The Smart Cities Approach:
The Opportunity and Possibility of Data Driven Communities

by

Sarah Lai Yu Chu
B.A., University of British Columbia, 2016

A Master's Project Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF PUBLIC ADMINISTRATION

in the School of Public Administration

University of Victoria

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Dr. Brunet-Jailly for his mentorship, patient, and support of this capstone project. Beside my supervisor, I would like to thank the rest of the Supervisory Committee: Dr. Speers, Dr. Warburton, and Mr. Rybicki, for their insightful comments, encouragement, and time. I would also like to acknowledge the University of Victoria School of Public Administration for many opportunities and supports it have given me. Finally, I must express my gratitude to my friends, partner, and family especially my mother, Tai Ren Wong, for providing continuous encouragement throughout my academic journey. This achievement would not be accomplished without their support. Thank you so much.

Executive Summary

INTRODUCTION

As technology is developing at a rapid speed, some municipalities in Canada are starting to implement smart city projects in their communities (Getting to the Open Smart City, p.4). Yet there are many complexities and challenges that comes with the implementation of smart city projects. The concept of smart cities was developed over 20 years ago (Life in the Smart City, The Economist). However, the implementation of smart cities occurred more than a decade ago, but as technologies develop smart city projects evolve along with problems and challenges (Smart Cities: Digital Solutions For A More Livable Future, p.VII, p.22).

According to the Government of Canada, a smart cities approach is to use data and smart technologies to achieve beneficial outcomes for residents by having openness, integration, transferability, and collaboration as the main components (The Challenge, Impact Canada Challenge Platform). In this research, smart city projects are a group of projects that uses data and smart technologies to achieve the "smart cities approach" in a municipality. Different countries, municipalities, and companies define smart cities slightly different. In the report, Smart Cities: Digital Solutions for a More Livable Future, was written by scholars around the world who argues that smart cities cannot be focus on technology and neglect residents (p.VII, p.1). The scholars argue that the goal of smart cities should be achieving positive outcomes for residents and promoting residents to be an active participator in developing smart city projects (p.VII).

The purpose of this research is to identify the implications of data collection and use of data in the smart cities approach to provide recommendations to mitigate the challenges or reduce the risks associated with these practices. This research would assist Infrastructure Canada and Canadian municipalities to understand better the opportunities and obstacles they will likely confront when implementing data-related smart city projects in Canadian communities.

The primary research question is: What are the implications of data collection and the use of data in smart cities and how does this affect citizens, businesses, and civil society as a whole?

The secondary research questions are:

1.) What government tools and approaches can Canada learn from other countries when it comes to data collection and the use of data in smart cities?
2.) How do privacy policies affect smart cities data collection and the use of data?
3.) What are the benefits and problems of data collection and the use of data that the government needs to be aware of when implementing the smart city approach?

METHODOLOGY AND METHODS

This research is based on qualitative methodology. The methods used in this research include a literature review, two case studies, and seven expert interviews. The literature review contains documents from journal articles, book, and government documents. The two case studies are from Estonia and Somerville and they look at how they benefit from using technology and data to make their government "smarter." Each expert interview provides an insight into the key themes discussed throughout the paper. The literature review, case studies, and expert interviews will be analyzed and used for making the ten recommendations.

The literature review examines the current state of knowledge on the implication of data collection and use of data in the smart cities approach. The literature review section is categorized into the following themes: definition of the smart cities approach, privacy laws in Canada, EU's General Data Protection Regulation (GDPR), types of data privacy, data ownership, smart governance, data ethics, data sovereignty, and cybersecurity. The case studies and interviews fill in the unknown information gap that is missing in the literature review documents.

In this research, the two case studies on Estonia and Somerville are helpful for Canadian municipalities and the federal government to understand the benefits of having "smart governance." The two case studies provide some "smart governance" opportunities for Canadian municipalities to implement to be more prepared in designing and implementing their data-related smart city projects. By having "smart governance," it can make municipal governments more efficiency and effectiveness in administrative operation, public engagement, and decision-making where it is needed when implementing smart city projects in their communities (Okner & Preston, p.351).

