glasses are more likely to be adopted by those who believe the technology will improve their lives in some way. Chuah et al. (2016) also find that perceived usefulness plays an important role in wearable technology adoption: they distinguish between smart watch users who view the technology as a technological item versus a fashion item. Smart watch users who perceive wearable technology as a technological item will adopt items they believe are useful, while users who perceive it as a fashion item will adopt items that look attractive (Chuah et al., 2016). Dehghani et al. (2018) argue that user attitudes towards technology influence perceived usefulness, thus inferring that users who view technology positively are more likely to adopt wearable technologies. This is supported by Chuah et al. (2016) who find that – in relation to perceived ease of use – attitudes towards technology influence adoption. Meanwhile, Wang et al. (2020) find that wearable technologies that provide useful information and services to users are more likely to be adopted. Therefore, throughout wearable technology adoption studies, perceived usefulness has been identified as an important adoption factor. In a government context, perceived benefit links to what citizens may stand to gain from giving up their privacy and using wearable technology in quarantine circumstances.

3.2.1.2 Perceived ease of use

In relation to perceived ease of use, Kim and Shin (2015) find that mobility (to what degree a wearable technology can be used on-the-go) and availability (to what degree a wearable technology is connected in real-time with information and services) have a positive association. This finding indicates that if users perceive that a wearable technology can be used in transit and they can access information and services at any time, they are likely to adopt the technology. Similarly, both Dehghani et al. (2018) and Wang et al. (2020) find that wearable technologies that give users happiness contribute greatly to adoption. Rauschnabel and Ro (2016) only find a partially significant

relationship between perceived ease of use and smart glasses adoption. Nevertheless, literature is largely consistent in finding that perceived ease of use is a meaningful antecedent in wearable technology adoption.

Additionally, while they do not use TAM, Karahanoğlu and Erbuğ (2011) find that a wearable technology's usefulness and ease of use have a positive relationship with pragmatic qualities such as product functionality. They argue that this quality is important in wearable technology adoption (Karahanoğlu & Erbuğ, 2011). Meanwhile, Miltgen et al. (2013) find that while both perceived usefulness and perceived ease of use are significant adoption antecedents for wearable technologies, the greatest drivers of adoption are related to trust and privacy. In a government context, perceived ease of use may refer to how easy it is for citizens to use the wearable technology.

3.2.1.3 Price value

Research investigating whether price is an important adoption factor is mixed. Park et al. (2016), Sergueeva et al. (2020), and Talukder et al. (2019) each state that price is not an important adoption factor. However, Dehghani et al. (2018) and Kim and Shin (2015) claim that price is an important antecedent to wearable technology adoption, with low to medium priced products being more consumer-friendly than products with high prices. Wen et al. (2017) argue that wearable technologies with high prices are unlikely to be adopted. This may be an important factor when investigating governmental use of wearable technologies, depending on whether governments would oblige their citizens to pay for the devices themselves or whether the devices would be subsidised.

3.2.2 Individual characteristics

In this section, Kalantari (2017) lists social demographics (namely age and gender) and technology innovativeness as key wearable technology adoption factors. The author will address social demographics, adding 'country and culture' as an important element. Additionally, technology innovativeness will be included, but the remainder of Kalantari's (2017) factors are not relevant to the research questions.

3.2.2.1 Social demographics

As the research questions consider whether citizens would adopt governmental wearable technologies in public health crises, it is imperative that this literature review considers social aspects of adoption. Numerous wearable technology adoption studies self-identify as having significant limitations in relation to social aspects of adoption. They note that they did not include variables such as age (Adapa et al., 2018; Sergueeva et al., 2020;

Talukder et al., 2019), gender (Adapa et al., 2018; Kim & Shin, 2015; Talukder et al., 2019), life experience (Adapa et al., 2018; Talukder et al., 2019), and race, ethnicity, and culture (Chau et al., 2019; Gao et al., 2015; Kim & Shin, 2015; Paluch & Tuzovic, 2019; Schomakers et al., 2019): therefore their findings may not be generalisable to broader populations. Furthermore, some studies focused on current users of wearable technologies, and their findings may not be representative of non-users (Kim & Shin, 2015; Paluch & Tuzovic, 2019; Sergueeva et al., 2020). This is problematic because research findings to-date may simply relate to niche segments of society and not be representative of broader societal groups. On this, Adapa et al. (2018, p. 407) state that "Our findings indicate that the factors that influence the adoption of WT can vary across different devices and different user groups". In light of these shortcomings, it is important that this thesis's research design acknowledges these social demographic limitations to the best possible extent. While this study does not aim to compare age and gender differences, country differences will be an important focus and will be discussed in greater detail in the methodology.

3.2.2.1.1Age

Age is important to consider because in general, older people are less likely to adopt technologies than younger people (Röcker et al., 2014; Spagnolli et al., 2014). Karahanoğlu and Erbuğ (2011) state that they focused exclusively on young people in their study because they are more interested in using novel technologies than older people. However, they also acknowledge that consequently their results cannot be extrapolated beyond their young sample (Karahanoğlu & Erbuğ, 2011). Gregor and Gwiaździński (2020) also surveyed young people – aged between 19-30 years of age – and even within their limited age bracket, they found age differences in knowledge of wearable technologies. Guillén-Gámez and Mayorga-Fernández (2019, p. 9) argue that "…age can significantly affect the acceptance and use of technological devices related to health and medical care". They demonstrate this through their findings that women aged under 30 years of age own more wearable devices than men in that same age bracket, and women aged over 45 years of age have the lowest acceptance wearable technology acceptance levels than any other age bracket (Guillén-Gámez & Mayorga-Fernández, 2019). Therefore, adoption attitudes may differ depending on age and this may be an important factor for governments to consider when rolling out wearable technology in public health crises.

3.2.2.1.2Gender

Numerous researchers have identified gender differences in wearable technology research. Duval and Hashizume (2005) find that gender (and culture) has a significant

impact on how people perceive wearable technologies. For example, women from both Japan and France perceive wearable technology that is fully controlled by artificial intelligence very negatively in comparison to men from both countries (Duval & Hashizume, 2005). However, while French men still perceive this control in a negative light, Japanese men are neutral towards it (Duval & Hashizume, 2005). Zhang et al. (2017) find that females who believe the device will provide health benefits associate higher levels of usefulness. Dehghani et al. (2018) also find that gender impacts wearable technology usage, with men more likely to use these devices because they tend to have a 'masculine' design. Guillén-Gámez and Mayorga-Fernández (2019) use gender as a variable when analysing wearable technology acceptance, and find that while women's acceptance is growing, men have a higher acceptance level. Gregor and Gwiaździński (2020) found that there are gender differences relating to whether wearable technologies securely store personal data, make daily life easier, and nurture one's health. Therefore, research indicates that wearable technology acceptance and adoption is higher amongst men. This is significant in relation to the research question because governments will target wearable technologies to all genders present in society.

3.2.2.1.3 Country and culture

Only two cross-cultural studies have been conducted to-date on wearable technology adoption: Duval and Hashizume (2005) and Yang Meier et al. (2020). This is in spite of many researchers commenting on the need for future research to include diverse, international samples (see Chau et al., 2019; Gao et al., 2015; Kim & Shin, 2015; Paluch & Tuzovic, 2019). Duval and Hashizume (2005) conduct a cross-country comparative analysis – in France and Japan – to investigate perceptions of wearable technologies in society. They find that gender and culture have a significant role in predicting wearable technology acceptance, with some key differences between participants from France and Japan (Duval & Hashizume, 2005). For example, Japanese participants are more comfortable with artificial intelligence in wearable technologies than French people.

Meanwhile, Yang Meier et al. (2020) conduct a cross-cultural survey – in China and Switzerland – to understand the antecedents and barriers to adoption of wearable health technologies. This is the most recent study to investigate this phenomenon from a cross-cultural perspective, with Duval and Hashizume (2005) having conducted a pioneering study more than a decade earlier. As many studies have acknowledged the lack of cross-cultural research in wearable technology adoption, Yang Meier et al.'s (2020) study is an important step forward in filling a significant research gap. They find that there is a difference between adoption intentions of wearable health technologies among Chinese and Swiss consumers: Chinese survey respondents were impacted by health

consciousness, whereas Swiss consumers were mostly affected by effort expectancy (Yang Meier et al., 2020). Therefore, wearable technology adoption attitudes can differ between cultures. This is significant in a government setting because adoption antecedents may therefore differ depending on the country and culture in question.

3.2.2.2 Technology innovation

A small number of studies have investigated whether innovativeness influences wearable technology adoption. Park et al. (2016), Rauschnabel and Ro (2016), and Jeong et al. (2017) each find that people with innovative tendencies are more motivated to adopt wearable technologies. Gregor and Gwiaździński (2020) suggest that wearable technologies are still a niche market, and therefore tend to attract people who are technology-savvy and prepared to take a risk. This is a valuable consideration for the research question because governmental use of wearable technology in public health crises is unlikely to be limited to citizens with innovative tendencies: instead, they would be rolled out on a whole-of-population basis to be used by people whenever needed. This adoption factor is also relevant to the research question related to data-first or privacy-first architectural structures, as citizens may not have the appropriate technology understandings to understand the privacy risks associated with the two structures.

3.2.3 Technology characteristics

A brief summary of research findings on functionality and fashion are included below, with an addition of types of wearable technology

3.2.3.1 Functionality and fashion

While not directly relevant to the research question, this section has been included because wearable technology aesthetics are one of the strongest adoption factors in a consumer setting (Kalantari, 2017). Researchers recommend that wearable technologies be small, lightweight and neutrally coloured (Koo & Fallon, 2018), comfortable (Duval & Hashizume, 2005), and light and discrete (Spagnolli et al., 2014). Thierer (2014) states that wearable technology adoption has been somewhat stunted because the products tend to be awkward to wear and aesthetically unappealing, and Coorevits and Coenen (2016) argue that common reasons for wearable technology attrition are due to the devices being uncomfortable and not fitting properly. Rauschnabel and Ro (2016) and Chuah et al. (2016) emphasise that some users see wearable technologies as fashion accessories: based on this, if users do not consider the devices to be fashionable, they are unlikely to adopt them. Adapa et al. (2018) find that the look and feel of smart glasses and smart watches is an important adoption factor, which links with Chuah et al.'s (2016) and Rauschnabel

and Ro's (2016) findings that people who view wearable technologies as fashion items hold aesthetics in high stead. Furthermore, Kim and Park (2019) claim that wearable technology adoption will increase if the devices are unique and attractive. These research focuses are heavily emphasised in the wearable technology adoption literature, but are not key factors for governments to consider because their interaction with wearable technology would not be to develop fashionable items. However, the significance of this strong focus further demonstrates that current wearable technology adoption literature is not totally applicable in a public sector setting and further research is required to establish what adoption factors are relevant beyond a consumer perspective.

3.2.3.2 Types of wearable technology

Some research differentiates between types of wearable technologies, while some research considers all technologies under a blanket term. This is important to include in this literature review because researchers found differences in adoption antecedents and barriers between different devices. Gao et al. (2015) compares two types of technologies: fitness wearables (used to track and monitor user fitness) and medical wearables (used to manage diseases and other medical conditions). They found that "…fitness devices users care more about hedonic motivation, functional congruence, social influence, perceived privacy risk, and perceived vulnerability, but medical device users pay more attention to perceived expectancy, self-efficacy, effort expectancy, and perceived severity" (Gao et al., 2015, p. 1705). Similarly, Schomakers et al. (2019) find that there are different acceptance factors between medical applications and fitness apps, with the former being influenced by privacy and facilitating conditions, and the latter being influenced by performance expectancy and social influence. Adapa et al. (2018) distinguish between smart glasses and smart watches, where smart glasses users care more about the product's look and feel, and smart watch users are invested in highly functional fitness apps and waterproof features. Finally, Gregor and Gwiaździński (2020) find adoption differences between smart phones and smart watches, namely that adoption is significantly lower for smart watches than for smart phones: this is because smart phones have achieved extremely high penetration rates, particularly amongst young people, whereas wearables continue to be a niche product. Governments may wish to investigate what type of wearable they wish to use in a public health setting, noting these difference adoption factors.

3.2.4 Social influence

There is significant support for social influence being a key wearable technology adoption factor. An older study by Feiner (1999) argues that what people choose to share will be

influenced by social protocols: "…no matter how accurate these technologies may become, social conventions may influence the accuracy with which we can track others, and, at times, even ourselves" (Feiner, 1999, p. 2). This statement is also reflected in more recent literature. Kim and Shin (2015) found that sub-cultural appeal is important for adoption. Gao et al. (2015) and Talukder et al. (2019) argue that social influence has a strong effect on wearable technology adoption, because users tend to draw on information and advice from their social networks when deciding to adopt or not adopt a wearable technology. Additionally, when investigating the role of innovativeness amongst early adopters of wearable technology, Jeong et al. (2016) found that users were more likely to use the devices if they believed it would improve their social prestige. Similarly, Canhoto and Arp (2017) found that peer pressure was a key adoption antecedent. Coorevits and Coenen (2016) found mixed results for the role of social influence: on one hand, being able to use the device to publicise one's health may be attractive to one person, but on the other hand, this kind of behaviour may discourage some people from engaging in such behaviour. This reinforces Gao et al.'s (2015) and Schomakers et al.'s (2019) observation that context influences technology acceptance and adoption. The public health crisis context for governmental use of wearable technology is therefore likely to have a strong impact on citizen adoption.

3.2.5 Perceived risks

Kalantari (2017, p. 299) provides six sub-categories of perceived risk factors when summarising wearable technology adoption factors. To maintain relevancy with the research focus on privacy, this literature review will be limited to assessing literature on privacy risk.

3.2.5.1 Privacy risk

A number of studies have investigated the relationship between privacy and wearable technology adoption, particularly in health contexts. The overwhelming majority of these studies find that privacy is a significant consideration in wearable technology adoption. While privacy and security risks have long been acknowledged in wearable technology usage, research focuses on privacy in the context of adoption are much newer. Li et al. (2016) argue that the majority of previous research has investigated wearable technology adoption in the context of technology and health, without dedicating much effort to understanding privacy dimensions. There is much truth in this statement, as there is limited research that investigates privacy in the context of wearable technology adoption before 2016 (see Gao et al., 2015; Miltgen et al., 2013; Motti & Caine, 2015; Nasir & Yurder, 2015; Spagnolli et al., 2014).

The resounding theme in wearable technology adoption research is that privacy is a crucial adoption factor. When investigating biometric identification techniques, Miltgen et al. (2013) find that privacy and trust are greater predictors of acceptance and adoption than traditional adoption models such as TAM or UTAUT. This finding resonates deeply with this thesis's research questions: a number of Kalantari's (2017) wearable technology adoption factors are irrelevant in a government context, and greater emphasis ought to be placed on privacy literature. She states that privacy concerns and aesthetics are the greatest themes that have emerged from adoption research (Kalantari, 2017). While the latter is not crucial in the context of this thesis's research objective, the spotlight on privacy is significant. Many researchers have found that perceived privacy risk negatively affects users' trust in wearable technology, which in turn leads to lower adoption levels (see Gao et al., 2015; Nasir & Yurder, 2015; Rauschnabel & Ro, 2016; Segura Anaya et al., 2018; Spagnolli et al., 2014). Additionally, Adapa et al. (2018) find that privacy is a significant adoption factor even when comparing different types of wearable technologies: in their study, privacy was important for both smart glasses and smart watch users.

There is a strong focus on balancing the benefits provided by wearable technologies with the privacy and security risks that may accompany them. Gao et al. (2015) and Li et al. (2016) produce comprehensive studies by incorporating the privacy calculus theory into their theoretical frameworks. On this, Li et al. (2016) find that if a wearable technology user's perceived benefit is higher than their perceived privacy risk, it is more likely that they will adopt the device than vice versa. This is consistent with Gao et al.'s (2015) findings, who further differentiate between fitness wearable technologies and medical wearable technologies: they were surprised to discover that fitness users feel stronger perceived privacy risks than medical users. A possible explanation for these unexpected findings could be that medical wearable technology users are already aware that their device is gathering sensitive information, and – consistent with the privacy calculus theory – are comfortable with disclosing this information in order to receive the best possible medical care (Lee et al., 2016; Li et al., 2016; Sergueeva et al., 2020). Additionally, Paluch and Tuzonic (2019) investigate how consumers perceive and react to persuaded self-tracking in a health insurance context. This refers to consumers tracking their health information – such as calories burned and sleep patterns – and providing the data to their health insurance provider in order to receive benefits, such as discounts (Paluch & Tuzovic, 2019). They find that consumers consider factors such as perceived benefit, privacy and security concerns, and perceived fairness/justice when deciding whether or not they engage in persuaded self-tracking (Paluch & Tuzovic, 2019). This further supports Laufer and Wolfe's (1977) privacy calculus theory, which in this case

refers to whether or not the perceived benefit of sharing self-tracking data to one's health insurance company will provide worthwhile benefits.

Schomakers et al. (2019) also find that the context of mobile health technologies affects perceived privacy risk – when comparing fitness apps and diabetes apps, they found that user perceptions differed. Therefore, both Gao et al. (2015) and Schomakers et al. (2019) demonstrate that the acceptance of wearable technologies is context dependent. However, in their cross-country comparative case study on adoption of wearable technologies, Yang Meier et al.'s (2020) results contrast with Gao et al. (2015) and Li et el. (2016). They use Gao et al.'s (2015) theoretical framework – which includes the privacy calculus theory – and find that perceived privacy risk did not significantly impact user's behavioural intention to adopt wearable technology (Yang Meier et al., 2020). This is supported by Sergueeva et al. (2020), who also find that privacy is not a significant adoption factor in wearable health technology. Acknowledging that their findings contrast with past research, Yang Meier et al. (2020) hypothesise that this discrepancy occurred because their study solely focused on smart watches, whereas Gao et al. (2015) compared fitness and medical wearable technologies. Meanwhile, Sergueeva et al. (2020) attribute their inconsistency to the health context of their study, reinforcing the idea that medical wearable technology users are more comfortable with exchanging their privacy for improved medical care (Lee et al., 2016; Li et al., 2016).

Another key theme when focusing on privacy in wearable technology adoption is user experience. Spagnolli et al. (2014, p. 96) find that experts have fewer privacy concerns than non-experts, stating that: "The kind of privacy loss that might be perceived as unacceptable to some categories of users might seem acceptable to others". As such, they argue that there is a difference in privacy expectations between people who are familiar with wearable technologies compared to those who are unfamiliar (Spagnolli et al., 2014). This difference in privacy expectations is supported by Koo and Fallon (2018), but they instead find that experienced wearable technology users have greater privacy concerns than novice users because they are more familiar with the technology's capabilities. These findings relate heavily to previous findings where wearable technology is more likely to be adopted by innovative and tech-savvy individuals (Jeong et al., 2017; Park et al., 2016; Rauschnabel & Ro, 2016). Consequently, there are no consistent findings regarding whether or not experienced wearable technology users have greater or fewer privacy concerns than inexperienced users.

