Privacy and Trust in Healthcare IoT Data Sharing:

A Snapshot of the Users' Perspectives

by

Laura Xavier Fadrique

A thesis

presented to the University of Waterloo

in fulfillment of the

thesis requirement for the degree of

Master of Applied Science

in

Public Health and Health Systems

Waterloo, Ontario, Canada, 2019

AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

ABSTRACT

Background: Healthcare services in Canada are slowly shifting from in-hospital care to more patient-centred, home-care services. Collecting and sharing personal data from individuals via Internet of Things (IoT) devices is a critical part of this change that potentially leads to better decision-making and better support for patients from healthcare providers. However, there are challenges that come from using technology, including concerns around trust in organizations holding individuals' data, as well as privacy and security related to data sharing that needs to be considered as part of this new model of care.

Objective: This study seeks to investigate users' trust in sharing their data collected using healthcare IoT devices via different types of organizations.

Methods: This research project leveraged a literature review and online questionnaires to understand how general users of IoT for Health trust different types of organizations (large companies, government, healthcare providers, and insurance companies). A total of 400 participants were recruited using Mechanical Turk for the online questionnaire, using a between-subjects design. Each participant answered questions about one type of organization, where a scenario related to the use of different IoT technologies, information about data sharing and a list of privacy concerns were presented. Based on this scenario, participants were asked to answer 16 trust-related questions. Results were analyzed using Analysis of Variance (ANOVA), followed by post-hoc comparisons using the pairwise t-test with the Bonferroni correction.

Results: The study showed no significant differences in regards to privacy concerns (LConcern) in Canada, United States (USA), and Europe ($F(2, 389) = 0.736$, $P = .480$). Overall levels of trust (LTrust) in the USA varied significantly between large companies, government, healthcare providers, and insurance companies ($F(3, 388) = 10.107$, $P < .05$). The same results

were observed in Canada with a significant difference between the four types of organizations (F (3, 125) = 6.882, $P < .05$), USA (F (3, 128) = 4.488, $P = .05$), and in Europe, as well (F (3, 127) = 4.451, $P < 0.05$).

Conclusion: Initial evidence supports differences in users' perception of trust in healthcare IoT data sharing among the aforementioned types of organizations and levels of concern amongst users regarding privacy and data ownership. Differences in the perception of trust were also identified between the different regions of the participants. Future research using more specific types of organization and larger samples for each age group are needed to fill knowledge gaps. In addition, further research is also needed to understand how external factors can affect user's levels of trust and acceptance of healthcare IoT with potential consequences for the implementation of new healthcare delivery models.

ACKNOWLEDGEMENTS

I wish to acknowledge the support I received from many individuals throughout my master's program at the University of Waterloo (UW). I want to thank my supervisor, Dr. Plinio P. Morita, for his encouragement, friendship and support, both emotional and academic. Thank you for providing me with extracurricular opportunities that made my master's program a unique and pleasant experience.

Much appreciated is the support of my committee members, Dr. Kathryn Henne and Dr. James Wallace. Their involvement and contributions have helped me to make my thesis more productive.

Finally, thanks to fellow graduate students from UbiLab for all your support, suggestions, advice and teamwork.

DEDICATION

I dedicate this thesis to my husband and family. To my husband, for always believing in me (usually more than I do), finding ways to encourage me throughout this journey, supporting me and being by my side even throughout the toughest times. For pursuing the same dreams and adventures as me and doing everything possible so we can get there. Thank you, without you, none of this would be possible.

I dedicate to my parents and siblings who have always believed and celebrated with me every achievement even though I am miles away. You gave me the foundation for everything.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AAL	Active Assistive Technology
AmI	Ambient Intelligence
CHA	Canada Health Act
CIHI	Canadian Institute for Health Information
DBMS	Database Management System
EPR	Electronic Patient Records
H-IoT	Healthcare IoT
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IMIA	International Medical Informatics Association
IoT	Internet of Things
LAwareness	Levels of Privacy Awareness
LConcern	Levels of Privacy Concern
LTrust	Levels of Trust
OECD	Organization for Economic Co-operation and Development
PA	Privacy Agreement
PIPEDA	Personal Information Protection and Electronic Documents Act
RPM	Remote Patient Monitoring
TAM	Technology Acceptance Model

1. INTRODUCTION

Canada is known for its universal healthcare system, Medicare, and social assistance programs to ensure the physical and mental well-being of Canadians, including both native Canadians and immigrants (Martin et al., 2018). The Medicare system was born in 1947 and was later standardized in 1984 by the Canada Health Act (CHA) (Martin et al., 2018). Despite being lauded globally, the Canadian healthcare system also faces many challenges. According to Canadians, long wait times and access to care present significant challenges (Marchildon, 2013). Long wait times to receive consultations and care are attributable to factors including a high number of unnecessary hospitalizations, readmissions, and increased incidence of chronic diseases (Marchildon, 2013).

Canada has the fifth most expensive health system in the world, spending about 11.5% of its GDP on healthcare in 2017 (Canadian Institute for Health Information, 2017a). According to Simpson (2018), the solution is not spending more money, but instead spending it in better and more efficient ways. Simpson also criticizes the system by stating that the healthcare business in Canada is more disconnected than ever, while the experiences and needs of patients are changing. Improving the system will require working to develop a properly integrated and transdisciplinary model of care in the community or at home (Canadian Medical Protective Association, 2014; Simpson, 2018).

Canada needs to start thinking about alternative forms of healthcare delivery beyond clinics and hospitals. A total of 65% of Canadians claim they have difficulties getting after-hours care unless they are going to the emergency room (Marchildon, 2013). There are movements in Canada towards patient empowerment and increased transparency, but Canada is still behind

other OECD countries with similar approaches (Marchildon, 2013). Increasing transparency and empowerment can lead patients to a greater interest in self-managing their health and more independence for ageing at home rather than moving to an institution (Koch, 2006; Rashidi & Mihailidis, 2013). According to the Canadian Institute for Health Information (CIHI) (2017b), expectations and preferences from the patient influence the care they receive. For that reason, it is essential to provide tools that facilitate communication between clinicians and patients, improving the decision-making process and reducing unnecessary expenses while delivering care (Canadian Institute for Health Information, 2017b; Koch, 2006).

Advances in technology, followed by an increased preference for self-management and home-care as a model of patient care, are moving our society towards independent living (Hubl et al., 2016). These changes will direct the healthcare system to a more decentralized model, going from in-hospital care to home-based care (Koch, 2006). Moreover, treating patients within their own homes can increase patient satisfaction since home-care treatment is patient-centred, less expensive, and is potentially more effective when dealing with chronic diseases (Tsasis & Bains, 2008). Advances in technology make home-care one of the fastest-growing areas of healthcare (Koch, 2006).

Dimitrov (2016) emphasizes that the intersection of information technology and medicine will transform our current healthcare model, reduce costs, decrease unnecessary treatments, and save lives. In order for all these benefits to be achieved, our team has determined that leveraging the collection of personal data from within an individual's home is necessary. The integration of data from medical devices with the health records of each individual will allow for a comprehensive view of health for individual and population-level health decisions (Knaup & Schöpe, 2014).

According to Hubl et al. (2016), individual data collection can be performed using wearables and other devices installed inside our homes using the Internet of Things (IoT). These devices allow the measurement, recording, and analysis of data collected from multiple facets of our lives, which can be used as solutions designed to serve us better (Lahlou, Langheinrich, & Röcker, 2005). The leading enabler behind the technologies in our homes is data (Dimitrov, 2016). Data collected by sensors and sent through networks is processed, analyzed and prepared to be presented in a more meaningful way in accordance with the needs of the user (e.g. patients, family members, healthcare providers), improving decision making (Knaup & Schöpe, 2014; Strielkina, Uzun, & Kharchenko, 2017). The use and analysis of large amounts of information have transformed the healthcare area into one of the primary users of big data (Dimitrov, 2016). It is expected that healthcare will be remodelled using IoT technology, and solutions derived from such technologies can help reduce the costs of delivering care to individuals in the future (Negash et al., 2018).

IoT and wearables empower us to collect vast amounts of personal information in real-time, continuously, and without the constraints of location (Lahlou et al., 2005). Nonetheless, the potential benefits of this technology can only be achieved once challenges with the technology have been addressed, including infrastructure (Allied Market Research (AMR), 2016) and concerns related to the privacy and security of one's data (Ahmed Abi Sen, Albouraey Eassa, Jambi, & Yamin, 2018; Culnan & Armstrong, 1999; Marchildon, 2013). Privacy and security challenges include the risk of exposing personal and sensitive information, causing loss of trust between parties (Ahmed Abi Sen et al., 2018). Not to mention the potential harm to individuals if they have personal information exposed (Solove, 2012).

While there are several privacy and trust challenges in the use of wearable and IoT technology for health monitoring that could be explored in a research project, this thesis focuses on two main topics of interest: (1) the individual's ability to understand data ownership regarding data collected by healthcare IoT manufacturers or service providers; and (2) understand the level of user trust in organizations that collect and share health-related data using healthcare IoT technologies. In the final analysis, this study highlights the impact of users' previous experience on the levels of trust in different types of organizations, as well as the impact of users' culture on the levels of trust comparing different regions.

2. LITERATURE REVIEW

2.1. HEALTHCARE SYSTEM

The Canada Health Act (CHA) is Canada's federal legislation for publicly funded healthcare insurance and specifies the conditions, standards, and criteria in which each province's and territory's programs must follow in order to receive federal funding (Government of Canada, 2018). According to a report from CIHI (2017a), Canada spent $242 billion in 2017 on healthcare, showing increased expenditures when compared with the 2016 cycle (see Figure 1). Health systems in most developed countries are facing the same problems, with an increase in the demand for care, ageing population, increase in the prevalence of chronic diseases, as well as problems in training and retaining skilled workers like doctors and nurses (Koch, 2006). Despite the growth of the elderly population, ageing alone is not the most significant burden on the healthcare system (Marchildon, 2013). As populations age, there is an increase in the incidence of chronic diseases that are overwhelming health systems (Tsasis & Bains, 2008). As an example, 55% of direct and indirect health costs in Ontario are for patients dealing with chronic diseases, with 80% of the population over 45 years of age with at least one chronic condition (Tsasis & Bains, 2008). In this scenario, a more significant investment in treatments and drugs for chronic conditions is needed. While an increase in prescription drugs is costly (Marchildon, 2013), it is more costly when these drugs are prescribed unnecessarily (both in terms of resources and money), additionally prescribing unnecessary tests and treatments also increases wait-times for patients in need of care increasing the burden on the healthcare system (Canadian Institute for Health Information, 2017b).

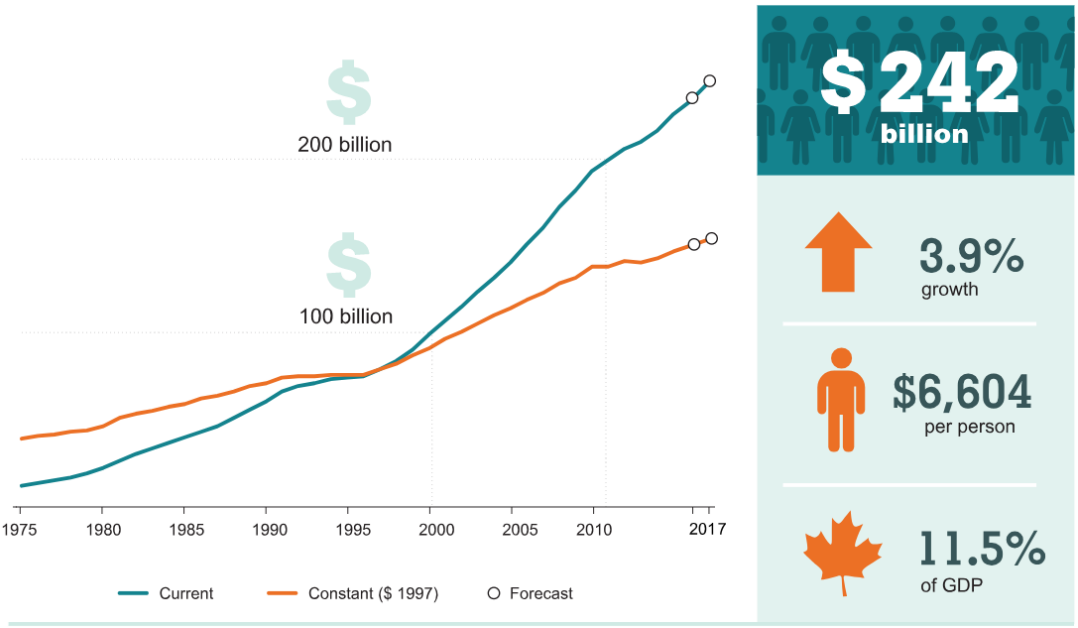


Figure 1. 2017 Canada's spending on health (Canadian Institute for Health Information, 2017a)

Readmissions are another major challenge faced by healthcare systems. In Canada, about 8.5% of patients are readmitted to the hospital in the first month of discharge. In Ontario alone, readmissions cost over $700 million per year (Ndegwa, 2011). Such readmission leads to hospitals overcrowding as well as an increase in the list of patients to be transferred home with the help of clinical support (Ndegwa, 2011). Home-based technologies based on Internet of Things (IoT) capable of supporting remote patient monitoring and self-management of chronic diseases have the potential to reduce care delivery costs while keeping patients independent.

2.2. Internet of Things (IoT)

Internet of Things (IoT) is the extension of the internet into physical technologies and everyday objects, which enables the creation of systems that operate over a network, collecting and exchanging data, and acting upon objects in our lives (Dimitrov, 2016; Gubbi, Buyya, Marusic, & Palaniswami, 2013; Islam, Kwak, Kabir, Hossain, & Kwak, 2015). By working 24

hours a day, IoT devices can collect and analyze a large amount of possibly identifiable personal data (Daubert, Wiesmaier, & Kikiras, 2015). Identifiable data, which is considered sensitive and personal, can include information about our social life, location, and relationship with co-workers (Bao, Chen, & Chen, 2012; Cao et al., 2016; Daubert et al., 2015; Yan, Zhang, & Vasilakos, 2014). Likewise, the use of wearables and mobile sensors allows the collection of individual health (e.g., heart rate) and contextual data, allowing the analysis of continuous health and rapid decision making (Azimi et al., 2019; Bhatia & Sood, 2017).

It is expected that by the year 2020, we will have around 30 billion internet-connected "things" (Statista, 2019). By the same year, 25% of the malicious cyber-attacks will involve IoT devices (Hung, 2017). However, less than 10% of the budget allocated to product development by companies developing and using IoT technology will be invested in IoT security (Hung, 2017). IoT devices work transparently inside our home or organization, but can also move along with users in the form of smartwatches and smartphones (Bao et al., 2012). These devices are often exposed to public wireless networks, and so become more vulnerable to malicious attacks (Bao et al., 2012).

Much of the intelligence behind the data analyzed by a fitness tracker is not built into the wearable we use on our wrist. The data is typically collected and treated in the cloud or on our smartphones, requiring data to be transferred over the networks (Hung, 2017). Due to the portability and ability of the devices to connect to different network environments, IoT has a profound impact on privacy, which creates an extra challenge for the security and protection of personal data about the habits, behaviours and activities of its owners (Bao et al., 2012). Additionally, IoT devices have limited power and storage capacity, requiring the collected data to be stored externally, typically in the cloud (Ahmed Abi Sen et al., 2018). Therefore, user

privacy and data security should be guaranteed by all vendors and manufacturers in this technology space. However, there is currently no single solution that can guarantee all the security requirements such as anonymity, confidentiality, access control, privacy and trust in the context of IoT technology (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015).

IoT devices can collect, send and act on data they acquire from their surrounding environments in a ubiquitous way, using sensors and embedded technology to enable the provision of innovative services (Sicari et al., 2015; Yan et al., 2014; Zanella et al., 2017) in the context of smart homes (automation), smart cities, ambient intelligence (AmI), E-Health, E-Learning, E-Business, remote patient monitoring (RPM), energy consumption control, traffic control, smart parking system, and personalized advertising (Ahmed Abi Sen et al., 2018; Sicari et al., 2015). Some of the applications of IoT technologies are explored in the next two sections on smart homes and ambient intelligence.

2.2.1. Smart Homes

Smart homes allow users to have greater control over their indoor environment and home resources like windows, lighting, and others. (Biocco, Keshavarz, Hines, & Anwar, 2018; Risteska Stojkoska & Trivodaliev, 2017). Built-in devices in the environment allow users to control appliances and home resources as well as collecting data about energy consumption (Risteska Stojkoska & Trivodaliev, 2017). In addition to energy consumption, smart home devices can interact with one another or with a smart hub that manages and shares data to provide home comfort services (Zhang, Liu, Wang, & Hu, 2016). In addition to comfort, smart homes have great potential for immediate emergency responses for vulnerable populations (e.g., elderly individuals) by providing health monitoring and fall prevention (Ferreira et al., 2017). Such equipment collects continuous data, which often results in many users losing control over

the data collected as they typically receive the default basic security packages with limited control of their data (Biocco et al., 2018).

2.2.2. Ambient Intelligence (AmI)

Ambient Intelligence (AmI) can be embedded into home environments in order to assist users in everyday activities (Blumendorf & Albayrak, 2009). AmI is based on low-cost hardware and provides complex networks of heterogeneous information and smart devices (Sadri, 2011). AmI applications are transparent and invisible for users, while security and privacy requirements are guaranteed (Abril-Jiménez, Vera-Muñoz, Cabrera-Umpierrez, Arredondo, & Naranjo, 2009). AmI goes beyond smart homes, allowing environments to adapt and be responsive to the presence of people in order to provide services and experiences (Avilés-López, García-Macías, & Villanueva-Miranda, 2010; Ferreira et al., 2017). The same tools can also sense, adapt, and respond to habits, gestures, and emotions (Bravo, Cook, & Riva, 2016). The sensing capability can be used to map objects' positions, environmental temperature, air humidity, and even the amount of chemicals in the air, thus helping in health monitoring within an intelligent environment (Cook, Augusto, & Jakkula, 2009). In the healthcare domain, AmI can be used to provide continued health monitoring and communication tools (Acampora, Cook, Rashidi, & Vasilakos, 2013; Salih & Abraham, 2013), as well as decision-making support for healthcare facility managers (Irizarry, Gheisari, Williams, & Roper, 2014). With AmI, it is also possible to anticipate users' needs and preferences in response to their habits, using intelligence to analyze the data collected by the sensors and provide better services such as energy efficiency, door locks, windows closure and health safety (Cook et al., 2009). IoT based healthcare application and its variations can improve the future of healthcare systems and the quality of life of patients in the community, as presented in the next section.

2.3. HEALTHCARE IOT (H-IOT)

As previously discussed, smart homes can be equipped with IoT technologies to monitor individuals through the use of wearables and built-in sensors (Demiris, Hensel, Skubic, & Rantz, 2008). One of the best uses of such technologies is the continuous monitoring and decision support for patients receiving home-care (Dimitrov, 2016; Mutlag, Abd Ghani, Arunkumar, Mohammed, & Mohd, 2019; Negash et al., 2018). Also, continuous monitoring enables us to collect, aggregate and analyze data more quickly and with better accuracy than manual data collection (Banerjee, Bhattacharya, Sen, Bhattacharya, & Sen, 2018). It is estimated that by the year 2020, 40% of all the IoT devices in the world will be health-related, more than any other IoT application, with a 117 billion dollar market (Dimitrov, 2016).

Healthcare IoT (H-IoT) can be defined as a system or an infrastructure with the purpose of facilitating the transmission and reception of health data enabling better treatments, remote monitoring, and improved decision making (Azimi et al., 2019; Banerjee et al., 2018; Sony & Sureshkumar, 2019). H-IoT systems are capable of monitoring patients' health in real time, with minimal burden to patients and caregivers (Kim, Youm, Jung, & Kim, 2015).

Since the infrastructure itself may not provide enough value for healthcare adoption, H-IoT solutions need to convert the collected data into meaningful information for organizations to consider its use (Chouffani, 2016). The benefits of H-IoT depend heavily on what is done with the data collected and what actions will be taken based on the predictions and patterns found on the data (Chouffani, 2016). Typical applications of IoT for healthcare purposes include: (1) telemonitoring of vital parameters, (2) prevention and detection of falls, and (3) detection of movement in bed using real-time data (Demiris et al., 2008; Knaup & Schöpe, 2014). IoT devices can also collect behavioural data from the patient's home, such as door openings and

closings, ambient temperatures, and indoor movements (Office of the Privacy Commissioner of Canada, 2016b). Screening of these events by health professionals can help prevent accidents and health deterioration by establishing patterns that allow providers to intervene when abnormal behaviour is detected (Chouffani, 2016). For example, changes in data patterns in a smart home can indicate the beginning of a new health problem or the worsening of an existing one (Knaup & Schöpe, 2014). For example, an individual who changes their bathroom habits could be in the initial stages of diabetes or presenting a problem with the administration of diuretics (Knaup & Schöpe, 2014).

Specific user groups may have different needs, leading to niche applications of H-IoT. Active Assistive Living (AAL) technologies for the elderly population and individuals with disabilities are a good example, which is described in the following sub-section.

2.3.1. Active Assistive Living (AAL)

The terms Active Assisted Living and Ambient Assisted Living are sometimes used interchangeably. This proposal will follow the terminology defined by the IEC Systems Committee on AAL (SyC AAL), which defines AAL as Active Assisted Living technology (IEC, 2017).

The elderly population (aged 65 and older) has been rapidly increasing in the past 40 years (Statistics Canada, 2017). This new life expectancy is demanding new models of positive ageing and new alternatives to improve the quality of life (Demiris et al., 2008). One of the possible methods is through the use of Active Assisted Living Technology (AAL) (Antonino, Schneider, Hofmann, & Nakagawa, 2011). AAL technology encompasses products, services, environments, and facilities used to support those whose independence, safety, wellbeing, and autonomy are compromised by their physical and/or mental status (Bamidis, Tarnanas,

Hadjileontiadis, & Tsolaki, 2015). AAL technology's purpose is to provide tools and services capable of improving the quality of life (at any stage of life) while helping individuals live independently (Avilés-López et al., 2010; Rashidi & Mihailidis, 2013).

AAL is an umbrella concept describing technologies designed to improve quality of life, independence, and healthier lifestyles for those who need assistance. AAL technologies use information and communication technologies (ICT), combined with social environments, to provide easy-to-use devices in the home or to support users' lifestyles outside their home environments (Pieper, Antona, & Cortés, 2011).

The AAL environment can integrate assistive technologies, AmI, smart homes and telehealth, using multiple sensors for gathering data and monitoring individuals in their homes (Savage et al., 2009). It can also combine IoT platforms and artificial intelligence to support the care of ageing and incapacitated individuals (Islam et al., 2015). Built-in devices in the home environment can collect metrics about sleep, eating habits, or indoor physical activity, and share useful insights with family members or healthcare providers (Bauer, 2019).

Considering that all IoT technologies require data exchange to deliver their service, understanding data sharing is an essential part of any IoT technology, including AAL, to improve the quality of life of its users. Data sharing is also one of the main gaps regarding standards and guidelines in the AAL field (Fadrique, Rahman, & Morita, 2019).

2.4. DATA SHARING

As maintained by Pasquetto, Randles, & Borgman (2017), data sharing is defined as "*the act of releasing data in a form that can be used by other individuals.*" Easy access to large volumes of structured data is beneficial in several areas such as: (1) smart technologies (Cao et

al., 2016), (2) research (Fecher, Friesike, & Hebing, 2015), (3) individual health (Zhu, Colgan, Reddy, & Choe, 2016), and (4) public health (Van Panhuis et al., 2014; Walport & Brest, 2011).

The recent growth of big data in healthcare, which in the H-IoT space can combine data from electronic patient records (EPR) and mobile health technologies, has not only created a data management challenge (Kostkova et al., 2016), but has also opened the door to new research opportunities and services (Ahlgren, Hidell, & Ngai, 2016). As reported by Fecher, Friesike and Hebing (2015), it will be necessary to create specific policies to compel data sharing in areas such as academia, as well as providing accessible data management platforms to all. According to the same authors, these policies are even more important when collecting data directly from individuals and will require the implementation of clear and transparent rules of consent and anonymization (Fecher et al., 2015).

An example of the benefits of data sharing in healthcare is the joint initiative between Oregon Health and Science University and Intel in 2015 to create the Collaborative Cancer Cloud (Dimitrov, 2016). The cloud solution offers high-performance analytics to collect and securely store private medical data for cancer research (Dimitrov, 2016). Connecting different health datasets helps researchers discover and understand new symptoms, enabling further research and development of possible treatments (Cavan, 2019; Kostkova et al., 2016).

Data sharing also benefits individual healthcare, providing a better understanding of specific diseases, improvements in long-term health conditions, and increasing opportunities for home-care of patients through technology (Kostkova et al., 2016). Access to individual health data through online solutions increases patient convenience and satisfaction, two critical points to keep patients motivated and engaged with the healthcare system (De Lusignan et al., 2014). In

fact, sharing individual data from wearables has been shown to reduce the number of incorrect diagnoses and readmissions to hospitals (Ghanchi, 2018).

In public health, data sharing is widely used for surveillance, to analyze and interpret health-related data to monitor and control diseases, as well as to disseminate the information to improve the health of populations (L. M. Lee & Thacker, 2011; Soucie, 2017). Nevertheless, the fifth major issue in advancing public health surveillance is access to and use of shared data (Frieden et al., 2012).

There are several challenges related to data sharing, for example, privacy, security, and interoperability of the data. Health data is particularly sensitive information and privacy is essential. Within existing systems, a centralized architecture that requires centralized trust is employed (Liang, Zhao, Shetty, Liu, & Li, 2017).

2.5. PRIVACY

Gillian Black (2011) describes privacy as the individual expectation of being free from intrusion. For privacy to exist, a "*reasonable expectation of privacy*" (FindLaw, 2019) or "*need for privacy*" (Daubert et al., 2015) is required by each individual. According to Duhaime's Law Dictionary (2019), privacy is "*a person's right to control access to his or her personal information.*" For this study, I focus on the privacy of personal information transmitted and collected through the Internet. Furthermore, the term privacy will be used to discuss the necessary protections that need to be in place to prevent third parties from exploiting the data without permission (Ahmed Abi Sen et al., 2018).

Privacy goes beyond the individuals' ability to control how their personal information is used (Awad & Krishnan, 2006). It also helps individuals preserve their autonomy and freedom of

expression (Westin, 1970). Through freedom of choice, individuals are more willing to reconsider their privacy and disclose personal data in exchange for social or economic benefits (Culnan & Armstrong, 1999; Leon, Schaub, Cranor, & Sadeh, 2015). On the other hand, companies are increasingly dependent on customer information to offer customized services to increase their value-added communications and maintain customer loyalty (Awad & Krishnan, 2006). Effective use of consumer information has become a competitive difference for many industries and organizations. However, our society must balance these benefits from the use of information with the need to maintain individual privacy (Culnan & Armstrong, 1999). With information overload, it is difficult to make a decision regarding the balance between immediate benefit and the risk associated with misuse or abuse of personal data (Schermer, Custers, & van der Hof, 2014). Companies are responsible for implementing solutions that have privacy by design (Chen, 2019).