The interview section consists of seven expert interviews, and each expert is knowledgeable in one or more of the key themes throughout this research. The interviews are structured into five sections: privacy law, data infrastructure (data sovereignty and data ownership), data ethics, cybersecurity, and municipal resources. The experts provided important information that was missing in the literature review documents since the study of data in the smart cities approach is still a relatively new research area. All the experts provided useful recommendations that assist in the ten recommendations listed in this paper.

ANALYSIS

There are many strengths, weaknesses, opportunities, and threats to the implication of data collection and use of data in the smart cities approach. The strengths of collecting and using data in the smart cities approach are to increase efficiency, provide better services for residents, and increase innovation.

The weaknesses and challenges are data biases, privacy issues, slow regulation/law development, and limited resource to implement data-driven communities. The opportunities are the implementation of "smart governance," increase efficiency in government services for the public and create better public policies by using the data collected. The significant threats municipalities need to address are cyber-attacks, data breaching, data ownership, and data sovereignty.

RECOMMENDATIONS

There are ten recommendations that address the implication of data collection and use of data in the smart cities approach. The ten recommendations are:

1.) Implementing a "smarter" government administration ("Smart Governance")
2.) Using Privacy Enhancing Technologies (PET)
3.) Implementing a Security Plan
4.) Reforming Personal Information Protection and Electronic Documents Act (PIPEDA)
5.) Using Privacy by Design (PbD)
6.) Having a diverse skill set
7.) Investing in digital literacy
8.) Implementing a cybersecurity life cycle

9.) Keeping data within Canadian borders
10.) Implementing a Data Ethics Guideline

Table of Contents

List of Tables

List of Figures

1.0 Introduction

There has been discussion about data being the "new oil" in recent years and how the five major private technology companies Apple, Amazon, Facebook, Microsoft, and Google are holding a massive volume of data that concerns many people (Pringle, 'Data is the new oil': Your personal information is now the world's most valuable commodity, CBC). From the private sector to the public sector, collecting data, using data, analyzing data, and disclosing data have been a tool for these institutions to make efficient and effective decisions to deliver better services for their users and clients (Eggers and Shah, The government CDO: Turning public data to the public good, Deloitte Insights) (Glaeser, Kim, Luca, How Companies Can Use the Data They Collect to Further the Public Good, Harvard Business Review). The significant difference is that data is now becoming more sophisticated with the Internet of Things (IoT). This includes mechanisms sensors that collect data and using Artificial Intelligent (AI) and machine learning to analyze this data and to make decisions (McDonald, The Internet of Things requires machine learning and AI, IBM). Since data itself is more than just a tool, it is a valuable product that can be bought and sold (Eddy, How Companies Turn Your Data Into Money, PC Magazine). It has been over 20 years since the concept of smart cities came mainstream, but many cities are still working or begin working on implementing the smart cities approach (Life in the Smart City, The Economist). The essence of the smart cities approach is to collect, use, and disclose data for municipal governments to make decisions (Building the smart city with data, digital, and design, Deloitte); however, there are many challenges with the implementation of the smart cities approach in communities; from privacy laws to data bias and cybersecurity (Scassa, Why Canada needs a national data strategy, Policy Options). The opportunity and possibility of data-driven communities would provide many benefits but the design and implementation of the smart cities approach should be taken with caution. The worst outcome of the smart cities approach is creating a community where IoT becomes a tool for surveillance of the public even in democratic countries (Cheung, Smart Cities: are we sleepwalking into a Big Brother future of constant surveillance in the name of improved efficiency and safety, South China Morning Post). Therefore, privacy and security need to be studied carefully for the implementation of the smart cities approach.

For example, with the development of the Toronto Waterfront Project, there have been many privacy concerns especially with data collection and use of data (Zochodne, Order of Canada architect, Silicon Valley investor call for a rethink of Sidewalk Lab's Toronto waterfront project, Financial Post). There have also been reports from the Government of Canada on having a data strategy roadmap for the federal public service on how to manage, collect, govern, and share the data (Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service, p.4). Therefore, having a discussion about data between government institutions, private companies and residents is critical to develop an inclusive, transparent, democratic, and accountable data collection and use of data in smart cities.