Some researchers claim that wearable technology users are not aware of the potential privacy and security risks when using the devices (Bellekens et al., 2016; Guillén-Gámez & Mayorga-Fernández, 2019). Using this logic, inexperienced users may not have great

privacy concerns because they fail to comprehend the risks, and as such privacy is not an adoption barrier for them. This is supported by Motti and Caine (2015), who state that:

> "Activity trackers that monitor heart rate, steps, and pulse, for instance, are usually seen as inoffensive to the users' privacy, however it is likely that users are not aware of how such data could be misused by third-parties or potential privacy implications when the data are collected in a long-term [sic] or associated with complementary information." (p. 241)

Additionally, Bellekens et al. (2016) demonstrate that while wearable technology users may claim to value their privacy and security, in reality their understanding of the risks is poor. Therefore, while many researchers argue that privacy is a significant theme within wearable technology adoption, people may not sufficiently understand privacy implications to the extent it could influence their adoption or non-adoption.

Meanwhile, Lee et al.'s (2016) privacy adoption research focuses on the general population instead of wearable technology users. They find that privacy and security are people's most pressing concerns when it comes to adoption of wearable technologies. They argue that privacy and security are the most highly ranked perceived risks, and that people are most concerned about wearable technologies non-consensually disclosing video capture or financial data. However, they note that "users are willing to tolerate risks if there is enough benefit associated with that risk" (Lee et al., 2016, p. 7). This corroborates Gao et al.'s (2015) and Li et al.'s (2016) finding that the potential benefit of using wearable technologies must be greater than the perceived privacy risks. In other words, in line with Laufer and Wolfe's (1977) privacy calculus theory, if the wearable technology provides appropriate benefits, the risks of usage may be more palatable.

In summary, privacy risk is a significant factor in the adoption of wearable technology in a consumer setting. While users may not fully understand the privacy risks associated with using wearable technology (Bellekens et al., 2016; Guillén-Gámez & Mayorga-Fernández, 2019; Motti & Caine, 2015), there is significant appetite to tolerate such risks if they obtain some kind of benefit in return (Gao et al., 2015; Lee et al., 2016; Li et al., 2016; Paluch & Tuzovic, 2019). This is also expected to be the case in a government setting. However, research is still unclear whether the characteristic of previous wearable technology experience has an important impact on adoption attitudes. There is a strong need on further research to more effectively understand adoption antecedents in a privacy setting, and to investigate whether the privacy risks identified in previous wearable technology adoption literature are relevant in a public sector context.

4 Methodology

4.1 Research design

This research is an exploratory multiple case-study that investigates citizen privacy attitudes towards adopting wearable technologies as tools to enforce quarantine obligations during the COVID-19 pandemic. An exploratory research design is appropriate for this research focus because this precise topic has never been researched before in a scientific manner (Stebbins, 2001; Yin, 2018). While there is extensive literature on wearable technology adoption, these studies have never focused on the public sector and have instead focused entirely on consumers. Scientific research on the effectiveness and legitimacy of public health mitigation measures such as digital contact tracing, wearable technologies, and social distancing is in its infancy, but governments have had no choice but to proceed with experimental rollouts (Bhattacharya & Ramos, 2021; Colizza et al., 2021; Elkhodr et al., 2021; Whitelaw et al., 2020). As a result, there is a strong justification for this exploratory research design.

The research background established that there is significant debate surrounding how governments should balance public health measures and citizens' personal privacy. However, countries with stricter lockdowns, quarantine rules, and restrictions on freedom of movement have had lower COVID-19 incidences and deaths (Lowy Institute, 2021). Therefore, there is some indication that sacrificing personal privacy and freedom may be necessary to effectively control public health crises such as COVID-19. This can also be seen in the design of digital contact tracing apps in the public sector: data-first and privacy-first (Fahey & Hino, 2020; Kapa et al., 2020). This study concentrates on wearable technologies, not software-based technologies such as digital contact tracing apps, because they are fitted directly on an individual's body. Consequently, they are more effective at enforcing quarantine because they cannot be left at home by the individual and they cannot be removed or tampered with without government authorities being alerted. Wrist-worn devices are the most popular in a consumer setting, so this study makes the assumption that governments would also pursue a wrist-worn device (Berglund et al., 2016). Therefore, this study investigates the following research questions:

1. What are the privacy attitudes of citizens towards adopting wearable technology as a tool for the government to enforce quarantine obligations during public health crises?

    a. Do citizen attitudes differ in relation to whether the wearable technology operates as data-first or privacy first?

b. Do citizen attitudes differ in relation to whether a government makes wearable technology mandatory or optional?

By doing so, this study aims to make a strong contribution to the wearable technology adoption field by broadening its horizons beyond the consumer perspective and moving academic discussion into the public sector domain.

4.1.1 Case study approach

Case studies are useful for researchers to understand similarities and differences between phenomena (Yin, 2018). This research adopts a multiple case study approach for two reasons: firstly, to avoid criticisms of generalisability; secondly, to respond to calls in wearable technology adoption literature to engage in more cross-country comparative research (see Chau et al., 2019; Gao et al., 2015; K. J. Kim & Shin, 2015; Paluch & Tuzovic, 2019). Single case studies are vulnerable to criticisms of generalisability (Flyvbjerg, 2006), with Yin (2018) describing how multiple case studies are more compelling than single case studies because there is room for contrasts and comparisons to be drawn. It is also important to emphasise that cases must be carefully selected to ensure that cases are comparable, and will either predict similar or contrasting results (Baxter & Jack, 2008; Yin, 2018).

Baxter and Jack (2008, p. 546) argue that "binding the case" is important for ensuring research scope. Without a reasonable research scope, researchers are susceptible to pursuing case study research that is too broad or unfeasible (Baxter & Jack, 2008). For this study, two country case studies of Australia and Singapore have been selected based on four parameters: their COVID-19 digital contact tracing app; their COVID-19 quarantine policy; their position on the COVID-19 Performance Index, and their government's existing use of wearable technology (see Table 3). As case selection in multiple case studies ought to be comparable (Baxter & Jack, 2008; Yin, 2018), Australia and Singapore were selected as country case studies on this basis of comparability. It is also important to note that Australia and Singapore are both island nations, with enhanced capacities to control their country borders.

Case	Australia	Singapore
COVID-19 digital contact tracing app	COVIDSafe – a privacy-enabled, centralised app powered by Bluetooth	TraceTogether – a partially privacy-enabled, centralised app powered by Bluetooth or a digital token

Quarantine policy	Hotel quarantine is mandatory for all travellers returning from overseas, with no exceptions[4]	Hotel quarantine is mandatory for some travellers returning from overseas, depending on their circumstances[5]
COVID-19 Performance Index[6]	8th best performance globally[7]	13th best performance globally[8]
Wearable technology use in government	The Howard Springs quarantine facility started a trial in November 2020 to monitor guests' vital signs using a wearable armband[9]	All people serving a stay at home notice outside a designated government facility must wear an electronic monitoring wristband[10]

Table 3: Country case selection overview

The purpose of using each country's digital contact tracing app as a selection parameter is to demonstrate how the respective governments have sought to balance the effectiveness of digital technology with citizens' privacy. Australia and Singapore have similar data collection standards, with the Singaporean app being slightly less privacy-enabled than the Australian app, but they are both examples of privacy-enabled architectures.

4.1.2 Case background

Australia has been selected as a case study because it has a strong privacy-enabled digital contact tracing app called COVIDSafe, it has implemented strict lockdowns and quarantine rules, and has been successful in managing COVID-19. Furthermore, it has started using wearable technology in the fight against COVID-19 – albeit not in a location-monitoring capacity, but to measure quarantine guests' vital signs. The Howard Springs quarantine facility in the Northern Territory is currently running a trial where wearable armbands are used to monitor citizens' vital signs (McDonald, 2020). Firstly, the main privacy elements of the COVIDSafe app include: multiple prompts of consent for data collection; the app only collecting data such as an encrypted user ID, and the date and time of contact with other COVIDSafe users; the app does not collect location data;

[4] (Australian Government Department of Health, 2020a)
[5] (Immigration and Checkpoints Authority Singapore, 2020)
[6] The COVID-19 Performance Index is "…a ranked comparison of the performance of countries in managing the COVID-19 pandemic in the 36 weeks following their hundredth confirmed case of the virus, using data available to 9 January 2021." (Lowy Institute, 2021)
[7] (Lowy Institute, 2021)
[8] (Lowy Institute, 2021)
[9] (McDonald, 2020)
[10] (Immigration and Checkpoints Authority Singapore, 2020)

and all data is deleted after 21 days, with severe penalties for those who attempt to decrypt the data (Australian Government Department of Health, 2020b). COVIDSafe has been set out in accordance with Australia's Privacy Act 1988, which was amended in May 2020 to outline stronger protections for app users (Australian Government Department of Health, 2020b). These interim measures included provisions that ensured the data collected from the app would only be used for COVID-19 contact-tracing efforts, that it would be deleted at the end of the pandemic, that decryption of user data is impossible, and that no one could be forced to download the app or provide their data (Australian Government Attorney-General's Department, 2021). Approximately 20% of the Australian population has downloaded COVIDSafe (Elkhodr et al., 2021).

Secondly, Australia's quarantine policy is strict: all people arriving from overseas or domestic risk areas – without exception – are obligated to quarantine in a government-designated facility for 14 days at their own cost. Costs of quarantine facilities are set by relevant State or Territory authorities, and range up to AU$3,000 (approximately €1,900) per adult (Australian Government Department of Health, 2020a). While Australia has virtually eliminated community transmission of COVID-19, people living in Australia who test positive for COVID-19 or are suspected as being positive must either isolate in hospital or their home until they return a negative test. Fines for breaching quarantine directives are severe: penalties are set by relevant State or Territory authorities, and range up to AU$63,000 (approximately €40,000) in fines and/or up to 2 years' imprisonment (Australian Government Department of Health, 2020a). As at February 2021, more than 211,000 people have completed Australia's quarantine program (Mao, 2021). There is no centralised data source to establish how many people breached their quarantine obligations (Australian Government Department of Health, 2020a).

Singapore has been selected as a case study because it has a privacy-enabled digital contact tracing app called TraceTogether, which can be paired with government-issued wearable technology, it has implemented strict quarantine rules, and has been successful in managing COVID-19. The country also has a sophisticated wearable technology strategy to monitor the whereabouts of quarantining individuals. The TraceTogether app is very similar to Australia's COVIDSafe app, but with the important distinction that the Singaporean government has the capacity and mandate to decrypt user identities (Government of Singapore, 2020), while the Australian Government does not. The TraceTogether app and token adoption rate has exceeded 70% (Smart Nation Singapore, 2020). While Australia's COVIDSafe app is rooted in strong privacy laws (Australian Government Department of Health, 2020b), Singapore only established their first comprehensive legal framework for privacy in 2012 and it is unclear how TraceTogether aligns with these national privacy laws (Goggin, 2020). Government authorities state that

they only store limited data, do not collect users' locations, third-party servers are unable to track users' identities, and citizens may request for their data to be deleted from government servers (Government of Singapore, 2020). As one of the world's leading smart cities, Singapore has an entrenched culture of mass surveillance and Goggin (2020) suggests that Singaporeans are used to providing their data to the government.

Singapore's quarantine policy is similar to Australia, except that international arrivals have the option to either quarantine at a designated government facility for 14 days, or to use a wearable device that allows them to quarantine at home under a stay at home notice (Immigration and Checkpoints Authority Singapore, 2021). The cost of quarantine in a government-designated facility is SG$2,000 (approximately €1,250) (Ministry of Foreign Affairs, Singapore, 2020), and is borne by the citizen. While initially government-designated facilities were mandatory since the start of the pandemic in March 2020, the government introduced electronic monitoring devices for people eligible to complete their quarantine at their place of residence in August 2020 (Immigration and Checkpoints Authority Singapore, 2020). These devices use GPS and fourth generation (4G)/Bluetooth signals to ensure that people stay at home, and the government assures citizens that the devices do not store any personal data and that they don't have any voice or video recording functions (Immigration and Checkpoints Authority Singapore, 2020). As at January 2021, more than 308,000 people were issued stay at home notices and approximately 367 breaches occurred (Min, 2021). People who breach their stay at home notice may be prosecuted under the Infectious Diseases Act and may face a fine of up to SG$10,000 (approximately €6,200) and/or up to 6 months' imprisonment (Immigration and Checkpoints Authority Singapore, 2020). However, like Australia, Singapore's COVID-19 management is amongst the best in the world, ranking 13th globally as at February 2021 (Lowy Institute, 2021).

4.2 Data collection

Kalantari (2017) criticises the wearable technology adoption field for lacking qualitative research methodologies, and calls for more studies to conduct qualitative interviews before commencing quantitative model testing. Therefore, this study uses semi-structured qualitative interviews to collect primary data from 20 adults (10 from Australia and 10 from Singapore) who have experience in using wearable technology (see Table 4). In order to achieve as representative a sample as possible, the author endeavoured to obtain roughly equal gender proportions and a spread across age groups of under 30, between

30-45, and over 46 years of age[11]. Semi-structured interviews are more flexible than structured interviews, but provide more participant guidance than unstructured interviews (Gill et al., 2008). They allow the interviewer to investigate their research questions in-depth, while also allowing participants to address topics that the interviewer may not have thought to include in the list of questions (Gill et al., 2008). This study's interview questions were developed based on literature from the research background and literature review. An interview discussion guide was developed and contains the theoretical justification for questions asked (see 9.2). Interviews were conducted over Zoom, on account of this author being located in Germany and the interviewees being located across Australia and Singapore. The interviews ranged between 20-40 minutes in length each.

Country	*Gender*	*Age*	*Number*
Australia	*Male*	<30	2
		30-45	2
		46+	2
	Female	<30	2
		30-45	2
		46+	-
Singapore	*Male*	<30	3
		30-45	2
		46+	1
	Female	<30	2
		30-45	2
		46+	-
Total			20

Table 4: Interviewee demographics

4.2.1 Sampling strategy

To source interviewees, the author used a convenience sampling method known as snowball sampling. This approach allows the researcher to access further interview participants based on information from current participants (Biernacki & Waldorf, 1981; Noy, 2008). This creates a 'snowball' effect where further participants are sourced via the recommendations of those who have already participated in the study. This type of sampling continues until data saturation has been achieved (Naderifar et al., 2017). The author initially reached out to wearable technology Facebook groups to access people who self-identify as using wearable technology. The chance to win an AU/SG$70

[11] It is important to note that for both Australia and Singapore, the author was unable to obtain female interviewees over the age of 46 years. This is not unexpected when considering existing wearable technology adoption literature, which finds that older women are the least likely social group to adopt wearables (Guillén-Gámez & Mayorga-Fernández, 2019).

(approximately €45) gift card was offered to enhance participation. From these initial interviews with members of these Facebook groups, the author obtained further interview participants based on recommendations.

The author selected a sample of adults who are experienced in using wearable technology. Wearable technology adoption studies have identified that prior experience is a key adoption parameter (Kalantari, 2017). Furthermore, having prior experience with wearable technology is associated with innovative tendencies and tech-savviness (see Gregor & Gwiaździński, 2020; Jeong et al., 2017; Park et al., 2016; Rauschnabel & Ro, 2016). By selecting this focus group, the author avoids a fully randomised sample and focuses on adults who have a prior understanding of the technology in question. While this sample excludes adults who have no experience in using wearable technology, wearable technology adoption studies have not determined whether experienced wearable users have higher or lower privacy concerns than non-experienced users (Koo & Fallon, 2018; Spagnolli et al., 2014). Therefore to "bind the case" (Baxter & Jack, 2008, p. 546), the author chose to focus on experienced users and recommends that further studies include comparisons with non-experienced users.

Additionally, wearable technologies are widely used recreationally in both Australia and Singapore. Approximately 20% of Australians own a wearable device (Pureprofile, 2015). Ownership is even higher in Singapore, with 33% of the population owning a fitness tracker, 16% owning a smartwatch, and 10% owning both of these devices (Statista, 2019a). Globally, the most popular form of wearable technology is a wrist-worn device, typically a watch (Berglund et al., 2016). The leading wearable technology brands globally are Apple, Huawei, Samsung, and Fitbit (now acquired by Google) (IDC Corporate USA, 2020). Apple holds 40% of the global market share, followed by Samsung at 10%, Huawei at 8%, and Fitbit at 7% (Tatler Singapore, 2021). In Australia, the most popular wearable technology brand is Apple, followed by Fitbit and Garmin (Shaw, 2019). Apple is also the most popular vendor in Singapore, but 32% of Singaporeans who owned a wearable device owned one from Fitbit (Statista, 2019b). Furthermore, the Singaporean government has formal relationships with both Apple and Fitbit through public health initiatives to encourage Singaporeans to engage in a healthy lifestyle: the Fitbit partnership ran from 2019-2020 through Live Healthy SG and the Apple partnership called LumiHealth has been running since 2020 (Apple, 2020; Fitbit, 2019).

4.3 Data analysis

It is important to acknowledge the criticism in wearable technology adoption research that it has overwhelmingly used a limited number of technology acceptance theories, such

as TAM and UTAUT (Kalantari, 2017). This, combined with fact that there is a total lack of wearable technology adoption studies that focus on the public sector, has prompted the author to use an inductive data analysis approach. This will allow themes to emerge organically from the qualitative data. Saunders et al. (2015) state that inductive research approaches are data-driven, while deductive approaches are theory-driven. The former allows researchers to explore and analyse their data in real-time, whereas the latter allows researchers to test an established theory (Saunders et al., 2015). The primary data collected from the interviews were qualitatively analysed using inductive coding. This is a qualitive data analysis method that allows researchers to categorise themes and attributes within their data, and use these themes or attributes to organise and assign meaning to their data (Saldaña, 2016). Inductive coding – also referred to as open coding – allows codes to emerge organically from the data, as opposed to deductive coding where the researcher begins their analysis with pre-selected codes (Saldaña, 2016). Using coding as a qualitative data analysis tool enables the transition from data, to codes, to categories, to themes/concepts, and finally to assertions/theory (Saldaña, 2016). This will facilitate the development of themes to guide further research into wearable technology adoption in the public sector. The semi-structured interviews were recorded and transcribed using the transcription tool Otter and the transcripts were coded using the software tool MAXQDA.

5 Results

This results section presents the findings of the 20 interviews with citizens from Australia and Singapore. Inductive coding using MAXQDA resulted in seven themes that indicate citizens' privacy attitudes to governmental use of wearable technology in public health crises. The first part of the results will briefly outline participants' experience with wearable technology, their privacy attitudes, and their use of governmental digital contact tracing apps. This section was not inductively coded, and is provided for background on citizens' experience and existing privacy attitudes. The second part presents the qualitative analysis of the interviews through inductive coding. These analysis findings emerged organically from a large group of categories within the transcripts, which were then summarised into a smaller group of overarching themes. The results are presented by theme, which are then each sub-divided by country.

5.1 Experience of wearable technology

As outlined in the methodology, all interview participants had experience with using wearable technology. There were no further prerequisites in this regard, and as such there was a wide degree of experience amongst participants. In both Australia and Singapore, participants had been using wearable technology for years – anywhere between 1-8 years. However, it is important to note that because there were no criteria placed on the extent of people's experiences, there were some outliers in the research. For example, A2 was a former elite athlete who has significant experience with wearables not only in his daily life, but to trial for large companies and to measure his health invasively for extended periods of time. Additionally, S6 works as a professional in the field of wearable technology and her insights are shaped not only by her personal use of the Apple watch, but from a deep understanding of how the technology works and what it is capable of. Then on the other side of the spectrum, S2 wore a Fitbit for a short amount of time and had a very limited understanding of what it did. As a result, there is a large skew in terms of wearable experience. However, all participants were able to answer the interview questions without needing to clarify many details about wearable technologies.