In the case of smart homes and AAL technology, the disclosure of household user data may allow large companies to identify the complete profiles of their customers for advertising or behaviour change (Biocco et al., 2018). The data can come from different manufacturers, service providers, and network operators (Cao et al., 2016). The challenge for governments and companies lies in implementing robust data management protocols, and gathering information while preserving privacy, ensuring that users are comfortable with sharing their information (Awad & Krishnan, 2006). An example of a robust solution includes collecting anonymous data and thus preserving the privacy of all parties (Ahmed Abi Sen et al., 2018); together with, decreasing the risk of privacy breaches by increasing the level of transparency between users and businesses and by increasing the level of control individuals have over their personal information (Awad & Krishnan, 2006). Moreover, when building data management solutions, companies

need to take into account the culture of their users, since cultural values have an influence on users' concerns about information privacy (Bellman, Johnson, Kobrin, Lauder, & Lohse, 2004).

Within the privacy realm, privacy agreements or privacy policies are required by law if any personal information is being collected from users. They must detail how the company handles user information in order to increase transparency (Awad & Krishnan, 2006; Biocco et al., 2018). The Personal Information Protection and Electronic Documents Act (PIPEDA) was created in Canada in April of 2000 as federal privacy law for private sector organizations, and it establishes the basic rules for how companies must handle personal information (OPC, 2018). According to PIPEDA, any violations of the confidentiality of a patient's health records can result in fines of up to $500,000 to health care providers (Contant, 2018). Transparency and control over ones' data are important antecedents for the establishment and maintenance of trust in institutions and corporations (Demiris et al., 2008). In like manner, even if companies have clear and lawful privacy agreements through the use of consent, they can still face trust issues with users when they feel they have been deceived (Schermer et al., 2014). These trust issues can be explained by a significant relationship between the content presented in privacy policies and trust, as well as, between privacy concerns and trust (Wu, Huang, Yen, & Popova, 2012).

2.6. TRUST

Trust is an essential element for proper interactions between two or more entities, for example, this is true between individuals, institutions, and technologies (Morita & Burns, 2014a; Parasuraman & Riley, 1997). In the case of IoT technology, trust is considered an enabler as it mediates the connection between devices and supporting technology collecting and processing customer data. It is crucial for such technology to act following users' needs while respecting

users' rights (Sicari et al., 2015). Users trust in technology relies on the policies that regulate technology and on the the idea of informed consent (Jensen, Potts, & Jensen, 2005). The result of a survey conducted by TrustArc (2014) in 2014 on consumer attitudes toward data collection through smart devices showed that users want to have more control and understanding of the personal data collected by such devices and are concerned about the type of information collected (TrustArc, 2014).

A common perspective on trust is that trust is directly related to accepting risks in exchange for benefits (J. D. Lee & See, 2004; Morita & Burns, 2014b). Without the establishment of proper trust, technology cannot provide all the benefits offered to its users. A trust relationship between different parties results from the belief that the parties involved are integral, consistent, honest, fair, responsible, helpful, and benevolent (Morgan & Hunt, 1994; Richards & Hartzog, 2015). Such trust is not built through conversations or intentions, but instead through demonstrated evidence gathered during interactions between the parties (Chen, 2019). According to Sicari et al. (2015), users privacy depends on their trustworthiness and anonymity.

In a connected world, trust is based on security and privacy (Chen, 2019). As an example, users who have had experiences with privacy breaches have a lesser tendency to provide their data for personalized advertising, but not for other personalized services as they see a higher value on the second one (Awad & Krishnan, 2006). Individuals often rely more on trusted technologies and reject technologies they do not trust (J. D. Lee & See, 2004). The same goes for organizations (Morgan & Hunt, 1994) and internet commerce (Müller, 1996). For instance, a survey conducted in 2009, before the Facebook scandals, shows that consumers relied more on

Facebook than MySpace because they believed their data was safer with Facebook since MySpace had been breached before (Fogel & Nehmad, 2009).

Privacy and trust are enablers for a successful data sharing process in the digital world (Frieden et al., 2012). Transparency is a prerequisite for building trust when sharing public health surveillance data (Chatham House, 2018). For example, the presence of government regulation can be considered a cue for transparency, increase user trust and reduce privacy concerns (Acquisti, Brandimarte, & Loewenstein, 2015). Moreover, trust and transparency facilitate collaboration and act as catalysts by generating applications for data collected through surveillance networks (Frieden et al., 2012).

Trust has a positive and strong influence on how technology is accepted by users (Barakat & Sheikh, 2010). Consequently, it is a critical factor for user adoption and acceptance of new technologies (Wintersberger, Frison, & Riener, 2018).

2.7. USER ACCEPTANCE

User acceptance reflects how willing a user is to adopt a new technology that was not used in the past (Wang, Wu, & Wang, 2009). A balance between the benefits of technology, the level of need for the technology, and the perception of loss of privacy needs to be achieved to make the technology worthwhile (Demiris et al., 2008). Just like trust, user acceptance is also crucial for proper interaction between people and technology. The same emotions and attitudes that influence the human-human relationship will also influence human-automation interactions working as a relationship-building factor alongside the security and performance of the technology (J. D. Lee & See, 2004). Some of the factors that affect user acceptance are subject normalcy, perceived usefulness, perceived ease of use, attitude, behavioural intentions and actual

usage (Sun & Zhang, 2006). The user's belief that technology will improve their performance (perceived usefulness) is a clear indicator of technology's intended use (Wang et al., 2009). However, not taking into consideration user behaviour, needs, and values can lead to a lack of perceived usefulness in the proposed technology, poor usability, low acceptability, increase risk, and lack of trust (Huldtgren, Ascencio, Pedro, Pohlmeyer, & Romero Herrara, 2014). The perception of risk is directly affected by the concern for data privacy and trust in technology, as described by Miltgen et al. (2013).

3. STUDY RATIONALE

There is a global increase in the number of individuals seeking healthcare, and the burden on existing systems is immense; consequently, this creates a higher demand for home-care services as patients become more comfortable with self-managing their health (Koch, 2006). While there is a rise in the need for home-care, there is a proliferation of available healthcare IoT solutions and AAL devices are expected to increase exponentially in the coming years, becoming a force in all organizations and having an expected economic growth of more than $3 trillion per year by 2026 (Newman, 2019). The growth of the IoT market also increases the amount of personal data collected on a daily basis at a global level; the amount of personal data grows faster than the IoT data collected from the manufacturing and finance industries (Kent, 2018).

As previously discussed, a significant barrier to the adoption of IoT devices and data sharing to improve quality of life are privacy and security (Ahmed Abi Sen et al., 2018; Dimitrov, 2016). Many of the privacy and security issues with IoT technologies are due to the limited computing power and the high number of interconnected devices (Sicari et al., 2015). This network of automated communication between devices allows little control over the data collected by users and provides limited opportunities for users to trust the tech companies holding their data (Daubert et al., 2015). Current standards for IoT and AAL technologies are currently under development with companies like the CSA Group that have invested in researching and developing standards to address the existing challenges, as demonstrated in our recent report from Ubilab (University of Waterloo) in partnership with the CSA Group over the last 2 years (Fadrique et al., 2019).

The general public stands to benefit from the increase in data availability and the development of better analytical tools to aid in clinical decision-making. Healthcare providers,

for example, can use this new intelligence to collect more data, sending it to the cloud for future analysis to support diagnosis and decision making.

While this technology has the power to benefit individual and clinical decision making, the value to vulnerable and elderly population may prove inestimable. H-IoT solutions and AAL devices have the potential to improve quality of life and support a more dignified and comfortable independent aging process. However, the average user is not fully informed about how his or her data is collected, stored, and shared through wearables and IoT devices (see Figure 2).

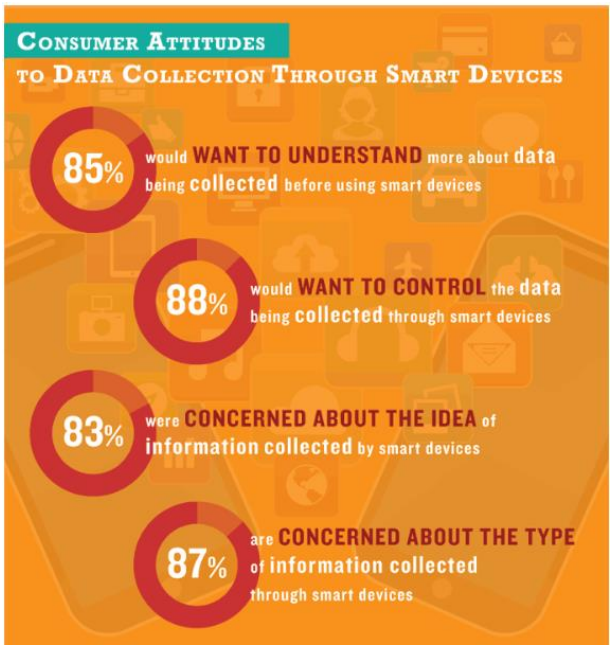


Figure 2. Consumer's attitude to data collection through smart devices. Image source: (TrustArc, 2014)

While concerns with data flow and usage are serious, the benefits of this technology are immense. One of the ways user trust might be fostered is through increasing transparency in privacy agreements, privacy policies, and data usage. Privacy agreements, or privacy policies, are standardized documents used to inform users of how companies handle their user information (Tsai, Cranor, Acquisti, & Fong, 2006). Yet, these documents contain jargon and legal

terminology that makes it possible for companies to remain ambiguous about data use (Biocco et al., 2018). As a result, trust can be compromised as transparency is essential for building consumer trust (Nati, 2018). In a global ranking, Canada ranks third in the number of cyber incidents and is ninth in the number of exposed patient records, with health services and financial services being the most affected sectors (Contant, 2018). With these rankings in mind, it is understandable that patients and caregivers may be distrustful in regards to how their data is used and protected.

4. OBJECTIVES AND RESEARCH QUESTION

This proposal seeks to explore (1) the user's perspective regarding trust when sharing their healthcare IoT data with different types of organizations (e.g., health providers, government); (2) how trust levels and privacy concerns are affected by socio-cultural frameworks established by different local privacy policies and regulations according to the specific region participants are in (e.g., Canada, United States, or Europe).

These objectives will be achieved by answering the following research questions through the studies presented in this thesis proposal:

RQ1: What are the differences in privacy concern levels and awareness levels on data ownership when comparing different regions?

H1: Levels of privacy concern and awareness levels on data ownership will be different between regions, driven by socio-cultural frameworks established by different local privacy policies and regulations, and dictated by which region participants are in.

RQ2: What are the users' perspectives on data sharing and trust in different types of organizations based on primary privacy concerns?

H2: User perspectives on trust will be different for different types of organizations, affected by historical data and existing privacy policies.

RQ3: What are the differences in trust levels for users from Canada, the USA, and Europe when trusting their Healthcare IoT data to other stakeholders?

H3: Canada, the USA, and Europe will have a significant difference in trust levels when trusting other stakeholders with their healthcare IoT data, driven by socio-cultural frameworks established by different local privacy policies and regulations, and dictated by which region participants are in.

5. METHODOLOGY

In order to examine the perspectives of users and researchers regarding privacy and trust in data sharing and IoT technology for health applications, this thesis will leverage data from a literature review and questionnaires.

This section describes the study design, sample, procedure, data collection, and data analysis to answer the research questions.

5.1.1. Study Design

The questionnaires were designed and deployed using a between-subject design (Charness, Gneezy, & Kuhn, 2012). Each participant answered trust questions regarding one, and only one, type of organization (e.g., healthcare providers or insurance companies). Each participant received and answered 3 sets of questionnaires: a demographics questionnaire, a privacy questionnaire, and a trust questionnaire (see Appendix A). The trust questionnaire had four variations to represent the different types of institutions: (1) big companies (e.g., Google, Facebook) (see Appendix A – Big Companies); (2) government (see Appendix A – Government); (3) healthcare providers (see Appendix A – Healthcare Providers); and (4) insurance companies (see Appendix A – Insurance Companies). Examples of "big companies" include Apple, Google, Amazon, Facebook, and Microsoft. The four variations representing the types of organizations were randomly allocated by Mechanical Turk using even proportions to maintain equal proportions between groups and to avoid order effect.

The questionnaire was designed using Qualtrics, which is the preferred survey platform at the University of Waterloo, and Mechanical Turk as a tool to support recruitment (see Appendix A: Questionnaire – Trust in Organizations). Mechanical Turk was chosen as a distribution tool as

it provides access to thousands of participants around the world with a significant presence in the USA and Canada (Difallah, Filatova, & Ipeirotis, 2018).

Table 1
List of seven surveys used as basis for the creation of the questionnaire for this study

Year	Authors	Title
2006	Tsai, Janice Cranor, Lorrie Faith Acquisti, Alessandro Fong, Christina M.	What's It To You? A Survey of Online Privacy Concerns and Risks (Tsai et al., 2006)
2007	Dwyer, Catherine Roxanne, Starr Passerini, Katia	Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace (Dwyer, Roxanne, & Passerini, 2007)
2016	Office of the Privacy Commissioner of Canada	2016 Survey of Canadians on Privacy (Office of the Privacy Commissioner of Canada, 2016a)
2017	Open Data Institute YouGov	Attitudes Towards Data Sharing (Open Data Institute & YouGov, 2017)
2018	Carras, Katherine Farmaha, Ramandeep Ramesh, Krishn Santasheva, Anastasia	Priv: Privacy Simplified (Carras, Farmaha, Ramesh, & Santasheva, 2018)
2018	Akamai	Research: Consumer Attitudes Toward Data Privacy Survey (Akamai, 2018)
2018	RSA	RSA Data Privacy & Security Report (RSA, 2018)

The questions were designed using Likert-type scales (ranging from 1 to 5, where 1 equals strongly disagree, and 5 equals strongly agree) and were developed with the following guiding questions:

- What types of privacy concerns do individuals have regarding their data?

- What differentiates users' trust in the four types of organizations from other trust-based contracts in terms of data sharing?

Statements like "*I can count on [type of organization] to protect customers' personal information from unauthorized use*" and "*I trust that [type of organization] will not use my personal information for any other purpose*" (Dwyer et al., 2007) will be used to identify users' perceptions of trust in data sharing with different types of organizations. In that sense, the higher the participant ranks each answer on the scale, the more the participant trusts the type of organization presented. The questionnaire's content was developed based on the results of the literature review, specifically on seven different surveys conducted between 2006 and 2018, as shown in *Table 1*.

5.1.2. Sampling Frame

This study targeted individuals from Canada, the USA, and Europe; over the age of 18; from any ethnic group and gender. The three regions were selected due to similar challenges with the ageing of their population (Christensen, Doblhammer, Rau, & Vaupel, 2009) and similar IoT market cultures, hence bringing essential insights around privacy and data sharing using H-IoT.

The necessary sample size was calculated using Qualtrics online sample size calculator based on a confidence level of 95%, a population size of 7300, and a margin of error of 5%. The population size was based on Difallah, Filatova, & Ipeirotis' (2018) analysis, which states that the real number of participants available for academic experiments in Mechanical Turk is approximately 7300. Basic demographic questions (e.g., age, education, and home country) relevant to understanding the representativeness of the participants were combined with questions about privacy, data sharing, and trust. Due to the technical nature of some of the concepts being covered in these studies and the need for participants to have been exposed to

data sharing in the IoT context, I am recruiting participants with a minimal knowledge of technology and understanding of the presented concepts. Typical participants in the MTurk sampling frame tend to be younger, heavier Internet users, and from lower and middle-income families (Cheung, Burns, Sinclair, & Sliter, 2017), which provide an excellent participant pool for the studies presented in this proposal.

Four hundred participants agreed to participate through MTurk, and 392 completed the questionnaire with 129 participants from Canada, 132 from the USA, 131 from Europe, and 6 from other countries and regions, which were excluded from the total. Participants' ages ranged from 18 to 90 years divided in 6 age range groups: (1) 18 – 25; (1) 26 – 30; (3) 26 – 30; (4) 36 – 45; (5) 46 – 55; and (6) 56 – 90.

5.1.3. Ethics

This study was reviewed and approved by the University of Waterloo Office of Research Ethics (ORE #40606). Each participant signed a consent form electronically after indicating that they understood what the study entailed (Appendix B: Information and Consent letter). The consent form, along with the personal information form, outlined the purpose of the study, their roles as participants, how their information would stay confidential, that their participation was voluntary, that they could withdraw from the study or part of the study at any time. Additionally, the forms had the contact information of both myself and that of my supervisor in the event that participants had further questions regarding the study. All questions in the questionnaire were carefully designed to specifically address the objectives of this thesis.

Mechanical Turk assigns participants a unique worker ID to help with anonymization. In this study, participants answered the questionnaire using an external survey software (Qualtrics), through which personal information from Mechanical Turk workers was not visible to the

requester (researchers) in the platform. Such approach ensures that subject response cannot be linked to their identity by any individual that has access to the data (Paolacci, Chandler, Ipeirotis, & Stern, 2010). Individual unique participant IDs will remain confidential and will not be disclosed in academic publications or in the release of the study findings. The data collected in this study will be encrypted and stored on servers located at the University of Waterloo for 7 (seven) years. The average time to complete each questionnaire was estimated at 10 minutes and each participant (MTurk worker) received $ 1.00 per survey (which would be the equivalent of $ 6 per hour). There are no anticipated risks or harm expected for participants in this study.

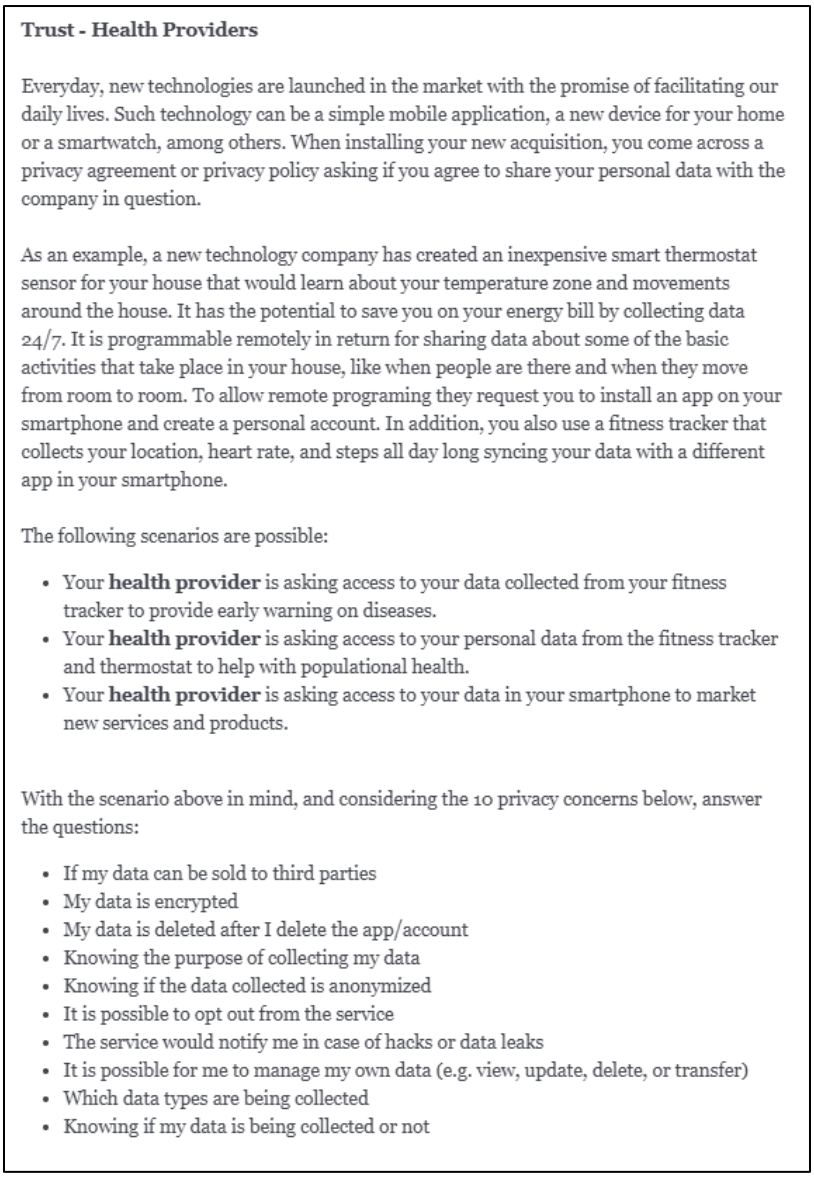
5.1.4. Data Collection

Recruitment for this study happened through Mechanical Turk. All study participants were already registered as workers in the MTurk tool. The questionnaire was first published on September 13, 2019, and made available to 80 participants from each region for five days. By the following day, the number of participants had been reached, allowing for a second publication, with 40 participants per region, targeting the age groups with the least number of participants.

When opening the questionnaire, each participant was presented with a short introduction and a link to access the questionnaire. By clicking the link, the participant was directed to the Qualtrics platform, which is a software for designing and hosting online surveys. When redirected, the participant was presented with the information and consent letter (Appendix B: Information and Consent letter). In order to continue with the questionnaire and be compensated for their participation by the MTurk tool, each participant has to agree to proceed.

The questions were aggregated into three groups: (1) the first group with 6 demographic questions (see Appendix A); (2) the second group with 5 privacy-related questions; and (3) the third group with 16 trust-related questions. In order to create a framework for the study and to

provide the necessary context, a scenario was presented to each participant at the beginning of the trust-related question group. The scenario describes the fictional use of a smart thermostat and a fitness tracker, listing three possible ways that the data collected could be used and shared. Each participant received the scenario tailored to the type of organization they had been assigned. A sample scenario associated with the insurance companies' use-case is presented in Figure 3.



Trust - Health Providers

Everyday, new technologies are launched in the market with the promise of facilitating our daily lives. Such technology can be a simple mobile application, a new device for your home or a smartwatch, among others. When installing your new acquisition, you come across a privacy agreement or privacy policy asking if you agree to share your personal data with the company in question.

As an example, a new technology company has created an inexpensive smart thermostat sensor for your house that would learn about your temperature zone and movements around the house. It has the potential to save you on your energy bill by collecting data 24/7. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house, like when people are there and when they move from room to room. To allow remote programing they request you to install an app on your smartphone and create a personal account. In addition, you also use a fitness tracker that collects your location, heart rate, and steps all day long syncing your data with a different app in your smartphone.

The following scenarios are possible:

- Your **health provider** is asking access to your data collected from your fitness tracker to provide early warning on diseases.
- Your **health provider** is asking access to your personal data from the fitness tracker and thermostat to help with populational health.
- Your **health provider** is asking access to your data in your smartphone to market new services and products.

With the scenario above in mind, and considering the 10 privacy concerns below, answer the questions:

- If my data can be sold to third parties
- My data is encrypted
- My data is deleted after I delete the app/account
- Knowing the purpose of collecting my data
- Knowing if the data collected is anonymized
- It is possible to opt out from the service
- The service would notify me in case of hacks or data leaks
- It is possible for me to manage my own data (e.g. view, update, delete, or transfer)
- Which data types are being collected
- Knowing if my data is being collected or not

Figure 3. Example of use-case scenario - Insurance Companies

Each participant receives questionnaires related to only one type of organization (e.g., government or big companies), which is randomized using the Qualtrics randomization function to ensure a balanced sample. Following this first scenario, the participant was asked to consider a list of ten privacy agreement concerns that were presented to them as a means to establish standard levels of exposure to IoT data-sharing challenges. Finally, participants were asked to answer the trust-related questions that are available in the Appendices, as well as a sample in Figure 4. (see complete questionnaire in Appendix A: Questionnaire – Trust in Organizations).

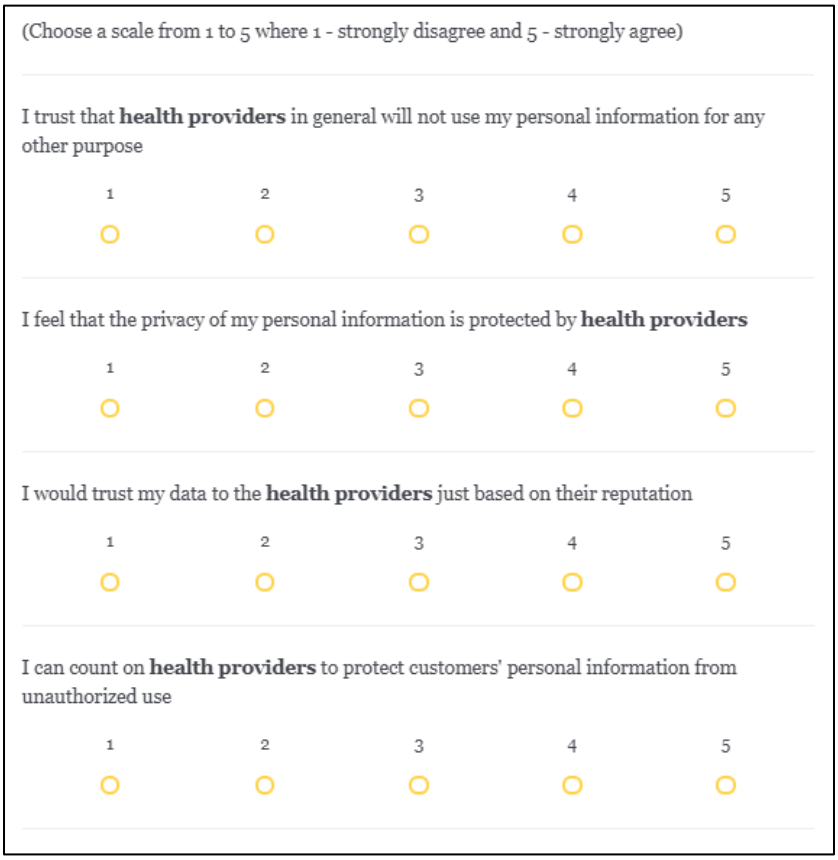


Figure 4. Trust-related sample questions

The list of the top 10 privacy concerns presented is the result of a previous project conducted by the UbiLab with the CSA Group aimed at identifying the main user concerns regarding privacy agreements and suggesting a new way to present the information using images

and pictograms. The results of that study will be presented as a research report that will be published by the CSA Group and later submitted as a peer-reviewed article.

All collected data were downloaded to a secure server at the University of Waterloo. Entries that were incomplete were deleted along with records from participants coming from regions other than Canada, the USA, and Europe.