My client, Jonathan Rybicki, for this research is interested in the implications of data collection and the use of data in the smart cities approach, especially in Canadian municipalities because of the Smart Cities Challenge. By researching this topic, it will help assist in addressing challenges with the implementation of data collection and use of data in smart city projects in Canadian municipalities. This report is structured as follows: the first few sections will set the context for the paper. The literature review, case studies, interviews, and discussion sections will encompass the core of the research. Finally, the recommendations

and conclusion sections will provide advice for my client to address the implications of using, collecting, and disclosing data in the smart cities approach.

1.1 Background and Defining the Issue

To understand the Smart Cities Challenge in Canada, it is important to first of all define what the smart cities approach means in a Canadian context because the definition is slightly different than the general definition applied anywhere else. According to the Canadian government, the smart cities approach is that "to achieve a meaningful outcome for residents by leveraging the fundamental benefits that data and connected technology have to offer: openness, integration, transferability, and collaboration." (The Challenge, Impact Canada Challenge Platform). The smart city approach uses technology and data to increase operational efficiency and quality of life for everyone in civil society. For example, operational efficiency would be using smart sensors for smart streetlights to dim the light when there are fewer cars and people on the street. The citizen's quality of life would improve by using smart technology that collects data to make a policy decision and increase operational efficiency in the community.

The Government of Canada has proposed a Smart Cities Challenge across the nation where municipalities, regional government, and Indigenous communities get together to bring forward ideas to create a positive impact in their communities by using data and connected technologies (Joint Letter to the Minister of Infrastructure and Communities on Smart Cities Challenge, Office of the Privacy Commissioner of Canada, 2018). The smart cities approach does not mean the municipality must be a city (The Challenge, Impact Canada Challenge Platform). It could be a town, a rural community, or Indigenous community (The Challenge, Impact Canada Challenge Platform). The Smart Cities Challenge is a competitive competition for federal government funding (The Challenge, Impact Canada Challenge Platform). There are three funding categories: 50 million dollars, 10 million dollars, and 5 million dollars (The Challenge, Impact Canada Challenge Platform). The 50 million dollars is open for all population sizes, the $10 million is open for communities under 500,000 residents, and the $5 million is open for communities under 30,000 residents (Applicant Guide, Impact Canada Challenge Platform). There are six focus areas in the Smart Cities Challenge: Economic opportunity, empowerment and inclusion, healthy living and recreation, safety and security, mobility, and environmental quality (Smart Cities Challenge: Spotlight on Finalist p.4).

For example, in the Canadian context of the Smart Cities Challenge, some municipalities have different smart city agendas than others. For instance, for one of the finalists of the $5 Million prize category, the Biigtigong Nishnaabeg (Pic River First Nation) in Ontario, their smart city plan is to use mobile-enabled technology called eAcquisition to deliver STEM education from Kindergarten to Grade 12 in both Nishnaabemwin and English (Smart Cities Challenge: Spotlight on Finalist, p.5). eAcquisition is also used as a meetup platform by connecting with other Nishnaabe community's members (Smart Cities Challenge: Spotlight on Finalist, p.5). Another example is in the City of Guelph and Wellington County, where one of the finalists for the $10 Million prize category focused on using technology and data to connect researchers, social innovators, farmers, entrepreneurs, and other community partners to address the food-secure ecosystem (Smart Cities Challenge: Spotlight on Finalist, p.17).

On the other hand, the City of Melbourne in Australia uses many technologies to collect and use data such as the 24 hours pedestrian counting system, waste collection (larger bins with a sensor indicating to collect when it is full), real-time parking sensors, internet trees (collect data on the trees in the cities), and bike

sensors (collect data on air contamination and traffic congestion) (City of Melbourne, 2018). The City of Melbourne claims there are many benefits of data collection in the smart cities approach such as reducing greenhouse gas emissions, reducing waste, promoting sustainable economic development, and increase the quality of life for the public (City of Melbourne, 2018). Different municipality have different smart city agendas to achieve different objectives for their communities. The Biigtigong Nishnaabeg, City of Guelph and Wellington County, and the City of Melbourne all have a smart city plan, but have different smart city projects and "smart city agenda." However, Biigtigong Nishnaabeg, City of Guelph and Wellington County, and the City of Melbourne does share similarity such as using the smart cities approach to increase the quality of life for the people.