When asked about their wearable technology experience, most participants discussed the reasons why they use wearables and the benefits they receive from doing so. All devices mentioned were wrist-worn and were used for health purposes, such as counting steps, measuring sleep and heartrate, and tracking exercise activities and patterns. Participants also spoke about more functional capabilities, such as sending and receiving messages.

5.2 Privacy attitudes

In both Australia and Singapore, there was a relatively wide spread of privacy attitudes in their general day-to-day lives. Responses could largely be classified into privacy being important, it not being important, and indifference about it. The majority of participants from both countries stated that privacy was important to them. Participants discussed how they knowingly provided data to companies which was then used for marketing purposes, and that they were not completely comfortable with this information being out there for anyone to use. Interestingly, few participants were able to identify steps they had taken to ensure their data privacy despite being concerned about their data being leaked. A8 discussed how he is much more careful with accepting cookies on websites, A7 stated that she considers the reputability of a website before entering her personal details, and multiple respondents from Singapore discussed how they changed their behaviour to avoid scams. On privacy in Australia, A5 notes that:

> *"In general, I'd say it's pretty important. Like, you know, yes, I use, you know, emails and apps and all sorts of things. But I would like to think that whatever I do on those things is secure within those apps, and that they don't go sharing it to marketing companies and that sort of stuff."*

On privacy in Singapore, S10 states that:

> *"Of course it's important, you know, I don't want my private data to be available to all, especially information related to my bank account and stuff like that. But general things like my name, my contact details, I'm relatively okay."*

A number of participants expressed their indifference about data privacy, saying that it is relatively important but not hugely so. A1 cared about her data privacy but was also fully aware that the way she handled her data privacy may put her at risk of attack, saying that: "*I know there are probably lots of things hacking into my data*". Meanwhile, S1 stated:

> *"I'm not that big on privacy…but big part is that outbreak of scams, you unwittingly give away your credit card numbers or some situation that you may be a victim of financial scams, but other than that, I'm not too worried."*

Here, participants were not actively worried about their data privacy and also had not taken active steps to protect themselves. A small number of Australian respondents claimed that they did not care about data privacy. A3 discussed how she appreciated

"*getting good ads*" from Google and did not see the need to change her behaviour, meanwhile A6 knew that his Google Nest was listening to his conversations all the time and he did not care. Therefore, it is clear from participants' responses that privacy attitudes vary within Australia, and to a lesser degree in Singapore. However, the common theme amongst participant responses was that no matter their attitude, they hoped and expected that authorised people were using their data and only for the right things. Data leakages were mentioned as abuses of their data that made them uncomfortable and affected their trust in the provider.

5.3 Digital contact tracing apps

Participants were also asked about their use of governmental digital contact tracing apps and their reasons for using them. This was to establish their appetite for innovative – yet, invasive – government uses of technology. The responses were markedly different between Australia and Singapore. The majority of Australian participants downloaded the COVIDSafe app, but only a small minority actively used it. Multiple participants stated they deleted it shortly after downloading it because it took up too much room on their phone and drained their battery. Stated reasons for downloading it revolved around social pressure – such as being urged by the government or their social circle – and a sense of the greater good to the community. It is important to note that in Australia, it is not mandatory to download the app. Only A6 was mandated to download the app, as he is a primary school teacher and it was required by the Department of Education. Most participants had no privacy concerns with the app, with the exception of A2, A3, and A10 who stated that they did not trust the Australian Government enough to download it. Additionally, A1 and A4 expressed scepticism as to whether the Australian Government was capable enough to use the data effectively in their pandemic response.

Meanwhile, in Singapore, downloading TraceTogether was not mandatory but participation in daily life was not possible without doing so. Citizens who wish to do activities in public places such as eating out at establishments and visiting shopping malls are required to check-in to these places using TraceTogether. Therefore, there is a different context to the app's use in Singapore than in Australia. Amongst the Singaporean participants, everyone downloaded and actively used the app except the people who were not in Singapore for the majority of the pandemic. Furthermore, no participant raised any privacy concerns about TraceTogether. S6 discussed how she had lived in five different countries and while she had an enormous level of trust in the Singaporean government, she would not trust any other country in the world with this degree of personal information. S1, S4, and S7 also emphasised their trust in the

Singaporean government to collect information related to their personal contacts. This is in stark contrast to the Australian participants, where no one explicitly stated that they trusted the Australian government.

Therefore, it is already possible to see a difference in participant responses from Australia and Singapore. While experiences of wearable technology are skewed both within and between countries, privacy attitudes are similarly spread out. It is the use of the digital contact tracing apps COVIDSafe and TraceTogether that differed greatly between the countries, as well as the attitudes towards this innovative technology.

5.4 Privacy adoption factors for governmental use of wearable technology

This second results section displays the analysis of participant responses, separated into seven themes derived from the inductive coding process. Each theme was found to impact citizens' privacy attitudes towards adopting governmental wearable technology during public health crises such as COVID-19.

5.4.1 Perceived benefit

In wearable technology adoption literature, perceived benefit has been widely researched as an adoption antecedent. This study's inductive coding process found that perceived benefit is also relevant in a governmental context. Participants from Australia and Singapore reflected on how the possibility of using a wearable would afford them benefits such as facilitating life without pandemic restrictions, and quarantining at home instead of a hotel, which some argued would be more comfortable and beneficial for mental health.

<u>Australia</u>

Australian participants were in favour of governmental use of wearable devices, with very few privacy concerns. They overwhelmingly considered wearables as a highly effective tool to preserve Australia's way of life in the pandemic. The benefits identified in this sense are freedom and ensuring that infected or potentially infected people are isolated from society. By isolating these people in hotel quarantine, the Australian Government has had the opportunity to virtually eradicate COVID-19 from the community. The participants were acutely aware of this, and each person was supportive of a quarantine system. They spoke of how people living in society only have a certain threshold of rules they can withstand that significantly affect their day-to-day lives, and that they were willing to accept short-term inconveniences that preserve their freedom to live their lives as they choose. Many participants discussed how now that community transmission of

COVID-19 is virtually impossible, the greatest risks of infection are from returning overseas travellers: as such, it is necessary to keep these individuals quarantined for the greater good of society. All participants with the exception of A2 and A8 were confident that wearable devices would be an effective tool to prevent people from breaching their quarantine. Many participants emphasised wanting to avoid "another Melbourne lockdown", with A5 stating:

> *"I think for people who are in quarantine, I think it's a great idea to make sure they're not breaching quarantine. Because I'm sure you would have heard, you know, particularly in Victoria, where it was rampant that there was people breaking, you know, quarantine and popping down to the shops and that kind of stuff. And so to be able to ping those people and go okay, you're getting fined, like, you know, there's consequences, you can't just run around, I think is a really good idea."*

Melbourne, Victoria had one of the world's strictest lockdowns for approximately four months in the second half of 2020, partially caused by the virus escaping the hotel quarantine system. The city's efforts eradicated community transmission of COVID-19 at enormous social and economic cost. It is not surprising that so many Australian participants were willing to sacrifice their privacy to avoid a lockdown of this magnitude and length. In this sense, participants considered the wearable devices effective enough to mitigate the risks of another lockdown, which was a more unacceptable option compared with wearing a government-issued device.

Furthermore, the majority of Australian participants emphasised that they would welcome the chance to quarantine in their own home as opposed to hotel quarantine. The two main factors for this were comfort and cost. All participants with the exception of A3 stated they would prefer to quarantine in the comfort of their own home with a wearable device as opposed to completing hotel quarantine. It is important to note that A3 was not opposed to the wearable, but made her choice based on preserving her mental health in a place with different scenery to her day-to-day life. Privacy concerns were largely overlooked in people's decision, which indicates that the benefit of staying in a comfortable and affordable location outweighs potential privacy issues. Participants spoke of wanting access to their belongings, having a garden to spend time in, and not being lonely. On discussing his preference for quarantining at home with a device, A4 stated: *"...I imagined that would be a very suitable way of keeping people in home isolation rather than in hotels, I think it's the better of the two evils"*.

A1, A3, A6, and A10 further emphasised the importance of mental health for quarantined individuals, discussing how being in a familiar environment was important for people to stay busy and positive. Furthermore, cost was a huge factor in people's decision to accept the wearable device. A4, A5, A6, and A7 each discussed how expensive hotel quarantine was, and that in itself was a huge factor for them to prefer the wearable device over staying in a hotel. A5 was indignant at those not wanting to wear a device if it removed her choice to do so:

> *"If you didn't want to wear the bracelet, that's up to you, and you can pay the 3000 bucks or whatever it is, you know, but I want to go home and not pay the money and throw a bracelet on."*

Meanwhile, A7 saw the wearable as an opportunity not only for individuals to save money, but the taxpayer as well:

> *"There's a lot of people who work for the government, like, in my case, I work with defence members, and they have to quarantine at the Commonwealth's expense, and it is the taxpayers who are paying for their quarantine. So, again, it will save a lot of money for taxpayers. So, I think having a device, it will be quite cost effective for the community."*

The enormous cost of the Australian quarantine system was a strong deterrent for people to choose it as an option, and participants also identified that having to stare at the same four walls for two weeks was just as much a privacy violation as the device itself. A4's statement of home quarantine being "*the better of the two evils*" resonates strongly here. Furthermore, A2 was the participant with the most concerns about the privacy aspects of the wearable device, but nonetheless preferred to quarantine with the device in his own home than without it in a hotel. When pressed for why, he stated that while he was deeply passionate about his privacy, it was important for him to feel safe in the first place and he felt he was more likely to feel this in his own home than in a hotel room. Therefore, Australian participants were unanimously willing to accept the wearable device, and the overwhelming majority indicated a preference for this device as a quarantine tool. The benefit of living in a community without a COVID-19 risk and the option to quarantine in their homes was ultimately greater than their privacy concerns.

<u>Singapore</u>

Singaporean participants were also in favour of governmental use of wearable devices, but they had more nuanced positions on the benefits it would bring. Firstly, S3 and S10

questioned why a wearable device was necessary instead of a smartphone. When explained it was for removability issues, both respondents maintained their stance and said that quarantined individuals should be staying home anyway, and leaving the phone at home or removing the wearable ought not to be a problem. This indicates high expectations of law-abiding community behaviour, and is also reflected in the very low rate of home quarantine breaches in Singapore.

Furthermore, as wearable devices at home is already an established quarantine approach in Singapore, Singaporean participants were very matter-of-fact about their use. When discussing the effectiveness of the device in keeping the community safe from COVID-19, participants rarely mentioned privacy. It was not a significant concern for the participants, and many saw it as a necessary and useful tool to facilitate day-to-day living. S1 emphasised that effective quarantine was the most important approach to control the virus:

> *"...we know that the best way to prevent COVID is actually behavioural, not medicine. And just as with SARS if you know the number of people who are infecting other people, having them quarantine is very useful…it's actually more effective than everyone staying home. Quarantining yourself is actually more effective than having the vaccine."*

Many participants also noted they were grateful that Singapore had never had high community cases, and did not experience a prolonged or recurrent lockdown. They were overwhelmingly in favour of adopting wearable devices for quarantine if it ensured that COVID-19 community cases did not occur: and only S10 was skeptical that wearables would be effective in achieving this. S10 stated he needed to see more evidence before making a decision. Furthermore, S4 stated that the effectiveness of wearable devices was quite high in quarantine situations:

> *"...because obviously our nation is doing quite a good job already so we don't have very high community cases…so I think if we actually really keep it very tight on like the few people who maybe like who you see needs to be on quarantine in they wear the devices, I think it would have helped the community in some sense, yeah."*

Singaporean respondents were split in half when it came to selecting quarantining at home with a wearable, or in a hotel without one. However, their decisions were not based on privacy, but on comfort and familial obligations. Cost was a minor consideration. The

benefit of quarantining at home included being in a comfortable, familiar environment and not being lonely in a room by themselves. When discussing his preference to quarantine at home with a wearable or in a hotel, A2 stated: *"Easy. Like, you're going to be at home…as long as I know I can come back home and can just better be done with it. I can stay home. That's the best thing"*.

However, for almost half the Singaporean participants, the wearable at home did not necessarily correlate with comfort. Multiple people stated that a hotel would be more luxurious and would give them access to nice amenities and great food, which they ordinarily would not get at home. This indicates that the stay in the hotel can be considered as a benefit for some individuals. However, a number of participants also explained that they lived at home with older relatives who were at risk of being seriously affected by COVID-19. For this reason, they did not want to risk quarantining at home and infecting their relatives. Therefore, the privacy aspect of the wearable paled in comparison to some participants' senses of morality. Finally, cost was raised several times as a factor in people's choice not to quarantine in a hotel, but it was not a significant factor. For the majority of 2020, hotel quarantine was free for Singaporean citizens. Only S2 emphasised that the cost of hotel quarantine was prohibitive, even though he much preferred the option of staying at home with a wearable. Meanwhile, cost was an almost decisive factor for S9: *"If I have to pay for it, then maybe I would most probably choose the lesser of two evils, I'll probably go stay in my house. But if the hotel is free, then guess what? Hello Grand Continental"*.

Therefore, Singaporean participants were very open to the wearable device and the benefits it provided. Privacy concerns were either not mentioned, or explicitly overlooked. Even when prompted, Singaporean participants did not raise any privacy concerns with the wearable device option. S6 stated: *"I think since I get to live at home, I would overlook the privacy"*. As a result, it is clear that the Singaporean participants found benefits in the temporary privacy loss as it afforded them to live in a more comfortable environment during the public health emergency.

5.4.2 Perceived privacy risk

In wearable technology adoption literature, perceived privacy risk has been a large research focus. There have been mixed findings about its role in encouraging or inhibiting wearable technology adoption. This study's inductive coding process found that perceived privacy risk is also relevant in a governmental context, but that citizens do not fully understand the interaction dynamics of privacy and necessary tracking information.

Participants from Australia and Singapore reflected on the impacts using a wearable on their privacy, and what kinds of conditions would make it acceptable or unacceptable for them.

Australia

Australian participants were overwhelmingly in favour of only accepting a governmental wearable device if it collected de-identified data. This indicates that their acceptance of the device is dependent on what kind of private information it collects, and in what way. While the device in question would only collect location data that was then linked to the wearer's identity, Australian participants were protective of their privacy in this regard. Initially, many participants were accepting of a device that collected identified information on their location because of the fact they were obligated to be at home anyway. For example, A7 argued that the government already knows where people live, what is the difference when wearing a device that confirms this: *"If you're quarantining at your place, you're supposed to wear the device at your place. So what? What sort of other information can they get? You know, you're supposed to be at home? Right?"*

But when then presented with a de-identified option, all respondents except A8 had a strong preference for this. Many respondents backtracked on their approval for an identifiable version upon hearing that an encrypted option with clearance controls was available. However, it is important to note that respondents were unable to justify the privacy risk behind governments collecting identified location data. Participants did not have an understanding of what freedoms and privacy they would lose if the government collected identified location data compared with de-identified location data: they simply appeared to be more comfortable knowing that their identity would be masked with an encrypted identifier, and that it could only be accessed and/or decrypted by a government authority with approval. For most Australian participants, such a device would only be acceptable from a privacy perspective if the data was de-identified. A1 describes this: *"Absolutely, for that to work and for me to be happy that the police are receiving that kind of information, it would have to be de-identified".* However, there were also misunderstandings on how carefully the data would be stored by the government. A6 expressed concern that his private information would become public knowledge through use of the wearable:

> *"…if it's de-identified, and it's used by the government, and it's kept secure, then that's a really good thing, I think. But if it's out there for the world to see, and access and unsecure, that's when it could be really problematic."*

Australian participants were therefore fearful that data meant only for government eyes would be accessible by anyone who wanted to see it. Again, participants were unable to articulate a concrete privacy risk beyond that they were uncomfortable with unauthorised people knowing their identity and location. Additionally, while the Australian participants insisted on the wearable collecting only de-identified data, they were also split between how easy it should be for the Australian Government to identify and catch quarantine violators. On one hand, identifiable data would significantly fast-track this process, but this would be to the discomfort of citizens; on the other hand, de-identified data would slow down the identification process, but citizens claimed to be more comfortable with this. But when presented with the scenario of a quarantined individual wearing a wearable breaching their quarantine-at-home order, the Australian participants were split down the middle. Half the participants wanted it to be very easy for the Australian Government to identify, catch, and punish the quarantine violators in order to protect the community from COVID-19. For example, A10 stated:

> *"I would prefer them to be able to detect violators. It's just location that they're looking for. And it's only a short period of time that concerns me. Yeah, much less than other scenarios for sure. And I think that the health of the population does need to be put above privacy in some situations, which this would be one of them."*

Meanwhile, the other half of participants felt that despite the public health crisis, citizens were still entitled to their privacy and there should be some complications for the Australian Government to identify them. For example, A4 stated: *"I think that's fair enough that there has to be a degree of difficulty, it's still the ability to access someone's identity and where they're going".* As a result, while Australian participants desired a de-identified wearable technology architecture, they were evenly split on how easy it should be for the Australian Government to identify and catch quarantine violators. This suggests an imbalance or a misunderstanding between what these Australians feel comfortable with privacy-wise and what they are willing to accept in a public health crisis.

<u>Singapore</u>

Singaporean participants were almost evenly split on whether they preferred an identified or de-identified governmental wearable device. The participants had a strong understanding of what kind of information would be required for collected by the government in order to enforce quarantine obligations. Similarly to Australia, participants felt that because quarantining people ought to be staying at home anyway, the wearable technology should not add any additional privacy burden. Multiple participants discussed Singapore's identity card which uniquely identifies each citizen and contains an

enormous amount of identifying information. This card is used in many daily activities in Singapore, both personal and professional, thus demonstrating that Singaporean citizens already live with a piece of governmental technology that uniquely identifies them. The main difference with a governmental wearable device would be that it is placed directly on their body and its sole use would be to enforce a time-bound quarantine period. Approximately half of the participants preferred an identified device because they felt it would be more effective. However, they also added that it would only be acceptable to them from a privacy perspective if their data was used responsibly. For example, S9 stated:

> *"No, I think they should be easily identified. I mean, the whole purpose is to ensure the safety of others. So as long as disclosure on why and how this is being used, I think they should be easily identifiable."*

However, upon hearing about a de-identified option, there was another group of Singaporean participants who wished for the device's information to be de-identified. S5 stated that:

> *"I think that would be better and it will give people like, more faith in the government. Yeah, sort of like they would trust the government more. If they were to bleep it out. Or like, only really, people really high rank can see it, but yeah that's probably about it."*

It was important to this group of Singaporean participants that the data gathered by the device could only be accessible by those with a certain level of data access. However, regardless of their preference for identified or de-identified data, Singaporean participants did prefer that their data could only be accessed by authorised government authorities. It was notable that they raised this preference without being prompted, showing that they understood data collection and storage issues to a high degree. Furthermore, they understood the privacy impact of having a government official accessing their data versus an unauthorised person.