5.1.5. Data Analysis

Analysis of variance (ANOVA)

This study uses a one-way Analysis of Variance (ANOVA) for the research questions to explore differences between response patterns as outlined in the research questions above. According to Venkatesh, Brown, & Bala (2013), "*ANOVA can be used to compare the means of several groups using only one way of data classification, the dependent variable."*

The outcome analysis focused on 16 trust-related questions and two privacy questions (questions 7 and 8) and awareness levels on data ownership (question 9). Each answer was re-coded to reflect positive and negative results. The scale used in the survey, which initially ranged from 1 a 5, where 1 is equal to strongly disagree, and 5 is equal to strongly agree, was changed to -2 to 2. The mean value of the trust-related questions from each participant was computed to use as a trust and dependent variable, while the types of organizations were treated as an independent variable. IBM SSPS from IBM was used for computing the statistical analysis.

Pair-wise t-test with Bonferroni correction

A Bonferroni correction is a mathematically equivalent adjustment or correction that is achieved by dividing the probability value (usually 0.05) by the number of tests conducted. The Post Hoc Bonferroni test from SPPS uses t-tests to perform pair-wise comparisons between group means but controls the overall error rate by setting the error rate for each test to the

experiment error rate divided by the total number of tests. The observed significance level is adjusted for the fact that multiple comparisons are being made. Pair-wise t-test was used to compare each test to the responses from each region, or type of organization, and was only performed once we found statistically significant results from the ANOVA.

6. RESULTS

Three hundred and ninety-two participants were recruited for this study through Mechanical Turk, with 129 participants from Canada, 132 from the USA, and 131 from Europe. The majority of participants were males (65.05%), and the majority had a university degree (54.59%). *Table 2* summarizes the results of the demographics questionnaire from all eligible participants included in the data analysis.

Table 2
Participants demographics by Type of Organization

Demographics (n (%))	**Big Companies**	**Govern-ment**	**Health Providers**	**Insurance Companies**	**Total**
Region					
Canada	33 (33.67%)	28 (28.57%)	34 (34.00%)	34 (35.42%)	129 (32.91%)
USA	37 (37.76%)	31 (31.63%)	38 (38.00%)	26 (27.08%)	132 (33.67%)
Europe	28 (28.57%)	39 (39.80%)	28 (28.00%)	36 (37.50%)	131 (33.42%)
Sex					
Female	31 (31.63%)	36 (36.73%)	31 (31.00%)	38 (39.58%)	136 (34.69%)
Male	67 (68.37%)	62 (63.27%)	68 (68.00%)	58 (60.42%)	255 (65.05%)
Others	-	-	1 (1.00%)	-	1 (0.26%)
Age range					
Age 18 - 25	17 (17.35%)	29 (29.59%)	28 (28.00%)	20 (20.83%)	94 (23.98%)
Age 26 - 30	26 (26.53%)	21 (21.43%)	26 (26.00%)	25 (26.04%)	98 (25.00%)
Age 31 - 35	21 (21.43%)	10 (10.20%)	8 (8.00%)	17 (17.71%)	56 (14.29%)
Age 36 - 45	17 (17.35%)	16 (16.33%)	18 (18.00%)	19 (19.79%)	70 (17.86%)
Age 46 - 55	14 (14.29%)	13 (13.27%)	14 (14.00%)	9 (9.38%)	50 (12.76%)
Age 55 - 90	3 (3.06%)	9 (9.18%)	6 (6.00%)	6 (6.25%)	24 (6.12%)
Highest level of education					
College and Trades	16 (16.33%)	21 (21.43%)	25 (25.00%)	22 (22.92%)	84 (21.43%)
High school	19 (19.39%)	24 (24.49%)	23 (23.00%)	25 (26.04%)	91 (23.21%)
University	63 (64.29%)	50 (51.02%)	52 (52.00%)	49 (51.04%)	214 (54.59%)
None of the above	-	3 (3.06%)	-	-	3 (0.77%)

Sections 6.1 to 6.3 will present the results of the data analysis executed for each of the three research questions. Each section will start with the results of the one-way ANOVA with descriptive statistics, followed by the results of the pair-wise t-test with the Bonferroni correction for multiple comparisons, and the boxplot representation of the results. Section 6.1 will present the other results grouped by age.

6.1. RESEARCH QUESTION 1

What are the differences in privacy concern levels and awareness levels on data ownership when comparing different regions?

A one-way ANOVA was used to determine if the level of privacy concern from questions 7 and 8, and awareness levels on data ownership (question 9) was different for each region in the study. Privacy concern levels (LConcern) were measured using a scale where the lower the response value, the lower the worry levels, and the higher the value, the higher the worry level. The awareness levels on data ownership (LAwareness) used the same type of scale where the lower the value, the lower the awareness, and the higher the value, the higher the awareness. The answers to each question were analyzed separately, and participants were classified into three regions: Canada (n = 129), the USA (n = 132), and Europe (n = 131). Descriptive statistics were used to assess the distribution of the overall data.

For the first privacy question - "*Are you concerned about your privacy while you are using the internet?"* – LConcern was different across regions but the difference between regions was not statistically significant (F (2, 389) = 0.157, *P* = .86) (See Table 3 and Figure 5). See Appendix C - Question 1 for tables and details.

Table 3
Descriptive for One-way ANOVA - Question 1 analysis by region (LConcern)

Descriptives

Question 7 - Are you concerned about your privacy while you are using the internet?

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Canada	129	.92	.924	.081	.76	1.08	-2	2
USA	132	.89	1.001	.087	.71	1.06	-2	2
Europe	131	.95	1.022	.089	.78	1.13	-2	2
Total	392	.92	.981	.050	.82	1.02	-2	2

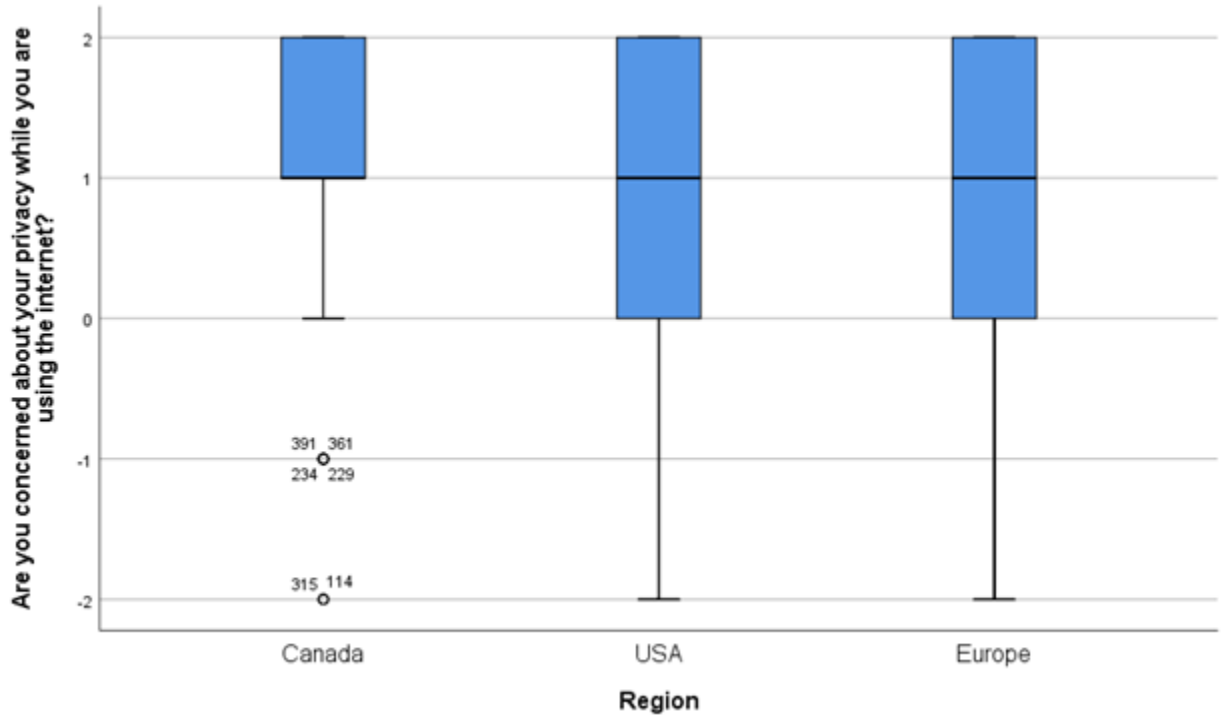


Figure 5. Boxplot one-way ANOVA comparing regions for privacy question 7

The second privacy question - *"Are you concerned about people you do not know obtaining personal information about you from your online activities?"* – LConcern was also different for each region, but the difference between the regions was not statistically significant

(F (2, 389) = 0.736, *P* = .48) (See *Table 4* and Figure 6). See Appendix C - Question 2 for tables and details.

Table 4
Descriptive for One-way ANOVA - Question 2 analysis by region (LConcern)

Descriptives

Question 8 - Are you concerned about people you do not know obtaining personal information about you from your online activities?

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Canada	129	.99	.923	.081	.83	1.15	-2	2
USA	132	.85	1.088	.095	.66	1.04	-2	2
Europe	131	.97	1.074	.094	.78	1.16	-2	2
Total	392	.94	1.031	.052	.83	1.04	-2	2

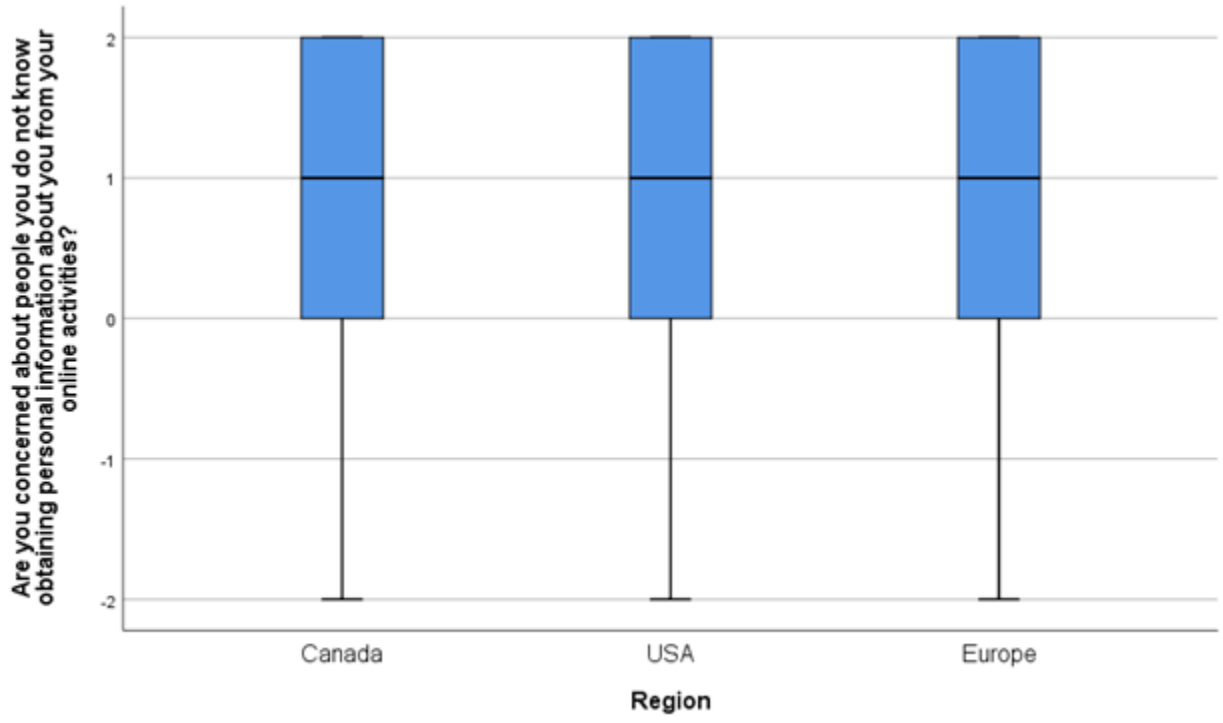


Figure 6. Boxplot one-way ANOVA comparing regions for privacy question 8

The question about awareness – *"I understand who has ownership of my online data."* – LAwareness was different across regions, but the difference between the regions was not

statistically significant (F (2, 389) = 2.447, *P* =.088) (See *Table 5* and Figure 7). See Appendix C - Question 3 for tables and details.

Table 5
Descriptive for One-way ANOVA - Question 3 analysis by region (LAwareness)

Descriptives

Question 9 - I understand who has ownership of my online data.

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Canada	129	-.40	1.208	.106	-.61	-.18	-2	2
USA	132	-.17	1.182	.103	-.38	.03	-2	2
Europe	131	-.08	1.181	.103	-.28	.13	-2	2
Total	392	-.21	1.195	.060	-.33	-.10	-2	2

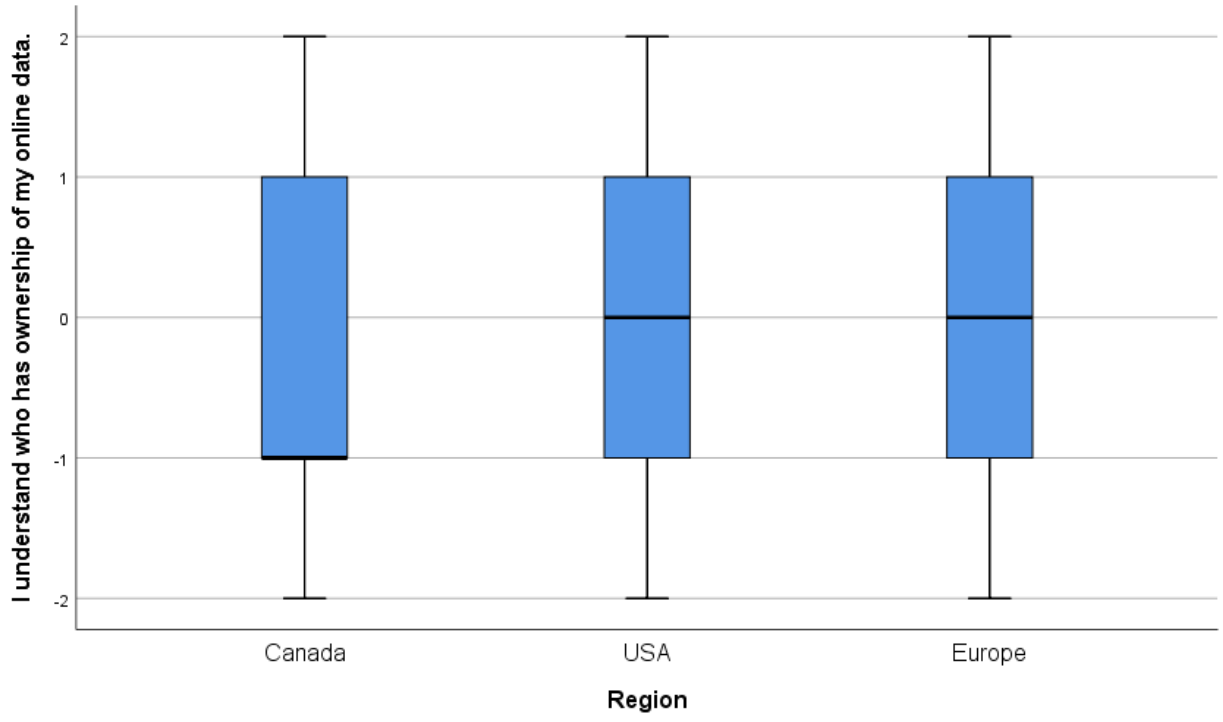


Figure 7. Boxplot one-way ANOVA comparing regions for privacy question 9

6.2. RESEARCH QUESTION 2

What are the users' perspectives on data sharing and trust in different types of organizations based on primary privacy concerns?

6.2.1. Overall Analysis

A one-way ANOVA was used to analyze trust – on a scale where the lower the value corresponds to lower trust, and the higher the value corresponds to higher trust – to determine if the level of trust (LTrust) was different for the four types of organizations. Participants were allocated into four groups: big companies (n = 98), government (n = 98), health providers (n = 100), and insurance companies (n = 96). Descriptive statistics were used to observe the distribution of the overall data (see *Table 6*).

Table 6
Descriptive for One-way ANOVA - Overall analysis by type of organization

Descriptives

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	98	-.1849	.57772	.05836	-.3008	-.0691	-2.00	1.13
Government	98	-.2423	.66310	.06698	-.3753	-.1094	-2.00	.88
Health Providers	100	.0688	.68122	.06812	-.0664	.2039	-1.69	1.75
Insurance	96	-.4492	.72759	.07426	-.5966	-.3018	-2.00	.88
Total	392	-.1993	.68719	.03471	-.2675	-.1311	-2.00	1.75

LTrust was statistically significant between different types of organizations only, F (3, 388) = 10.107, *P* =.000. LTrust increased from insurance companies (M = -0.4492, SD = 0.7276) to government (M = -.2423, SD = 0.6631), big companies (M = -0.1849, SD = 0.5777), and health providers (M = 0.0688, SD = 0.6812), in that order. Figure 8 shows side-by-side boxplots

to better visualize the results from the ANOVA. See Appendix D, subsection 9.4.1 for tables and details.

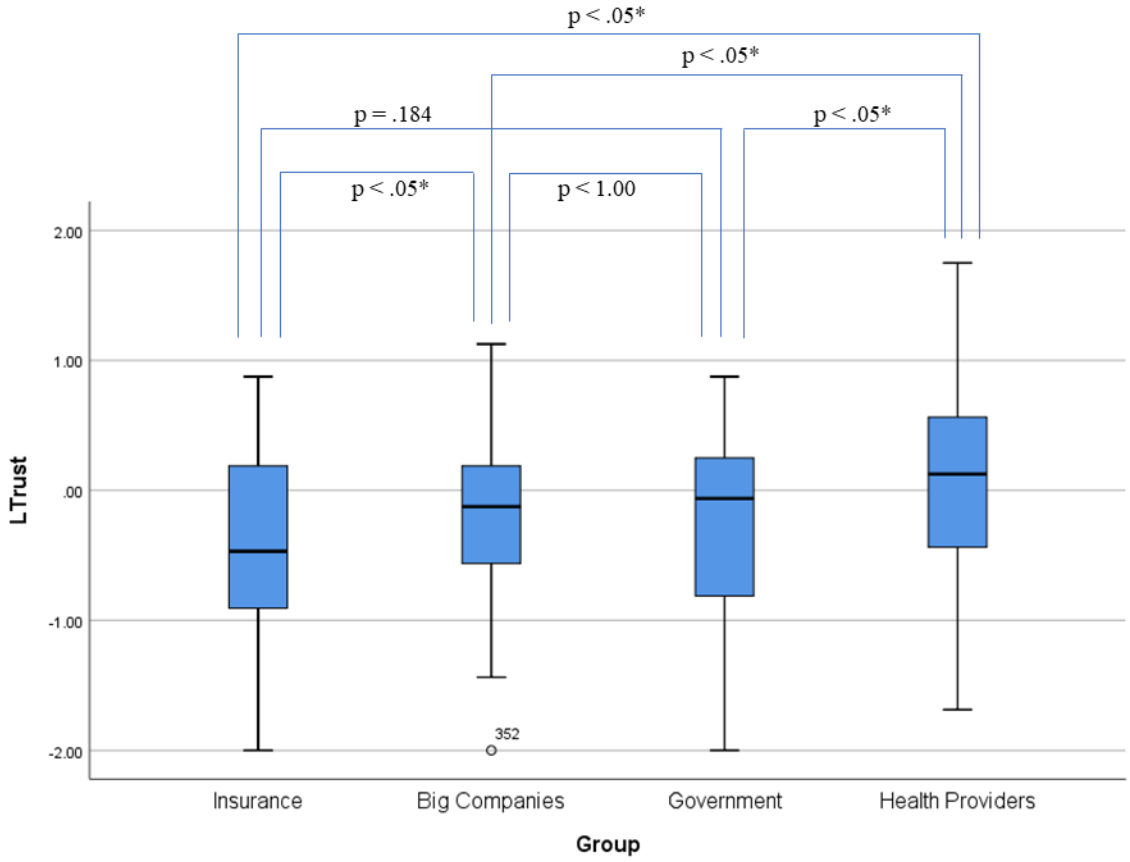


Figure 8. Boxplot one-way ANOVA comparing types of organizations

Pair-wise t-tests with Bonferroni correction indicated that the mean score for the big companies (M = -0.1849, SD = 0.5777) was significantly different (*P* = 0.045) than health providers (M = 0.0688, SD = 0.6812), and significantly different (*P* = 0.035) than insurance companies (M = -0.4492, SD = 0.7276). However, big companies (M = -0.1849, SD = 0.5777) did not significantly differ from government (M = -0.2423, SD = 0.6631).

Pair-wise t-test with Bonferrani correction also indicated that the mean score for health providers (M = 0.0688, SD = 0.6812) was significantly different (*P* = 0.006) than government (M = -0.2423, SD = 0.6631), and significantly different (*P* = 0.000) than insurance companies

(M = -0.4492, SD = 0.7276). Finally, government (M = -0.2423, SD = 0.6631) did not significantly differ from insurance companies (M = -0.4492, SD = 0.7276). See Appendix D, subsection 9.4.2 for tables and details.

6.2.2. Results Grouped by Region

To be able to answer survey question number three, the dataset was grouped by region (Canada, the USA, and Europe), and a one-way ANOVA was used, so the difference between the types of organizations can be assessed separately for each region.

Canada

A one-way ANOVA was used to determine if the level of trust (LTrust) was different for the four types of organizations within our Canadian sub-sample. Participants responses were classified into four groups: big companies (n = 33), government (n = 28), health providers (n = 34) and insurance companies (n = 34). Descriptive statistics were used to analyze the distribution of the overall data (see *Table 7*).

Table 7
Descriptive for One-way ANOVA - Canada

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	33	-.1932	.52416	.09125	-.3790	-.0073	-1.44	1.00
Government	28	-.1853	.56404	.10659	-.4040	.0334	-1.31	.88
Health Providers	34	.1581	.56496	.09689	-.0390	.3552	-1.06	1.75
Insurance	34	-.4926	.69132	.11856	-.7339	-.2514	-2.00	.75
Total	129	-.1778	.63061	.05552	-.2877	-.0679	-2.00	1.75

a. Region = Canada

LTrust was statistically significantly between different types of organizations only, F (3, 125) = 6.882, *P* =.000. LTrust increased from insurance companies (M = -0.4926, SD = 0.6913) to big companies (M = -0.1932, SD = 0.5242), government (M = -0.1853, SD = 0.5640), and health providers (M = 0.1581, SD = 0.5650), in that order. Figure 9 shows side-by-side boxplots to better visualize the results from ANOVA analysis. See Appendix E, subsection 9.5.1 for tables and details.

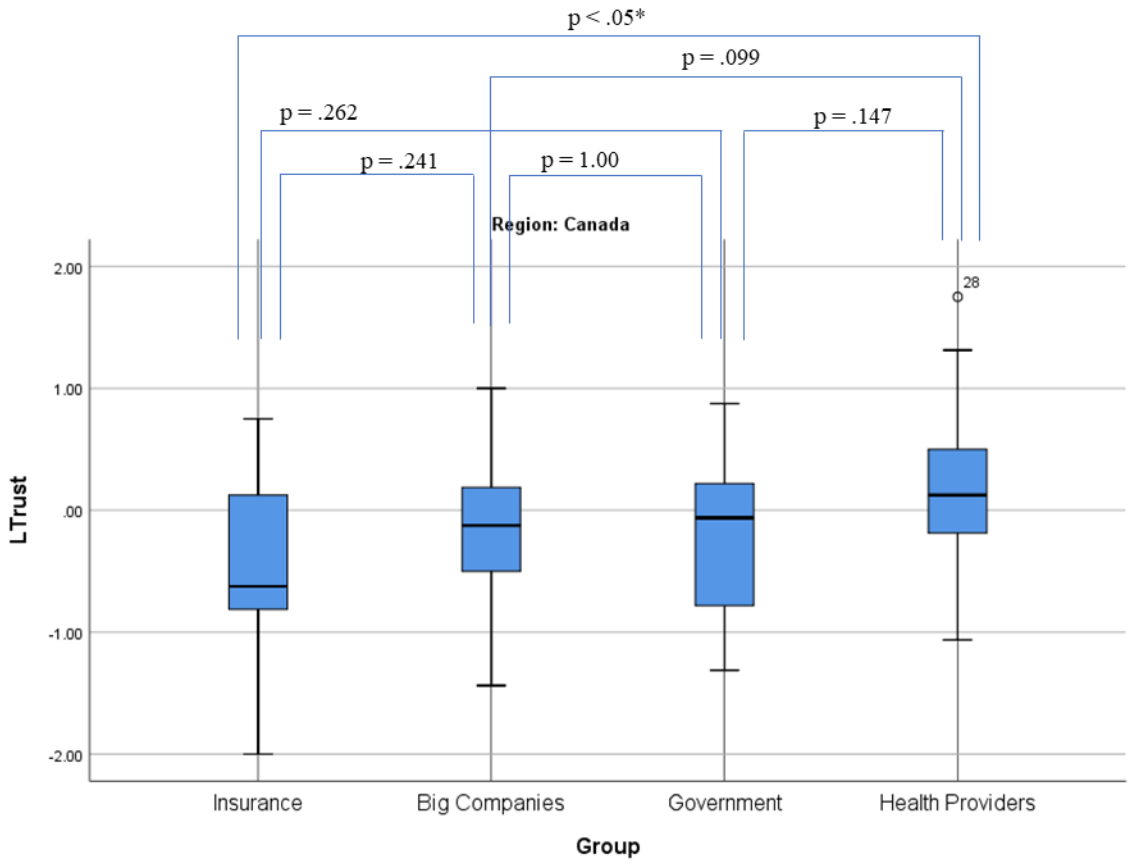


Figure 9. Boxplot one-way ANOVA comparing types of organizations for Canada

Pair-wise t-tests with Bonferroni correction indicated that the mean score for health providers (M = 0.1581, SD = 0.5650) was significantly different (*P* = 0.000) than insurance companies (M = -0.4926, SD = 0.6913). However, any other combination did not present significant difference. See Appendix E, subsection 9.5.2 for tables and details.

United States of America (USA)

A one-way ANOVA was used to determine if the level of trust (LTrust) was different for the four types of organizations within our American sub-sample. Participant responses were classified into four groups: big companies (n = 37), government (n = 31), health providers (n = 38), and insurance companies (n = 26). Descriptive statistics were used to observe the distribution of the overall data (See *Table 8*).