Furthermore, there have been privacy concerns with how smart cities collected, protected, and used the data (Sali, 'Web of data' collected by smart city tech stokes privacy fears). The public tends to be divided on this issue because some see using and collecting data as contributing to better efficiency in the community and some see it as a major breach of privacy (Sali, 'Web of data' collected by smart city tech stokes privacy fears). In this paper, it discusses data ethics on collecting and using data in the smart cities approach. Apart from the discussion of data ethics, there are six key challenges and opportunities will be discussed in this paper. The six key challenges and opportunities are smart governance, privacy law, data ethics, data sovereignty, cybersecurity, and municipal resources (Data Governance in the Digital Age: Special Report, CIGI) (Smart Cities: Foundations, Principles and Applications, 2017)

The objective of this research paper is to identify and assess the implications of data collection and the use of data in the smart cities approach and how it affects the citizens, businesses, and civil society as a whole. Furthermore, to determine the benefits and challenges of data collection and use of data when municipalities implement the smart cities approach in their communities. In this research, civil society means organizations or institutions that are not part of the business community such as non-profit organizations. Also, it would be beneficial for Canada to learn from other countries' success and understand some of the concerns (e.g., data collection and the use of data) of implementing a smart cities approach. This research will look at the implications of the smart cities approach in collecting and using data and will develop guiding principles to address these issues.

1.2 Project Client

My client is Jonathan Rybicki from the Smart Cities Challenge Branch in Infrastructure Canada. Infrastructure Canada is a federal department that invests in public infrastructure by working with all levels of governments and other stakeholders to deliver public infrastructure that benefits all Canadians. Infrastructure Canada's mandate is to invest in public transit, trade and transportation, green infrastructure, rural and northern communities, and social infrastructure. Infrastructure Canada's objectives are to reduce greenhouse emissions, grow the economy, and build a more inclusive community. For the Smart Cities Challenge Office, it conducts the Smart Cities Challenge across the country, where communities submit their proposals to receive funding from the federal government. The smart cities challenge is for communities to use federal funding to create positive outcomes through connected technology and data.

The research being conducted in this Report is significant because it will outline and discuss the outstanding issues of the smart cities approach. This report will provide four deliverables to the client: the analysis of the literature review, case studies, expert interviews, and recommendations. The completion of this report

would provide useful information for my client and the organization to be aware of any alarming data issues when it comes to the smart cities approach.

1.3 Project Objectives and Research Questions

The main research question is "What are the implications of data collection and the use of data in smart cities and how does this affects citizens, businesses, and civil society as a whole?"

There are three sub-questions:

1.) What government tools and approaches can Canada learn from other countries when it comes to data collection and the use of data in smart cities?

2.) How do privacy policies affect smart cities' data collection and the use of data?

3.) What are the benefits and problems of data collection and the use of data that the government needs to be aware of when implementing the smart city approach?

The literature review documents facilitate the research questions and three sub-questions. At the beginning of the research process, reviewing news articles assisted with the general understanding of the data issues in the smart cities approach. Subsequently, the examination of books, journal articles, and government documents supported the development of the leading research questions and sub-questions (Data Governance in the Digital Age: Special Report, CIGI) (Smart Cities: Foundations, Principles and Applications, 2017). Many literature review documents on data collection or use of data in the smart cities approach raised privacy and security issues (Townsend, Smart Cities: Big Data, Civic Hackers and the Quest for a New Utopia) (Ratti and Claudel, The City of Tomorrow: Sensors, Networks, Hackers, and the Future of Urban Life).

Moreover, the literature review raises these key issues such as privacy law, data ethics, data sovereignty, cybersecurity, and municipal resources when collecting and using data in the smart cities approach (Data Governance in the Digital Age: Special Report, CIGI) (Smart Cities: Foundations, Principles and Applications, 2017). The challenges listed above are not just from one author that talks about all of these challenges. Each journal article or chapter has an author or a few authors writing a specific challenge regarding data collection and use of data in the smart cities approach. The case studies and interviews assist in the research where the literature review is lacking. The case studies focus on smart governance that may help municipalities to implement their own customized smart governance. In this research, smart governance means a government that uses technology to engage with residents and improves governmental administration. The interviews with experts provide insight into privacy law, data ethics, data sovereignty, cybersecurity, and municipal resources. There are many recommendations made by experts as part of a mitigation plan for municipalities to implement. The purpose of this capstone project is to find the implication of data collection and the use of data in the smart cities approach, as well as how it affects citizens, businesses, and civil society. The research will identify the issues and provide recommendations to address the challenges.