But noting that Singaporean participants were divided on whether the wearable device should be identified or de-identified, they were almost unanimously in favour of the Singaporean Government being able to easily identify quarantine violators. Multiple participants spoke of how Singapore is known for having strict laws and that the vast majority of citizens abide by them carefully. S5 and S6 noted that while some people laughed at Singapore banning chewing gum, citizens never questioned the rule and

followed it from the beginning. Singaporean participants discussed how they valued the freedoms they were given in the COVID-19 pandemic to live their lives, and that they were willing to sacrifice elements of their privacy to maintain this freedom. However, the culture of information sharing and lack of privacy from the institutionalisation of the Singaporean identity card demonstrates that the perceived privacy risk of the wearable device is very low for Singaporeans. Overall, participants did not see how this device would collect data that was any more personal than what was already on their identity card. Therefore, participants were very comfortable with the Singaporean Government being able to easily identify quarantine violators, as summarised by S6:

> *"...given the condition of COVID and the way it's spreading now, it's clearly, this is I think, directly proportionate to the adversity of the diseases when COVID was not this bad in the first wave. But after the new strain, and the way it's spreading like wildfire, especially in India, and bigger countries, it's really showed its potential of destroying the world, I really think that effective measures as of now need to be taken very, very seriously. So with that in mind, I would probably prefer that the government easily identifies whoever's violating it and catch them so they don't spread it to 15 other people."*

These findings indicate that Singaporean participants have a high technological literacy, because they have a refined understanding that prioritising privacy would have a negative influence on the device's effectiveness at enforcing quarantine obligations. Regardless of whether the device collects identified or de-identified information, Singaporean participants want assurance that their data will only be accessed by authorised people. However, given the severity of the COVID-19 situation and Singapore's culture of following the law, participants believed that quarantine violators should be identified and found quickly regardless of the impact on privacy.

5.4.3 Context

The context of the COVID-19 public health crisis had a strong impact on citizens' privacy attitudes. Overall, the wearable device's privacy impacts were justifiable in the context of this public health emergency. But across both Australia and Singapore, there was no appetite for governmental use of wearable technology to continue beyond the pandemic: the extraordinary circumstances of COVID-19 fostered acceptance of short-term privacy violations amongst participants.

Australia

The Australian participants frequently mentioned the severity and seriousness of the COVID-19 pandemic when discussing their privacy attitudes. There were no participants who were fully comfortable with the government knowing their identity and location via a wearable device, and this discomfort ranged across a spectrum from mildly unsettled to extremely uncomfortable. However, the Australian participants acknowledged that the pandemic required extreme governmental responses and that while this would impact their privacy, it was necessary in order to manage the virus's impact on and transmission within the community. All participants believed that the Australian Government was justified in using the device to enforce quarantine obligations, with multiple participants referring to how badly managed COVID-19 was in many countries overseas. Furthermore, the participants also discussed that there needed to be strict quarantine arrangements to prevent the virus from getting into the community. The majority of participants backed the wearable device entirely, with the specification that it is only used in a pandemic environment. Anything beyond a public health emergency made people feel uncomfortable and they would not accept it. For example, A3 stated:

> *"In any of those outside contexts, I don't think I would really have approved of such a thing for the government to be tracking that specifically. But because of quarantine, I just think does this lead to a slippery slope with the government tracking more locations?"*

Other participants were willing to accept the privacy invasion in a quarantine context, but to varying degrees. A4 and A5 provided positions at varying ends of the spectrum. For example, A4 stated:

> *"Yeah I mean if you'd asked me before COVID, I'd be probably aghast, but then bad situations require some ideas to be a bit extreme and this is one of them…overall I'm not terrifically concerned, cuz I usually believe that it's for the greater good."*

A5 also supported the device, but was notably less flexible in his acceptance:

> *"I think the only justification would be if it was going to lock down the whole of Australia again…I think if we're in a really bad situation again, we have like another massive outbreak. Those kind of steps might be necessary."*

Participants also made reference to the greater good. In this sense, while they understood the privacy impacts of a wearable device to enforce quarantine obligations, they also

respected the current way of life in Australia and the need for innovative ways to protect the country from COVID-19. The balance between public health and privacy was a strong theme, with A10 stating:

> *"Is my privacy more important than the health of other people? Or is like each individual person's privacy more important than the public health of society? And I think that yeah, I think that the public health of society is more important than each individual's privacy, especially when it comes down to location."*

Therefore, while Australian participants expressed their discomfort with the device, they also acknowledged that the use of this technology hinged on the pandemic situation and this consequently made a significant difference on how they felt about the privacy impact.

Singapore

Singaporean participants also spoke of how important it was for the country to avoid COVID-19 to the greatest extent possible. While the participants had varying degrees of comfort on governmental use of wearable technology to enforce quarantine obligations, the appetite for privacy violations was stronger because of the identity card and existing use of wearable technology in pandemic management. Through the TraceTogether app and token system, the Singaporean Government was already using wearable technology to ensure that citizens were responsibly fulfilling their quarantine obligations and with very few breaches. As discussed in a previous theme, Singaporean participants were used to their government collecting large quantities of private information on them through their identity card. As a result, it was natural for them that the Singaporean Government would continue gathering private information on citizens by using appropriate and innovative technologies during a pandemic. S9 spoke of how the pandemic context meant that citizens ought to behave with the collective society in mind, not their personal preferences:

> *"So, to me, I think it's absolutely necessary, and especially when it is considered as a pandemic, everyone has a role to play. So it's no longer an individualistic option when I choose to or not, if this is the way that we're to help with the situation, then I think we should take it.*

S4 discussed how citizens should be accommodating of this short-term privacy loss in order to maintain the current standard of living in Singapore:

> *"We are all able to travel freely, I know that because we kept the numbers really low so I think that's why is why I'm supportive of this whole entire policy. So that like as a nation we don't have to lock down again."*

These emphases on living in a collective society and coming together to support the nation of Singapore are reinforced by the majority of participants, with S1, S2, S5, S6, and S7 each mentioning "the greater good" when discussing the privacy impacts of a wearable device. While none of the Singaporean participants were eager for the use of wearable technology, nor were they happy about the idea of quarantine, the acceptance and understanding of these pandemic mitigation tools were contingent on Singapore being able to maintain a pre-pandemic standard of living. A temporary loss of privacy and freedom was required to achieve that, so the Singaporean participants were prepared to accept this loss and adopt the device.

5.4.4 Time

The length of time that citizens would be required to wear a government-issued wearable was a strong concern for both Australian and Singaporean participants. Their appetite for giving up their privacy for COVID-19 quarantine measures was not only limited to the pandemic itself, but for a specified amount of time within the crisis.

<u>Australia</u>

All participants specified that the government should only enforce the device for the quarantine period and not beyond this window. The quarantine period of approximately 14 days was mentioned by participants, and while there were differing levels of acceptance overall for the device, they were united in only being willing to wear such a device during a period of quarantine and not generally throughout the pandemic. A2 and A3 discussed how the pandemic had lasted for much longer than anyone expected, and it was hard living their lives not knowing the end date of the pandemic. They added that in addition to this uncertainty, they would be totally unwilling to provide their personal information to the government for such an extended and unspecified amount of time. This emphasis on government wearables being suitable only as a short-term solution was a common thread amongst Australian participants. For example, A8 stated:

> *"Yeah, then I guess it makes sense, if it's quarantine only, I think I'm only generally for it if it's only like very limited temporary use. So if it's only within a 14 day period, like you can't really do much anyway."*

The idea of wearing such a device outside the quarantine period and amongst the broader population was totally unacceptable to the Australian participants. While this thesis focuses on the use of wearables in a quarantine context, several participants discussed wearables that could be distributed to the wider population to manage the pandemic. For example, A5 was firm in giving her support for the wearable device strictly in a quarantine context and not for the wider population: *"If it was to wear all the time for COVID tracing that would, I'd feel differently…if you had to wear them all the time, and then it was to contact trace, I would have big issues with that".* Therefore, the Australian participants were willing to adopt a governmental wearable device for quarantine, but this acceptance did not extent to any circumstance beyond this limited time period.

Singapore

The Singaporean respondents were similarly insistent that governments should only use these wearables for a limited period of time. However, it is important to note that the Singaporean Government's TraceTogether digital contact tracing approach also incorporates a physical token that can be used in lieu of a phone. In this way, Singapore has already taken steps to providing optional wearable technology to the wider population for contact tracing. Singaporean participants were very understanding of the need for effective technological responses to the pandemic, but also specified that these devices could not be kept beyond the pandemic. For example, S6 stated:

> *"I don't think it can be abused because the device is taken off as soon as you're out of the quarantine. And so yeah, it doesn't really matter…If they were using short term now, I would say very justified. But if we keep using it for the time to come when the virus subsides, then not justified."*

In this sense, the privacy effects of the device were acceptable for the limited time period of quarantine but could not be extended beyond the lifespan of the pandemic. Furthermore, multiple Singaporean participants went beyond the privacy implications of the physical devices themselves, and spoke of how the data collected by the devices ought to be destroyed in a short time period. For example, S7 stated:

> *"…I think for as long as there is a holding period of information. Say example, they are holding the information up to maximum six months. Then after six months, they will discard the information and I think that is justifiable, I think to me, as long as they do not hold it for too long."*

Therefore, for Singaporean participants, the two time-related dimensions for citizens to accept and adopt governmental wearable devices was linked to both the limited time period of the quarantine and the timely deletion of the data collected by the wearables.

5.4.5 Choice

Having a choice in whether or not to adopt the devices was an important theme amongst the Australian and Singaporean participants. The main difference here was that mandatory devices were linked to acceptance, while optional devices were linked to adoption. In this sense, if a device was mandatory, citizens would have no choice about whether or not they adopt it and their thoughts were instead in relation to what degree they would accept such a device. Meanwhile, if they were given a choice about whether or not to adopt the device, the conversation focused on whether or not they would choose to adopt it.

<u>Australia</u>

Overall, Australian participants were almost equally divided on whether they would prefer the wearable device to be mandatory or optional. Each of these approaches would have different impacts on privacy. Those who preferred a mandatory device made reference to "the greater good": their choice did not indicate that they were comfortable with the government using a wearable to collect private information about them, but to demonstrate their willingness to cooperate in exceptional circumstances. The wearable's impact on their privacy remained to be considerable, but they were willing to live with the temporary privacy invasion to protect public health. For example, A10 stated: *"...I think if I can see that it's the best option for society at large, I'm happy to sacrifice my own security to make sure others are healthy and safe. Yeah"*. Meanwhile, others felt passionately about being given a choice by the government as to whether or not they had to wear the device. While the vast majority of Australian participants preferred the idea of quarantining at their home with a wearable device instead of quarantining in a hotel, they nevertheless wanted to be given a choice about doing it or not. For example, A2 stated:

> *"Weirdly, even though I wouldn't choose the hotel I will be more comfortable with having the choice. Yeah, yeah that's weird all these choices that I would never take up make me more comfortable…I think that has a lot more to do with psychology than the actual impact it has. And that effect is simply because by having that little bit of choice, you feel a little bit more free. Even if that choice doesn't materially give you any more or less freedom."*

By having a choice, these participants felt more comfortable with sacrificing their privacy for the benefit of public health in Australia. However, A5 notes that regardless of whether the device is mandatory or optional, it records the same information. In this way, the issue is not in relation to the data that the government would receive from the wearable, but how comfortable citizens would be to accept or adopt it. To summarise, A5 stated:

> *"You know, I think optional, is more comfort about the process. But I think either way that they're mandatory, or optional, they're still recording the same stuff. They're still storing it the same way. So my concerns about privacy probably don't change. Just you know, my willingness to participate is different."*

This is an important finding for governments because it demonstrates that citizens want to feel as if they have a choice in the matter when they use these devices: even though it would function the same way regardless of whether it is mandatory or optional, citizens would have a higher level of comfort if they were given a choice.

A number of participants also likened mandatory devices to house arrest. Through this frame, the loss of privacy was given strong links to criminality. Numerous participants described how they would feel deeply uncomfortable with "being treated like a criminal" in order to protect the Australian community from the virus. This was not only linked to whether the device was mandatory, but how easily it could be removed. For example, A9 discussed that while he would be willing to accept a government wearable to ensure he was staying at home during the quarantine obligation, it reminded him a lot of home detention: *"Yeah. But to say here's an ankle bracelet, like clip it on, and you're stuck with it for two weeks. That's a different conversation. Then that's, yeah, that's definitely like a home detention arrangement".* Therefore, for Australian participants, having a choice is a strong factor in whether they would accept the device. However, if the device is made mandatory, while they would be forced to adopt it, their level of comfort would be heavily impacted.

<u>Singapore</u>

The majority of Singaporean participants argued that the device would need to be mandatory in order for it to work. This was not about their comfort with sharing their private data, but about the effectiveness of the government's pandemic management response. These participants made clear that while the privacy implications of such a device were less than ideal, they were prepared to accept this temporary invasion for the greater good of Singaporean society. Furthermore, they preferred that the device be

mandatory rather than optional because they wanted it to work effectively. S2 stated that "*I think people would be really worried about privacy if it's mandatory*" but at the same time felt that the device could only successfully manage to enforce quarantine if the government required people to wear it. Singaporean respondents were not comfortable with it, but were willing to sacrifice their choice for the greater good. For example, S1 stated:

> *"I don't like it, but I understand why it's done. And as long as it's been clear to me why, why is the rationale behind and there's a start and end date to when I have the right I'm fine with it. I know it's a necessary evil. So, I don't like it, but I will follow it…in order for this to work, has to be mandatory because people who play by the rule wouldn't mind wearing them, there is that one of the 100 who will not play by rules…"*

Therefore, the device is not only a "necessary evil", but it being mandatory is hinged on the reality that some people would breach quarantine and the government needs some kind of safeguard to minimise this risk from occurring. Some participants also described how they would adhere to the mandatory requirement if the government required it. For example, S5 stated:

> *"I think I would be a little like, against it. But like, at the same time, if I want to come back to Singapore, then I kind of have to adhere to the rules and regulations so like, I would just end up doing it. Probably will not question it too much, but be like complaining and whining a lot."*

In this sense, participants are willing to follow government directives even if it makes them feel uncomfortable. But the majority of Singaporean participants were ultimately accepting of the short-term privacy violation that accompanied the wearable device. Therefore, the Singaporean respondents did not feel strongly about having a choice, but about the effectiveness of the device in enforcing quarantine obligations. In this sense, privacy considerations were secondary to ensuring that the device facilitated desired behaviour changes in society.

5.4.6 Trust in government

The factor of trust in government was also a strong theme in participant responses. This indicates that people's privacy attitudes are shaped by how much (or little) trust they have

in their governments and additionally by their culture. There are significant differences here between Australia and Singapore.

Australia

The Australian participants did not convey a huge level of trust in their government. This was not just in relation to protecting their privacy when using the wearable device, but whether they trusted the Australian Government to have the capacity to deliver such a significant innovation. Throughout their responses to the interview questions, Australian participants mostly did not mention their trust in government, or explicitly mentioned that they either did not trust the Australian Government, or that they did not believe the government would be able to integrate wearable technology into the pandemic response. For example, A1, A2, and A3 each discussed how they were uncertain of the privacy implications that would result from wearables from the Australian Government. A1 described how because she works for the government – at the state level – she is aware of their low IT proficiencies and capabilities, and therefore did not believe that the government has the technological capacity to use wearables. Furthermore, A3 described how she did not trust the Australian Government with her data, although she was unable to explain why. Meanwhile, while A2 believed that the government would be justified in using wearable technology to invade people's privacy in a pandemic situation, he did not trust them with his private information: *"Yeah, I mean, I'm not a huge fan of the Australian Federal Government. But I honestly think, I think, I think it would be justified. I wouldn't be comfortable with it."*

A4 and A7 stated that they trusted the government enough to trade their privacy for the freedom to quarantine at their place of residence, but this was with strict conditions such as correct data handling. Other participants discussed governmental trust and culture in countries outside Australia. For example, A4 was comfortable with the Australian Government having access to his private information using a wearable device, but said that this was highly country-dependent: *"…I suppose some governments, if I wasn't living in Australia, probably a bit different. Think about it."*

Additionally, A8 felt that governmental control over society was necessary to overcome a pandemic situation. He specifically mentioned the pandemic success of authoritative countries in the Asian region, and the failure of more liberal countries in the European region:

> *"Maybe in a lot of Asian countries. I think that's how they've been able to contain the virus as well, purely because they live in a society where it's fundamentally*

> *controlled by the government. Right? I guess, or, yeah, I think that will be very hard to have that implemented in Australia, purely because I think we value our, our privacy as well. Maybe not as much as some places in Europe, from the way I see things, but still, we value it. And then we don't easily share private data."*

In this sense, Australian participants did not speak strongly about trust in government and its links to privacy. Attitudes were largely linked to them not having faith in the government to achieve such a project, as opposed to handling their data correctly. However, some participants acknowledged that if they lived in another country than Australia, their attitudes may change.

Singapore

The topic of trust in government and culture was a strong factor in Singaporean participant responses. Their responses reflected privacy attitudes that were accepting of governmental gathering and possession of personal information, largely owing to an established culture of governmental surveillance in Singapore. Without being prompted, the vast majority of the Singaporean participants stated that they had a high level of trust in the government: not just in relation to their privacy in this wearable technology example, but in relation to daily life. Citizens already have an identity card that collects a large quantity of personal information, and so a wearable device only collects a wearer's location for a set amount of time in a window where one is supposed to be staying at home regardless. Singaporean participants understood this concept well, and had lived experience that the Singaporean Government could be trusted with their private information. Multiple participants discussed how Singapore is a collective society instead of an individualistic society, and therefore its citizens are willing to tolerate some privacy invasions to protect the community. For example, S1 stated:

> *"Regarding individualistic society versus a collective society is if you see yourself, your own rights, more important than everybody else, then that is a big issue. But you know, Asian society, we value the bigger picture, it is a small sacrifice that you have to stay home for the quarantine period."*

Furthermore, participants discussed how they are used to being tracked in Singapore. While the TraceTogether digital contact tracing has an optional physical token for those who prefer not to use their smartphone for the app, prior to the pandemic Singapore was known for being one of the most surveilled cities in the world. For example, S3 stated:

> *"I think it's always a running joke in Singapore that we say, there's really nowhere that we are not tracked. So if you take a look around, there are cameras everywhere…you're pretty much monitored all the time. Even if you go to like the MRT stations or public transport, you can probably see a camera nearby as well. Yeah, so in terms of citizen privacy, I think it just increases the surveillance kind of mentality."*

The Singaporean participants discussed how government control is not only normalised, but widely accepted. The proliferation of tracking devices and systems is a commonly known part of society, that Singaporean citizens are used to living with in their daily lives even before the pandemic. The trust in government is immense, with S1, S2, S4, S6, S8, and S10 each going into detail about the fact they trust the Singaporean Government. Therefore, the idea of a wearable device collecting personal information such as their identity and location does not phase the Singaporean respondents so greatly because there is already an entrenched culture of surveillance and a high level of trust in government. In this sense, while the Singaporean respondents are not entirely comfortable with their location being monitored with a wearable device, they nevertheless trust the Singaporean Government to execute such an initiative.

5.4.7 Data access

Who would have access to the data collected by the wearables had a significant influence on both Australian and Singaporean participants' privacy attitudes.

<u>Australia</u>

For Australians, data access was more complex than specifying that the Australian Government ought to be the only body able to access the wearable data. This extended to different groups of people having various qualms about government access to data, with an emphasis on vulnerable groups. In general, Australian participants were split over whether it should just be authorised government officials who would have access to the data, or whether it does not matter because the government has personal information such as your address anyway. In the case of the latter, participants were not fussed about who had access to the data and they also trusted that it would only be accessed in necessary circumstances, such as if a person breached their quarantine. For example, A7 stated:

> *"The government already has the information available to them, right, like they already know where you live, they can access, you know, hold your, you know, they already have like all these your tax information."*

Through this lens, data access was indeed limited to government officials, but fell short of specifying an authorisation protocol. There was no privacy breach because the government was not receiving any new information. However, multiple other participants emphasised that only a select group of officials within the government itself should have access to the data, to ensure that it was being used for the right reasons. A4 and A5 believed that governmental health officials ought to be the only workers with right of access to the data. In this sense, privacy attitudes were partially dependent on what areas of the government would have access to the wearables' data.