Table 8
Descriptive for One-way ANOVA - USA

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	37	-.2922	.64230	.10559	-.5064	-.0781	-2.00	1.00
Government	31	-.6935	.73480	.13197	-.9631	-.4240	-2.00	.44
Health Providers	38	-.1168	.80252	.13019	-.3806	.1470	-1.69	1.19
Insurance	26	-.6178	.78249	.15346	-.9338	-.3017	-2.00	.63
Total	132	-.4001	.76950	.06698	-.5326	-.2676	-2.00	1.19

a. Region = USA

LTrust was statistically significantly between different types of organizations only, F (3, 128) = 4.488, *P* = .005. LTrust increased from government (M = -0.6935, SD = 0.7348) to insurance companies (M = -0.6178, SD = 0.7825), big companies (M = -0.2922, SD = 0.1056), and health providers (M = -0.1168, SD = 0.8025), in that order. Figure 10 shows side-by-side boxplots to better visualize the results from ANOVA analysis. See Appendix E, subsection 9.5.3 for tables and details.

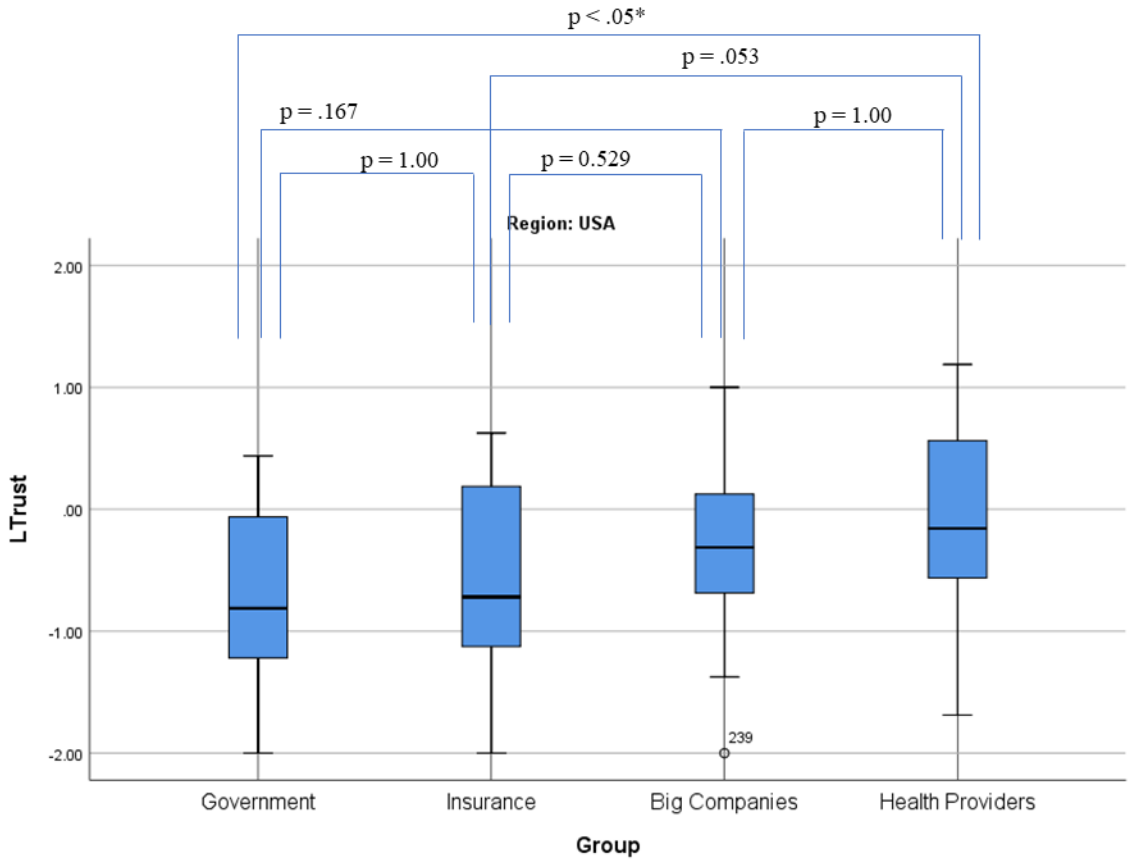


Figure 10. Boxplot one-way ANOVA comparing types of organizations for the USA

Pair-wise t-tests with Bonferroni correction indicated that the mean score for health providers (M = -0.1168, SD = 0.8025) was significantly different (*P* = 0.010) than insurance or government (M = -0.6935, SD = 0.7348). However, the other combination did not present significant difference. See Appendix E, subsection 9.5.4 for tables and details.

Europe

A one-way ANOVA was used to determine if the level of trust (LTrust) was different for the four types of organizations within our European sub-sample. Participant responses were classified into four groups: big companies (n = 28), government (n = 39), health providers (n = 28) and insurance companies (n = 36). Descriptive statistics were used to observe the distribution of the overall data (See *Table 9*).

Table 9
Descriptive for One-way ANOVA - Europe

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	28	-.0335	.53264	.10066	-.2400	.1731	-1.06	1.13
Government	39	.0753	.44500	.07126	-.0689	.2196	-.81	.69
Health Providers	28	.2121	.59081	.11165	-.0170	.4411	-1.31	1.13
Insurance	36	-.2865	.70622	.11770	-.5254	-.0475	-1.81	.88
Total	131	-.0181	.59800	.05225	-.1215	.0852	-1.81	1.13

a. Region = Europe

LTrust was statistically significant between different types of organizations only, F (3, 127) = 4.451, *P* = .005. LTrust increased from insurance companies (M = -0.2865, SD = 0.7062) to big companies (M = -0.0335, SD = 0.5326), government (M = 0.0753, SD = 0.4450), and health providers (M = 0.2121, SD = 0.5908), in that order. Figure 11 shows side-by-side boxplots to better visualize the results from ANOVA analysis. See Appendix E, subsection 9.5.5 for tables and details.

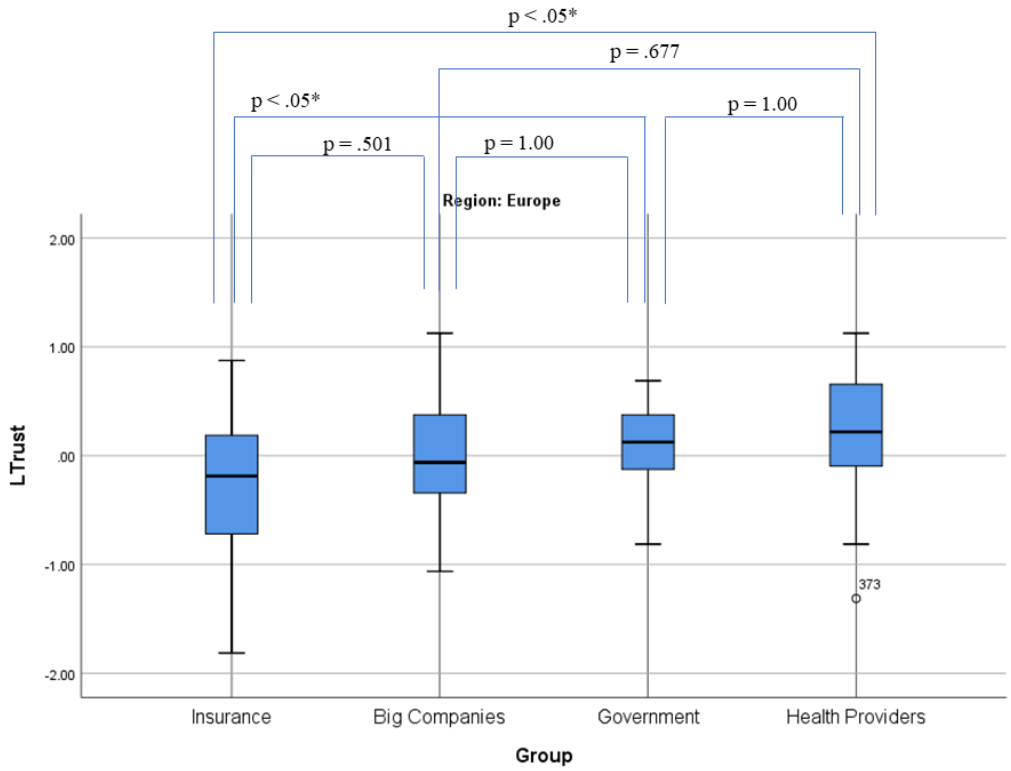


Figure 11. Boxplot one-way ANOVA comparing types of organizations for Europe

Pair-wise t-tests with Bonferroni correction indicated that the mean score for insurance companies (M = -0.2865, SD = 0.7062) was significantly different (*P* = 0.045) than government (M = 0.0753, SD = 0.4450), and significantly different (*P* = 0.005) than health providers (M = 0.2121, SD = 0.5908). However, the other combinations did not present significant differences. See Appendix E, subsection 9.5.6 for tables and details.

6.3. RESEARCH QUESTION 3

What are the differences in trust levels for users from Canada, the USA, and Europe when trusting their Healthcare IoT data to other stakeholders?

An analogous one-way ANOVA to analyze trust was used to determine if the level of trust (LTrust) was different across each of the three regions. Participant responses were classified into three groups: Canada (n = 129), the USA (n = 132), and Europe (n = 131) independently of

the type of institution they were evaluating. Descriptive statistics were used to observe the distribution of the overall data (See *Table 10*).

Table 10
Descriptive for One-way ANOVA - Overall Analysis by Region

Descriptives

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Canada	129	-.1778	.63061	.05552	-.2877	-.0679	-2.00	1.75
USA	132	-.4001	.76950	.06698	-.5326	-.2676	-2.00	1.19
Europe	131	-.0181	.59800	.05225	-.1215	.0852	-1.81	1.13
Total	392	-.1993	.68719	.03471	-.2675	-.1311	-2.00	1.75

LTrust was statistically, significantly different between different regions only, F (2, 389) = 10.763, *P* =.000. LTrust increased from the USA (M = -0.4001, SD = 0.7695), followed by an increase in Canada (M = -0.1778, SD = 0.6306), and then Europe (M = -0.0181, SD = 0.5980). Figure 12 shows side-by-side boxplots to better visualize the results from ANOVA. See Appendix F, subsection 9.6.1 for tables and details.

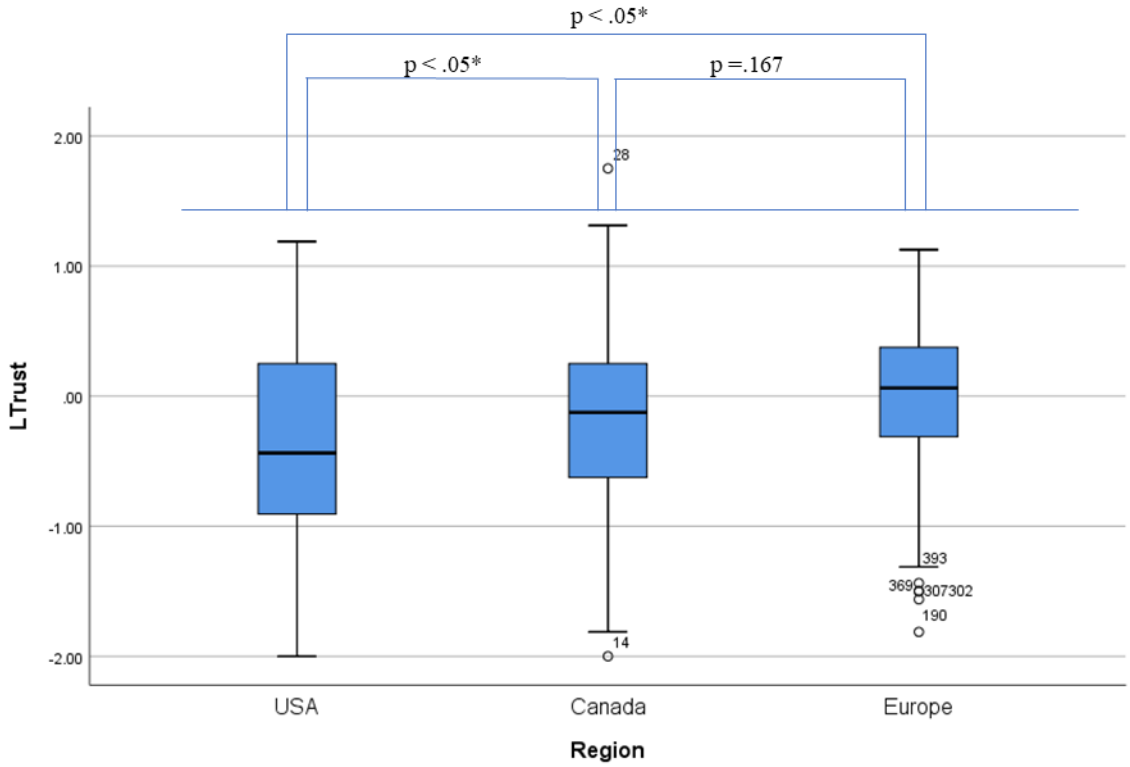


Figure 12. Boxplot one-way ANOVA comparing regions

Pair-wise t-tests with Bonferroni correction indicated that the mean score for Canada (M = -0.1778, SD = 0.6306) was significantly different (*P* = 0.023) than that of the USA (M = -0.4001, SD = 0.7695). However, Canada (M = -0.1778, SD = 0.6306) did not significantly differ from Europe (M = -0.0181, SD = 0.5980). The results also indicated that the mean score for Europe (M = -0.0181, SD = 0.5980) was significantly different (*P* = 0.000) than USA (M = -0.4001, SD = 0.7695). See Appendix F, subsection 9.6.2 for tables and details.

6.4. OTHER RESULTS

6.4.1. One-way ANOVA by age group

One-way ANOVA to analyze trust and determine if the level of trust (LTrust) was different for the six age ranges. Participants were classified into six age groups: between 18 – 25 (n = 94), between 26 – 30 (n = 98), between 31 – 35 (n = 56), between 36 – 45 (n = 70), between

46 – 55 (n = 50), and between 56 – 90 (n = 24). Descriptive statistics were used to analyze the distribution of the overall data. LTrust was different for the age ranges, and the difference between the groups was found to be statistically significant (F (5, 386) = 2.893, *P* = .014).

See Appendix G for tables and details.

6.4.2. One-way ANOVA for the type of organizations by age range

A one-way ANOVA was also conducted to determine if the level of trust (LTrust) was different amongst the four types of organizations according to the groupings of individuals according to age range. Participants were classified into the same four groups: big companies, government, health providers, and insurance companies. LTrust was different for the types of organizations, and the differences between the groups were statistically significant between those aged 18-25 and 26-30. For those between the ages of 31-35, 36-45, 46-55, and 56-90, the differences between the groups were not statistically significant.

See Appendix H for tables and details.

7. DISCUSSION

As previously described in this thesis, Canada is shifting from an in-hospital model of care to an in-home model to reduce the costs of healthcare delivery and to improve patients' quality of life (Koch, 2006). Home-based models of care delivery often rely on qualified personnel delivering home care, coupled with the use of technology (Reinhard, Given, Petlick, & Bemis, 2008). Remote patient monitoring technologies (Ahmed Abi Sen et al., 2018; Sicari et al., 2015) and medical devices adapted to operate in in-home settings (Islam et al., 2015; Koch, 2006) have been widely used to prevent patients from unnecessary visits to the hospital.

One type of technology that promises to revolutionize how healthcare will be delivered, focusing on a more patient-centered approach to healthcare delivery and potentially improving patients' quality of life is the Internet of Things (IoT) (Negash et al., 2018). Along with IoT, the healthcare domain is becoming one of the primary users of big data, and through the use of IoT, the healthcare system could improve their awareness of how patients are performing between visits to the clinic (Dimitrov, 2016). Moreover, data is considered the leading enabler behind IoT technologies and is a critical component for supporting decision-making, a fundamental part of healthcare IoT (Dimitrov, 2016). Nevertheless, privacy and security challenges need to be addressed to ensure users' trust in sharing their data with the organizations responsible for providing IoT technology. Such organizations are able to leverage the data collected and improve their own patient care, develop new methods by using real-world data to training their models, and for agencies responsible for monitoring population health (public health surveillance) (Knaup & Schöpe, 2014; L. M. Lee & Thacker, 2011; Soucie, 2017). This study seeks to understand the user's perspective on trust and data sharing with organizations such as healthcare providers, insurance companies, government, and large companies. It is also part of this study to

understand how user confidence levels are affected by the region in which they live (e.g., Canada, the USA, and Europe). In this section, we connect our findings to our initial research questions.

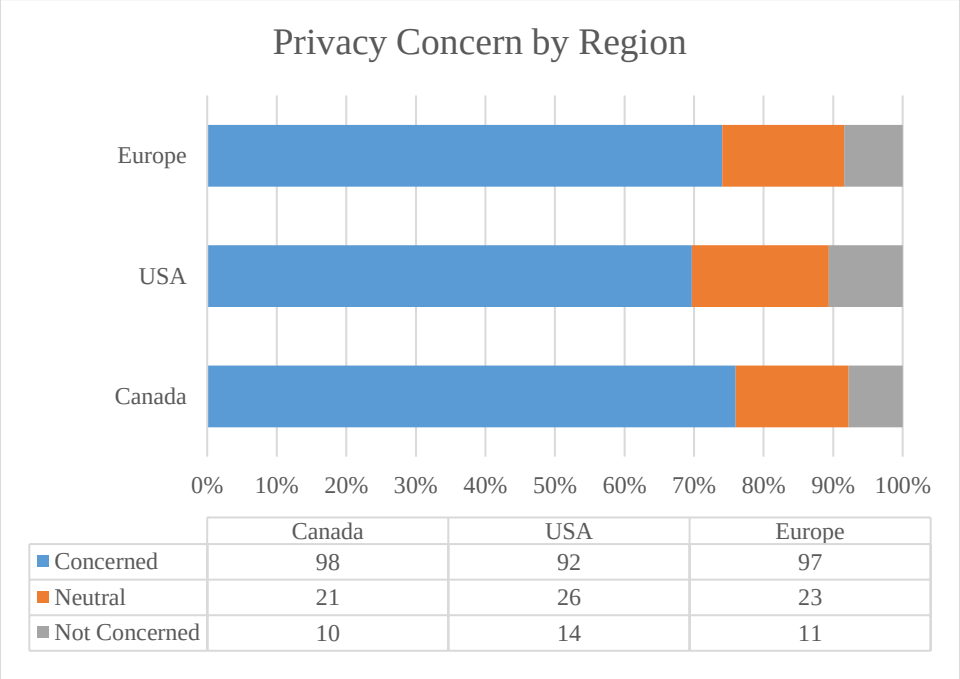
7.1. PRIVACY AND TRUST DIFFERENCES BETWEEN REGIONS

The results from this study did not identify statistically significant differences in privacy concern levels and awareness levels on data ownership when comparing Canada, the USA, and EuropeHence, these results do not support the first hypothesis that assumes the existence of differences between the regions of Canada, the USA, and Europe, according to differences in legislation and culture. The similarities in privacy concerns may be related to the fact that privacy is highly valued as an expression and safeguard of personal dignity in the regions of Canada, the USA, and Europe (Dinev, Masssimo, Hart, Christian, & Vincenzo, 2005), which contradicts my hypothesis. This contradiction may exist because these regions use privacy agreements drawn from the same principles as the Federal Trade Commission's (FTC) guidelines to build trust and reduce fear of disclosure (Wu, Huang, Yen, & Popova, 2012).

One possible explanation for the non-significant results for the first hypothesis, assuming that concern levels would be different across the three regions, is that privacy concerns are highly independent of the region or culture of the participants (Clement, 2019). However, this contradicts studies presented by Bellman et al. (2004) and Milberg et al. (2000), describing which cultural values influence user concerns about information privacy. Bellman's and Milberg's respective studies confirm the principle of the first hypothesis presented in this study. Yet, this hypothesis is unsupported in the results of questionnaires from across Canada, the USA, and Europe. Another possible explanation for similar levels of privacy concerns across regions is

the increase in governmental initiatives around privacy and security, which has enhanced collective surveillance. This connects with Swire's work describing concerns about the security rules of health standards such as HIPPA following the September 11 terrorist attacks in the USA, changes in regulations were initiated by the USA and followed by regions that have the same risk and vulnerability (Swire & Steinfeld, 2001), and Dinev's work about cross-country differences on privacy concerns and attitudes towards government surveillance (Dinev et al., 2005).

After recoding the results according to the following criteria: "concerned" representing responses ranging from agree and strongly agree, and neutral and "not concerned" for responses ranging from disagree and strongly disagree, the results showed that all regions have similar response patterns as presented in Figure 13, with approximately 1 in 7 users concerned about their privacy while using the internet. Likewise, the results also show that more than 70% of the users are concerned that strangers might gain access to their personal data through their online activities.



	Canada	USA	Europe
Concerned	98	92	97
Neutral	21	26	23
Not Concerned	10	14	11

Figure 13. Users privacy concern by region

The results of my study align with the results of a survey conducted by Foresight Factory on behalf of GDMA in ten global markets, exploring public attitudes towards privacy and data exchange (Acxiom, GDMA, & Foresight Factory, 2018). Both studies show that over 70% of users are concerned about privacy on both continents. Our study has an average of 73% of concerned users (see Figure 13), while the Foresight Factory study has an average of 74% of concerned users (see Figure 14). (Acxiom et al., 2018).

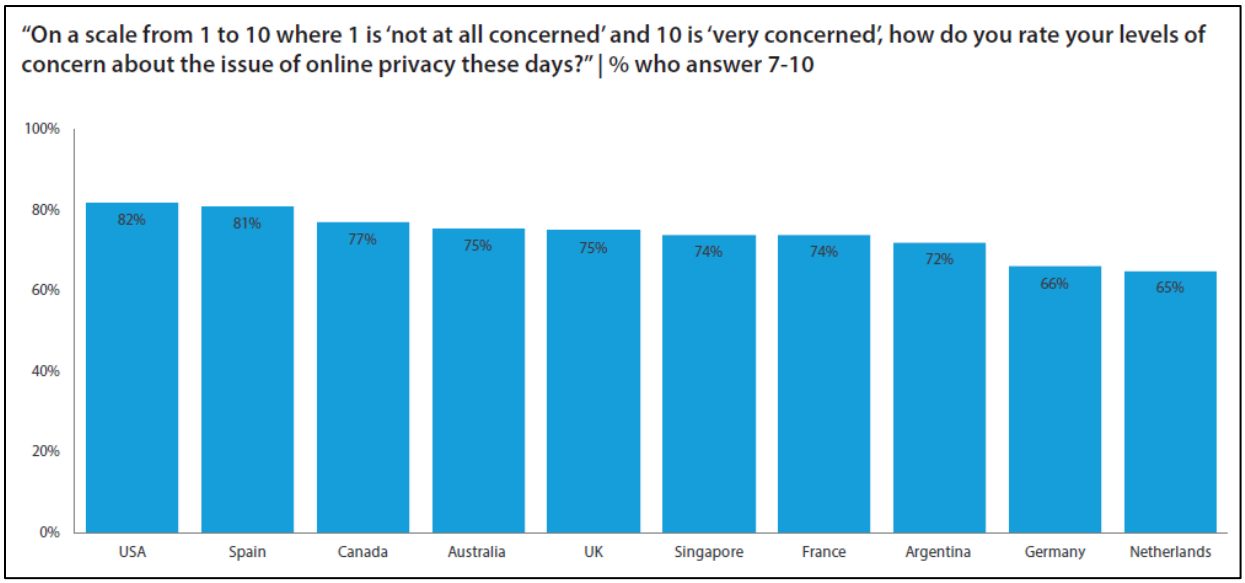
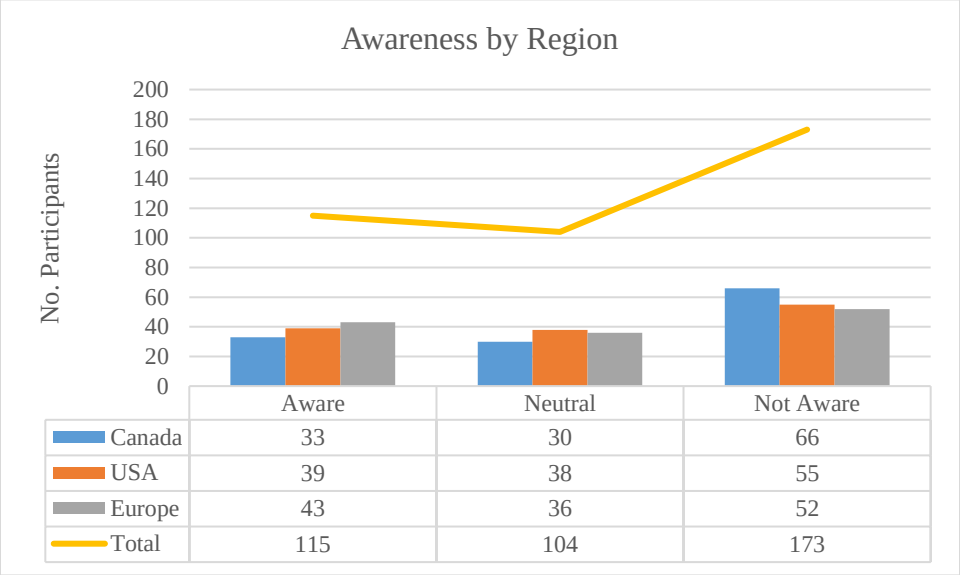


Figure 14. Foresight Factory on global data privacy (Acxiom et al., 2018)

Results from the analysis about awareness levels on data ownership also did not support the first hypothesis, with non-significant ANOVA results when comparing Canada, the USA, and Europe. Moreover, the results show a contradiction between data ownership awareness and privacy concerns. While the results demonstrate that users have a serious concern for their online privacy, the results also show that users have little knowledge of their rights and data ownership, with only 29% of the participants agreeing with the statement, "*I understand who has ownership of my online data*." (Figure 15). Although the results show no difference between the three regions, it shows that much remains to be done to increase awareness and transparency regarding

data ownership, which aligns with the work of Al-Khouri that describes the need to create better privacy protection laws to minimize risk and misuse (Al-Khouri, 2012). At the same time, these results support the idea that policymakers need to develop a shared policy and regulatory framework to safeguard personal information, limit exploitation by businesses, and enable data collection for research with transparency while maintaining user privacy (Kostkova et al., 2016).



	Aware	Neutral	Not Aware
Canada	33	30	66
USA	39	38	55
Europe	43	36	52
Total	115	104	173

Figure 15. Levels of awareness by region

The high number of participants concerned about privacy and with low awareness of data ownership may be related to the increase in data breach-related scandals, demonstrating that users have little control and knowledge about the destination of data collected online (Acxiom et al., 2018). Not to mention the inability to trust companies to protect users' data, as demonstrated by the following publication from The Manifest (2019), which states that we still cannot trust companies to properly follow privacy rules and laws (e.g., GDPR). With the implementation of policies and laws that mandate that companies disclose data breach cases in Canada (PIPEDA Amendment, 2017), the USA (Data Breach Notification Laws by State, 2006), and Europe

(GDPR, 2018), the number of data breaches exposed in the media has also increased, bringing more information to users but also more concerns about possible risks.