2.0 Methodology and Methods

2.1 Methodology

This research paper uses a qualitative methodology to collect documents, case studies, and interviews (Habib, Mamun, Bishwajit B. Pathik, and Hafsa Maryam, p.9). The benefit of using qualitative research is that it can explain multifaceted challenges that include the "social aspect" such as socio-economic status and social norms (Qualitative Research Methods: A Data Collector's Field Guide, p.1). This research looks at the more "social aspect" of the implication of data collection and the use of data such as data ethics. In this paper, it contains a variety of documents such as primary sources and secondary sources. The primary sources are government documents, news articles, and interviews (Habib, Mamun, Bishwajit B. Pathik, and Hafsa Maryam, p.57). The secondary sources are books, journal articles, and scholarly reports (Habib, Mamun, Bishwajit B. Pathik, and Hafsa Maryam, p57). This research determines and assesses gaps between the current state of knowledge of data in the smart cities approach and the unknown state of knowledge of data in the smart cities approach. The two case studies and seven interviews would fill in the gap of the unknown state of knowledge. This methodology is the current state analysis (Albrice, Current State Analysis).

2.2 Methods

The data collected from the literature, case studies, and interviews support the recommendations for Canadian municipalities and the federal government. There are six key themes in this research to assess the implication of data collection and use of data: smart governance, privacy law, data ethics, data sovereignty, cybersecurity, and municipal resources.

Literature Review

The literature review gives an overview of the current state of knowledge of the implications of data collection and the use of data in the smart cities approach. Since studies on the implication of data in the smart cities approach is a very recent public policy, documents collected for the literature review are not substantial enough for this research. The research on the smart cities approach is growing, but the information published is not keeping up with the technical development. Moreover, the data in the smart cities approach is a very interdisciplinary public policy, so there needs to be a diversity of different experts from different academic background (Estevez, Lopes, and Janowski, p.35). Many documents in the literature review do not contain an interdisciplinary framework such as a computer science expert discussing data in a smart city context. The data sources for the literature review composes of journal articles, books, government documents, reports, and news articles.

Case Studies

The two case studies consist of Estonia and Somerville. Estonia was chosen as one of the case study because of their advanced digital service for their residents and their administration system. The size of Estonia in 2019 is approximately 1.3 million (Statistics Estonia, More births and smaller emigration increased the population figure). The population of Estonia is similar or smaller to the population size of a few Canadian cities such as the Ottawa-Gatineau region is approximately 1.3 million, the Metro Vancouver Regional District is about 2.5 million, the Greater Montreal is about 4.1 million, and the Greater Toronto Area is over

6.3 million (Statistic Canada, Population). Also, by having a case study on Estonia, a country on smart governance and digital service would help Canada at the Federal level to learn how to implement similar digital services and smart governance. The other case study is Somerville, Massachusetts because it is important to look at a local level of the smart cities approach. The City of Somerville focus on residents when designing and implementing the smart cities approach and less focus on technology as the main component. Both case studies focus on the idea of "smart governance", which is one of the key themes throughout this research. The information collected for the two case studies comprises of government documents and journal articles.

Interviews

The interview component contributes to the unknown state of knowledge that is not found in the literature review and case studies. The interviews include the key themes, and each interviewee is an expert in privacy law, data ethics, data sovereignty, cybersecurity, and municipal resources. The interviews are categorized into five components: Privacy law, data infrastructure, data ethics, cybersecurity, and municipal resources. The interviewees are chosen based on your expertise in one or more of the key themes listed above and understand how some smart cities' concerns emerge from these key themes. The interviewees for privacy law, data ethics, data infrastructure, and cybersecurity are university professors who have expertise in smart cities and one or more of the key themes listed above. The two interviewees for municipal resources are either Chief Technology Officer or the Information Services Manager in their municipality who are involve with the development of smart cities. Each interview includes approximately five to eight questions (See interview questions in the Appendices), and the interview assists the unknown knowledge not found in the literature review and case studies. The total number of interviewees in this research is seven experts, and it was conducted one-on-one over Skype video conference. The interview section in this research paper brings social science, law, and computer science experts together, which is missing in most literature on data in a smart city context.