A large number of participants expressed concern for vulnerable people and what unfettered data access might mean. A1 and A2 were extremely sceptical of the police force, and felt deeply uncomfortable that anyone in a law enforcement position might have access to the wearables' data. A1 distinguished between someone in the police force having access to a citizen's address in comparison to someone in the electoral office. Additionally, A1, A3, A4, A6, and A10 each expressed concern that the wearable data could have negative impacts on vulnerable people. For them, while they themselves did not have privacy concerns for themselves, they recognised that this may not be the case for everyone in society. For example, domestic violence was outlined as an issue, and it may an enormous privacy impact for someone experiencing domestic violence to have their location monitored with a wearable device by the government. Participants also expressed that vulnerable groups in society may be unfairly penalised by the government having access to their location data. A4 described how two young women of colour were bullied and abused when the government discovered they had defrauded the country's existing quarantine system. He believed that while they did the wrong thing, the public outcry amounted to racism that went beyond the severity of the crime. A4 stated:

> *"Clearance is important, not the silly person at the tax office or whatever, so it has to be well guarded for privacy, not open slather like you see in the media. Some of these people who've done things that are breaching quarantine have been pretty much crucified unfairly at times because people decide to hate them. You got those three girls that went to Brisbane or two girls and they were absolutely pilloried and they were young people who didn't deserve that."*

Therefore, the information collected by a wearable could be used in ways that disproportionately affect vulnerable people in society, and as a result, these individuals may have greater privacy concerns as to who can access their data. Therefore, Australian participants' privacy attitudes were shaped by to what extent they wanted to scope the

data access within the government, and how they saw the wearable impacting the privacy and well-being of vulnerable people in Australian society.

Singapore

In Singapore, there was very little emphasis on what government data access could mean for vulnerable groups. Rather, participants saw government access as a positive thing because it could assist in the government's duty of care towards citizens, such as tracking and finding missing persons. It has been established in other themes that Singaporean citizens are used to their government having a significant amount of information gathered about them, such as through their identity card and the smart city surveillance system in place across Singapore. For the Singaporean participants, data access did not have a significant effect on their privacy attitudes. They did specify that they would not accept their data being misused, but essentially they did not feel that the information collected by the wearable posed any greater privacy risk than what the Singaporean Government knew about them already. Only one participant expressed concern for vulnerable people, and even then they did not dismiss the idea of a wearable device for quarantine: just that the government ought to ensure more safeguards for these circumstances.

6 Discussion

This section describes how the findings of this study provide an in-depth, exploratory insight into citizens' privacy attitudes towards governmental use of wearable technologies in public health crises. The COVID-19 pandemic has been used as an example of a public health crisis, and quarantine obligations are used as the setting for which wearable technologies can be used. The qualitative data gathered through semi-structured interviews were inductively analysed, resulting in seven themes that contribute to privacy attitudes. The country case examples of Australia and Singapore were used to add breadth to the findings by providing the opportunity for comparison of citizen attitudes. A summary of the differences and similarities in citizen privacy attitudes in Australia and Singapore can be found in Table 6 at 9.3. As per existing findings in cross-cultural wearable technology adoption studies, this study found similarities and differences in adoption across Australia and Singapore (see Duval & Hashizume, 2005; Yang Meier et al., 2020).

6.1 Citizen privacy attitudes

The findings answer the overarching research question by demonstrating that – for both countries – citizens' privacy attitudes towards governmental wearable technology are mediated by their existing privacy and trust attitudes. This study's findings reinforce those from Miltgen et al. (2013), who state that privacy and trust are the most important adoption factors, as opposed to general adoption factors – such as those in technology acceptance models. This is different to many existing wearable technology adoption studies, as the majority have delivered findings by using these models: while technology acceptance models may be useful to understand consumer-level adoption, they are insufficient to understand adoption in a government context. There were some similarities between Australia and Singapore: across both countries, citizens were willing to overlook the privacy concerns posed by wearable technology to manage the pandemic even though they were not fully comfortable with providing this information to the government. The greater good was seen to be more important than the protection of their individual privacy, and citizens understood the necessity for strict and effective quarantine arrangements to keep their communities free of COVID-19. This was also reflected in their desire for authorities to quickly identify and find people who breached their quarantine orders, while Australia was more divided than Singapore in this regard. Furthermore, citizens from Australia and Singapore would not be willing to accept a governmental wearable outside the COVID-19 pandemic context, indicating that the privacy invasion ought to be temporary. This reinforces findings from wearable technology adoption literature where context is a significant adoption antecedent (Gao et al., 2015; Schomakers et al., 2019).

Approaches to privacy and trust varied between Australia and Singapore, and therefore citizen privacy attitudes towards governmental wearable technology varied also. Australia and Singapore have different privacy cultures, which affected privacy attitudes to a great extent. Australia's privacy culture is stronger than that of Singapore – this is not to say that Singaporeans do not care about their data privacy, but that Australia has stronger legal protections and therefore higher public expectations of what kind of data is gathered about citizens, and by what kind of authority. Australia's Privacy Act was established in 1988, and was specially amended in May 2020 to accommodate temporary changes in data gathering and storage with the COVIDSafe app (Australian Government Department of Health, 2020b). Meanwhile, Singapore's first legal framework for privacy was established in 2012 and it is unclear how or if any special amendments were made for the TraceTogether app (Goggin, 2020). Furthermore, Singapore's lived experience as one of the world's leading smart cities and one of the most surveilled places in the world also contributes to a privacy culture where citizens are used to the government collecting their personal information.

Additional to the privacy culture, there were large differences in how Australian and Singaporean citizens understood the privacy risks posed by governmental use of wearable technology. This was a resounding theme in the wearable technology adoption literature, finding that users often did not fully comprehend the privacy risks associated with using a wearable device (Bellekens et al., 2016; Guillén-Gámez & Mayorga-Fernández, 2019; Motti & Caine, 2015). However, in a government context, Australians expressed concern over their government collecting information about them, even though they could not identify what risk this information posed to them. Meanwhile, Singaporeans had more nuanced understandings of what information their government already collected about them, and how this information could be protected and used. In this sense, Australians had weaker understandings of privacy than Singaporeans, and yet had stricter privacy attitudes towards governmental use of wearables.

Citizen privacy attitudes were shaped in both countries by citizens weighing up the perceived benefits and perceived privacy risks associated with governmental wearable technology in this public health context. This finding provides strong support for Laufer and Wolfe's (1977) privacy calculus theory, whereby people assess and compare the benefits of what they might get when sacrificing their privacy with what they may lose in the process. Other wearable technology adoption studies had found that privacy calculus theory applies in the context of wearables, finding that when people's perceived benefit is higher than the perceived privacy risk, they are more likely to adopt the technology

(Gao et al., 2015; Li et al., 2016). Furthermore, wearable technology adoption studies without a privacy calculus theory focus also identified the influence of perceived benefit on adoption (see Adapa et al., 2018; Chuah et al., 2016; Dehghani et al., 2018; K. J. Kim & Shin, 2015; Rauschnabel & Ro, 2016; Talukder et al., 2019; Wang et al., 2020). While there were slight differences in the perceived benefits for Australian and Singaporean citizens, both groups critically considered how these benefits compared to the perceived privacy risk of adopting or accepting a government-issued wearable.

For both Australians and Singaporeans, the perceived benefits of quarantining in the comfort of their own homes while also protecting the community from COVID-19 outweighed their discomfort with their governments collecting their location data. Australians valued comfort, saving money, and the greater good as important benefits, while Singaporeans had a stronger focus on the collective benefit for society. Singaporean citizens were also more likely than Australians to consider the current hotel arrangement as more comfortable or appropriate than quarantining in their homes, but this was unrelated to the perceived privacy risk of the wearable and instead linked to their personal living situation (such as having vulnerable or older family members living at home). In this sense, while citizens' privacy attitudes from both countries demonstrated various degrees of concern for governments gathering personal data through a wearable, there was also a willingness to exchange privacy for certain benefits.

It is important to here note that while the perceived benefits were similar across the countries, the perceived privacy risk and general understandings of privacy differed between countries. While Bellekens et al. (2016) found that people generally have a poor understanding of privacy risks, this was the case for Australian participants but not for Singaporean participants. Singaporeans had a stronger understanding of the privacy risks involved with the government collecting location data, and also had a larger appetite for this because of the strong surveillance culture in their society (Goggin, 2020). They understood that the privacy risk was low and they also trusted the Singaporean Government to safely and effectively gather and store the data. Meanwhile, Australians had a general distrust of the Australian Government's capacity to do this. These privacy attitudes convey Smith et al.'s (2011) privacy paradox, whereby citizens state that they are concerned about privacy, but are simultaneously willing to exchange their privacy for certain benefits. The privacy paradox is important for the adoption of governmental wearable technology in public health crises because it ignites a debate on whether privacy is an interest or a right. Privacy literature is undecided on this, but the fact that citizens exhibit cost-benefit analysis behaviours in relation to their privacy supports the argument that while privacy is an important part of people's lives, it is also exchangeable for benefits (Bennett, 1995). In the context of government-issued wearable technology,

citizens are willing to adopt it under certain circumstances because it provides them with benefits such as a more comfortable quarantine and preserving pre-pandemic lifestyles in the wider community at the seemingly small cost of temporarily sacrificing their privacy.

Therefore, this study's findings are that citizen privacy attitudes towards governmental wearable technology further support the privacy calculus theory and challenge the notion that privacy is a right as opposed to an interest. Future studies on privacy and governmental wearable technology adoption ought to draw upon the privacy calculus theory, and move away from technology acceptance models.

6.2 Data-first versus privacy-first

The findings also demonstrate that citizens do not fully understand the difference between data-first and privacy-first wearable technology architectures. On one hand, citizens tend to want their privacy to be preserved, but on the other hand they also want the government to quickly identify and find people who have breached their quarantine. Owing to the different wearable technology architectural structures, these preferences do not necessarily work simultaneously. As data-first architectures gather and store identifiable citizen data, it is easier for governments to identify and pursue individuals who have breached quarantine (Fahey & Hino, 2020; Kapa et al., 2020). Meanwhile, privacy-first architectures de-identify this information through an encryption process and public authorities would have a more complex – and presumably slower – process in identifying and pursuing individuals who have breached quarantine (Fahey & Hino, 2020; Kapa et al., 2020). There were strong differences between Australian and Singaporean citizen preferences in this regard. In Australia, citizens expressed a preference for the government collecting de-identified data on those wearing the device, yet were divided on whether it should be easy or difficult to identify and catch quarantine violators. Meanwhile, Singaporean citizens were divided on whether the device should gather and store identified or de-identified information, and exhibited an almost unanimous preference for the government to be able to quickly catch quarantine violators. Therefore, citizens have preferences for elements of both data-first and privacy-first architectures.

These findings indicate that citizens want to reap the benefits of both types of architecture: to have their privacy preserved as much as possible when wearing the devices, but for the government to also be able to quickly identify and catch those who decide to breach their quarantine orders. Therefore, when developing wearable technology architectures, governments cannot necessarily take citizen preferences at face value. Wearable technology literature has demonstrated that there are many potential security and privacy risks in wearables (see Cusack et al., 2017; Goyal et al., 2016; Hiremath et al., 2014; Yaqoob et al., 2019): however, Australians were largely unable to explain what privacy

risks may occur when the government collected their data through a wearable and some did not have faith that the government could sufficiently manage these risks. While Singaporeans had a stronger understanding of these risks, they also expressed a high degree of trust in their government that these security and privacy risks would not occur. Therefore, citizen privacy attitudes do not differ in relation to whether the wearable technology operates as data-first or privacy-first: consistent with Miltgen et al.'s (2013) findings, their attitudes revolve around their existing privacy and trust attitudes. These attitudes are highly culture dependent, as well as being dependent on the severity of the public health crisis in question.

6.3 Mandatory versus optional

Finally, the findings demonstrate that citizen privacy attitudes differ in relation to whether the wearable technology is made mandatory or optional by the government. While this study focused on adoption, the analysis identified that acceptance is a relevant focus in addition to wearable adoption. If the device is mandatory, citizens have no choice in whether they adopt it or not and the analytical focus then lies on whether they accept the technology. If the device is optional, this gives citizen a choice as to whether or not they adopt the technology. This paper's literature review established that all wearable technology adoption studies to date have focused on voluntary wearable adoption. This is because governmental uses of wearable technologies up until the COVID-19 pandemic have been in a criminal behaviour management setting (Schwartz, 2020). The decision by governments throughout the world to use wearable technologies as a pandemic management tool demonstrates a need for academic research into wearable technology adoption, and this study takes a first step in adding a building block to this budding research area. The distinction between the adoption of optional devices and the acceptance of mandatory devices is important because citizens have different approaches depending on the level of choice associated with the devices.

In Australia, citizens felt uncomfortable with not having a choice despite understanding the need for effective technological solutions in the government's pandemic management approach. Having a choice was a strong factor in how comfortable they felt with using the wearable technology. Not having control over whether or not they used the device led to comparisons between public health wearables and wearables to facilitate home detention arrangements. Australians expressed an overall concern for how these devices could affect vulnerable people's sense of safety: this resonates with Payne et al.'s (2009) research that found that people of colour have greater fears of inequalities as a result of government electronic monitoring. Meanwhile, Singaporeans expressed a strong preference for mandatory devices despite feeling similarly uncomfortable with the lack

of choice: this was consistent with their desire to protect Singapore's way of life during the pandemic. Therefore, if government-issued wearable devices are mandatory in public health crises, citizens' acceptance from a privacy perspective revolves around their level of comfort. Singaporeans felt more comfortable with the situation because of their high levels of trust in government and their society's pre-existing surveillance culture. Australians were less comfortable because of their lower level of trust in government and acknowledgement of the potentially greater impact on vulnerable people in society. A further finding of this study is that vulnerable people – such as those experiencing or at risk of domestic violence – may require additional data access protections to ensure their location data is secure. This finding reflects Xu et al.'s (2009) statement that different wearable technology user groups require different privacy approaches.

6.4 Theoretical implications

This study provides a range of theoretical implications that ought to be addressed and incorporated into future research. Firstly, this is the first study that has investigated wearable technology adoption in a public sector context. All prior studies have focused on this through a consumer lens, where users make a voluntary, personal decision whether or not they wish to adopt a wearable. In a government context, many established adoption factors are irrelevant and therefore are not suitable for public sector contexts. For example, these established adoption factors have resulted in recommendations such as ensuring wearable devices are fashionable and comfortable (Adapa et al., 2018; Chuah et al., 2016; Kim & Park, 2019; Rauschnabel & Ro, 2016), and are appropriately priced (Dehghani et al., 2018; Kim & Shin, 2015; Wen et al., 2017). This study has demonstrated these factors are not important in a government context, and instead, researchers ought to focus on adoption factors such as perceived benefit, perceived privacy risk, and context. This study has also validated privacy calculus theory in a public sector context: while past wearable adoption studies have demonstrated this theory's applicability in a consumer setting, this study's research findings do so in a government setting.

Secondly, because governments may make wearables mandatory or optional, this study differentiates between wearable technology acceptance and adoption. Wearable technology adoption literature has often considered technology acceptance and adoption to be one and the same: in a government context, this is not the case. Furthermore, technology acceptance models such as TAM and UTAUT assume voluntariness of use, which may not be the case for public sector rollouts. For public sector use, optional use is associated with adoption and has strong links with factors such as trust in government, perceived benefit, perceived privacy risk, and context. Meanwhile, mandatory use is associated with acceptance and is predominantly linked to trust in government. Future

research on governmental use of wearable technology should make clear whether device use is mandatory or optional, as this will have different theoretical implications. Finally, this study reiterates the need for cross-cultural wearable technology adoption studies. This study responds to an identified research need that more cross-country comparisons ought to be conducted to understand the nuances of why people adopt wearable technology (Chau et al., 2019; Gao et al., 2015; Kim & Shin, 2015; Paluch & Tuzovic, 2019). The varied results between Australia and Singapore confirm the continued need to investigate wearable technology adoption across different countries and/or cultures in order to develop more nuanced frameworks and conceptual models. This is a finding that applies to both governmental and consumer contexts. Overall, these findings contribute to broadening the wearable technology adoption literature focus to investigate beyond the consumer context, and to explore the public sector context. There are different acceptance and adoption factors to consider, and as public health crises such as COVID-19 can occur on national and global scales, it is crucial that academia is prepared with deep insights before these crises hit.

6.5 Practical implications

This study also provides a range of practical implications that governments ought to consider when planning to use wearable technology in public health crises. This is to ensure ideal levels of adoption and/or acceptance amongst citizens. While wearable technology has been identified by technology and health experts as having an important role to play in managing and mitigating the effects of public health crises (Nasajpour et al., 2020; Sun et al., 2020; Whitelaw et al., 2020), governments have practical considerations to ensure that they implement these devices in a way that citizens accept and respect. This study demonstrated citizens' willingness to temporarily sacrifice their privacy for the greater good. However, this sacrifice was dependent on numerous factors: the device could only be used for a limited time period, the device ought to save citizens money or provide them convenience in some way, and the data gathered by the device ought to be subject to high security standards and accessible only to authorised government officials. Furthermore, this study's findings demonstrate that the Australian Government ought to explore the possibility of complementing hotel quarantine arrangements with wearable devices at home, with significant financial savings to the citizen.

Additionally, high levels of trust in government is a necessary acceptance and adoption antecedent. For governments to successfully rollout wearable technology as a quarantine monitoring tool in public health crises, they will need to demonstrate how they have addressed the above factors. If citizens' benefit from using the devices does not outweigh

their perceived privacy risk, governments are unlikely to achieve appropriate levels of acceptance and/or adoption. Governments with lower or volatile levels of trust in government ought to expect citizen resistance, and should incorporate this into their decision-making process and rollout strategy.

6.6 Limitations

This thesis is subject to a number of limitations. These issues do not delegitimise this study's findings and proposed directions for future research, but must be acknowledged when evaluating the validity of the research design's outputs. Firstly, the results are subject to the unavoidable limitations of exploratory studies. This type of research design is qualitative, rather than quantitative by nature (Stebbins, 2001): while this was useful to create a foundation for expanding wearable technology adoption research beyond the consumer perspective and into a public sector perspective, the findings are not statistically generalisable. Qualitative data can suffer from bias and is subject to interpretation, meanwhile using quantitative data is more useful to detect patterns and generalise findings to wider populations than the sample size (Stebbins, 2001). In this sense, while exploratory research is especially useful to understand new topics – such as the one outlined in this study –further research and validation is recommended to build on the findings..

Additionally, while the snowball sampling method was the most appropriate way to source interviewees, this method does not stand without criticism. The final sample has an inherent risk of bias, because interviewees are linked with each other and the author also had to rely on current participants' willingness to assist in recruiting other wearable users to interview (Naderifar et al., 2017). The author also encountered issues with recruiting interview participants within the time scope of the study. Snowball sampling methods are known to be a gradual process and more time-consuming than other sampling strategies, and this must be taken into account when designing studies (Biernacki & Waldorf, 1981; Naderifar et al., 2017). While data saturation was achieved after 20 interviews, it is nevertheless important to mention that the limited time period to conduct this study added complications to who could participate in the research.