Online privacy concerns can lead to a lack of willingness to provide personal information online and, consequently, a considerable barrier for trust (Wu et al., 2012). When comparing the levels of user's trust between regions the results confirm the third hypothesis which states that Canada (M = -0.1778, SD = 0.6306), the USA (M = -0.4001, SD = 0.7695) and Europe (M = -0.0181, SD = 0.5980) will have a significant difference in trust levels when trusting other stakeholders with their healthcare IoT data, driven by socio-cultural frameworks established by different local privacy policies and regulations dictated by the respective regions the participants are in. However, the results show a significant difference between Canada and the USA, and the USA and Europe, but not between Canada and Europe (see Figure 12). One way to explain the results from the study is to look at the impact of culture on trust, as explored by Altinay et al. (2014). While there are various ways in which trust can be built, trust is established by the norms and social values that guide people's behaviour and beliefs (Doney, Cannon, & Mullen, 1998). For this reason, the more the organization's values are aligned with the user's values, the higher the level of trust (Cazier, M Shao, & St Louis, 2007; Li, Hess, & Valacich, 2008). In addition, these same values and norms that guide behaviour can define culture and are frequently shared by the population (Doney et al., 1998). Furthermore, it is essential to understand that the cultural differences between nations are becoming thin with globalization (Fukuyama, 1995). Generally speaking, culture is not only made up of norms and values, but there are also factors conditioned on background, education, and similar life experiences, which suggest that when individuals share these factors, a higher chance of building trust is observed (Doney et al., 1998). It is also important to recognize the limits of culture in explaining the results of confidence levels, as

culture does not respond to all previous variations in values, behaviour, and experiences, and must consider social and psychological factors (Wood, 2007). Cultural studies require a historical perspective to better explain the impact of culture over time in any variable of interest (e.g. trust levels in this thesis) with a focus on the changing balance of power in Western culture (Rojek & Turner, 2000).

Europe presents with the highest levels of trust, as demonstrated by our results in section 6.3, with an average trust level of -0.0181 when compared to Canada (-0.1778) and the USA (-0.4001). We would assume that the General Data Protection Regulation (GDPR) implemented in 2018 would be part of the increased overall trustworthiness observed in Europe. However, European levels of trust on the internet are decreasing, and in 2018, a few months after the GDPR, Europe reached the lowest trust level in over a decade (Castro & Chivot, 2019).

In this case, we must assume that factors linked to culture (background, education, and life experiences) may be the agents responsible for higher levels of trust across the regions of Europe, Canada, and the USA. This hypothesis is deserving of further attention and research.

7.2. TRUST DIFFERENCES BETWEEN TYPES OF ORGANIZATIONS

Regarding the differences in levels of trust between types of organizations, the results confirm the second hypothesis showing significant differences between big companies (M = -0.1849, SD = 0.5777), government (M = -.2423, SD = 0.6631), healthcare providers (M = 0.0688, SD = 0.6812), and insurance companies (M = -0.4492, SD = 0.7276). When comparing each type of organization separately, the results presented in section 6.2.1 show a significant difference between healthcare providers and the other three types of organizations and no significant difference between the government, big companies, and insurance companies (see

Figure 16). Such results are similar to other surveys conducted in the past, which showed that consumers are more willing to share their data with health-related institutions (e.g., health clinics and pharmacies) than government and tech companies (Day & Zweig, 2018). According to the results, the study participants showed higher levels of trust in healthcare providers (M = 0.0688, SD = 0.6812), followed by big corporations (M = -0.1849, SD = 0.5777), government (M = -.2423, SD = 0.6631), and insurance companies (M = -0.4492, SD = 0.7276) (see Figure 8). The results are equivalent to previous surveys where big companies usually place behind government like the one presented by Rock Health saying that only about 11% of users are willing to share their health data with big technology companies (Day & Zweig, 2018). Comparatively, the results of a survey by Harvard T.H. Chan School of Public Health shows a slight difference between levels of trust in government and large companies (showing Amazon above government and Google below), similar to the results of this study (Harvard T.H. Chan School of Public Health, 2019). In fact, it is safe to assume that lower levels of trust in big companies is likely to affect the healthcare industry as healthcare services are moving to technology-based home care using IoT technology, as presented by this study.

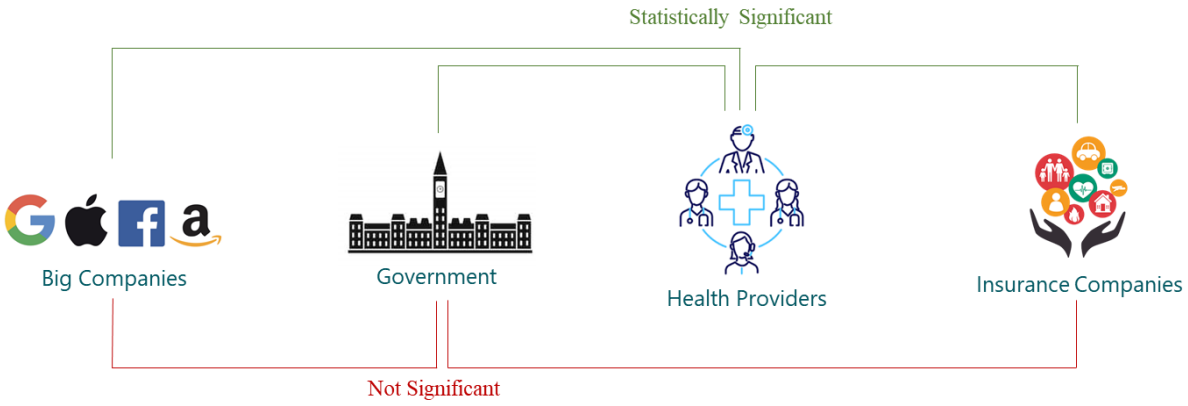


Figure 16. Differences between types of organizations

There has been considerable debate and discussion in the literature about data sharing for research and supporting healthcare delivery (Fecher et al., 2015; Parker & Bull, 2015; Walport & Brest, 2011), trust between patients and healthcare providers (Brennan et al., 2013; McDonald, 2019; McGraw, Dempsey, Harris, & Goldman, 2009), consumer trust (Metzger, 2017; Wu et al., 2012; Yoon & Occeña, 2015), and organizational trust (Morita & Burns, 2014a), particularly in terms of the effect of data sharing and trust on building stronger relationships between parties and better acceptance of technology (Pavlou, 2003). However, very little research has been reported regarding trust in data sharing from healthcare IoT. Research, related to IoT and trust, addresses technology issues, privacy and trust measurements, and trust models (Bao et al., 2012; Cao et al., 2016; Lu, Wang, Bhargava, & Xu, 2006; Yan et al., 2014). This study differs, however, by focusing specifically on how users trust different types of organizations when sharing data generated by their healthcare IoT.

Although the results from this study show that health providers are the most trusted organizations to share data with, it is essential to point out that 24% of all data breaches in 2018 happened with healthcare organizations, most of them by ransomware attacks (Verizon, 2018). Statistics from the Department of Health and Human Services' Office for Civil Rights (USA) show that Healthcare data breaches are being reported at an average of more than one per day (HIPAA Journal, 2019). In Canada, around 19 million people had their data breached in the period between November 2018 and June 2019 (Gibbons, 2019). With all this knowledge, we can hypothesize that users trust healthcare providers more fully based on their past experiences with the healthcare providers and their trust in physicians (Advisory Board, 2019). Further research needs to be done to evaluate the differences in trust in different types of healthcare agents (e.g. physicians, caregivers, clinics.

When stratifying the levels of trust by the types of organizations by region, the results presented differences between the three regions with Canada and Europe following the same pattern with the least trusted type of organization being insurance companies, followed by big companies, government, and healthcare providers. The results for the USA differ from the previous two, with the government being the least trusted type of organization, then insurance companies, big companies, and healthcare providers as the most trusted type of organization. The differences in results across the three regions may be partially explained by a common variation in Americans' lack of trust in the government (Dalton, 2005). Poor government communication, unclear agendas, and a lack of transparency are some of the factors affecting current levels of trust. Levels of education, age, and race also influence the outcome (Stevens, 2019). Another possible explanation for the differences in the results between the regions is the fact that Americans are so opposed to increasing government surveillance in the USA because of the fear of terrorism and potential attacks (Dinev et al., 2005).

Table 11
Count of number of items chosen by each participant

Num of items chosen	**Number of Participants**			
	Canada	**Europe**	**USA**	**Total**
1	34	25	61	120
2	15	16	17	48
3	17	24	16	57
4	21	24	12	57
5	17	16	8	41
6	12	9	7	28
7	5	7	5	17
8	1	5	2	8
9	2	2	2	6
10	4			4
11	1	3	2	6

Moreover, the differences in confidence levels between the three regions, found in the results of this study and presented in section 6.3, can also be seen in the results from the question "*I would trust in the following with data about me.*" To answer this question, each participant was asked to select as many items as he thought necessary, and the results confirm distrust in the government by Americans (see Table 12). On average, USA participants (avg = 2.76) chose fewer items than Canadian (avg = 3.63) and European participants (avg = 3.81), showing lower overall trust than the other two regions. Table 11 lists the number of possible items to choose from for the question "I would trust in the following with data about me" and the number of participants who answered each combination. The results from Canada and Europe showcase a similar order in the selected items, with a slight variation in the order between the fourth and eighth items, and the two regions have a similar total number of selected items.

Similar to the level of distrust in the government in the USA, the results show that insurance companies are the least trusted type of organization in Canada and Europe even though they are not the most vulnerable industry and usual target for data breaches (Apcela, 2019; Proton Data Security, 2017). The mistrust in insurers likely comes from (1) the negative image they leave on people, with 53% having had a negative experience with their coverage and claims (Littlejohns, 2019); and (2) concerns about sharing private information with insurance companies that may affect their chances of getting insurance in the future or of having future claims denied (Harvard T.H. Chan School of Public Health, 2019).

Table 12
List of organizations that participants would trust their data - n (rank)

	Canada *	**USA**	**Europe**
Central government	75 (1)	40 (3)	80 (1)
National Health Service (NHS) and healthcare providers	70 (2)	34 (5)	67 (2)
Universities	68 (3)	45 (2)	65 (3)
Banks and credit card companies	52 (4)	29 (7)	53 (5)
Offline retailers (i.e., physical shops)	46 (5)	48 (1)	51 (6)
Online retailers (i.e., Amazon)	45 (6)	36 (4)	54 (4)
Medical research charities (e.g., cancer research, multiple sclerosis society)	30 (7)	29 (7)	30 (8)
Insurance companies	24 (8)	24 (8)	37 (7)
Local government (e.g., local council departments)	18 (9)	20 (9)	21 (9)
Social media organizations	13 (10)	32 (6)	15 (10)
Family and friends	12 (11)	13 (10)	14 (11)
None of these	9 (12)	9 (11)	12 (12)
Don't know	6 (13)	5 (12)	0 (13)
Total of selected items	468	364	499

* Sorted by Canada

Ultimately, lack of trust in large companies, government, and insurers can have significant consequences for the implementation of future population and individual health solutions in Canada. The transition from an in-hospital model to patient-centered healthcare is based on the use of technology (IoT) and data -- technology that comes from mistrusted big companies and services often offered by the government. The findings of my research thesis once again underscore the importance of addressing privacy and trust through the creation of new policies, improved communication transparency, and user experience.

7.3. LIMITATIONS

Despite the strengths and significance of the proposed research, there are limitations that should be acknowledged. In this thesis, no additional data was used in conjunction with MTurk data to supplement unbalanced samples, which in other studies have included undergraduate students, working professionals, and graduate students (Cheung, Burns, Sinclair, & Sliter, 2017). While using MTurk as a tool to recruit participants with a diverse background and from multiple different countries is a strength, the Mechanical Turk tool is not entirely pervasive across the population. According to Paolacci et al. (2010), the MTurk sample represents the USA population as any other survey, with gender, race, age and education distributions from online participants all matching the general population more closely than college and undergraduate samples often used in these studies. A study from Kees et al. (2017) compared five distinct samples (student samples, samples from professional research companies, and nonstudent sample of MTurk workers) and indicated that MTurk is a viable data collection platform for advertising research experiments. However, it is not possible to extrapolate to other regions as Canada and Europe, as the MTurk population may not correctly represent the desired population as the platform currently presents a higher penetration in countries like the USA and India (Ipeirotis & G., 2010). This is demonstrated by the lack of senior participants from regions other than the USA. Compared to the general population, MTurk users are younger, underemployed, more liberal, less religious, and heavier Internet users (Cheung et al., 2017). Consequently, participants that do not fit this profile have been neglected from our study. Nevertheless, the lack of representativeness is major issue not only in MTurk, but also in any other online survey tool using common sampling methods in organizational psychology, including organizational samples and college student samples (Cheung et al., 2017).

MTurk has also other methodological concerns as subject inattentiveness, selection biases, repeated participation, range restrictions, among other issues presented by Cheung et al. (2017). Recommendations presented by Cheung et al. (2017) were adopted when possible throughout this research project. In addition, it should be noted that not all countries in Europe have English as their first language, and this may impact participant understanding and interpretation of the scenarios and questions posed. Additionally, language limitations may have prevented other potential participants from participating in the study.

7.4. FUTURE WORK

The purpose of the study was to understand users' perspectives on trust in different types of organizations, and my results have shown that there is a difference in trust. Further analysis using effect size to measure the strength of the relationship between the variables could bring new light to the results. The priority for future work is to evaluate high and low trust organizations and further delineate differences in organizations (e.g., tech companies, social media, health insurance, life insurance, hospitals, clinics, pharmacies) to determine where trust already exists and where it needs to be fostered. This will allow for a better understanding of the reasons behind users' trust and distrust. Additionally, it is important to explore in future work, the effect of culture and others external factors on levels of trust and privacy, acknowledging the limits of culture when combining behaviour, society and culture and addressing culture as an interdisciplinary discipline. Future research across different age groups, with a more significant number of participants, may provide insight into the differences between generations, in particular a better understanding of how the senior population trust in data sharing, as they represent the largest target for homecare and AAL technologies. This new understanding could

help address the creation of new transparency and privacy policies to increase users' knowledge and hence, trust in data sharing for the benefit of better healthcare service delivery using H-IoT and innovative technology.

Other directions for future research include (1) exploring the effect of culture and age on the degree to which users accept H-IoT technologies; and (2) identifying and exploring external factors that influence privacy concerns and trust in these organizations.

8. CONCLUSION

Healthcare IoT is a new reality in our healthcare system and will change the way we deliver patient care. Data collected by these systems and shared with stakeholders is at the core of service provision and is fundamental to making this system operate to our benefit.

However, the results of this study show that users are concerned about their privacy and the ownership of their H-IoT data, which is a barrier to the successful deployment of large-scale H-IoT solutions (Daubert et al., 2015). Additionally, the results of my study show that user trust levels may vary according to previous experiences that occurred between users and the different organizations. This same trust may still vary by where the user currently lives, reflecting possible differences in culture, norms, values, and background (Doney, Cannon, & Mullen, 1998). Moreover, the results show that a lack of trust in big companies, those that are likely to provide H-IoT technology, can undermine the implementation of health services needed for an in-home healthcare model that Canada is developing.

To our knowledge, this project represents a pioneering study on data sharing trust specifically for healthcare IoT. As such, the contribution of this project includes results that can be used to analyze future actions to increase trust between organizations and users. In order for new models of healthcare using H-IoT technologies to be implemented in Canada, we need to further investigate the causes of mistrust and privacy concerns on data sharing. In the hope that, by improving trust, we will also increase user acceptance of new technologies.

This study contributes to research fields related to health technology, wearables, IoT, policymakers, and any other field interested in using data collected through H-IoT to improve the quality of life by implementing a home healthcare model.

8. REFERENCES

Abril-Jiménez, P., Vera-Muñoz, C., Cabrera-Umpierrez, M. F., Arredondo, M. T., & Naranjo, J. C. (2009). Design Framework for Ambient Assisted Living Platforms (pp. 139–142). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-02710-9_16

Acampora, G., Cook, D. J., Rashidi, P., & Vasilakos, A. V. (2013). A Survey on Ambient Intelligence in Healthcare. *Proceedings of the IEEE*, *101*(12), 2470–2494. https://doi.org/10.1109/JPROC.2013.2262913

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science (New York, N.Y.)*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Acxiom, GDMA, & Foresight Factory. (2018). *Global data privacy: What the consumer really thinks*.

Advisory Board. (2019). Only 11% of patients trust Big Tech with their health data. See who's trusted most—and least. Retrieved October 29, 2019, from https://www.advisory.com/daily-briefing/2019/02/21/data-sharing

Ahlgren, B., Hidell, M., & Ngai, E. C.-H. (2016). Internet of Things for Smart Cities: Interoperability and Open Data. *IEEE Internet Computing*, *20*(6), 52–56. https://doi.org/10.1109/MIC.2016.124

Ahmed Abi Sen, A., Albouraey Eassa, F., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. *Journal of Information Technology*, *10*(2), 189–200. https://doi.org/10.1007/s41870-018-0113-4

Akamai. (2018). *Research: Consumer Attitudes Toward Data Privacy Survey, 2018*.

Al-Khouri, A. M. (2012). Data Ownership: Who Owns "My Data"?, *2*(1). Retrieved from

www.ijmit.com

Allied Market Research (AMR). (2016). Internet of Things (IoT) Healthcare Market is Expected to Reach $136.8 Billion Worldwide, by 2021 - MarketWatch. Retrieved March 1, 2019, from https://www.marketwatch.com/press-release/internet-of-things-iot-healthcare-market-is-expected-to-reach-1368-billion-worldwide-by-2021-2016-04-12-8203318

Altinay, L., Saunders, M. N. K., & Wang, C. L. (2014). The Influence of Culture on Trust Judgments in Customer Relationship Development by Ethnic Minority Small Businesses. *Journal of Small Business Management*, *52*(1), 59–78. https://doi.org/10.1111/jsbm.12033

Antonino, P. O., Schneider, D., Hofmann, C., & Nakagawa, E. Y. (2011). Evaluation of AAL Platforms According to Architecture-Based Quality Attributes (pp. 264–274). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25167-2_36

Apcela. (2019). Data Breach Statistics: by Source, Industry, Country & Size | Apcela. Retrieved November 6, 2019, from https://www.apcela.com/blog/data-breach-statistics/

Avilés-López, E., García-Macías, J. A., & Villanueva-Miranda, I. (2010). *Developing Ambient Intelligence Applications for the Assisted Living of the Elderly*. Retrieved from http://usuario.cicese.mx/~jagm/docs/aviles-ant10acc.pdf

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*, *30*(1), 13. https://doi.org/10.2307/25148715

Azimi, I., Pahikkala, T., Rahmani, A. M., Niela-Vilén, H., Axelin, A., & Liljeberg, P. (2019). Missing data resilient decision-making for healthcare IoT through personalization: A case study on maternal health. *Future Generation Computer Systems*, *96*, 297–308. https://doi.org/10.1016/J.FUTURE.2019.02.015

Bamidis, P. D., Tarnanas, I., Hadjileontiadis, L. J., & Tsolaki, M. (2015). *Handbook of research on innovations in the diagnosis and treatment of dementia*. IGI Global.

Banerjee, S., Bhattacharya, A., Sen, S., Bhattacharya, A., & Sen, S. (2018). Healthcare IoT (H-IoT). In *Machine Learning and IoT* (pp. 247–263). Boca Raton : Taylor & Francis, 2019.: CRC Press. https://doi.org/10.1201/9781351029940-15

Bao, F., Chen, I.-R., & Chen, R. (2012). Trust Management for the Internet of Things and Its Application to Service Composition. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a* (pp. 1–6).

Barakat, S., & Sheikh, A. El. (2010). *Trust and User Acceptance of Mobile Advertising*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.3629&rep=rep1&type=pdf

Bauer, K. A. (2019). *Home-Based Telemedicine: A Survey of Ethical Issues*. *Cambridge Quarterly of Healthcare Ethics* (Vol. 10). Retrieved from https://www.cambridge.org/core/terms.

Bellman, S., Johnson, E. J., Kobrin, S. J., Lauder, J. H., & Lohse, G. L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, *20*, 313–324. https://doi.org/10.1080/01972240490507956

Bhatia, M., & Sood, S. K. (2017). A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: A predictive healthcare perspective. *Computers in Industry*, *92–93*, 50–66. https://doi.org/10.1016/j.compind.2017.06.009

Biocco, P., Keshavarz, M., Hines, P., & Anwar, M. (2018). A Study of Privacy Policies across Smart Home Companies. In *An Interactive Workshop on the Human aspects of Smarthome Security and Privacy (WSSP 2018), Symposium on Usable Privacy and Security (SOUPS).*

Black, G. (2011). *Publicity rights and image: exploitation and legal control*. Hart.

Blumendorf, M., & Albayrak, S. (2009). Towards a Framework for the Development of Adaptive Multimodal User Interfaces for Ambient Assisted Living Environments (pp. 150–159). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-02710-9_18

Bravo, J., Cook, D. J., & Riva, G. (2016). Ambient Intelligence for Health Environments. *Article in Journal of Biomedical Informatics*. https://doi.org/10.1016/j.jbi.2016.10.009

Brennan, N., Barnes, R., Calnan, M., Corrigan, O., Dieppe, P., & Entwistle, V. (2013). Trust in the health-care provider-patient relationship: a systematic mapping review of the evidence base. https://doi.org/10.1093/intqhc/mzt063

Canadian Institute for Health Information. (2017a). *How much does Canada spend on health care?* Retrieved from https://www.cihi.ca/en/how-much-does-canada-spend-on-health-care-2017

Canadian Institute for Health Information. (2017b). *Unnecessary Care in Canada*. Retrieved from www.cihi.cacopyright@cihi.caISBN978-1-77109-569-3

Canadian Medical Protective Association. (2014). Reducing unplanned hospital readmissions. Retrieved March 26, 2019, from https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2014/reducing-unplanned-hospital-readmissions

Cao, Q. H., Khan, I., Farahbakhsh, R., Madhusudan, G., Lee, G. M., & Crespi, N. (2016). A Trust Model for Data Sharing in Smart Cities. *ArXiv Preprint ArXiv:1603.07524*. Retrieved from http://arxiv.org/abs/1603.07524

Carras, K., Farmaha, R., Ramesh, K., & Santasheva, A. (2018). *Priv: Privacy Simplified*.

Castro, D., & Chivot, E. (2019). The GDPR Was Supposed to Boost Consumer Trust. Has it Succeeded? Retrieved October 29, 2019, from https://www.european-

views.com/2019/06/the-gdpr-was-supposed-to-boost-consumer-trust-has-it-succeeded/

Cavan, J. (2019). Opting in just makes sense: The benefits of sharing medical data for the greater good. Retrieved April 8, 2019, from https://medcitynews.com/2019/02/opting-in-just-makes-sense-the-benefits-of-sharing-medical-data-for-the-greater-good/

Cazier, J. A., M Shao, B. B., & St Louis, R. D. (2007). Sharing information and building trust through value congruence. *Springer Science*. https://doi.org/10.1007/s10796-007-9051-6

Charness, G., Gneezy, U., & Kuhn, M. A. (2012). Experimental methods: Between-subject and within-subject design. *Journal of Economic Behavior and Organization*, *81*(1), 1–8. https://doi.org/10.1016/j.jebo.2011.08.009

Chatham House. (2018). Principles for Sharing the Data and Benefits of Public Health Surveillance. Retrieved April 4, 2019, from https://datasharing.chathamhouse.org/

Chen, J. (2019). The Simple Solution To The Technology Trust Crisis. Retrieved from https://www.linkedin.com/pulse/simple-solution-technology-trust-crisis-john-chen/

Cheung, J. H., Burns, D. K., Sinclair, R. R., & Sliter, M. (2017). Amazon Mechanical Turk in Organizational Psychology: An Evaluation and Practical Recommendations. *Journal of Business and Psychology*, *32*(4), 347–361. https://doi.org/10.1007/s10869-016-9458-5

Chouffani, R. (2016). Value of healthcare IoT devices resides in data collection. Retrieved March 1, 2019, from https://internetofthingsagenda.techtarget.com/tip/Value-of-healthcare-IoT-devices-resides-in-data-collection

Clement, J. (2019). Global opinion: concern about online privacy 2019. Retrieved October 31, 2019, from https://www.statista.com/statistics/373338/global-opinion-concern-online-privacy/

Contant, J. (2018). Where Canada ranks worldwide in cyber breaches. Retrieved April 8, 2019,

from https://www.canadianunderwriter.ca/technology/canada-ranks-worldwide-cyber-breaches-1004136764/

Cook, D. J., Augusto, J. C., & Jakkula, V. R. (2009). Ambient intelligence: Technologies, applications, and opportunities. *Pervasive and Mobile Computing*, *5*(4), 277–298. https://doi.org/10.1016/J.PMCJ.2009.04.001

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*. https://doi.org/10.1287/orsc.10.1.104

Dalton, R. J. (2005). The social transformation of trust in government. *International Review of Sociology*, *15*(1), 133–154. https://doi.org/10.1080/03906700500038819

Daubert, J., Wiesmaier, A., & Kikiras, P. (2015). A view on privacy & trust in IoT. *2015 IEEE International Conference on Communication Workshop, ICCW 2015*, 2665–2670. https://doi.org/10.1109/ICCW.2015.7247581

Day, S., & Zweig, M. (2018). Beyond Wellness For the Healthy: Digital Health Consumer Adoption 2018 | Rock Health | We're powering the future of healthcare. Rock Health is a seed and early-stage venture fund that supports startups building the next generation of technologies transfor. Retrieved October 29, 2019, from https://rockhealth.com/reports/beyond-wellness-for-the-healthy-digital-health-consumer-adoption-2018/?mc_cid=0c97d69dbe&mc_eid=452e95c5c5

De Lusignan, S., Mold, F., Sheikh, A., Majeed, A., Wyatt, J. C., Quinn, T., … Rafi, I. (2014). Patients' online access to their electronic health records and linked online services: a systematic interpretative review. *BMJ Open*, *4*, 6021. https://doi.org/10.1136/bmjopen-2014-006021

Demiris, G., Hensel, B. K., Skubic, M., & Rantz, M. (2008). Senior residents' perceived need of and preferences for "smart home" sensor technologies. *International Journal of Technology Assessment in Health Care*, *24*(01), 120–124. https://doi.org/10.1017/S0266462307080154

Difallah, D., Filatova, E., & Ipeirotis, P. (2018). Demographics and Dynamics of Mechanical Turk Workers, *9*. https://doi.org/10.1145/3159652.3159661

Dimitrov, D. V. (2016). Medical Internet of Things and Big Data in Healthcare. *Healthcare Informatics Research*, *22*(3), 156–163. https://doi.org/10.4258/hir.2016.22.3.156

Dinev, T., Masssimo, B., Hart, P., Christian, C., & Vincenzo, R. (2005). Internet Users, Privacy Concerns and Attitudes towards Government Surveillance-An Exploratory Study of Cross-Cultural Differences between Italy and the United States. *BLED 2005 Proceedings*, *30*. Retrieved from http://aisel.aisnet.org/bled2005/30

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of Management Review*, *23*(3), 601–620. https://doi.org/10.5465/AMR.1998.926629

Duhaime's Law Dictionary. (2019). Privacy Definition. Retrieved April 16, 2019, from http://www.duhaime.org/LegalDictionary/P/Privacy.aspx

Dwyer, C., Roxanne, S., & Passerini, K. (2007). *Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace* (Vol. 339). Retrieved from http://aisel.aisnet.org/amcis2007/339Dwyeret.al.