2.3 Data Analysis

The analytical framework of this report will consist of using the SWOT analysis. The SWOT analysis standards for strengths, weaknesses, opportunities, and threats (SWOT Analysis, Mindtools). The SWOT analysis is a framework to comprehend the strengths and weaknesses while also identifying opportunities and addressing threats when it comes to data collection and use of data in the smart cities approach (SWOT Analysis, Mindtools). By analyzing the strengths and weaknesses, the researcher identified the opportunities and threats of data collection and the use of data in the smart cities approach.

2.4 Project Limitations and Delimitations

The strong validity of the qualitative data being collected is mostly dependent on the quality of primary sources and secondary sources, as well as the number of participants for the interview. However, interviewing experts in the field has strengthened the qualitative data in the report because research on the smart cities approach specifically in data and public policy is very young. In this paper, it will be discussing the challenges in smart cities data breaching, data ethics, cybersecurity, and resources of local governments. Moreover, by looking at how other countries address data issues in smart cities as smart practice, it can help Canada address similar data issues when implementing smart cities. This report will get expertise and

opinions from experts in their field since the smart cities approach is very interdisciplinary. The experts come from law, Information Technology (IT), data ethics, and local governance backgrounds.

3.0 Literature Review

3.1 Introduction

The literature review will first define what a smart city means in different governmental institutions and private companies. Secondly, the literature review will determine what the smart cities approach means in the context of the Smart Cities Challenge in Canada. By clearly explaining the definition of the smart cities approach, it shows what the objective of using data and smart technology in Canadian communities is. After defining what the smart cities approach is, the literature review will be organized into key themes: data privacy, data ownership, data sovereignty, data ethics, and cybersecurity. No literature contains all of the key themes together in one literature document on data collection and the use of data in the smart cities approach. In the open letter written by the federal, provincial, and territorial privacy guardians in Canada to the Minister of Infrastructure and Communities, they outline key themes such as privacy laws, data ethics, cybersecurity, and "smart governance" (OPC, Joint letter to the Minister of Infrastructure and Communities on Smart Cities Challenge). Moreover, the Data Governance in the Digital Age: Special Report from the Centre for International Governance Innovation and the Smart Cities: Foundations, Principles, and Application book both discuss the key themes of data privacy, data ownership, data sovereignty, data ethics, and cybersecurity. Both of these documents are written by multiple experts who only focus on one key theme. In this research, it focuses on numerous key themes because different components affect data collection and the use of data.

3.2 Definition: The Smart Cities Approach

It is challenging to define what a "Smart City" is because there are many different interpretations. In this section, it will look at the different definitions of a smart city from what other governments in the world define a smart city to how the private sectors define a smart city. For the European Commission, they define a smart city as "a place where traditional networks and services are made more efficient with the use of digital and telecommunication technologies for the benefit of its inhabitants and business" (Smart Cities, European Commission). Moreover, the European Commission focus on partnership in smart cities with different stakeholders to achieve a positive outcome by focusing on knowledge sharing, open data governance, policy and regulation, citizen focus, and other components (Smart Cities, European Commission). Furthermore, the UK's Department for Business Innovation & Skills defines smart cities as "a process, or series of steps, by which cities become more "liveable" and resilient and hence, able to respond quickly to new challenges" (Smart Cities: Background Paper, 2013, p.7).