There are also notable limitations in relation to the sample's representativeness. Firstly, no females over 46 years of age were included from either country, and only one male over 46 years of age from Singapore was interviewed. This issue of representativeness is a general issue in country-wide analyses (Yang Meier et al., 2020), and past wearable technology adoption studies have narrowed their sample sizes using parameters such as age, gender, and experience with technology. Beyond this study's variables of country and wearable experience, other variables such as age and gender may influence citizens'

privacy attitudes. Assessing the influence of age and gender was not a goal of this study and was therefore not included in the analysis, but this does not mean that these variables did not influence privacy attitudes. Furthermore, the author selected experienced wearable technology users and chose not to include non-experienced users. While this decision was justified by previous studies being undecided on how experience influences privacy attitudes (see Koo & Fallon, 2018; Spagnolli et al., 2014) and to ensure that interviewees would understand the interview questions, this study lacks the perspective of people who have no experience with wearables. Past wearable technology research has identified that focusing strictly on users has its limitations, namely that identified adoption factors may not be generalisable beyond this group to non-users (see Kim & Shin, 2015; Paluch & Tuzovic, 2019; Sergueeva et al., 2020). Additionally, existing technology adoption research has been criticised for being fragmented (Bagozzi, 2007): while this study makes a meaningful contribution to the wearable technology adoption literature, it nevertheless requires future research attention that addresses different countries and wider ranges of variables.

These criticisms towards the study's representativeness limits the generalisability of this study's research findings because governments may mandate or provide the option of wearable technology to any of their citizens, not just the sample within this research study. With 20 interviews conducted in total, this qualitative data is useful for theoretical – and not statistical – generalisability. As such, the author emphasises that this is an exploratory study that lays the groundwork for future research. Therefore, future studies ought to consider these variables in their analyses to establish their impact on people's willingness to adopt governmental wearable technology. Authors wishing to further address governmental use of wearable technology ought to build upon this qualitative study with quantitative analyses – such as through a survey, similar to the majority of wearable technology adoption studies (see Table 5) – or more in-depth qualitative analyses.

While wearable technology can be used by governments for a variety of functions other than enforcing quarantine – such as monitoring COVID-19 patients' vital signs or enforcing social distancing – the author has selected the focus on quarantine to keep the research scope achievable. The findings of this study are therefore relevant in a quarantine context, and are not necessarily applicable beyond this (particularly noting that this study did not investigate privacy attitudes in a health context). Future research ought to also investigate the wider uses for wearables in the public sector, beyond a quarantine context.

Additionally, the data is not longitudinal and interviews occurred at a time where COVID-19 restrictions in both Australia and Singapore were not strict. The interviews took place in late March and early April 2021, and by the time of submission in late May 2021,

Singapore and a part of Australia were subject to reinstated COVID-19 restrictions of varying degrees of strictness. A longitudinal qualitative study was not feasible in light of this study's time restrictions, but such a study may have provided more in-depth insights to citizens' privacy attitudes. An additional limitation is applicable to Australia, where the author did not place further geographic restrictions on research participants: this was problematic because the State of Victoria was subject to the country's strictest lockdown for four months in 2020, whereas the rest of Australia had a very limited lockdown experience. This meant that Victorian respondents had a different perspective on COVID-19 than respondents from the rest of Australia. The author recommends that future studies consider geographic spread during the sampling strategy's scoping phase.

Despite these limitations, this study offers new insights into a highly topical and relevant area of wearable technology use that has never been researched in this way before. The seven themes that emerged from the interviews are a promising foundation for further research into governmental use of wearable technology, and for governments to critically consider when rolling out wearable technology in a quarantine environment. Without such research, researchers and governments would be forced to rely on established wearable adoption antecedents, and this study has demonstrated that not all of these factors are relevant in a public sector context.

7 Conclusion

This study investigated citizens' privacy attitudes towards adopting governmental use of wearable technology in public health crises, with an addition focus on data-first and privacy-first structures, and mandatory or optional use. The research gap present at the beginning of this study was immense: to date, no research had explored wearable technology adoption in a public sector setting. This was problematic because – while governments around the world had employed wearables in criminal justice settings – the COVID-19 pandemic encouraged a great deal of ad hoc technological innovations in order to mitigate the effect of the virus. Public health experts advised that wearable technology may be a highly useful tool in situations such as enforcing quarantine, measuring people's vital signs, and ensuring social distancing. However, the privacy implications of governments using these technologies were significant and there was no concrete evidence base to support such an approach in the public sector. To keep the research scope manageable, this thesis focused on wearables as a quarantine enforcement tool in Australia and Singapore.

By interviewing 20 citizens across Australia and Singapore, this study obtained valuable insights into what is important for governments to consider when deciding to roll out wearable technology in crises such as COVID-19. Furthermore, that privacy attitudes can differ based on country and culture. The inductive analysis found that there are seven themes that influence citizens' privacy attitudes: perceived benefit, perceived privacy risk, context, time, choice, trust in government, and data access. This study identified important similarities and differences in privacy attitudes between citizens from Australia and Singapore. Overall, Australia has a stronger privacy culture than Singapore and this affected how citizens from the respective countries perceived adopting governmental wearable technology. Singapore's established culture of mass governmental surveillance created an ecosystem where Singaporeans were trusting of the government to collect, store, and use their data responsibly. While Singaporeans were not totally comfortable privacy-wise with their government using wearable technology to enforce quarantine, the vast majority agreed to it under the unique pandemic circumstances. Meanwhile, Australians had weaker understandings of privacy and also stricter privacy attitudes, based on an established culture of privacy and lower use of innovative technology by government.

The privacy calculus theory was found to be an effective theoretical framework to assess citizens' intention to accept or adopt governmental wearable technology, as for both Australia and Singapore, citizens weighed up the perceived benefits and perceived privacy risks when considering their appetite for wearable technology in a quarantine

setting. Additionally, themes such as the pandemic context, length of time and their choice in wearing the device, their trust in government to effectively implement the technology, and who would have access to data all had strong relationships with their privacy attitudes.

Citizens do not fully understand the difference between data-first and privacy-first wearable technology architectures. In order to suit their desired benefits and mitigate their privacy concerns, citizens from Australia and Singapore demonstrated they wanted to benefit as much as possible from a governmental wearable device and sacrifice as little of their privacy as was feasible. Therefore, governments may not be able to accommodate citizen preferences when designing policies for wearable technology and must instead be prepared to face and navigate citizens' pre-existing privacy and trust attitudes.

Additionally, whether a device is made mandatory or optional impacts privacy attitudes. The difference between acceptance and adoption was important, as mandatory devices can be accepted while optional devices can be adopted. Australian citizens preferred to have a choice in whether they adopt a governmental wearable, while Singaporean citizens preferred the device to be mandatory in order to maximise its effectiveness. The context of the COVID-19 crisis evoked a strong affinity for the greater good, demonstrating that while the devices posed some perceived privacy risks, citizens were nevertheless willing to accept or adopt the devices under the circumstances.

Other key findings included that while wearable technology adoption studies to date have tended to frame their research with technology acceptance models, this is not suitable for a government context. For adoption studies in a public sector context, researchers ought to draw upon privacy and trust literature, as opposed to technology acceptance models. Furthermore, governments seeking to use wearables in public health crises ought to critically consider this study's seven themes in order to facilitate greater acceptance or adoption. As an exploratory study, the findings of this thesis provide a strong foundation for future research to further investigate wearable technology adoption in the public sector using quantitative approaches, or with different country case studies.

8 References

Adapa, A., Nah, F. F.-H., Hall, R. H., Siau, K., & Smith, S. N. (2018). Factors influencing the adoption of smart wearable devices. *International Journal of Human–Computer Interaction*, *34*(5), 399–409. https://doi.org/10.1080/10447318.2017.1357902

Alrige, M., & Chatterjee, S. (2015). Toward a taxonomy of wearable technologies in healthcare. In B. Donnellan, M. Helfert, J. Kenneally, D. VanderMeer, M. Rothenberger, & R. Winter (Eds.), *New horizons in design science: broadening the research agenda* (pp. 496–504). Springer International Publishing. https://doi.org/10.1007/978-3-319-18714-3_43

Apple. (2020, September 15). *Singapore and Apple partner on national health initiative using Apple Watch*. Retrieved March 14, 2021 from https://www.apple.com/newsroom/2020/09/singapore-and-apple-partner-on-national-health-initiative-using-apple-watch/

Australian Government Attorney-General's Department. (2021). *COVIDSafe legislation*. Retrieved March 16, 2021 from https://www.ag.gov.au/rights-and-protections/privacy/covidsafe-legislation

Australian Government Department of Health. (2020a). *National review of hotel quarantine*. Retrieved March 16, 2021 from https://www.health.gov.au/resources/publications/national-review-of-hotel-quarantine

Australian Government Department of Health. (2020b). *Privacy policy*. Retrieved March 10, 2021 from https://covidsafe.gov.au/privacy-policy.html

Australian Signals Directorate. (2020). *Internet of things devices*. Australian Cyber Security Centre. Retrieved February 16, 2021 from https://www.cyber.gov.au/acsc/view-all-content/advice/internet-things-devices

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: study design and implementation for novice researchers. *The Qualitative Report*, *13*(4), 544–559. https://doi.org/10.46743/2160-3715/2008.1573

Bagozzi, R. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems*, *8*(4), 244–254. https://doi.org/10.17705/1jais.00122

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, *35*(4),

1017–1041. https://doi.org/10.2307/41409971

Bellekens, X., Nieradzinska, K., Bellekens, A., Seeam, P., Hamilton, A., & Seeam, A. (2016). A study on situational awareness security and privacy of wearable health monitoring devices. *International Journal on Cyber Situational Awareness*, *1*(1), 1–25. https://www.researchgate.net/profile/Xavier_Bellekens/publication/309987479_A_Study_on_Situational_Awareness_Security_and_Privacy_of_Wearable_Health_Monitoring_Devices/links/5827374d08ae5c0137edd4b0/A-Study-on-Situational-Awareness-Security-and-Privacy-of-Wearable-Health-Monitoring-Devices.pdf

Bennett, C. J. (1995). *The political economy of privacy: a review of the literature*. Center for Social and Legal Research.

Berglund, M. E., Duvall, J., & Dunne, L. E. (2016). A survey of the historical scope and current trends of wearable technology applications. *Proceedings of the 2016 Association for Computing Machinery International Symposium on Wearable Computers*, 40–43. https://doi.org/10.1145/2971763.2971796

Bhattacharya, D., & Ramos, L. (2021). COVID-19: privacy and confidentiality issues with contact tracing apps. *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2009–2018. https://doi.org/10.24251/HICSS.2021.246

Biernacki, P., & Waldorf, D. (1981). Snowball sampling: problems and techniques of chain referral sampling. *Sociological Methods & Research*, *10*(2), 141–163. https://doi.org/10.1177/004912418101000205

Brodeur, A., Clark, A. E., Flèche, S., & Powdthavee, N. (2020). *Assessing the impact of the coronavirus lockdown on unhappiness, loneliness, and boredom using Google Trends*. The SAO/NASA Astrophysics Data System. Retrieved May 16, 2021 from https://ui.adsabs.harvard.edu/abs/2020arXiv200412129B/abstract

Brooks, S. K., Webster, R. K., Smith, L. E., Woodland, L., Wessely, S., Greenberg, N., & Rubin, G. J. (2020). The psychological impact of quarantine and how to reduce it: rapid review of the evidence. *The Lancet*, *395*(10227), 912–920. https://doi.org/10.1016/S0140-6736(20)30460-8

Bülow, W. (2014). Electronic monitoring of offenders: an ethical review. *Science and Engineering Ethics*, *20*(2), 505–518. https://doi.org/10.1007/s11948-013-9462-3

Camara, C., Peris-Lopez, P., & Tapiador, J. E. (2015). Security and privacy issues in implantable medical devices: a comprehensive survey. *Journal of Biomedical*

Informatics, *55*, 272–289. https://doi.org/10.1016/j.jbi.2015.04.007

Canhoto, A. I., & Arp, S. (2017). Exploring the factors that support adoption and sustained use of health and fitness wearables. *Journal of Marketing Management*, *33*(1–2), 32–60. https://doi.org/10.1080/0267257X.2016.1234505

Chatterjee, A., Aceves, A., Dungca, R., Flores, H., & Giddens, K. (2016). Classification of wearable computing: a survey of electronic assistive technology and future design. *2016 Second International Conference on Research in Computational Intelligence and Communication Networks*, 22–27. https://doi.org/10.1109/ICRCICN.2016.7813545

Chau, K. Y., Lam, M. H. S., Cheung, M. L., Tso, E. K. H., Flint, S. W., Broom, D. R., Tse, G., & Lee, K. Y. (2019). Smart technology for healthcare: exploring the antecedents of adoption intention of healthcare wearable technology. *Health Psychology Research*, *7*(1), 33–39. https://doi.org/10.4081/hpr.2019.8099

Ching, K. W., & Singh, M. M. (2016). Wearable technology devices security and privacy vulnerability analysis. *International Journal of Network Security & Its Applications*, *8*(3), 19–30. https://doi.org/10.5121/ijnsa.2016.8302

Chuah, S. H.-W., Rauschnabel, P. A., Krey, N., Nguyen, B., Ramayah, T., & Lade, S. (2016). Wearable technologies: the role of usefulness and visibility in smartwatch adoption. *Computers in Human Behavior*, *65*, 276–284. https://doi.org/10.1016/j.chb.2016.07.047

Colizza, V., Grill, E., Mikolajczyk, R., Cattuto, C., Kucharski, A., Riley, S., Kendall, M., Lythgoe, K., Bonsall, D., Wymant, C., Abeler-Dörner, L., Ferretti, L., & Fraser, C. (2021). Time to evaluate COVID-19 contact-tracing apps. *Nature Medicine, 27*, 361–362. https://doi.org/10.1038/s41591-021-01236-6

Coorevits, L., & Coenen, T. (2016). The rise and fall of wearable fitness trackers. *Academy of Management Proceedings*, 1–24. https://doi.org/10.5465/ambpp.2016.17305abstract

Cusack, B., Antony, B., Ward, G., & Shaunak M. (2017). Assessment of security vulnerabilities in wearable devices. *The Proceedings of 15th Australian Information Security Management Conference*, *5–6*, 42–48. https://doi.org/10.4225/75/5A84E6C295B44

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

DeCew, J. (2018). Privacy. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Spring 2018 ed.). Metaphysics Research Lab, Stanford University. Retrieved from https://plato.stanford.edu/archives/spr2018/entries/privacy/

Dehghani, M., Kim, K. J., & Dangelico, R. M. (2018). Will smartwatches last? Factors contributing to intention to keep using smart wearable technology. *Telematics and Informatics*, *35*(2), 480–490. https://doi.org/10.1016/j.tele.2018.01.007

Ding, X., Clifton, D., Ji, N., Lovell, N. H., Bonato, P., Chen, W., Yu, X., Xue, Z., Xiang, T., Long, X., Xu, K., Jiang, X., Wang, Q., Yin, B., Feng, G., & Zhang, Y.-T. (2021). Wearable sensing and telehealth technology with potential applications in the coronavirus pandemic. *IEEE Reviews in Biomedical Engineering*, *14*, 48–70. https://doi.org/10.1109/RBME.2020.2992838

Duval, S., & Hashizume, H. (2005). Perception of Wearable Computers for Everyday Life by the General Public: Impact of Culture and Gender on Technology. In L. T. Yang, M. Amamiya, Z. Liu, M. Guo, & F. J. Rammig (Eds.), *Embedded and ubiquitous computing EUC 2005* (pp. 826–835). Springer, Berlin, Heidelberg. https://doi.org/10.1007/11596356_82

Elkhodr, M., Mubin, O., Iftikhar, Z., Masood, M., Alsinglawi, B., Shahid, S., & Alnajjar, F. (2021). Technology, privacy, and user opinions of COVID-19 mobile apps for contact tracing: systematic search and content analysis. *Journal of Medical Internet Research*, *23*(2), 1–17. https://doi.org/10.2196/23467

European Commission. (2019). *The internet of things*. Retrieved February 16, 2021 from https://ec.europa.eu/digital-single-market/en/internet-of-things

Fahey, R. A., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*, *55*, 1–5. https://doi.org/10.1016/j.ijinfomgt.2020.102181

Feiner, S. K. (1999). The importance of being mobile: some social consequences of wearable augmented reality systems. *Proceedings 2nd IEEE and ACM International Workshop on Augmented Reality*, 145–148. https://doi.org/10.1109/IWAR.1999.803815

Fitbit. (2019, August 21). *Fitbit Collaborates with Singapore's Health Promotion Board on Population-Based Public Health Initiative in Singapore*. Retrieved March 14, 2021 from https://investor.fitbit.com/press-releases/press-release-details/2019/Fitbit-Collaborates-with-Singapores-Health-Promotion-Board-on-Population-Based-Public-Health-Initiative-in-Singapore/default.aspx

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry*, *12*(2), 219–245. https://doi.org/10.1177/1077800405284363

Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems*, *115*(9), 1704–1723. https://doi.org/10.1108/IMDS-03-2015-0087

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal*, *204*(6), 291–295. https://doi.org/10.1038/bdj.2008.192

Godfrey, A., Hetherington, V., Shum, H., Bonato, P., Lovell, N. H., & Stuart, S. (2018). From A to Z: wearable technology explained. *Maturitas*, *113*, 40–47. https://doi.org/10.1016/j.maturitas.2018.04.012

Goggin, G. (2020). COVID-19 apps in Singapore and Australia: reimagining healthy nations with digital technology. *Media International Australia*, *177*(1), 61–75. https://doi.org/10.1177/1329878X20949770

Government of Singapore. (2020). *TraceTogether privacy safeguards*. Retrieved March 10, 2021 from https://www.tracetogether.gov.sg/common/privacystatement

Goyal, R., Dragoni, N., & Spognardi, A. (2016). Mind the tracker you wear: a security analysis of wearable health trackers. *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, 131–136. https://doi.org/10.1145/2851613.2851685

Gregor, B., & Gwiaździński, E. (2020). Wearable technology in the perception of young consumers. *Marketing of Scientific and Research Organizations*, *36*(2), 61–76. https://doi.org/10.2478/minib-2020-0017

Guillén-Gámez, F. D., & Mayorga-Fernández, M. J. (2019). Empirical study based on the perceptions of patients and relatives about the acceptance of wearable devices to improve their health and prevent possible diseases. *Mobile Information Systems*, *2019*, 1–12. https://doi.org/10.1155/2019/4731048

Harari, Y. N. (2020, March 20). *The world after coronavirus*. Financial Times. Retrieved December 29, 2020 from https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Heffernan, T. (2021, January 20). *Lockdown, quarantine and self-isolation: how different COVID restrictions affect our mental health*. The Conversation. Retrieved May 18, 2021 from http://theconversation.com/lockdown-quarantine-and-self-isolation-how-different-covid-restrictions-affect-our-mental-health-

153595

Hiremath, S., Yang, G., & Mankodiya, K. (2014). Wearable internet of things: concept, architectural components and promises for person-centered healthcare. *Proceedings of the 4th International Conference on Wireless Mobile Communication and Healthcare*, 304–307. https://doi.org/10.4108/icst.mobihealth.2014.257440

IDC Corporate USA. (2020, December 2). *Shipments of wearable devices leap to 125 million units, up 35.1% in the third quarter*. Retrieved March 14, 2021 from https://www.idc.com/getdoc.jsp?containerId=prUS47067820