Fadrique, L. X., Rahman, D., & Morita, P. P. (2019). *The Active Assisted Living Landscape in Canada – Insights for Standards, Policies, and Governance - CSA Group*. Retrieved from https://www.csagroup.org/article/the-active-assisted-living-landscape-in-canada/

Fecher, B., Friesike, S., & Hebing, M. (2015). What Drives Academic Data Sharing? *PLOS*

ONE, *10*(2), e0118053. https://doi.org/10.1371/journal.pone.0118053

Ferreira, G., Penicheiro, P., Bernardo, R., Mendes, L., Barroso, J., & Pereira, A. (2017). Low Cost Smart Homes for Elders (pp. 507–517). Springer, Cham. https://doi.org/10.1007/978-3-319-58700-4_41

FindLaw. (2019). Invasion of Privacy. Retrieved April 16, 2019, from https://injury.findlaw.com/torts-and-personal-injuries/invasion-of-privacy.html

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. https://doi.org/10.1016/J.CHB.2008.08.006

Frieden, T. R., Harold Jaffe, D. W., Thacker, S. B., Moolenaar, R. L., Lee, L. M., Meyer, P. A., … John Ward, G. W. (2012). *CDC's Vision for Public Health Surveillance in the 21st Century*. *Centers for Disease Control and Prevention* (Vol. 61). Retrieved from https://www.cdc.gov/mmwr/pdf/other/su6103.pdf

Fukuyama, F. (1995). *Trust: The social virtues and the creation of prosperity* (Vol. 99). Free press New York, NY.

Ghanchi, J. (2018). How the Heath Care Industry Is Using Wearable Data. Retrieved April 8, 2019, from https://www.colocationamerica.com/blog/wearable-data-helping-doctors

Gibbons, D. (2019). Over half of Canadians had their online data breached between November and June - The Post Millennial. Retrieved October 29, 2019, from https://www.thepostmillennial.com/over-half-of-canadians-had-their-online-data-breached-between-november-and-june/

Government of Canada. (2018). Canada's Health Care System. Retrieved February 22, 2019, from https://www.canada.ca/en/health-canada/services/health-care-system/reports-

publications/health-care-system/canada.html

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/J.FUTURE.2013.01.010

Harvard T.H. Chan School of Public Health. (2019). *Americans' views on data privacy & e-cigarettes*. Retrieved from https://www.cdc.gov/mmwr/volumes/67/wr/mm6745a5.htm?s_cid=mm6745a5_w

HIPAA Journal. (2019). Healthcare Data Breach Statistics. Retrieved October 31, 2019, from https://www.hipaajournal.com/healthcare-data-breach-statistics/

Hubl, M., Pohl, O., Noack, V., Hahlweg, P., Ehm, C., Derleh, M., … Ngo, H.-D. (2016). Embedding of wearable electronics into smart sensor insole. In *2016 IEEE 18th Electronics Packaging Technology Conference (EPTC)* (pp. 597–601). IEEE. https://doi.org/10.1109/EPTC.2016.7861550

Huldtgren, A., Ascencio, G., Pedro, S., Pohlmeyer, A. E., & Romero Herrara, N. A. (2014). *AAL-Technology Acceptance through Experience*. Retrieved from https://pdfs.semanticscholar.org/5ea6/12855635f91ea3774aa400083267c1dd9706.pdf

Hung, M. (2017). *Leading the IoT*. Retrieved from https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

IEC. (2017). SyC AAL – Active Assisted Living. IEC. Retrieved from http://www.iec.ch/public/miscfiles/sbp/SYCAAL.pdf

Ipeirotis, P. G., & G., P. (2010). Analyzing the Amazon Mechanical Turk marketplace. *XRDS: Crossroads, The ACM Magazine for Students*, *17*(2), 16. https://doi.org/10.1145/1869086.1869094

Irizarry, J., Gheisari, M., Williams, G., & Roper, K. (2014). Ambient intelligence environments for accessing building information. *Facilities*, *32*(3/4), 120–138. https://doi.org/10.1108/F-05-2012-0034

Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. (2015). The Internet of Things for Health Care : A Comprehensive Survey. *Access, IEEE*, *3*, 678–708. https://doi.org/10.1109/ACCESS.2015.2437951

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human Computer Studies*, *63*(1–2), 203–227. https://doi.org/10.1016/j.ijhcs.2005.04.019

Kees, J., Berry, C., Burton, S., & Sheehan, K. (2017). An Analysis of Data Quality: Professional Panels, Student Subject Pools, and Amazon's Mechanical Turk. *Journal of Advertising*, *46*(1), 141–155. https://doi.org/10.1080/00913367.2016.1269304

Kent, J. (2018). Big Data to See Explosive Growth, Challenging Healthcare Organizations. Retrieved April 8, 2019, from https://healthitanalytics.com/news/big-data-to-see-explosive-growth-challenging-healthcare-organizations

Kim, T.-Y., Youm, S., Jung, J.-J., & Kim, E.-J. (2015). Multi-Hop WBAN Construction for Healthcare IoT Systems. In *2015 International Conference on Platform Technology and Service* (pp. 27–28). IEEE. https://doi.org/10.1109/PlatCon.2015.20

Knaup, P., & Schöpe, L. (2014). Using data from ambient assisted living and smart homes in electronic health records. *Methods of Information in Medicine*, *53*(3), 149–151. https://doi.org/10.3414/ME14-10-0003

Koch, S. (2006). Home telehealth—Current state and future trends. *International Journal of Medical Informatics*, *75*(8), 565–576. https://doi.org/10.1016/J.IJMEDINF.2005.09.002

Kostkova, P., Brewer, H., de Lusignan, S., Fottrell, E., Goldacre, B., Hart, G., … Tooke, J. (2016). Who Owns the Data? Open Data for Healthcare. *Frontiers in Public Health*, *4*, 7. https://doi.org/10.3389/fpubh.2016.00007

Lahlou, S., Langheinrich, M., & Röcker, C. (2005). Privacy and trust issues with invisible computers. *Communications of the ACM*, *48*(3), 59. https://doi.org/10.1145/1047671.1047705

Lee, J. D., & See, K. A. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *46*(1), 50–80. https://doi.org/10.1518/hfes.46.1.50_30392

Lee, L. M., & Thacker, S. B. (2011). Public Health Surveillance and Knowing About Health in the Context of Growing Sources of Health Data. *American Journal of Preventive Medicine*, *41*(6), 636–640. https://doi.org/10.1016/J.AMEPRE.2011.08.015

Leon, P. G., Schaub, F., Cranor, L., & Sadeh, N. M. (2015). *Why People Are (Un)willing to Share Information with Online Advertisers Trading Agent Competition View project Secure, usable passwords View project*. Retrieved from https://www.researchgate.net/publication/279176801

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. https://doi.org/10.1016/j.jsis.2008.01.001

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* (pp. 1–5). IEEE. https://doi.org/10.1109/PIMRC.2017.8292361

Littlejohns, P. (2019). The Geneva Association says underinsurance is fuelled by public mistrust. Retrieved October 29, 2019, from https://www.nsinsurance.com/analysis/the-geneva-association-survey/

Lu, Y., Wang, W., Bhargava, B., & Xu, D. (2006). Trust-based privacy preservation for peer-to-peer data sharing. *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*, *36*(3), 498–502. https://doi.org/10.1109/TSMCA.2006.871795

Marchildon, G. P. (2013). *Health Systems in Transition*. *Canada Health system review* (Vol. 15). Retrieved from http://www.euro.who.int/__data/assets/pdf_file/0011/181955/e96759.pdf

Martin, D., Miller, A. P., Quesnel-Vallée, A., Caron, N. R., Vissandjée, B., & Marchildon, G. P. (2018). Canada's universal health-care system: achieving its potential. *The Lancet, 391*(10131), 1718–1735. https://doi.org/10.1016/S0140-6736(18)30181-8

McDonald, R. (2019). Beyond the exam room: How data privacy builds patient trust | Healthcare IT News. Retrieved October 29, 2019, from https://www.healthcareitnews.com/news/beyond-exam-room-how-data-privacy-builds-patient-trust

McGraw, D., Dempsey, J. X., Harris, L., & Goldman, J. (2009). Privacy As An Enabler, Not An Impediment: Building Trust Into Health Information Exchange. *Health Affairs*, *28*(2), 416–427. https://doi.org/10.1377/hlthaff.28.2.416

Metzger, M. J. (2017). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*, *9*(4), 00–00. https://doi.org/10.1111/j.1083-6101.2004.tb00292.x

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science, 11*(1).

https://doi.org/10.1287/orsc.11.1.35.12567

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

Morgan, R. M., & Hunt, S. D. (1994). The Commitment-Trust Theory of Relationship Marketing. *Journal of Marketing*, *58*(3), 20. https://doi.org/10.2307/1252308

Morita, P. P., & Burns, C. M. (2014a). Trust tokens in team development. *Team Performance Management: An International Journal*, *20*(1/2), 39–64. https://doi.org/10.1108/TPM-03-2013-0006

Morita, P. P., & Burns, C. M. (2014b). Understanding "interpersonal trust" from a human factors perspective: insights from situation awareness and the lens model. *Theoretical Issues in Ergonomics Science*, *15*(1), 88–110. https://doi.org/10.1080/1463922X.2012.691184

Müller, G. (1996). Secure communication Trust in technology or trust with technology? *Interdisciplinary Science Reviews*, *21*(4), 336–347. https://doi.org/10.1179/isr.1996.21.4.336

Mutlag, A. A., Abd Ghani, M. K., Arunkumar, N., Mohammed, M. A., & Mohd, O. (2019). Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems*, *90*, 62–78. https://doi.org/10.1016/J.FUTURE.2018.07.049

Nati, M. (2018). *Personal Data Receipts: How transparency increases consumer trust*. Retrieved from https://assets.ctfassets.net/nubxhjiwc091/6LIJp62XscyqI6OcweoSiy/5522b10976e57f20de4966bcafdd006a/Personal_Data_Receipts_r1.5_2.pdf

Ndegwa, S. (2011). The Use of Virtual Wards to Reduce Hospital Readmissions in Canada.

Canadian Agency for Drugs and Technologies in Health. Retrieved from https://www.cadth.ca/media/pdf/ES-27_virtual_wards_e.pdf

Negash, B., Gia, T. N., Anzanpour, A., Azimi, I., Jiang, M., Westerlund, T., … Tenhunen, H. (2018). Leveraging Fog Computing for Healthcare IoT. In *Fog Computing in the Internet of Things* (pp. 145–169). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-57639-8_8

Newman, P. (2019). Internet of Things Report: Technology Trends & Market Growth in 2019. Retrieved April 8, 2019, from https://www.businessinsider.com/internet-of-things-report

Office of the Privacy Commissioner of Canada. (2016a). 2016 Survey of Canadians on Privacy. Retrieved July 4, 2019, from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/#toc3-1

Office of the Privacy Commissioner of Canada. (2016b). The Internet of Things. *Scientific American*, (February), 13–15. https://doi.org/10.1177/1461444815621893a

OPC. (2018). The Personal Information Protection and Electronic Documents Act (PIPEDA). Retrieved November 2, 2018, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Open Data Institute, & YouGov. (2017). Attitudes Towards Data Sharing - ODI/YouGov poll results - 2017-11-29. Retrieved July 4, 2019, from https://docs.google.com/spreadsheets/d/1A_y1XioG2Y4gSy7wXE3kivE40ZiwXrpIbj-YujY_-CQ/edit#gid=471882920

Paolacci, G., Chandler, J., Ipeirotis, P. G., & Stern, L. N. (2010). *Running experiments on Amazon Mechanical Turk. Judgment and Decision Making* (Vol. 5). Retrieved from

https://poseidon01.ssrn.com/delivery.php?ID=199020086001025023126015119124122099104015006077091033071075022106070095067002068103097114000125006036111064126066071114069125062015046052031094097115028015064124110095033053092083112065084077004097086109076006083065025108121105096120100120071094096066&EXT=pdf

Parasuraman, R., & Riley, V. (1997). Humans and Automation: Use, Misuse, Disuse, Abuse, *39*(2), 230–253. https://doi.org/10.1518/001872097778543886

Parker, M., & Bull, S. (2015). Sharing Public Health Research Data: Toward the Development of Ethical Data-Sharing Practice in Low- and Middle-Income Settings. *Journal of Empirical Research on Human Research Ethics*, *10*(3), 217–224. https://doi.org/10.1177/1556264615593494

Pasquetto, I. V, Randles, B. M., & Borgman, C. L. (2017). On the Reuse of Scientific Data. *Data Science Journal*, *16*(8), 1–9. https://doi.org/10.5334/dsj

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, *7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Pieper, M., Antona, M., & Cortés, U. (2011). Ambient Assisted Living. *ERCIM News*, (October), 18–19.

Proton Data Security. (2017). Top 5 industries most vulnerable to a data breach. Retrieved November 6, 2019, from https://www.protondata.com/blog/degaussing-equipment/top-5-industries-vulnerable-data-breach/

Rashidi, P., & Mihailidis, A. (2013). A Survey on Ambient-Assisted Living Tools for Older Adults. *IEEE Journal of Biomedical and Health Informatics*, *17*(3), 579–590.

https://doi.org/10.1109/JBHI.2012.2234129

Reinhard, S. C., Given, B., Petlick, N. H., & Bemis, A. (2008). *Supporting Family Caregivers in Providing Care*. *Patient Safety and Quality: An Evidence-Based Handbook for Nurses*. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/21328765

Richards, N., & Hartzog, W. (2015). Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review*, *19*. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/stantlr19&id=447&div=19&collection=journals

Risteska Stojkoska, B. L., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, *140*, 1454–1464. https://doi.org/10.1016/J.JCLEPRO.2016.10.006

Rojek, C., & Turner, B. (2000). Decorative Sociology: Towards a Critique of the Cultural Turn. *The Sociological Review*, *48*(4), 629–648. https://doi.org/10.1111/1467-954X.00236

RSA. (2018). *RSA Data Privacy & Security Report*.

Sadri, F. (2011). Ambient intelligence. *ACM Computing Surveys*, *43*(4), 1–66. https://doi.org/10.1145/1978802.1978815

Salih, A. S. M., & Abraham, A. (2013). *A Review of Ambient Intelligence Assisted Healthcare Monitoring*. *International Journal of Computer Information Systems and Industrial Management Applications* (Vol. 5). Retrieved from www.mirlabs.net/ijcisim/index.html

Savage, R., Yon, Y., Campo, M., Wilson, A., Kahlon, R., & Sixsmith, A. (2009). Market potential for ambient assisted living technology: the case of Canada, 57–65. https://doi.org/10.1007/978-3-642-02868-7_8

Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger

legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, *16*(2), 171–182. https://doi.org/10.1007/s10676-014-9343-8

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Simpson, C. (2018). How to solve Canada's wait time problem. Retrieved March 27, 2019, from http://theconversation.com/how-to-solve-canadas-wait-time-problem-96170

Solove, D. J. (2012). Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126*. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/hlr126&id=1910&div=87&collection=journals

Sony, P., & Sureshkumar, N. (2019). Concept-Based Electronic Health Record Retrieval System in Healthcare IOT (pp. 175–188). Springer, Singapore. https://doi.org/10.1007/978-981-13-0617-4_17

Soucie, J. M. (2017). Public Health Surveillance and Data Collection: General Principles and Impact on Hemophilia Care. *Hematology*, *4*(11), 1–6. https://doi.org/10.1016/S2214-109X(16)30265-0.Cost-effectiveness

Statista. (2019). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). Retrieved February 19, 2019, from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Statistics Canada. (2017). Statistics Canada: Seniors. Retrieved February 20, 2019, from https://www150.statcan.gc.ca/n1/pub/11-402-x/2011000/chap/seniors-aines/seniors-aines-eng.htm

Stevens, M. (2019). Falling Trust in Government Makes It Harder to Solve Problems, Americans Say - The New York Times. Retrieved October 31, 2019, from https://www.nytimes.com/2019/07/22/us/politics/pew-trust-distrust-survey.html

Strielkina, A., Uzun, D., & Kharchenko, V. (2017). Modelling of healthcare IoT using the queueing theory. In *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (pp. 849–852). IEEE. https://doi.org/10.1109/IDAACS.2017.8095207

Sun, H., & Zhang, P. (2006). The role of moderating factors in user technology acceptance. *International Journal of Human-Computer Studies*, *64*(2), 53–78. https://doi.org/10.1016/J.IJHCS.2005.04.013

Swire, P. P., & Steinfeld, L. B. (2001). Security and Privacy after September 11: The Health Care Example. *Minnesota Law Review*, *86*. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/mnlr86&id=1525&div=43&collection=journals

The Manifest. (2019). Data Privacy Concerns: An Overview for 2019 - The Manifest - Medium. Retrieved October 31, 2019, from https://medium.com/@the_manifest/data-privacy-concerns-an-overview-for-2019-2ccea79aa6f8

TrustArc. (2014). 73% Open to Wearables at Work but Potential Privacy Issues Could Be a Concern. Retrieved from https://www.trustarc.com/blog/tag/workplace/

Tsai, J., Cranor, L. F., Acquisti, A., & Fong, C. M. (2006). What's It To You? A Survey of Online Privacy Concerns and Risks. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.941708

Tsasis, P., & Bains, J. (2008). Management of complex chronic disease: facing the challenges in

the Canadian health-care system. *Health Services Management Research*, *21*(4), 228–235. https://doi.org/10.1258/hsmr.2008.008001

Van Panhuis, W. G., Paul, P., Emerson, C., Grefenstette, J., Wilder, R., Herbst, A. J., … Burke, D. S. (2014). A systematic review of barriers to data sharing in public health. *BMC Public Health*, *14*(1), 1–9. https://doi.org/10.1186/1471-2458-14-1144

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. *MIS Quarterly*. Management Information Systems Research Center, University of Minnesota. https://doi.org/10.2307/43825936

Verizon. (2018). *2018 Data Breach Investigations Report 11 th edition*. Retrieved from http://bfy.tw/HJvH

Walport, M., & Brest, P. (2011). Sharing research data to improve public health. https://doi.org/10.1016/S0140-6736(10)61514-0

Wang, Y.-S., Wu, M.-C., & Wang, H.-Y. (2009). Investigating the determinants and age and gender differences in the acceptance of mobile learning. *British Journal of Educational Technology*, *40*(1), 92–118. https://doi.org/10.1111/j.1467-8535.2007.00809.x

Westin, A. (1970). Privacy and freedom. 1967. *Atheneum, New York*.

Wintersberger, P., Frison, A.-K., & Riener, A. (2018). Fostering User Acceptance and Trust in Fully Automated Vehicles: Evaluating the Potential of Augmented Reality. *Presence*, *27*(1), 46–62. https://doi.org/10.1162/PRES_a_00320

Wood, C. C. (2007). The Limits of Culture?, *4*(1), 95–114. https://doi.org/10.1080/14780038.2007.11425739

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy

on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889–897. Retrieved from https://www.sciencedirect.com/science/article/pii/S0747563211002767

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, *42*, 120–134. https://doi.org/10.1016/j.jnca.2014.01.014

Yoon, H. S., & Occeña, L. G. (2015). Influencing factors of trust in consumer-to-consumer electronic commerce with gender and age. *International Journal of Information Management*, *35*(3), 352–363. https://doi.org/10.1016/j.ijinfomgt.2015.02.003

Zanella, A., Member, S., Bui, N., Castellani, A., Vangelista, L., Member, S., & Zorzi, M. (2017). Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, *1*(1), 22–32. https://doi.org/10.1109/JIOT.2014.2306328

Zhang, M., Liu, Y., Wang, J., & Hu, Y. (2016). A New Approach to Security Analysis of Wireless Sensor Networks for Smart Home Systems. In *2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS)* (pp. 318–323). IEEE. https://doi.org/10.1109/INCoS.2016.15

Zhu, H., Colgan, J., Reddy, M., & Choe, E. K. (2016). Sharing Patient-Generated Data in Clinical Practices: An Interview Study. *AMIA ... Annual Symposium Proceedings. AMIA Symposium*, *2016*, 1303–1312. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/28269928

9. APPENDICES

9.1. APPENDIX A: QUESTIONNAIRE – TRUST IN ORGANIZATIONS

9.1.1. Big Companies

Demographics
1. Age [drop down menu → 18 yrs min, 90 yrs max]
2. Gender [drop down → F, M, other, prefer not to answer]
3. Ethnicity [drop down- with following options]
a. White
b. Chinese
c. South Asian (e.g. East Indian, Sri Lankan, etc.)
d. Black
e. Filipino
f. Latin American
g. Southeast Asian (e.g. Vietnamese, Cambodian, etc.)
h. Arab
i. West Asian (e.g. Iranian, Afghan, etc.)
j. Japanese
k. Korean
l. Aboriginal
m. Other
4. Occupation

5. Highest level of education completed? [drop down → Elementary, HS, Some college, College, Some post-secondary, Post secondary...etc]

6. Country of residence

Privacy Concerns

(Choose a scale from 1 to 5 where 1 – strongly disagree and 5 – strongly agree)

7. Are you concerned about your privacy while you are using the internet?

   Strongly Disagree 1 2 3 4 5 Strongly Agree

8. Are you concerned about people you do not know obtaining personal information about you from your online activities?

   Strongly Disagree 1 2 3 4 5 Strongly Agree

9. I understand who has ownership of my online data

   Strongly Disagree 1 2 3 4 5 Strongly Agree

10. I think the party most responsible for protecting personal data should be
    a. Government
    b. People
    c. Business/Organizations
    d. Government & Myself
    e. Government & Business
    f. Myself & Business
    g. All of them

11. I would trust in the following with data about me (Please select all that apply)
    a. Central government
    b. Local government (e.g. local council departments)
    c. National Health Service (NHS) & healthcare providers
    d. Offline retailers (i.e. physical shops)
    e. Online retailers (i.e. amazon)
    f. Banks and credit card companies
    g. Medical research charities (e.g. cancer research, multiple sclerosis society)
    h. Insurance companies
    i. Social media organization
    j. Universities
    k. Family and friends
    l. None of these
    m. Don't know

Trust – Big Companies (Google, Amazon, Microsoft, Facebook)

Every day new technologies are launched in the market with the promise of making our daily lives easier and more efficient. Such technology can be a simple mobile application or a new device for your home or a smartwatch. When installing your new acquisition, you come across a privacy agreement or privacy policy asking if you agree to share your personal data with the company in question.

For example, a new technology company has created an inexpensive smart thermostat sensor for your house that would learn about your temperature zone and movements around the house. It has the potential to save you on your energy bill by collecting data 24/7. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room. To allow remote programing, they request you to install an app on your smartphone and create a personal

account. In addition, you use a fitness tracker that collects your location, heart rate, and steps all day long syncing your data with a different app in your smartphone.

The following scenarios are possible:

- The **companies** that provide the thermostat are asking you to share the data collected from the device to be able to create better algorithms and help you save on power bill.
- The **companies** that provide the fitness tracker are asking you to share data like location, steps, and heart rate collected from the device to create better algorithms and provide better and personalized service.
- The **companies** that provide the thermostat and fitness tracker are asking to have access to your smartphone through the app installed to customize advertisement.

With the scenario above in mind, and considering the 10 privacy concerns below, answer the questions:

- If my data can be sold to third parties
- My data is encrypted
- My data is deleted after I delete the app/account
- The purpose of collecting my data
- The data collected is anonymized
- It is possible to opt out from the service
- The service would notify me in case of hacks or data leaks
- It is possible for me to manage my own data (e.g. view, update, delete, or transfer)
- Which data types are being collected (e.g. heart rate, steps, etc.)
- My data is being collected

(Choose a scale from 1 to 5 where 1 – strongly disagree and 5 – strongly agree)

12. I trust that companies in general will not use my personal information for any other purpose

    Strongly Disagree 1 2 3 4 5 Strongly Agree

13. I feel that the privacy of my personal information is protected by companies

    Strongly Disagree 1 2 3 4 5 Strongly Agree

14. I would trust my data to a company just based on their reputation

    Strongly Disagree 1 2 3 4 5 Strongly Agree

15. I can count on companies to protect customers' personal information from unauthorized use

    Strongly Disagree 1 2 3 4 5 Strongly Agree

16. I have boycotted/would boycott a company that repeatedly showed they have no regard for protecting customer data

    Strongly Disagree 1 2 3 4 5 Strongly Agree

17. I would provide and trust my personal information/ data to companies for improve my experience/services

    Strongly Disagree 1 2 3 4 5 Strongly Agree

18. I would provide and trust my anonymized personal information/ data to companies for improve overall (population) experience/service

    Strongly Disagree 1 2 3 4 5 Strongly Agree

19. I have felt coerced into sharing personal data with companies that is not relevant to the product/service I am purchasing

    Strongly Disagree 1 2 3 4 5 Strongly Agree

20. I feel like I have no choice but to hand over personal data in return for products/services from companies

    Strongly Disagree 1 2 3 4 5 Strongly Agree

21. If a company loses my personal data/information I feel inclined to blame them above anyone else, even the hacker

    Strongly Disagree 1 2 3 4 5 Strongly Agree

22. I think that companies having more of their customer data than before means that they offer better and more personalized products/services

    Strongly Disagree 1 2 3 4 5 Strongly Agree

23. I would forgive a brand for data breaches if they immediately informed about the attack and told how the company is responding to it Strongly Disagree 1 2 3 4 5 Strongly Agree
24. I would share data about me with a company if it helped develop new medicines or treatments, even if it means I have to share some medical data about me Strongly Disagree 1 2 3 4 5 Strongly Agree
25. I would share data about me with a company if it provided me with insights about myself and my behaviour (e.g., fitness, eating habits, spending habits, travel, social activities) even if it means I need to allow third parties to see that behaviour too Strongly Disagree 1 2 3 4 5 Strongly Agree
26. I would share data about me with a company if it were used to advance academic understanding of particular areas (e.g. medicine, human behaviour, psychology etc.), even if I have to share information about my background, health and preferences Strongly Disagree 1 2 3 4 5 Strongly Agree

9.1.2. Government

Demographics
1. Age [drop down menu → 18 yrs min, 90 yrs max]
2. Gender [drop down → F, M, other, prefer not to answer]
3. Ethnicity [drop down- with following options]
b. White
c. Chinese
d. South Asian (e.g. East Indian, Sri Lankan, etc.)
e. Black
f. Filipino

g. Latin American
h. Southeast Asian (e.g. Vietnamese, Cambodian, etc.)
i. Arab
j. West Asian (e.g. Iranian, Afghan, etc.)
k. Japanese
l. Korean
m. Aboriginal
n. Other
4. Occupation
5. Highest level of education completed? [drop down → Elementary, HS, Some college, College, Some post-secondary, Post secondary...etc]
6. Country of residence

Privacy Concerns (Choose a scale from 1 to 5 where 1 – strongly disagree and 5 – strongly agree)
7. Are you concerned about your privacy while you are using the internet? Strongly Disagree 1 2 3 4 5 Strongly Agree
8. Are you concerned about people you do not know obtaining personal information about you from your online activities? Strongly Disagree 1 2 3 4 5 Strongly Agree
9. I understand who has ownership of my online data Strongly Disagree 1 2 3 4 5 Strongly Agree

10. I think the party most responsible for protecting personal data should be
    h. Government
    i. People
    j. Business/Organizations
    k. Government & Myself
    l. Government & Business
    m. Myself & Business
    n. All of them

11. I would trust in the following with data about me (Please select all that apply)
    n. Central government
    o. Local government (e.g. local council departments)
    p. National Health Service (NHS) & healthcare providers
    q. Offline retailers (i.e. physical shops)
    r. Online retailers (i.e. amazon)
    s. Banks and credit card companies
    t. Medical research charities (e.g. cancer research, multiple sclerosis society)
    u. Insurance companies
    v. Social media organization
    w. Universities
    x. Family and friends
    y. None of these
    z. Don't know

Trust – Government

Every day new technologies are launched in the market with the promise of making our daily lives easier and more efficient. Such technology can be a simple mobile application or a new device for your home or a smartwatch. When installing your new acquisition, you come across

a privacy agreement or privacy policy asking if you agree to share your personal data with the company in question.