Immigration and Checkpoints Authority Singapore. (2020, August 3). *Media release detail: all incoming travellers, including returning residents, long-term pass holders, work pass holders and their dependants, serving their stay-home notice outside of dedicated facilities to don electronic monitoring device*. Retrieved March 15, 2021 from https://www.ica.gov.sg/news-and-publications/media-releases/media-release/all-incoming-travellers-including-returning-residents-long-term-pass-holders-work-pass-holders-and-their-dependants-serving-their-stay-home-notice-outside-of-dedicated-facilities-to-don-electronic-monitoring-device

Immigration and Checkpoints Authority Singapore. (2021). *SHN Electronic Monitoring Device*. SafeTravel. Retrieved February 16, 2021 from https://safetravel.ica.gov.sg/health/shn-monitoring

Jeong, S. C., Kim, S.-H., Park, J. Y., & Choi, B. (2017). Domain-specific innovativeness and new product adoption: a case of wearable devices. *Telematics and Informatics*, *34*(5), 399–412. https://doi.org/10.1016/j.tele.2016.09.001

Judd, B. (2021, February 13). *How other countries handle returned travellers without hotel quarantine*. ABC News. Retrieved February 16, 2021 from https://www.abc.net.au/news/2021-02-14/what-can-we-learn-about-hotel-quarantine-from-around-the-world/13143546

Kalantari, M. (2017). Consumers' adoption of wearable technologies: Literature review, synthesis, and future research agenda. *International Journal of Technology Marketing, 12*(3), 274–307. https://doi.org/10.1287/d553d554-3a61-4194-ab18-7a95da29fc7e

Kapa, S., Halamka, J., & Raskar, R. (2020). Contact tracing to manage COVID-19 spread—balancing personal privacy and public health. *Mayo Clinic*

Proceedings, *95*(7), 1320–1322. https://doi.org/10.1016/j.mayocp.2020.04.031

Kapoor, V., Singh, R., Reddy, R., & Churi, P. (2020). Privacy issues in wearable technology: an intrinsic review. *Proceedings of the International Conference on Innovative Computing & Communications*, 1–7. https://doi.org/10.2139/ssrn.3566918

Karahanoğlu, A., & Erbuğ, Ç. (2011). Perceived qualities of smart wearables: determinants of user acceptance. *Proceedings of the 2011 Conference on Designing Pleasurable Products and Interfaces*, 1–8. https://doi.org/10.1145/2347504.2347533

Karp, P. (2020, October 23). *Apps and ankle bracelets options for returning travellers instead of hotel quarantine*. The Guardian. Retrieved February 16, 2021 from http://www.theguardian.com/australia-news/2020/oct/23/apps-and-ankle-bracelets-options-for-returning-travellers-instead-of-hotel-quarantine

Kim, D., Park, K., Park, Y., & Ahn, J.-H. (2019). Willingness to provide personal information: perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273–281. https://doi.org/10.1016/j.chb.2018.11.022

Kim, J., & Park, E. (2019). Beyond coolness: predicting the technology adoption of interactive wearable devices. *Journal of Retailing and Consumer Services*, *49*, 114–119. https://doi.org/10.1016/j.jretconser.2019.03.013

Kim, K. J., & Shin, D.-H. (2015). An acceptance model for smart watches: implications for the adoption of future wearable technology. *Internet Research*, *25*(4), 527–541. https://doi.org/10.1108/IntR-05-2014-0126

Kirby, B., Kirby, A., & Birch, J.-L. (2016). Wearable tech: why architectures matter. *Proceedings of the 30th International BCS Human Computer Interaction Conference.* https://doi.org/10.14236/ewic/HCI2016.69

Kitchin, R. (2020). Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity*, *24*(3), 1–20. https://doi.org/10.1080/13562576.2020.1770587

König, M., & Winkler, A. (2021). COVID-19: lockdowns, fatality rates and GDP growth. *Intereconomics*, *56*(1), 32–39. https://www.intereconomics.eu/contents/year/2021/number/1/article/covid-19-lockdowns-fatality-rates-and-gdp-growth.html

Koo, S. H., & Fallon, K. (2018). Explorations of wearable technology for tracking self and others. *Fashion and Textiles*, *5*(1), 1–16. https://doi.org/10.1186/s40691-

017-0123-z

Krauss, J. (2020, April 14). *Israeli police use drones to check in on virus patients*. AP NEWS. Retrieved November 6, 2020 from https://apnews.com/article/68dce1a1fc8be75618a63db16fcf2804

Lee, L., Lee, J., Egelman, S., & Wagner, D. (2016). Information disclosure concerns in the age of wearable computing. *Proceedings of the NDSS Workshop on Usable Security*, 1–10. https://www.icsi.berkeley.edu/icsi/node/5542

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, *88*, 8–17. https://doi.org/10.1016/j.ijmedinf.2015.12.010

Loncar-Turukalo, T., Zdravevski, E., Machado da Silva, J., Chouvarda, I., & Trajkovik, V. (2019). Literature on wearable technology for connected health: scoping review of research trends, advances, and barriers. *Journal of Medical Internet Research*, *21*(9), 1–23. https://doi.org/10.2196/14017

Lowy Institute. (2021, March 13). *COVID performance index*. Retrieved March 10, 2021 from https://interactives.lowyinstitute.org/features/covid-performance/

Malmivaara, M. (2009). The emergence of wearable computing. In J. McCann & D. Bryson (Eds.), *Smart clothes and wearable Technology* (pp. 3–24). Woodhead Publishing Limited. https://doi.org/10.1533/9781845695668.1.3

Mao, F. (2021, February 8). COVID: why Australia's 'world-class' quarantine system has seen breaches. *BBC News*. Retrieved April 15, 2021 from https://www.bbc.com/news/world-australia-55929180

Martinez-Martin, N., Wieten, S., Magnus, D., & Cho, M. K. (2020). Digital contact tracing, privacy, and public health. *Hastings Center Report*, *50*(3), 43–46. https://doi.org/10.1002/hast.1131

McDonald, K. (2020, November 11). *South Western Sydney, Howard Springs using armband sensor for COVID monitoring*. Pulse+IT. Retrieved April 16, 2021 from https://www.pulseitmagazine.com.au:443/australian-ehealth/5809-south-western-sydney-howard-springs-using-armband-sensor-for-covid-monitoring

Mewara, D., Purohit, P., & Rathore, B. P. S. (2016). Wearable devices applications & its future. *International Journal For Technological Research in Engineering*, 59–64. https://www.ijtre.com/images/scripts/16113.pdf

Miltgen, C. L., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: integrating the "Big 3" of technology acceptance with privacy context. *Decision Support Systems*, *56*, 103–114. https://doi.org/10.1016/j.dss.2013.05.010

Min, A. H. (2021, February 2). *More than 360 COVID-19 stay-home notice breaches and 130 quarantine order violations so far: MHA*. CNA. Retrieved April 15, 2021 from https://www.channelnewsasia.com/news/singapore/covid-19-shn-quarantine-order-breach-crime-mha-14094458

Ministry of Foreign Affairs, Singapore. (2020). *Travellers to bear costs of COVID-19 tests and stay at Dedicated SHN Facilities*. Retrieved April 16, 2021 from http://www.mfa.gov.sg/Overseas-Mission/Mumbai/Announcements/Travellers-to-bear-costs-of-COVID-19-tests-and-stay-at-Dedicated-SHN-Facilities

Mordor Intelligence. (2020). *Wearable technology market size, share, trends, analysis 2020-25*. Retrieved February 22, 2021 from https://www.mordorintelligence.com/industry-reports/wearable-technology-market

Motti, V. G., & Caine, K. (2015). Users' privacy concerns about wearables: impact of form factor, sensors and type of data collected. In M. Brenner, N. Christin, B. Johnson, & K. Rohloff (Eds.), *Financial cryptography and data security* (pp. 231–244). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48051-9

Muftić, L. R., Payne, B. K., & Maljević, A. (2015). Bosnian and American students' attitudes toward electronic monitoring: is it about what we know or where we come from? *International Journal of Offender Therapy and Comparative Criminology*, *59*(6), 611–630. https://doi.org/10.1177/0306624X13516286

Murphy, K. (2020, August 24). *Essential poll: Australians back strong surveillance and banning all international flights to curb Covid*. The Guardian. Retrieved February 16, 2021 from http://www.theguardian.com/australia-news/2020/aug/25/essential-poll-australians-back-strong-surveillance-and-banning-all-international-flights-to-curb-covid

Naderifar, M., Goli, H., & Ghaljaie, F. (2017). Snowball sampling: a purposeful method of sampling in qualitative research. *Strides in Development of Medical Education*, *14*(3), 1–6. https://doi.org/10.5812/sdme.67670

Nasajpour, M., Pouriyeh, S., Parizi, R. M., Dorodchi, M., Valero, M., & Arabnia, H. R. (2020). Internet of things for current COVID-19 and future pandemics: an exploratory study. *Journal of Healthcare Informatics Research*, *4*(4), 325–364.

https://doi.org/10.1007/s41666-020-00080-6

Nasir, S., & Yurder, Y. (2015). Consumers' and physicians' perceptions about high tech wearable health products. *Procedia - Social and Behavioral Sciences*, *195*, 1261–1267. https://doi.org/10.1016/j.sbspro.2015.06.279

Nelson, C., Lurie, N., Wasserman, J., & Zakowski, S. (2007). Conceptualizing and defining public health emergency preparedness. *American Journal of Public Health*, *97*(S1), S9–S11. https://doi.org/10.2105/AJPH.2007.114496

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Noy, C. (2008). Sampling knowledge: the hermeneutics of snowball sampling in qualitative research. *International Journal of Social Research Methodology*, *11*(4), 327–344. https://doi.org/10.1080/13645570701401305

Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: desperately seeking the "IT" in IT research—a call to theorizing the IT artifact. *Information Systems Research*, *12*(2), 121–134. https://doi.org/10.1287/isre.12.2.121.9700

Paluch, S., & Tuzovic, S. (2019). Persuaded self-tracking with wearable technology: carrot or stick? *Journal of Services Marketing*, *33*(4), 436–448. https://doi.org/10.1108/JSM-03-2018-0091

Park, E., Kim, K. J., & Kwon, S. J. (2016). Understanding the emergence of wearable devices as next-generation tools for health communication. *Information Technology & People*, *29*(4), 717–732. https://doi.org/10.1108/ITP-04-2015-0096

Park, S., Chung, K., & Jayaraman, S. (2014). Wearables: fundamentals, advancements, and a roadmap for the future. In E. Sazonov (Ed.), *Wearable sensors: fundamentals, implementation and applications* (pp. 1–23). Elsevier. https://doi.org/10.1016/B978-0-12-418662-0.00001-5

Payne, B. K., DeMichele, M., & Okafo, N. (2009). Attitudes about electronic monitoring: minority and majority racial group differences. *Journal of Criminal Justice*, *37*(2), 155–162. https://doi.org/10.1016/j.jcrimjus.2009.02.002

Perpitch, N. (2020, August 20). *Some WA arrivals to be fitted with tracking bracelets under new hotel quarantine rules*. ABC News. Retrieved February 19, 2021 from https://www.abc.net.au/news/2020-08-20/ankle-bracelets-may-be-used-to-enforce-hotel-quarantine-in-wa/12577496

Psychoula, I., Chen, L., & Amft, O. (2020). Privacy risk awareness in wearables and the internet of things. *IEEE Pervasive Computing*, *19*(3), 60–66. https://doi.org/10.1109/MPRV.2020.2997616

Pureprofile. (2015, April 23). *Press release: wearables work - Australians more active with fitness trackers.* Retrieved March 14, 2021 from https://business.pureprofile.com/press-release-wearables-work-australians-more-active-with-fitness-trackers/

Raij, A., Ghosh, A., Kumar, S., & Srivastava, M. (2011). Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems*, 11–20. https://doi.org/10.1145/1978942.1978945

Rauschnabel, P. A., & Ro, Y. K. (2016). Augmented reality smart glasses: an investigation of technology acceptance drivers. *International Journal of Technology Marketing*, *11*(2), 1–26. https://doi.org/10.1504/IJTMKT.2016.075690

Röcker, C., Ziefle, M., & Holzinger, A. (2014). From computer innovation to human integration: current trends and challenges for pervasive healthtechnologies. In A. Holzinger, M. Ziefle, & C. Röcker (Eds.), *Pervasive health* (pp. 1–17). Springer London. https://doi.org/10.1007/978-1-4471-6413-5_1

Rodriguez, K., Windwehr, S., & Schoen, S. (2020, June 15). *Bracelets, beacons, barcodes: wearables in the global response to COVID-19*. Electronic Frontier Foundation. Retrieved February 16, 2021 from https://www.eff.org/deeplinks/2020/06/bracelets-beacons-barcodes-wearables-global-response-covid-19

Rothstein, M. A. (2020). Public health and privacy in the pandemic. American Journal of Public Health, 110(9), 1374–1375. https://doi.org/10.2105/AJPH.2020.305849

Rowe, F. (2020). Contact tracing apps and values dilemmas: a privacy paradox in a neo-liberal world. *International Journal of Information Management*, *55*, 1–5. https://doi.org/10.1016/j.ijinfomgt.2020.102178

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3rd ed.). SAGE Publications, Inc.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2015). *Research methods for business students* (7th ed.). Pearson Education.

Schomakers, E.-M., Lidynia, C., & Ziefle, M. (2019). Exploring the acceptance of mhealth applications—do acceptance patterns vary depending on context? In T. Z. Ahram (Ed.), *Advances in Human Factors in Wearable Technologies and Game Design* (pp. 53–64). Springer International Publishing. https://doi.org/10.1007/978-3-319-94619-1_6

Schwartz, A. (2020, May 20). *COVID-19 patients' right to privacy against quarantine surveillance*. Electronic Frontier Foundation. Retrieved February 16, 2021 from https://www.eff.org/deeplinks/2020/05/covid-19-patients-right-privacy-against-quarantine-surveillance

Segura Anaya, L. H., Alsadoon, A., Costadopoulos, N., & Prasad, P. W. C. (2018). Ethical implications of user perceptions of wearable devices. *Science and Engineering Ethics*, *24*(1), 1–28. https://doi.org/10.1007/s11948-017-9872-8

Sergueeva, K., Shaw, N., & Lee, S. H. (2020). Understanding the barriers and factors associated with consumer adoption of wearable technology devices in managing personal health. *Canadian Journal of Administrative Sciences / Revue Canadienne Des Sciences de l'Administration*, *37*(1), 45–60. https://doi.org/10.1002/cjas.1547

Shaw, R. (2019, February 5). *Telsyte: iPhone prices up, iPhone sales down, down, down*. GadgetGuy. Retrieved March 14, 2021 from https://www.gadgetguy.com.au/telsyte-iphone-prices-up-iphone-sales-down-down-down/

Simko, L., Calo, R., Roesner, F., & Kohno, T. (2020). COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences. *ArXiv*. Retrieved March 2, 2021 from http://arxiv.org/abs/2005.06056

Smart Nation Singapore. (2020, December 23). *TraceTogether adoption surpasses 70% ccs to re-open for token collection progressively*. Retrieved May 21, 2021 from https://www.smartnation.gov.sg/whats-new/press-releases/tracetogether-adoption-surpasses-70-ccs-to-re-open-for-token-collection-progressively

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Spagnolli, A., Guardigli, E., Orso, V., Varotto, A., & Gamberini, L. (2014). Measuring user acceptance of wearable symbiotic devices: validation study across application scenarios. In G. Jacucci, L. Gamberini, J. Freeman, & A. Spagnolli

(Eds.), *Symbiotic interaction* (pp. 87–98). Springer International Publishing. https://doi.org/10.1007/978-3-319-13500-7_7

Statista. (2019a). *Singapore: ownership of wearable tech 2019*. Retrieved March 14, 2021 from https://www.statista.com/statistics/1053344/singapore-ownership-of-wearable-tech/

Statista. (2019b). *Singapore: ownership of wearable tech by brand 2019*. Retrieved March 14, 2021 from https://www.statista.com/statistics/1053376/singapore-ownership-of-wearable-tech-by-brand/

Statista. (2021). *Global connected wearable devices 2016-2022*. Retrieved March 22, 2021 from https://www.statista.com/statistics/487291/global-connected-wearable-devices/

Stebbins, R. A. (2001). *Exploratory research in the social sciences*. SAGE Publications, Inc.

Sun, S., Folarin, A. A., Ranjan, Y., Rashid, Z., Conde, P., Stewart, C., Cummins, N., Matcham, F., Dalla Costa, G., Simblett, S., Leocani, L., Lamers, F., Sørensen, P. S., Buron, M., Zabalza, A., Guerrero Pérez, A. I., Penninx, B. W., Siddi, S., Haro, J. M., … RADAR-CNS Consortium. (2020). Using smartphones and wearable devices to monitor behavioral changes during COVID-19. *Journal of Medical Internet Research*, *22*(9), 1–19. https://doi.org/10.2196/19992

Swan, M. (2012). Sensor mania! The internet of things, wearable computing, objective metrics, and the quantified self 2.0. *Journal of Sensor and Actuator Networks*, *1*(3), 217–253. https://doi.org/10.3390/jsan1030217

Talukder, M. S., Chiong, R., Bao, Y., & Hayat Malik, B. (2019). Acceptance and use predictors of fitness wearable technology and intention to recommend: an empirical study. *Industrial Management & Data Systems*, *119*(1), 170–188. https://doi.org/10.1108/IMDS-01-2018-0009

Tatler Singapore. (2021, March 11). *Apple watch maintains its number one spot in the smartwatch market*. Retrieved March 14, 2021 from https://sg.asiatatler.com/life/apple-watch-number-one-smartwatch-market

Tavani, H. T. (2007). Philosophical theories of privacy: implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1–22. https://doi.org/10.1111/j.1467-9973.2006.00474.x

The Government of the Hong Kong Special Administrative Region. (2021). *"StayHomeSafe" mobile app user guide*. Retrieved February 16, 2021 from

https://www.coronavirus.gov.hk/eng/stay-home-safe.html

The Lancet Respiratory Medicine. (2016). Data protection: balancing personal privacy and public health. *The Lancet Respiratory Medicine*, *4*(1), 1. https://doi.org/10.1016/S2213-2600(15)00514-7

Thierer, A. (2014). *The internet of things and wearable technology: addressing privacy and security concerns without derailing innovation*. George Mason University.

U.A.E. Government. (n.d.). *Smart solutions to fight COVID-19—the official portal of the UAE Government*. Retrieved February 16, 2021, from https://u.ae/en/information-and-services/justice-safety-and-the-law/handling-the-covid-19-outbreak/smart-solutions-to-fight-covid-19

United Nations. (n.d.). *Universal Declaration of Human Rights 1948*. Retrieved April 16, 2021 from https://www.un.org/en/about-us/universal-declaration-of-human-rights

U.S. Department of Commerce. (2019, October 25). *Internet of things*. Retrieved February 16, 2021 from https://www.commerce.gov/news/blog/2019/10/internet-things

Vaudenay, S. (2020). Centralized or decentralized? The contact tracing dilemma. *OpenAIRE*, 1–31. https://covid-19.openaire.eu/search/publication?articleId=od_____185::b333a9cdf196cdc396fede6971196acc

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157–178. https://doi.org/10.2307/41410412

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Wang, C., Guo, X., & Wang, Y. (2016). Friend or foe? Your wearable devices reveal your personal PIN. *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 189–200. https://doi.org/10.1145/2897845.2897847

Wang, H., Tao, D., Yu, N., & Qu, X. (2020). Understanding consumer acceptance of healthcare wearable devices: an integrated model of UTAUT and TTF. *International Journal of Medical Informatics*, *139*, 1–10.

https://doi.org/10.1016/j.ijmedinf.2020.104156

Weizman, Y., Tan, A. M., & Fuss, F. K. (2020). Use of wearable technology to enhance response to the Coronavirus (COVID-19) pandemic. *Public Health*, *185*, 221–222. https://doi.org/10.1016/j.puhe.2020.06.048

Wen, D., Zhang, X., & Lei, J. (2017). Consumers' perceived attitudes to wearable devices in health monitoring in China: a survey study. *Computer Methods and Programs in Biomedicine*, *140*, 131–137. https://doi.org/10.1016/j.cmpb.2016.12.009

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Westin, A. F. (2003). Social and political dimensions of privacy: social and political. *Journal of Social Issues*, *59*(2), 431–453. https://doi.org/10.1111/1540-4560.00072

Whitelaw, S., Mamas, M. A., Topol, E., & Van Spall, H. G. C. (2020). Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health*, *2*(8), e435–e440. https://doi.org/10.1016/S2589-7500(20)30142-4

Wiggins, N., & Carrick, D. (2020, August 16). *People are breaking quarantine rules. Electronic monitoring is 'certainly an option' to stop that*. ABC News. Retrieved February 16, 2021 from https://www.abc.net.au/news/2020-08-17/covid-coronavirus-quarantine-tracking-devices-to-stop-breaches/12557736

Winchester, H. (2015, May 6). *A brief history of wearable tech*. Wareable. Retrieved February 16, 2021 from https://www.wareable.com/wearable-tech/a-brief-history-of-wearables

World Health Organisation. (2020, October 13). *Impact of COVID-19 on people's livelihoods, their health and our food systems*. Retrieved May 23, 2021 from https://www.who.int/news/item/13-10-2020-impact-of-covid-19-on-people's-livelihoods-their-health-and-our-food-systems

World Health Organisation. (2021a). *Timeline: WHO's COVID-19 response*. Retrieved March 3, 2021 from https://www.who.int/emergencies/diseases/novel-coronavirus-2019/interactive-timeline

World Health Organisation. (2021b). *WHO Coronavirus (COVID-19) Dashboard*. Retrieved May 23, 2021 from https://covid19.who.int

Wright, R., & Keith, L. (2014). Wearable technology: if the tech fits, wear it. *Journal of Electronic Resources in Medical Libraries*, *11*(4), 204–216. https://doi.org/10.1080/15424065.2014.969051

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems*, *26*(3), 135–174. https://doi.org/10.2753/MIS0742-1222260305

Yang Meier, D., Barthelmess, P., Sun, W., & Liberatore, F. (2020). Wearable technology acceptance in health care based on national culture differences: cross-country analysis between chinese and swiss consumers. *Journal of Medical Internet Research*, *22*(10), 1–15. https://doi.org/10.2196/18801

Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review. *IEEE Communications Surveys & Tutorials*, *21*(4), 3723–3768. https://doi.org/10.1109/COMST.2019.2914094

Yin, R. K. (2018). *Case study research and applications: design and methods* (6th ed.). SAGE Publications, Inc.

Zhang, M., Luo, M., Nie, R., & Zhang, Y. (2017). Technical attributes, health attribute, consumer attributes and their roles in adoption intention of healthcare wearable technology. *International Journal of Medical Informatics*, *108*, 97–109. https://doi.org/10.1016/j.ijmedinf.2017.09.016

9 Appendix

9.1 Summary of wearable technology adoption studies

Author/Year	Type of wearable	Framework (if used)	Method	Key findings
Adapa et al. (2018)	Smart glasses; smart watch	TAM & UTAUT	Interviews	There was a difference in adoption attitudes depending on the type of wearable: fashion was important for smart glasses adoption, while having useful fitness apps was important for smart watch adoption Privacy is a key concern for all types of wearable devices, and this has to be balanced alongside the device's functionalities
Bellekens et al. (2016)	Wearable technology	-	Survey	Wearable devices are subject to privacy complacency by their users, as they tend to trust the linked applications and the device manufacturer. This is in spite of the fact that users expressed concern for their data security and privacy. Furthermore, users believe they have more control over their data than is the case in reality.
Canhoto & Arp (2017)	Wearable fitness technology	-	Interviews	There is a difference between adoption factors and sustained use factors, and strong adoption factors include technology affinity, gender, and context.
Coorevits & Coenen (2016)	Wearable technology	-	Netography	User attrition is influenced by discomfort, selectability, and usefulness.
Chau et al. (2019)	Wearable health devices	TAM & health belief model	Survey	User adoption intention is shaped by perceived usefulness, which is in turn influenced by perceived convenience and perceived irreplaceability. Furthermore, user adoption intention is also influenced by health belief.
Chuah et al. (2016)	Smart watch	TAM	Survey	User adoption intention is shaped by perceived usefulness and visibility, and by whether users view the smart watch as a technology or a fashion item

Dehghani et al. (2018)	Smart watch	Own model	Survey	User adoption intention is influenced by healthology.
Duval & Hashizume (2005)	Wearable technology	-	Survey	There are gender and cultural effects on people's perceptions of wearable computers.
Gao et al. (2015)	Fitness devices vs medical devices	UTAUT2, Protection motivation theory, & privacy calculus theory	Survey	Fitness device users are more affected by HM, SI, privacy, while medical device users are more affected by EE
Gregor & Gwiaździński, (2020)	General (glasses, bands, watches, jewellery, headphones, clothes, tattoos, contact lenses, skin implants)	-	Survey	Use of wearable devices is twice as low as the level of knowledge
Guillén-Gámez & Mayorga-Fernández (2019)	General (wrist-worn, clothes, smart glasses, shoes)	Conceptual framework of utility, comfort, emotions, privacy, and intended use	Survey	Men are more likely to accept and adopt wearable devices, but there is a growing interest amongst young women. Furthermore, privacy is a strong user concern.
Jeong et al. (2017)	Wearable technology	Domain-specific innovativeness, Product-possessing innovativeness, Information-possessing innovativeness	Survey	Users with high levels of tech-savviness are more likely to adopt wearable technology than those without.
Karahanoğlu & Erbuğ (2011)	Wearable technology	Perceived qualities - hedonic qualities and pragmatic qualities	Focus groups	The qualities in smart wearables have a hierarchy of importance and are associated with one another, where a failure in one quality can have negative impacts on the wearable product as a whole
Kim & Shin (2015)	Smart watch	TAM	Survey	Perceived usefulness is influenced by affective quality and relative advantage. Perceived ease of use is influenced by mobility and availability.
Koo & Fallon (2018)	Wearable technology	-	Interviews	Wearable trackers should be small, lightweight, and neutrally coloured Novice users are more likely to use wearable trackers to track the physical health of other people, while experienced users prefer to monitor others' activity

Lee et al. (2016)	Wearable technology	-	Survey	Users are greatly concerned about privacy and security, with their greatest concern being video capture and financial information being gathered without their consent.
Li et al. (2016)	Wearable health devices	Privacy calculus theory	Survey	A person is more likely to adopt a wearable device if the perceived benefit is higher than the perceived privacy risk.
Miltgen et al. (2013)	Biometrics	TAM, diffusion of innovation model (DOI), & UTAUT	Survey	Trust and privacy are amongst the most important adoption factors, beyond the factors introduced in adoption models such as TAM, DOI, UTAUT
Motti & Caine (2015)	Wrist-mounted wearable devices & head-mounted wearable devices	-	Content analysis	The type of wearable impacts users' privacy concerns.
Nasir & Yurder (2015)	Wearable health devices	TAM	Survey	User adoption intention is influenced by perceived benefit and perceived risk.
Paluch & Tuzovic (2019)	Wearable technology	TAM & privacy calculus theory	Interviews	User reactions to wearable technology adoption fall into the following categories: embracing, considering, debating, and avoiding.
Park et al. (2016)	Wearable health devices	TAM	Survey	User adoption intention is influenced by their perceived control of the device and their own innovative tendencies. Perceived cost has no significant effect on adoption intention.
Rauschnabel & Ro (2016)	Smart glasses	TAM & innovation diffusion theory	Survey	User adoption is influenced more by fashion than by privacy concerns, and users with high levels of tech-savviness are particularly motivated to adopt smart glasses.
Segura Anaya et al. (2018)	Wearable technology	-	Survey	Users are greatly concerned by wearable device privacy and place huge importance on informed consent for third-party information sharing.
Sergueeva et al. (2020)	Wearable technology	UTAUT2	Survey	User adoption intention is influenced by performance expectancy, social influence, facilitating conditions, hedonic motivation, habit, and personalisation, while it is not significantly influenced by price, privacy, or health consciousness.

Spagnolli et al. (2014)	Wearable technology	TAM	Survey	User acceptance of wearable technology is influenced by perceived usefulness, perceived comfort, facilitating conditions, and technology attitude.
Talukder et al. (2019)	Wearable fitness technology	UTAUT2 & DOI	Survey	User adoption is influenced by performance expectancy, effort expectancy, social influence, habit, compatibility, and innovativeness.
Yang et al. (2020)	Wearable health devices	UTAUT2, protection motivation theory & privacy calculus theory	Survey	User adoption intention is influenced by performance expectancy, social influence, and hedonic motivation, while effort expectancy, functional congruence, health consciousness, and perceived privacy risk do not have a significant influence.
Wang et al. (2020)	Wearable health devices	UTAUT & task-technology fit	Survey	User adoption intention is influenced by performance expectancy, effort expectancy, facilitating conditions, social influence, and task-technology fit.
Wen et al. (2017)	Wearable technology	-	Survey	User adoption intention is influenced by perceived ease of use and the device's features. Other factors such as damage potential, poor recommendations or discomfort influenced user rejection.
Zhang et al. (2017)	Wearable health devices	TAM, health belief model, snob effect & conformity and reference group	Survey	User adoption intention is influenced by technical, health, and consumer attributes.

Table 5: Summary of wearable technology adoption studies

9.2 Interview Discussion Guide

This guide is to outline the theoretical underpinnings of this study's interview questions. The goal of the qualitative semi-structured interviews is to gather the data required to answer the research questions

Introductory questions

1. **What is your experience with using wearable technology?**

Wearable technology adoption studies found that people with innovative tendencies are more likely to adopt wearable technology (Gregor & Gwiaździński, 2020; Jeong et al., 2017; Park et al., 2016; Rauschnabel & Ro, 2016). While prior experience with wearable technology was a prerequisite for participation, this question aims to establish the extent of the participant's experience.

2. **How important is data privacy to you personally?**

While there is no universally accepted definition of privacy (Solove, 2008), this question aims to establish the participant's attitude towards data privacy in their daily life. The answer to this question is also intended to set the scene for the upcoming privacy-themed questions.

3. **Have you downloaded and actively used the Australian Government's COVIDSafe app / the Singaporean Government's TraceTogether app or token?**
    a. **If yes, why have you used it?**

Digital contact tracing has been a widely-adopted governmental tool for addressing community spread of COVID-19 (Bhattacharya & Ramos, 2021; Elkhodr et al., 2021; Weizman et al., 2020). This question aims to establish the participant's appetite for governmental use of innovative technologies in COVID-19.

Data-first vs privacy-first wearable technology architectures

These questions aim to establish how participants perceive data-first and privacy first wearable technology architectures, in relation to their privacy.

I am now going to ask you a series of questions regarding how you feel about your government using wearable devices to enforce COVID-19-related quarantine obligations. The device in question is wrist-worn and tracks your location at all times. Users would be obliged to wear the device for the duration of the quarantine period to ensure that they do not leave their place of residence.

Data-first wearable technology architecture: citizen data is identifiable when it is gathered and stored, and government authorities have full access (Kapa et al., 2020).

1. **In relation to these wearable devices, please describe how you feel about governments collecting location data that makes the users easily identifiable and can be easily accessed by government authorities.**

This question aims to encourage the participant to actively consider the privacy implications of such a device.

2. **How do you see these devices impacting people's privacy?**

Privacy-first wearable technology architecture: citizen data is protected – through encryption, or other means – and government authorities have limited access (Kapa et al., 2020)

3. **In relation to these wearable devices, please describe how you feel about governments collecting location data on users that is fully de-identified and only able to be accessed under specific circumstances by government authorities.**

This question prompts the participant to choose whether they would prefer a data-first or privacy-first wearable technology architecture in COVID-19.

4. **If you had to choose, would you prefer that the devices made the user easily identifiable so the government could find quarantine violators quickly, or that fully de-identified the user to protect their privacy but make it more difficult to detect quarantine violators?**

The following two questions prompt the participant to consider how effective the devices would be and how justified they think the government would be in using them. This is to encourage them to consider whether there is a genuine need for these devices, regardless of their own privacy attitudes.

5. **How effective do you think these devices would be in protecting the community from COVID-19?**
6. **How justified do you think the government would be in using these devices?**

These questions prompt the participant to consider how effective the devices would be as a public health crisis management tool, and how justified the government would be in officially rolling them out.

Mandatory vs optional use of governmental wearable technology

The below questions aim to establish how participants perceive optional or mandated wearable technologies, in relation to their privacy. The entirety of wearable technology adoption literature is oriented from a consumer perspective: as a result, there are no adoption factors for mandated wearable technology. These questions aim to gather data to fill this gap.

1. **I have a scenario to propose to you: if you were a returning international traveller or otherwise at risk of having COVID-19, and you had the option of quarantining in a hotel or quarantining at home while your location is monitored with a wearable device, which would you choose and why?**

2. **How would your opinion change if you weren't given a choice about wearing one of these devices while you are quarantining?**

3. **How do you think people's privacy is affected with these devices, depending on whether they're optional or mandatory?**

9.3 Citizens' privacy attitudes

Theme	Country	Attitude
Perceived benefit	Australia	Wearables offer citizens the choice to quarantine at their home without paying for hotel quarantine, having the comfort of home, and supporting their mental health by being in a familiar space. Furthermore, having effective quarantine arrangements - facilitated with wearable devices - was perceived to protect the broader community from experiencing further lockdowns.
	Singapore	Wearables benefit the community by ensuring an effective quarantine system, which protects the community from COVID-19. There was a strong emphasis on preserving Singapore's way of life, more than the individual benefits. Citizens appreciated the option to stay at home and live comfortably, but several citizens saw a hotel stay as equally comfortable.
Perceived privacy risk	Australia	There was an imbalance between what citizens felt comfortable with privacy-wise and how they wanted the government to monitor quarantining individuals. Citizens were unable to identify what privacy risks could be posed by wearables, but discussed how their use would only be acceptable from a privacy perspective if they collected de-identified data. They wanted strong clearance controls within the government yet approximately half of them wanted it to be easy to catch people who have violated quarantine.
	Singapore	Citizens have a strong understanding of the privacy risk involved in governmental use of wearables, and are comfortable with their use as long as their data is used responsibly by authorised government officials. There were very limited perceived privacy risks, and there were divided opinions on whether the wearable ought to be identified or de-identified to protect privacy. However, there was a strong preference for the government to easily catch quarantine violators.
Context	Australia	While citizens were not totally comfortable with the government collecting their location data, they recognised that extreme measures were necessary to manage COVID-19's impact on the community. The pandemic context had a significant effect on their privacy attitudes, leading them to indicate acceptance/adoption of governmental wearables.
	Singapore	As above. Furthermore, citizens are already used to their personal information being gathered by the government through their IC and smart city surveillance systems. Their privacy attitudes were already shaped by digitalisation.
Time	Australia	Wearables would only be acceptable if their use was limited to the quarantine requirement, and not for broader use within the pandemic. Any use beyond the pandemic would be an unacceptable privacy violation.
	Singapore	As above, however citizens were already exposed to governmental wearables beyond the quarantine requirement through the TraceTogether token. There was a strong support for effective technological responses to the pandemic despite the privacy issues they posed.
Choice	Australia	Having a choice is a strong factor in whether citizens would accept or adopt a government wearable. While citizens understood the need for such devices, many felt uncomfortable about not having a choice.
	Singapore	Mandatory devices were favoured despite the privacy concerns because it was perceived to be more effective in mitigating the pandemic. This does not mean that citizens were totally comfortable with the wearable, but that they understood the need for it.
Trust in government	Australia	There was limited trust in government to protect citizen privacy effectively when using wearables in this context. Not only were they not totally comfortable with the use, but they did not have faith that the government could use the data appropriately.

	Singapore	There was high trust in government to protect citizen privacy effectively when using wearables in this context. While they were not totally comfortable with the device, they trusted the government to do the right thing with the data and believed they had the capacity to use the data appropriately.
Data access	Australia	There were strong opinions on who should be able to access the data, with an overwhelming majority indicating that authorised government officials ought to be the only ones with access to the wearable data. There was also an emphasis on additional considerations for vulnerable people in society who may have additional privacy needs.
	Singapore	As above, the vast majority believed that authorised government officials ought to be the only ones with access to the wearable data. However, they did not believe that the wearable posed any greater privacy risk to them than what the government already knew about them. As long as there are safeguards against data misuse, they would be willing to adopt the wearable.

Table 6: Summary of citizens' privacy attitudes

Declaration of Authorship

I hereby declare that, to the best of my knowledge and belief, this Master Thesis titled "Balancing public health and privacy: an exploration of citizen privacy attitudes towards governmental use of wearable technologies in public health crises" is my own work. I confirm that each significant contribution to and quotation in this thesis that originates from the work or works of others is indicated by proper use of citation and references.

Berlin, 28 May 2021

Grace Annalise Milne

Consent Form

for the use of plagiarism detection software to check my thesis

Name: Milne
Given Name: Grace Annalise
Student number: 0772014
Course of Study: Public Sector Innovation and eGovernance
Address: Richard Sorge Strasse 36, 10249 Berlin, Germany
Title of the thesis: Balancing public health and privacy: an exploration of citizen privacy attitudes towards governmental use of wearable technologies in public health crises

What is plagiarism? Plagiarism is defined as submitting someone else's work or ideas as your own without a complete indication of the source. It is hereby irrelevant whether the work of others is copied word by word without acknowledgment of the source, text structures (e.g. line of argumentation or outline) are borrowed or texts are translated from a foreign language.

Use of plagiarism detection software. The examination office uses plagiarism software to check each submitted bachelor and master thesis for plagiarism. For that purpose the thesis is electronically forwarded to a software service provider where the software checks for potential matches between the submitted work and work from other sources. For future comparisons with other theses, your thesis will be permanently stored in a database. Only the School of Business and Economics of the University of Münster is allowed to access your stored thesis. The student agrees that his or her thesis may be stored and reproduced only for the purpose of plagiarism assessment. The first examiner of the thesis will be advised on the outcome of the plagiarism assessment.

Sanctions. Each case of plagiarism constitutes an attempt to deceive in terms of the examination regulations and will lead to the thesis being graded as "failed". This will be communicated to the examination office where your case will be documented. In the event of a serious case of deception the examinee can be generally excluded from any further examination. This can lead to the exmatriculation of the student. Even after completion of the examination procedure and graduation from university, plagiarism can result in a withdrawal of the awarded academic degree.

I confirm that I have read and understood the information in this document. I agree to the outlined procedure for plagiarism assessment and potential sanctioning.

BERLIN, 28/05/2021

Grace Annalise Milne