For example, a new technology company has created an inexpensive smart thermostat sensor for your house that would learn about your temperature zone and movements around the house. It has the potential to save you on your energy bill by collecting data 24/7. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room. To allow remote programing, they request you to install an app on your smartphone and create a personal account. In addition, you use a fitness tracker that collects your location, heart rate, and steps all day long syncing your data with a different app in your smartphone.

The following scenarios are possible:

- The **government** is asking you to share the data collected from the thermostat to create better environmental programs on a federal level.
- The **government** is asking you to share your information from the fitness tracker (steps, heart rate) and information like location, age and sex with them for the purpose of mapping the regions with better health and create specific health programs for population health.
- The **government** is asking you to share your location data to help police enforcement.

With the scenario above in mind, and considering the 10 privacy concerns below, answer the questions:

- If my data can be sold to third parties
- My data is encrypted
- My data is deleted after I delete the app/account
- The purpose of collecting my data
- The data collected is anonymized
- It is possible to opt out from the service
- The service would notify me in case of hacks or data leaks
- It is possible for me to manage my own data (e.g. view, update, delete, or transfer)

- Which data types are being collected (e.g. heart rate, steps, etc.)
- My data is being collected

(Choose a scale from 1 to 5 where 1 – strongly disagree and 5 – strongly agree)

12. I trust that the government in general will not use my personal information for any other purpose

    Strongly Disagree 1 2 3 4 5 Strongly Agree

13. I feel that the privacy of my personal information is protected by the government

    Strongly Disagree 1 2 3 4 5 Strongly Agree

14. I would trust my data to a government entity just based on their reputation

    Strongly Disagree 1 2 3 4 5 Strongly Agree

15. I can count on the government to protect customers' personal information from unauthorized use

    Strongly Disagree 1 2 3 4 5 Strongly Agree

16. I have boycotted/would boycott a government entity that repeatedly showed they have no regard for protecting customer data

    Strongly Disagree 1 2 3 4 5 Strongly Agree

17. I would provide and trust my personal information/ data to the government for improve my experience/services

    Strongly Disagree 1 2 3 4 5 Strongly Agree

18. I would provide and trust my anonymized personal information/ data to the government for improve overall (population) experience/service

    Strongly Disagree 1 2 3 4 5 Strongly Agree

19. I have felt coerced into sharing personal data with the government that is not relevant to the product/service I am purchasing

    Strongly Disagree 1 2 3 4 5 Strongly Agree

20. I feel like I have no choice but to hand over personal data in return for products/services from the government

Strongly Disagree 1 2 3 4 5 Strongly Agree

21. If the government loses my personal data/information I feel inclined to blame them above anyone else, even the hacker

Strongly Disagree 1 2 3 4 5 Strongly Agree

22. I think that the government having more of their users data than before means that they offer better and more personalized products/services

Strongly Disagree 1 2 3 4 5 Strongly Agree

23. I would forgive a government entity for data breaches if they immediately informed about the attack and told how the company is responding to it

Strongly Disagree 1 2 3 4 5 Strongly Agree

24. I would share data about me with the government if it helped develop new medicines or treatments, even if it means I have to share some medical data about me

Strongly Disagree 1 2 3 4 5 Strongly Agree

25. I would share data about me the government if it provided me with insights about myself and my behaviour (e.g., fitness, eating habits, spending habits, travel, social activities) even if it means I need to allow third parties to see that behaviour too

Strongly Disagree 1 2 3 4 5 Strongly Agree

26. I would share data about me the government if it were used to advance academic understanding of particular areas (e.g. medicine, human behaviour, psychology etc.), even if I have to share information about my background, health and preferences

Strongly Disagree 1 2 3 4 5 Strongly Agree

9.1.3. Healthcare Prviders

Demographics
1. Age [drop down menu → 18 yrs min, 90 yrs max]
2. Gender [drop down → F, M, other, prefer not to answer]
3. Ethnicity [drop down- with following options]
c. White
d. Chinese
e. South Asian (e.g. East Indian, Sri Lankan, etc.)
f. Black
g. Filipino
h. Latin American
i. Southeast Asian (e.g. Vietnamese, Cambodian, etc.)
j. Arab
k. West Asian (e.g. Iranian, Afghan, etc.)
l. Japanese
m. Korean
n. Aboriginal
o. Other
4. Occupation
5. Highest level of education completed? [drop down → Elementary, HS, Some college, College, Some post-secondary, Post secondary...etc]
6. Country of residence

Privacy Concerns

(Choose a scale from 1 to 5 where 1 – strongly disagree and 5 – strongly agree)

7. Are you concerned about your privacy while you are using the internet?

   Strongly Disagree 1 2 3 4 5 Strongly Agree

8. Are you concerned about people you do not know obtaining personal information about you from your online activities?

   Strongly Disagree 1 2 3 4 5 Strongly Agree

9. I understand who has ownership of my online data

   Strongly Disagree 1 2 3 4 5 Strongly Agree

10. I think the party most responsible for protecting personal data should be

    o. Government
    p. People
    q. Business/Organizations
    r. Government & Myself
    s. Government & Business
    t. Myself & Business
    u. All of them

11. I would trust in the following with data about me (Please select all that apply)
    - aa. Central government
    - bb. Local government (e.g. local council departments)
    - cc. National Health Service (NHS) & healthcare providers
    - dd. Offline retailers (i.e. physical shops)
    - ee. Online retailers (i.e. amazon)
    - ff. Banks and credit card companies
    - gg. Medical research charities (e.g. cancer research, multiple sclerosis society)
    - hh. Insurance companies
    - ii. Social media organization
    - jj. Universities
    - kk. Family and friends
    - ll. None of these
    - mm. Don't know

Trust – Health Providers

Every day new technologies are launched in the market with the promise of making our daily lives easier and more efficient. Such technology can be a simple mobile application or a new device for your home or a smartwatch. When installing your new acquisition, you come across a privacy agreement or privacy policy asking if you agree to share your personal data with the company in question.

For example, a new technology company has created an inexpensive smart thermostat sensor for your house that would learn about your temperature zone and movements around the house. It has the potential to save you on your energy bill by collecting data 24/7. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room. To allow remote programing, they request you to install an app on your smartphone and create a personal

account. In addition, you use a fitness tracker that collects your location, heart rate, and steps all day long syncing your data with a different app in your smartphone.

The following scenarios are possible:

- Your **health provider** is asking access to your data collected from your fitness tracker to provide early warning on diseases.
- Your **health provider** is asking access to your personal data from the fitness tracker and thermostat to help with populational health.
- Your **health provider** is asking access to your data in your smartphone to market new services and products.

With the scenario above in mind, and considering the 10 privacy concerns below, answer the questions:

- If my data can be sold to third parties
- My data is encrypted
- My data is deleted after I delete the app/account
- The purpose of collecting my data
- The data collected is anonymized
- It is possible to opt out from the service
- The service would notify me in case of hacks or data leaks
- It is possible for me to manage my own data (e.g. view, update, delete, or transfer)
- Which data types are being collected (e.g. heart rate, steps, etc.)
- My data is being collected

(Choose a scale from 1 to 5 where 1 – strongly disagree and 5 – strongly agree)

12. I trust that health providers in general will not use my personal information for any other purpose

    Strongly Disagree 1 2 3 4 5 Strongly Agree

13. I feel that the privacy of my personal information is protected by health providers

    Strongly Disagree 1 2 3 4 5 Strongly Agree

14. I would trust my data to a health provider just based on their reputation Strongly Disagree 1 2 3 4 5 Strongly Agree
15. I can count on health providers to protect customers' personal information from unauthorized use Strongly Disagree 1 2 3 4 5 Strongly Agree
16. I have boycotted/would boycott a health provider that repeatedly showed they have no regard for protecting customer data Strongly Disagree 1 2 3 4 5 Strongly Agree
17. I would provide and trust my personal information/ data to health providers for improve my experience/services Strongly Disagree 1 2 3 4 5 Strongly Agree
18. I would provide and trust my anonymized personal information/ data to health providers for improve overall (population) experience/service Strongly Disagree 1 2 3 4 5 Strongly Agree
19. I have felt coerced into sharing personal data with health providers that is not relevant to the product/service I am purchasing Strongly Disagree 1 2 3 4 5 Strongly Agree
20. I feel like I have no choice but to hand over personal data in return for products/services from health providers Strongly Disagree 1 2 3 4 5 Strongly Agree
21. If a health provider loses my personal data/information I feel inclined to blame them above anyone else, even the hacker Strongly Disagree 1 2 3 4 5 Strongly Agree
22. I think that health providers having more of their users data than before means that they offer better and more personalized products/services Strongly Disagree 1 2 3 4 5 Strongly Agree

23. I would forgive a health provider for data breaches if they immediately informed about the attack and told how the company is responding to it Strongly Disagree 1 2 3 4 5 Strongly Agree
24. I would share data about me with health providers if it helped develop new medicines or treatments, even if it means I have to share some medical data about me Strongly Disagree 1 2 3 4 5 Strongly Agree
25. I would share data about me with health providers if it provided me with insights about myself and my behaviour (e.g., fitness, eating habits, spending habits, travel, social activities) even if it means I need to allow third parties to see that behaviour too Strongly Disagree 1 2 3 4 5 Strongly Agree
26. I would share data about me with health providers if it were used to advance academic understanding of particular areas (e.g. medicine, human behaviour, psychology etc.), even if I have to share information about my background, health and preferences Strongly Disagree 1 2 3 4 5 Strongly Agree

9.1.4. Insurance Companies

Demographics
1. Age [drop down menu → 18 yrs min, 90 yrs max]
2. Gender [drop down → F, M, other, prefer not to answer]
3. Ethnicity [drop down- with following options]
d. White
e. Chinese
f. South Asian (e.g. East Indian, Sri Lankan, etc.)
g. Black

h. Filipino
i. Latin American
j. Southeast Asian (e.g. Vietnamese, Cambodian, etc.)
k. Arab
l. West Asian (e.g. Iranian, Afghan, etc.)
m. Japanese
n. Korean
o. Aboriginal
p. Other
4. Occupation
5. Highest level of education completed? [drop down → Elementary, HS, Some college, College, Some post-secondary, Post secondary...etc]
6. Country of residence

Privacy Concerns (Choose a scale from 1 to 5 where 1 – strongly disagree and 5 – strongly agree)
7. Are you concerned about your privacy while you are using the internet? Strongly Disagree 1 2 3 4 5 Strongly Agree
8. Are you concerned about people you do not know obtaining personal information about you from your online activities? Strongly Disagree 1 2 3 4 5 Strongly Agree
9. I understand who has ownership of my online data Strongly Disagree 1 2 3 4 5 Strongly Agree

10. I think the party most responsible for protecting personal data should be

    v. Government
    w. People
    x. Business/Organizations
    y. Government & Myself
    z. Government & Business
    aa. Myself & Business
    bb. All of them

11. I would trust in the following with data about me (Please select all that apply)

    nn. Central government
    oo. Local government (e.g. local council departments)
    pp. National Health Service (NHS) & healthcare providers
    qq. Offline retailers (i.e. physical shops)
    rr. Online retailers (i.e. amazon)
    ss. Banks and credit card companies
    tt. Medical research charities (e.g. cancer research, multiple sclerosis society)
    uu. Insurance companies
    vv. Social media organization
    ww. Universities
    xx. Family and friends
    yy. None of these
    zz. Don't know

Trust – Insurance Companies

Every day new technologies are launched in the market with the promise of making our daily lives easier and more efficient. Such technology can be a simple mobile application or a new device for your home or a smartwatch. When installing your new acquisition, you come across

a privacy agreement or privacy policy asking if you agree to share your personal data with the company in question.

For example, a new technology company has created an inexpensive smart thermostat sensor for your house that would learn about your temperature zone and movements around the house. It has the potential to save you on your energy bill by collecting data 24/7. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room. To allow remote programing, they request you to install an app on your smartphone and create a personal account. In addition, you use a fitness tracker that collects your location, heart rate, and steps all day long syncing your data with a different app in your smartphone.

The following scenarios are possible:

- Your **insurance company** is asking access to your data collected from your fitness tracker and thermostat to provide lower rates in the future.
- Your **insurance company** is asking access to your personal data from the fitness tracker to create better solutions for population health.
- Your **insurance company** denies service to you based on your personal data shared through your fitness tracker.

With the scenario above in mind, and considering the 10 privacy concerns below, answer the questions:

- If my data can be sold to third parties
- My data is encrypted
- My data is deleted after I delete the app/account
- The purpose of collecting my data
- The data collected is anonymized
- It is possible to opt out from the service
- The service would notify me in case of hacks or data leaks
- It is possible for me to manage my own data (e.g. view, update, delete, or transfer)
- Which data types are being collected (e.g. heart rate, steps, etc.)

- My data is being collected

(Choose a scale from 1 to 5 where 1 – strongly disagree and 5 – strongly agree)

12. I trust that insurance companies in general will not use my personal information for any other purpose

    Strongly Disagree 1 2 3 4 5 Strongly Agree

13. I feel that the privacy of my personal information is protected by insurance companies

    Strongly Disagree 1 2 3 4 5 Strongly Agree

14. I would trust my data to an insurance company just based on their reputation

    Strongly Disagree 1 2 3 4 5 Strongly Agree

15. I can count on insurance companies to protect customers' personal information from unauthorized use

    Strongly Disagree 1 2 3 4 5 Strongly Agree

16. I have boycotted/would boycott an insurance company that repeatedly showed they have no regard for protecting customer data

    Strongly Disagree 1 2 3 4 5 Strongly Agree

17. I would provide and trust my personal information/ data to insurance companies for improve my experience/services

    Strongly Disagree 1 2 3 4 5 Strongly Agree

18. I would provide and trust my anonymized personal information/ data to insurance companies for improve overall (population) experience/service

    Strongly Disagree 1 2 3 4 5 Strongly Agree

19. I have felt coerced into sharing personal data with insurance companies that is not relevant to the product/service I am purchasing

    Strongly Disagree 1 2 3 4 5 Strongly Agree

20. I feel like I have no choice but to hand over personal data in return for products/services from insurance companies

Strongly Disagree 1 2 3 4 5 Strongly Agree

21. If an insurance company loses my personal data/information I feel inclined to blame them above anyone else, even the hacker

Strongly Disagree 1 2 3 4 5 Strongly Agree

22. I think that insurance companies having more of their users data than before means that they offer better and more personalized products/services

Strongly Disagree 1 2 3 4 5 Strongly Agree

23. I would forgive an insurance company for data breaches if they immediately informed about the attack and told how the company is responding to it

Strongly Disagree 1 2 3 4 5 Strongly Agree

24. I would share data about me with health providers if it helped develop new medicines or treatments, even if it means I have to share some medical data about me

Strongly Disagree 1 2 3 4 5 Strongly Agree

25. I would share data about me with health providers if it provided me with insights about myself and my behaviour (e.g., fitness, eating habits, spending habits, travel, social activities) even if it means I need to allow third parties to see that behaviour too

Strongly Disagree 1 2 3 4 5 Strongly Agree

26. I would share data about me with health providers if it were used to advance academic understanding of particular areas (e.g. medicine, human behaviour, psychology etc.), even if I have to share information about my background, health and preferences

Strongly Disagree 1 2 3 4 5 Strongly Agree

9.2. APPENDIX B: INFORMATION AND CONSENT LETTER

Information and Consent Letter

You are invited to participate in a survey about Privacy and Trust that belongs to a project entitled "Privacy Agreement for Sharing Health Data." The study is being conducted by **Laura Fadrique** of the **School of Public Health and Health Systems** at the University of Waterloo, under the supervision of Professor **Plinio Morita**.

The goal of this study is to provide users with more direct access and visual representation of the most important information of Privacy Agreements (PAs) and Terms and Conditions (TC) by bringing the most important information as a summary section in the front of the agreement, also incorporating a diagram representing critical insights. The results from the study will lead to development of a better understanding at how we can make better privacy agreement.

Your participation in the research will contribute to a better understanding of the trust between individuals and organizations (government and private) in the sharing of personal data. We estimate that it will take 10 to 15 minutes of your time to complete the survey. You are free to contact the investigator at the address provided at the bottom to discuss the survey.

There are no known or anticipated risks of any kind involved in this study.

You will receive $1.00 for your participation in the study.

When information is transmitted over the internet, privacy cannot be guaranteed. There is always a risk your responses may be intercepted by a third party (e.g., government agencies, hackers). University of Waterloo researchers will not collect or use internet protocol (IP) addresses or other information which could link your participation to your computer or electronic device without first informing you.

Your identity will be confidential, and information will be securely stored in a protected server inside of the University of Waterloo. The de-identified data will be stored for a minimum of 7 years. We will assure confidentiality upon publication of results. No identifying participation information will be presented as researchers will use de-identified data in our reports.

Your participation in this research is voluntary. You may decline to answer any questions that you do not wish to answer, and you can withdraw your participation at any time by ceasing to answer questions, without penalty or loss of remuneration. To receive remuneration, please proceed to the end of the questionnaire, obtain the unique code for this HIT, and submit it.

This study has been reviewed and received ethics clearance through a University of Waterloo Research Ethics Committee (ORE #40606). If you have questions for the Committee, contact the Office of Research Ethics, at 1-519-888-4567 ext. 36005 or ore-ceo@uwaterloo.ca.

By agreeing to participate in the study, you are not waiving your legal rights or relesasing

the investigator(s) or involved institution(s) from their legal and professional responsibilities.

If you have any questions, please email Laura Fadrique at lxavierf@uwaterloo.com or Plinio Morita at plinio.morita@uwaterloo.ca.

- ○ I agree to participate in this study
- ◉ I do not wish to participate in the study (please, return to main MTurk main page)

9.3. APPENDIX C: ANOVA RESULTS – PRIVACY CONCERN BETWEEN REGIONS

9.3.1. One-way ANOVA – Question 1

Question 1 - Are you concerned about your privacy while you are using the internet?

Descriptives

LConcern

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Canada	129	.92	.924	.081	.76	1.08	-2	2
USA	132	.89	1.001	.087	.71	1.06	-2	2
Europe	131	.95	1.022	.089	.78	1.13	-2	2
Total	392	.92	.981	.050	.82	1.02	-2	2

Test of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
LConcern	Based on Mean	1.419	2	389	.243
	Based on Median	1.308	2	389	.271
	Based on Median and with adjusted df	1.308	2	388.143	.271
	Based on trimmed mean	1.755	2	389	.174

ANOVA

LConcern

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.303	2	.152	.157	.855
Within Groups	376.245	389	.967		
Total	376.548	391			

9.3.2. Post Hoc Test – Question 1

Multiple Comparisons

Dependent Variable: LConcern

Bonferroni

(I) Region	(J) Region	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Canada	USA	.036	.122	1.000	-.26	.33
	Europe	-.032	.122	1.000	-.33	.26
USA	Canada	-.036	.122	1.000	-.33	.26
	Europe	-.068	.121	1.000	-.36	.22
Europe	Canada	.032	.122	1.000	-.26	.33
	USA	.068	.121	1.000	-.22	.36

9.3.3. One-way ANOVA – Question 2

Question 2 - Are you concerned about people you do not know obtaining personal information about you from your online activities?

Descriptives

LConcern

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Canada	129	.99	.923	.081	.83	1.15	-2	2
USA	132	.85	1.088	.095	.66	1.04	-2	2
Europe	131	.97	1.074	.094	.78	1.16	-2	2
Total	392	.94	1.031	.052	.83	1.04	-2	2

Test of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
LConcern	Based on Mean	4.136	2	389	.017
	Based on Median	2.496	2	389	.084
	Based on Median and with adjusted df	2.496	2	384.393	.084
	Based on trimmed mean	2.911	2	389	.056

ANOVA

LConcern

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1.566	2	.783	.736	.480
Within Groups	413.840	389	1.064		
Total	415.406	391			

9.3.4. Post Hoc Test – Question 2

Multiple Comparisons

Dependent Variable: LConcern

Bonferroni

(I) Region	(J) Region	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Canada	USA	.144	.128	.783	-.16	.45
	Europe	.023	.128	1.000	-.28	.33
USA	Canada	-.144	.128	.783	-.45	.16
	Europe	-.121	.127	1.000	-.43	.18
Europe	Canada	-.023	.128	1.000	-.33	.28
	USA	.121	.127	1.000	-.18	.43

9.3.5. One-way ANOVA – Question 3

Question 3 - I understand who has ownership of my online data.

Descriptives

LAwareness

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Canada	129	-.40	1.208	.106	-.61	-.18	-2	2
USA	132	-.17	1.182	.103	-.38	.03	-2	2
Europe	131	-.08	1.181	.103	-.28	.13	-2	2
Total	392	-.21	1.195	.060	-.33	-.10	-2	2

Test of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
LAwareness	Based on Mean	.488	2	389	.614
	Based on Median	.424	2	389	.655
	Based on Median and with adjusted df	.424	2	372.968	.655
	Based on trimmed mean	.445	2	389	.641

ANOVA

LAwareness

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	6.934	2	3.467	2.447	.088
Within Groups	551.066	389	1.417		
Total	558.000	391			

9.3.6. Post Hoc Test – Question 3

Multiple Comparisons

Dependent Variable: LAwareness

Bonferroni

(I) Region	(J) Region	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Canada	USA	-.221	.147	.403	-.58	.13
	Europe	-.319	.148	.094	-.67	.04
USA	Canada	.221	.147	.403	-.13	.58
	Europe	-.098	.147	1.000	-.45	.26
Europe	Canada	.319	.148	.094	-.04	.67
	USA	.098	.147	1.000	-.26	.45

9.4. APPENDIX D: ANOVA RESULTS - COMPARISON BETWEEN TYPES OF ORGANIZATIONS

9.4.1. One-way ANOVA

Descriptives

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	98	-.1849	.57772	.05836	-.3008	-.0691	-2.00	1.13
Government	98	-.2423	.66310	.06698	-.3753	-.1094	-2.00	.88
Health Providers	100	.0688	.68122	.06812	-.0664	.2039	-1.69	1.75
Insurance	96	-.4492	.72759	.07426	-.5966	-.3018	-2.00	.88
Total	392	-.1993	.68719	.03471	-.2675	-.1311	-2.00	1.75

Test of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	2.655	3	388	.048
	Based on Median	2.393	3	388	.068
	Based on Median and with adjusted df	2.393	3	381.490	.068
	Based on trimmed mean	2.597	3	388	.052

ANOVA

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	13.383	3	4.461	10.107	.000
Within Groups	171.258	388	.441		
Total	184.641	391			

9.4.2. Post Hoc Tests

Multiple Comparisons

Dependent Variable: LTrust

Bonferroni

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Big Companies	Government	.05740	.09491	1.000	-.1943	.3091
	Health Providers	-.25370*	.09443	.045	-.5041	-.0033
	Insurance	.26427*	.09540	.035	.0113	.5173
Government	Big Companies	-.05740	.09491	1.000	-.3091	.1943
	Health Providers	-.31110*	.09443	.006	-.5615	-.0607
	Insurance	.20687	.09540	.184	-.0461	.4599
Health Providers	Big Companies	.25370*	.09443	.045	.0033	.5041
	Government	.31110*	.09443	.006	.0607	.5615
	Insurance	.51797*	.09493	.000	.2662	.7697
Insurance	Big Companies	-.26427*	.09540	.035	-.5173	-.0113
	Government	-.20687	.09540	.184	-.4599	.0461
	Health Providers	-.51797*	.09493	.000	-.7697	-.2662

*. The mean difference is significant at the 0.05 level.

9.5. APPENDIX E: ANOVA RESULTS – TYPES OF ORGANIZATIONS BY REGION

9.5.1. One-way ANOVA - Canada

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	33	-.1932	.52416	.09125	-.3790	-.0073	-1.44	1.00
Government	28	-.1853	.56404	.10659	-.4040	.0334	-1.31	.88
Health Providers	34	.1581	.56496	.09689	-.0390	.3552	-1.06	1.75
Insurance	34	-.4926	.69132	.11856	-.7339	-.2514	-2.00	.75
Total	129	-.1778	.63061	.05552	-.2877	-.0679	-2.00	1.75

a. Region = Canada

Test of Homogeneity of Variances[a]

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	1.037	3	125	.379
	Based on Median	.766	3	125	.515
	Based on Median and with adjusted df	.766	3	117.703	.515
	Based on trimmed mean	1.085	3	125	.358

a. Region = Canada

ANOVA[a]

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	7.216	3	2.405	6.882	.000
Within Groups	43.686	125	.349		
Total	50.902	128			

a. Region = Canada

9.5.2. Post Hoc Tests - Canada

Multiple Comparisons[a]

Dependent Variable: LTrust

Bonferroni

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Big Companies	Government	-.00791	.15190	1.000	-.4151	.3993
	Health Providers	-.35127	.14446	.099	-.7386	.0360
	Insurance	.29947	.14446	.241	-.0878	.6868
Government	Big Companies	.00791	.15190	1.000	-.3993	.4151
	Health Providers	-.34336	.15087	.147	-.7478	.0611
	Insurance	.30738	.15087	.262	-.0971	.7118
Health Providers	Big Companies	.35127	.14446	.099	-.0360	.7386
	Government	.34336	.15087	.147	-.0611	.7478
	Insurance	.65074*	.14338	.000	.2663	1.0351
Insurance	Big Companies	-.29947	.14446	.241	-.6868	.0878
	Government	-.30738	.15087	.262	-.7118	.0971
	Health Providers	-.65074*	.14338	.000	-1.0351	-.2663

*. The mean difference is significant at the 0.05 level.

a. Region = Canada

Homogeneous Subsets

LTrust[a]

Means for groups in homogeneous subsets are displayed.

a. Region = Canada

9.5.3. One-way ANOVA - USA

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	37	-.2922	.64230	.10559	-.5064	-.0781	-2.00	1.00
Government	31	-.6935	.73480	.13197	-.9631	-.4240	-2.00	.44
Health Providers	38	-.1168	.80252	.13019	-.3806	.1470	-1.69	1.19
Insurance	26	-.6178	.78249	.15346	-.9338	-.3017	-2.00	.63
Total	132	-.4001	.76950	.06698	-.5326	-.2676	-2.00	1.19

a. Region = USA

Test of Homogeneity of Variances[a]

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	1.548	3	128	.205
	Based on Median	1.449	3	128	.232
	Based on Median and with adjusted df	1.449	3	123.095	.232
	Based on trimmed mean	1.540	3	128	.207

a. Region = USA

ANOVA[a]

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	7.382	3	2.461	4.488	.005
Within Groups	70.187	128	.548		
Total	77.569	131			

a. Region = USA

9.5.4. Post Hoc Tests - USA

Multiple Comparisons[a]

Dependent Variable: LTrust

Bonferroni

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Big Companies	Government	.40132	.18030	.167	-.0819	.8845
	Health Providers	-.17545	.17103	1.000	-.6338	.2829
	Insurance	.32556	.18950	.529	-.1823	.8334
Government	Big Companies	-.40132	.18030	.167	-.8845	.0819
	Health Providers	-.57677*	.17922	.010	-1.0570	-.0965
	Insurance	-.07576	.19692	1.000	-.6035	.4520
Health Providers	Big Companies	.17545	.17103	1.000	-.2829	.6338
	Government	.57677*	.17922	.010	.0965	1.0570
	Insurance	.50101	.18847	.053	-.0041	1.0061
Insurance	Big Companies	-.32556	.18950	.529	-.8334	.1823
	Government	.07576	.19692	1.000	-.4520	.6035
	Health Providers	-.50101	.18847	.053	-1.0061	.0041

*. The mean difference is significant at the 0.05 level.

a. Region = USA

Homogeneous Subsets

LTrust[a]

Means for groups in homogeneous subsets are displayed.

a. Region = USA

9.5.5. One-way ANOVA - Europe

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	28	-.0335	.53264	.10066	-.2400	.1731	-1.06	1.13
Government	39	.0753	.44500	.07126	-.0689	.2196	-.81	.69
Health Providers	28	.2121	.59081	.11165	-.0170	.4411	-1.31	1.13
Insurance	36	-.2865	.70622	.11770	-.5254	-.0475	-1.81	.88
Total	131	-.0181	.59800	.05225	-.1215	.0852	-1.81	1.13

a. Region = Europe

Test of Homogeneity of Variances[a]

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	2.153	3	127	.097
	Based on Median	1.679	3	127	.175
	Based on Median and with adjusted df	1.679	3	110.595	.176
	Based on trimmed mean	2.034	3	127	.112

a. Region = Europe

ANOVA[a]

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4.423	3	1.474	4.451	.005
Within Groups	42.065	127	.331		
Total	46.488	130			

a. Region = Europe

9.5.6. Post Hoc Tests - Europe

Multiple Comparisons[a]

Dependent Variable: LTrust

Bonferroni

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Big Companies	Government	-.10880	.14256	1.000	-.4909	.2733
	Health Providers	-.24554	.15381	.677	-.6578	.1667
	Insurance	.25298	.14502	.501	-.1357	.6417
Government	Big Companies	.10880	.14256	1.000	-.2733	.4909
	Health Providers	-.13673	.14256	1.000	-.5188	.2453
	Insurance	.36178*	.13302	.045	.0053	.7183
Health Providers	Big Companies	.24554	.15381	.677	-.1667	.6578
	Government	.13673	.14256	1.000	-.2453	.5188
	Insurance	.49851*	.14502	.005	.1098	.8872
Insurance	Big Companies	-.25298	.14502	.501	-.6417	.1357
	Government	-.36178*	.13302	.045	-.7183	-.0053
	Health Providers	-.49851*	.14502	.005	-.8872	-.1098

*. The mean difference is significant at the 0.05 level.

a. Region = Europe

Homogeneous Subsets

LTrust[a]

Means for groups in homogeneous subsets are displayed.

a. Region = Europe

9.6. APPENDIX F: ANOVA RESULTS - COMPARISON BETWEEN REGIONS

9.6.1. One-way ANOVA

Descriptives

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Canada	129	-.1778	.63061	.05552	-.2877	-.0679	-2.00	1.75
USA	132	-.4001	.76950	.06698	-.5326	-.2676	-2.00	1.19
Europe	131	-.0181	.59800	.05225	-.1215	.0852	-1.81	1.13
Total	392	-.1993	.68719	.03471	-.2675	-.1311	-2.00	1.75

Test of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	7.172	2	389	.001
	Based on Median	7.075	2	389	.001
	Based on Median and with adjusted df	7.075	2	385.306	.001
	Based on trimmed mean	7.368	2	389	.001

ANOVA

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	9.681	2	4.841	10.763	.000
Within Groups	174.959	389	.450		
Total	184.641	391			

9.6.2. Post Hoc Tests

Multiple Comparisons

Dependent Variable: LTrust

Bonferroni

(I) Region	(J) Region	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Canada	USA	.22228*	.08303	.023	.0227	.4219
	Europe	-.15968	.08319	.167	-.3597	.0403
USA	Canada	-.22228*	.08303	.023	-.4219	-.0227
	Europe	-.38196*	.08271	.000	-.5808	-.1831
Europe	Canada	.15968	.08319	.167	-.0403	.3597
	USA	.38196*	.08271	.000	.1831	.5808

*. The mean difference is significant at the 0.05 level.

9.7. APPENDIX G: ANOVA RESULTS - COMPARISON BETWEEN AGE RANGES

9.7.1. One-way ANOVA

Descriptives

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Age 18 - 25	94	-.1164	.71017	.07325	-.2618	.0291	-2.00	1.75
Age 26 - 30	98	-.0721	.64681	.06534	-.2017	.0576	-2.00	1.31
Age 31 - 35	56	-.1607	.59982	.08015	-.3213	-.0001	-1.81	.75
Age 36 - 45	70	-.3893	.67844	.08109	-.5511	-.2275	-2.00	1.13
Age 46 - 55	50	-.3900	.70367	.09951	-.5900	-.1900	-2.00	.88
Age 56 - 90	24	-.1823	.79889	.16307	-.5196	.1550	-1.75	1.19
Total	392	-.1993	.68719	.03471	-.2675	-.1311	-2.00	1.75

Test of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	.749	5	386	.587
	Based on Median	.612	5	386	.691
	Based on Median and with adjusted df	.612	5	377.351	.691
	Based on trimmed mean	.751	5	386	.586

ANOVA

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	6.668	5	1.334	2.893	.014
Within Groups	177.972	386	.461		
Total	184.641	391			

9.7.2. Post Hoc Tests

Multiple Comparisons

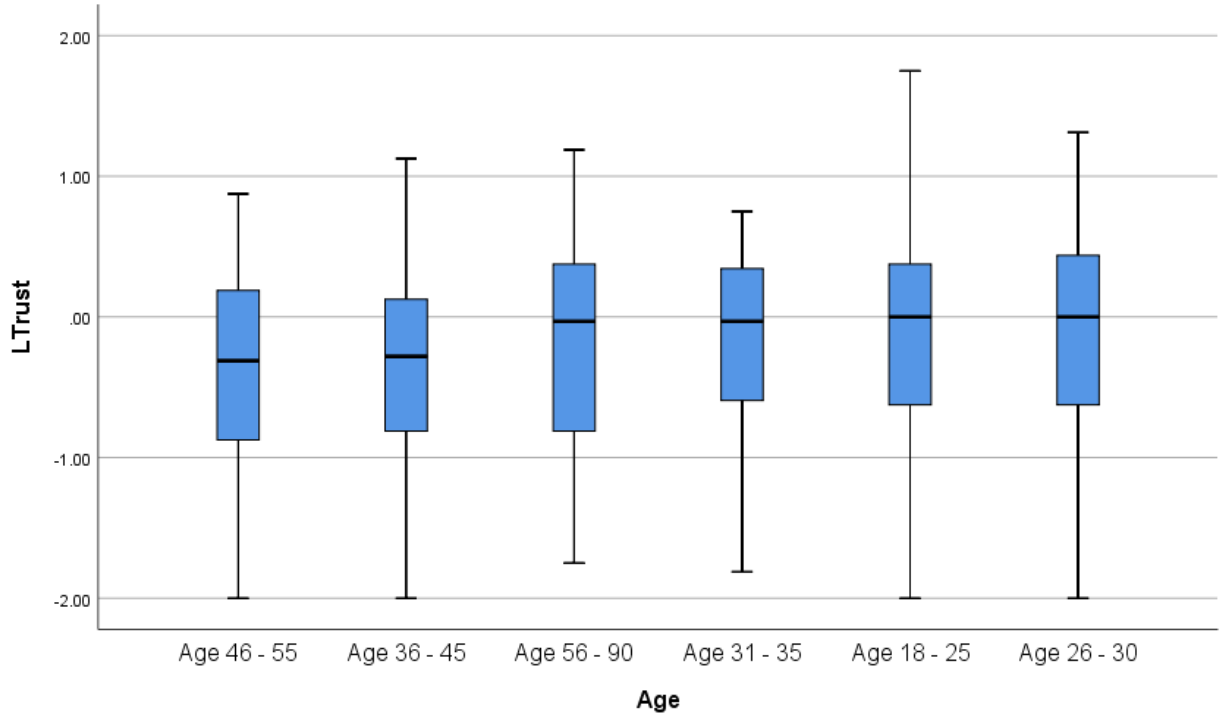
Dependent Variable: LTrust

Bonferroni

(I) Age	(J) Age	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Age 18 - 25	Age 26 - 30	-.04429	.09803	1.000	-.3338	.2452
	Age 31 - 35	.04436	.11462	1.000	-.2942	.3829
	Age 36 - 45	.27293	.10720	.169	-.0437	.5896
	Age 46 - 55	.27364	.11885	.328	-.0774	.6247
	Age 56 - 90	.06594	.15529	1.000	-.3927	.5246
Age 26 - 30	Age 18 - 25	.04429	.09803	1.000	-.2452	.3338
	Age 31 - 35	.08865	.11375	1.000	-.2473	.4246
	Age 36 - 45	.31722*	.10626	.045	.0034	.6311
	Age 46 - 55	.31793	.11801	.110	-.0306	.6665
	Age 56 - 90	.11023	.15465	1.000	-.3465	.5670
Age 31 - 35	Age 18 - 25	-.04436	.11462	1.000	-.3829	.2942
	Age 26 - 30	-.08865	.11375	1.000	-.4246	.2473
	Age 36 - 45	.22857	.12174	.918	-.1310	.5881
	Age 46 - 55	.22929	.13212	1.000	-.1609	.6195
	Age 56 - 90	.02158	.16566	1.000	-.4677	.5109
Age 36 - 45	Age 18 - 25	-.27293	.10720	.169	-.5896	.0437
	Age 26 - 30	-.31722*	.10626	.045	-.6311	-.0034
	Age 31 - 35	-.22857	.12174	.918	-.5881	.1310
	Age 46 - 55	.00071	.12573	1.000	-.3706	.3721
	Age 56 - 90	-.20699	.16062	1.000	-.6814	.2674
Age 46 - 55	Age 18 - 25	-.27364	.11885	.328	-.6247	.0774
	Age 26 - 30	-.31793	.11801	.110	-.6665	.0306
	Age 31 - 35	-.22929	.13212	1.000	-.6195	.1609
	Age 36 - 45	-.00071	.12573	1.000	-.3721	.3706
	Age 56 - 90	-.20771	.16862	1.000	-.7057	.2903
Age 56 - 90	Age 18 - 25	-.06594	.15529	1.000	-.5246	.3927
	Age 26 - 30	-.11023	.15465	1.000	-.5670	.3465
	Age 31 - 35	-.02158	.16566	1.000	-.5109	.4677
	Age 36 - 45	.20699	.16062	1.000	-.2674	.6814
	Age 46 - 55	.20771	.16862	1.000	-.2903	.7057

*. The mean difference is significant at the 0.05 level.

9.7.3. Boxplot


2.00
1.00
.00
-1.00
-2.00
LTrust
Age 46 - 55
Age 36 - 45
Age 56 - 90
Age 31 - 35
Age 18 - 25
Age 26 - 30
Age

9.8. APPENDIX H: ANOVA RESULTS – TYPES OF ORGANIZATIONS BY AGE RANGE

9.8.1. One-way ANOVA - Age 18 - 25

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	17	-.0735	.51026	.12376	-.3359	.1888	-1.19	.75
Government	29	-.1552	.64707	.12016	-.4013	.0910	-1.50	.69
Health Providers	28	.1719	.71940	.13595	-.1071	.4508	-1.50	1.75
Insurance	20	-.5000	.78457	.17543	-.8672	-.1328	-2.00	.88
Total	94	-.1164	.71017	.07325	-.2618	.0291	-2.00	1.75

a. Age = Age 18 - 25

Test of Homogeneity of Variances[a]

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	.938	3	90	.426
	Based on Median	.636	3	90	.594
	Based on Median and with adjusted df	.636	3	82.098	.594
	Based on trimmed mean	.894	3	90	.448

a. Age = Age 18 - 25

ANOVA[a]

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	5.345	3	1.782	3.858	.012
Within Groups	41.558	90	.462		
Total	46.903	93			

a. Age = Age 18 - 25

9.8.2. Post Hoc Tests - Age 18 - 25

Multiple Comparisons[a]

Dependent Variable: LTrust

Bonferroni

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Big Companies	Government	.08164	.20757	1.000	-.4783	.6416
	Health Providers	-.24540	.20893	1.000	-.8091	.3183
	Insurance	.42647	.22417	.362	-.1783	1.0312
Government	Big Companies	-.08164	.20757	1.000	-.6416	.4783
	Health Providers	-.32705	.18004	.436	-.8128	.1587
	Insurance	.34483	.19751	.505	-.1880	.8777
Health Providers	Big Companies	.24540	.20893	1.000	-.3183	.8091
	Government	.32705	.18004	.436	-.1587	.8128
	Insurance	.67188*	.19895	.006	.1352	1.2086
Insurance	Big Companies	-.42647	.22417	.362	-1.0312	.1783
	Government	-.34483	.19751	.505	-.8777	.1880
	Health Providers	-.67187*	.19895	.006	-1.2086	-.1352

*. The mean difference is significant at the 0.05 level.

a. Age = Age 18 - 25

Homogeneous Subsets

LTrust[a]

Means for groups in homogeneous subsets are displayed.

a. Age = Age 18 - 25

9.8.3. One-way ANOVA - Age 26 - 30

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean Lower Bound	95% Confidence Interval for Mean Upper Bound	Minimum	Maximum
Big Companies	26	-.1611	.58234	.11421	-.3963	.0742	-1.25	1.00
Government	21	-.2202	.65747	.14347	-.5195	.0790	-2.00	.69
Health Providers	26	.3053	.55518	.10888	.0810	.5295	-1.06	1.31
Insurance	25	-.2475	.66499	.13300	-.5220	.0270	-1.81	.69
Total	98	-.0721	.64681	.06534	-.2017	.0576	-2.00	1.31

a. Age = Age 26 - 30

Test of Homogeneity of Variances[a]

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	.582	3	94	.628
	Based on Median	.614	3	94	.608
	Based on Median and with adjusted df	.614	3	83.854	.608
	Based on trimmed mean	.614	3	94	.608

a. Age = Age 26 - 30

ANOVA[a]

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	5.139	3	1.713	4.543	.005
Within Groups	35.442	94	.377		
Total	40.581	97			

a. Age = Age 26 - 30

9.8.4. Post Hoc Tests - Age 26 - 30

Multiple Comparisons[a]

Dependent Variable: LTrust

Bonferroni

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Big Companies	Government	.05918	.18016	1.000	-.4264	.5447
	Health Providers	-.46635*	.17030	.044	-.9254	-.0073
	Insurance	.08644	.17200	1.000	-.3771	.5500
Government	Big Companies	-.05918	.18016	1.000	-.5447	.4264
	Health Providers	-.52553*	.18016	.027	-1.0111	-.0400
	Insurance	.02726	.18176	1.000	-.4626	.5171
Health Providers	Big Companies	.46635*	.17030	.044	.0073	.9254
	Government	.52553*	.18016	.027	.0400	1.0111
	Insurance	.55279*	.17200	.011	.0892	1.0164
Insurance	Big Companies	-.08644	.17200	1.000	-.5500	.3771
	Government	-.02726	.18176	1.000	-.5171	.4626
	Health Providers	-.55279*	.17200	.011	-1.0164	-.0892

*. The mean difference is significant at the 0.05 level.

a. Age = Age 26 - 30

Homogeneous Subsets

LTrust[a]

Means for groups in homogeneous subsets are displayed.

a. Age = Age 26 - 30

9.8.5. One-way ANOVA - Age 31 - 35

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	21	-.0536	.43404	.09472	-.2511	.1440	-1.00	.69
Government	10	-.0875	.53457	.16905	-.4699	.2949	-.81	.63
Health Providers	8	-.0703	.54837	.19388	-.5288	.3881	-.94	.56
Insurance	17	-.3787	.79748	.19342	-.7887	.0313	-1.81	.75
Total	56	-.1607	.59982	.08015	-.3213	-.0001	-1.81	.75

a. Age = Age 31 - 35

Test of Homogeneity of Variances[a]

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	4.667	3	52	.006
	Based on Median	4.630	3	52	.006
	Based on Median and with adjusted df	4.630	3	45.951	.007
	Based on trimmed mean	4.702	3	52	.006

a. Age = Age 31 - 35

ANOVA[a]

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1.168	3	.389	1.087	.363
Within Groups	18.620	52	.358		
Total	19.788	55			

a. Age = Age 31 - 35

9.8.6. Post Hoc Tests - Age 31 - 35

Multiple Comparisons[a]

Dependent Variable: LTrust

Bonferroni

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Big Companies	Government	.03393	.22991	1.000	-.5967	.6646
	Health Providers	.01674	.24862	1.000	-.6652	.6987
	Insurance	.32511	.19523	.611	-.2104	.8606
Government	Big Companies	-.03393	.22991	1.000	-.6646	.5967
	Health Providers	-.01719	.28385	1.000	-.7958	.7614
	Insurance	.29118	.23848	1.000	-.3630	.9453
Health Providers	Big Companies	-.01674	.24862	1.000	-.6987	.6652
	Government	.01719	.28385	1.000	-.7614	.7958
	Insurance	.30836	.25656	1.000	-.3954	1.0121
Insurance	Big Companies	-.32511	.19523	.611	-.8606	.2104
	Government	-.29118	.23848	1.000	-.9453	.3630
	Health Providers	-.30836	.25656	1.000	-1.0121	.3954

a. Age = Age 31 - 35

Homogeneous Subsets

LTrust[a]

Means for groups in homogeneous subsets are displayed.

a. Age = Age 31 - 35

9.8.7. One-way ANOVA – Age 36 - 45

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	17	-.2316	.55935	.13566	-.5192	.0560	-1.12	1.13
Government	16	-.5273	.68159	.17040	-.8905	-.1641	-1.69	.25
Health Providers	18	-.1319	.67719	.15962	-.4687	.2048	-1.31	1.06
Insurance	19	-.6579	.69515	.15948	-.9929	-.3228	-2.00	.19
Total	70	-.3893	.67844	.08109	-.5511	-.2275	-2.00	1.13

a. Age = Age 36 - 45

Test of Homogeneity of Variances[a]

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	.787	3	66	.505
	Based on Median	.606	3	66	.614
	Based on Median and with adjusted df	.606	3	65.218	.614
	Based on trimmed mean	.719	3	66	.544

a. Age = Age 36 - 45

ANOVA[a]

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	3.290	3	1.097	2.543	.064
Within Groups	28.469	66	.431		
Total	31.759	69			

a. Age = Age 36 - 45

9.8.8. Post Hoc Tests – Age 36 - 45

Multiple Comparisons[a]

Dependent Variable: LTrust

Bonferroni

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Big Companies	Government	.29573	.22876	1.000	-.3265	.9180
	Health Providers	-.09967	.22212	1.000	-.7039	.5045
	Insurance	.42628	.21926	.337	-.1701	1.0227
Government	Big Companies	-.29573	.22876	1.000	-.9180	.3265
	Health Providers	-.39540	.22566	.506	-1.0092	.2184
	Insurance	.13055	.22285	1.000	-.4756	.7367
Health Providers	Big Companies	.09967	.22212	1.000	-.5045	.7039
	Government	.39540	.22566	.506	-.2184	1.0092
	Insurance	.52595	.21602	.106	-.0617	1.1136
Insurance	Big Companies	-.42628	.21926	.337	-1.0227	.1701
	Government	-.13055	.22285	1.000	-.7367	.4756
	Health Providers	-.52595	.21602	.106	-1.1136	.0617

a. Age = Age 36 - 45

Homogeneous Subsets

LTrust[a]

Means for groups in homogeneous subsets are displayed.

a. Age = Age 36 - 45

9.8.9. One-way ANOVA – Age 46 - 55

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	14	-.6250	.68421	.18286	-1.0201	-.2299	-2.00	.38
Government	13	-.2019	.69229	.19201	-.6203	.2164	-1.87	.88
Health Providers	14	-.1339	.67264	.17977	-.5223	.2544	-1.69	.81
Insurance	9	-.6944	.66691	.22230	-1.2071	-.1818	-1.56	.38
Total	50	-.3900	.70367	.09951	-.5900	-.1900	-2.00	.88

a. Age = Age 46 - 55

Test of Homogeneity of Variances[a]

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	.064	3	46	.978
	Based on Median	.077	3	46	.972
	Based on Median and with adjusted df	.077	3	42.453	.972
	Based on trimmed mean	.073	3	46	.974

a. Age = Age 46 - 55

ANOVA[a]

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.985	3	.995	2.151	.107
Within Groups	21.277	46	.463		
Total	24.262	49			

a. Age = Age 46 - 55

9.8.10. Post Hoc Tests – Age 46 - 55

Multiple Comparisons[a]

Dependent Variable: LTrust

Bonferroni

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Big Companies	Government	-.42308	.26195	.679	-1.1453	.2992
	Health Providers	-.49107	.25706	.374	-1.1998	.2177
	Insurance	.06944	.29057	1.000	-.7317	.8706
Government	Big Companies	.42308	.26195	.679	-.2992	1.1453
	Health Providers	-.06799	.26195	1.000	-.7902	.6543
	Insurance	.49252	.29491	.610	-.3206	1.3056
Health Providers	Big Companies	.49107	.25706	.374	-.2177	1.1998
	Government	.06799	.26195	1.000	-.6543	.7902
	Insurance	.56052	.29057	.359	-.2406	1.3617
Insurance	Big Companies	-.06944	.29057	1.000	-.8706	.7317
	Government	-.49252	.29491	.610	-1.3056	.3206
	Health Providers	-.56052	.29057	.359	-1.3617	.2406

a. Age = Age 46 - 55

Homogeneous Subsets

LTrust[a]

Means for groups in homogeneous subsets are displayed.

a. Age = Age 46 – 55

9.8.11. One-way ANOVA – Age 56 - 90

Descriptives[a]

LTrust

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Big Companies	3	.3750	.54486	.31458	-.9785	1.7285	.00	1.00
Government	9	-.2986	.80391	.26797	-.9165	.3193	-1.75	.69
Health Providers	6	-.1771	.99091	.40454	-1.2170	.8628	-1.44	1.19
Insurance	6	-.2917	.75897	.30985	-1.0882	.5048	-1.44	.75
Total	24	-.1823	.79889	.16307	-.5196	.1550	-1.75	1.19

a. Age = Age 56 - 90

Test of Homogeneity of Variances[a]

		Levene Statistic	df1	df2	Sig.
LTrust	Based on Mean	.794	3	20	.512
	Based on Median	.770	3	20	.524
	Based on Median and with adjusted df	.770	3	19.334	.525
	Based on trimmed mean	.793	3	20	.512

a. Age = Age 56 - 90

ANOVA[a]

LTrust

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1.125	3	.375	.554	.652
Within Groups	13.554	20	.678		
Total	14.679	23			

a. Age = Age 56 - 90

9.8.12. Post Hoc Tests – Age 56 - 90

Multiple Comparisons[a]

Dependent Variable: LTrust

Bonferroni

(I) Group	(J) Group	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Big Companies	Government	.67361	.54881	1.000	-.9328	2.2800
	Health Providers	.55208	.58210	1.000	-1.1518	2.2560
	Insurance	.66667	.58210	1.000	-1.0372	2.3705
Government	Big Companies	-.67361	.54881	1.000	-2.2800	.9328
	Health Providers	-.12153	.43387	1.000	-1.3915	1.1485
	Insurance	-.00694	.43387	1.000	-1.2769	1.2630
Health Providers	Big Companies	-.55208	.58210	1.000	-2.2560	1.1518
	Government	.12153	.43387	1.000	-1.1485	1.3915
	Insurance	.11458	.47528	1.000	-1.2766	1.5058
Insurance	Big Companies	-.66667	.58210	1.000	-2.3705	1.0372
	Government	.00694	.43387	1.000	-1.2630	1.2769
	Health Providers	-.11458	.47528	1.000	-1.5058	1.2766

a. Age = Age 56 - 90

Homogeneous Subsets

LTrust[a]

Means for groups in homogeneous subsets are displayed.

a. Age = Age 56 - 90