Many other Asian countries are also implementing the smart city concept in their cities. Their definitions of smart cities are also slightly different from the EU. The Chinese government defines a smart city as "a new concept and model which utilises the next generation of information technology. This includes the Internet of Things (IoT), cloud computing, big data, promoting smart urban planning, construction, management and services for cities" (Smart Cities and Social Governance: Guide for Participatory Indicator Development, UNDP China, p.6). The Chinese government's definition focuses more on the data and technology of smart cities whereas the EU tends to emphasize more on the citizen-centric way of a smart city. For the Indian government, they state that there is no universal definition of a smart city and it is challenging even in India to define what a smart city is (What is Smart City, Ministry of Housing and Urban Affairs, Government of India). The Indian government states that the objective of a smart city is to "provide

core infrastructure and give a decent quality of life to its citizens, a clean and sustainable environment and application of "Smart" Solutions" (What is Smart City, Ministry of Housing and Urban Affairs, Government of India). The Indian government defines core infrastructure as e-Governance, citizen participation, sustainable environment, public transport, waste management, water and electricity supply, safety, IT connectivity, and other urban infrastructures (What is Smart City, Ministry of Housing and Urban Affairs, Government of India).

On the other hand, some private companies define a smart city slightly differently from government institutions by focusing on the data-driven aspect of a smart city (Smart Cities Definition, 2014, Centre for Cities). For instance, IBM interprets smart city "as one that makes optimal use of all the interconnected information available today to better understand and control its operations and optimize the use of limited resources" (Smart Cities Definition, 2014, Centre for Cities). Cisco, another privacy company, defines a smart city as "scalable solutions that take advantage of information and communications technology (ICT) to increase efficiencies, reduce costs, and enhance the quality of life" (Smart Cities Definition, 2014, Centre for Cities). The private sector and government institutions both have common elements in their definition of a smart city such as provide better efficiency, using data and technology. It seems government institutions tend to emphasize more on a human-centered part of the smart city compared to private companies who focus more on the data part of the smart city.

The Smart Cities Challenge in Canada defines the smart cities concept differently than the general definition. According to the Government of Canada, a smart cities approach is to use data and smart technologies to achieve beneficial outcomes for residents by having openness, integration, transferability, and collaboration as the main components (The Challenge, Impact Canada Challenge Platform). In this context, openness, integration, transferability, and collaboration means:

"Openness:

When communities make their data truly accessible, usable and barrier-free, their decision-making processes become transparent, empowering citizens and strengthening the relationship between residents and public organizations.

Integration:

Data and connected technology empower communities to break down silos that exist within local governments and public organizations.

Transferability:

When tools and technological approaches are open-source, transparent and standardized, they can be used by communities across the country, no matter their size or capacity.

Collaboration:

Connected technology enables communities to bring traditional and non-traditional partners together to collaborate." (The Challenge, Impact Canada Challenge Platform).

There are some similarities and differences with Canada's definition of the smart cities approach compared to other government institutions in the world and private companies. The Canadian definition shares similarities with the EU when it comes to being more focused on the human-centric part of a smart city. However, the significant difference between Canada's definition is that the smart cities approach does not only apply to cities but all municipalities regardless of population and Indigenous communities. Moreover, Canada's definition also includes a data-driven and integrating system similar to the private sector's definition. Canada's definition of a smart city is more inclusive to all communities and strikes a balance between data, technology, collaboration, and a human-centric approach to a smart city.

In recent years, the smart cities approach has captured the interest of governments, businesses, and civil society. As a result, there are many reports on the role of data in the smart cities approach. This includes not only Canadian scholars, but international scholars as well. There are key search terms and databases the researcher will use in this report: Internet of Things, Big Data, City Data Commons, Participatory Data Infrastructure, Open Data, and information technology. Corporations such as IBM have been very involved with the idea of a smart city and collaborating with municipalities around the world to implement smart city projects (Wilson, Smarter Cities Challenge aims to make lasting urban improvements, IBM). IBM conducted a Smarter Cities Challenge around the world where IBM gave grant money to support smart city projects in winning municipalities (Wilson, Smarter Cities Challenge aims to make lasting urban improvements, IBM). Moreover, there are institutions such as the World Council on City Data (WCCD) is a platform for cities around the world to collaborate and learn from each other to improve services and quality of life for their residents (What is the WCCD, World Council on City Data).

There are a few case studies that show the benefits of data in the city from the Open Knowledge International, a non-profit organization that promotes the idea of open data and sharing information (About, Open Knowledge Foundation). Many of the case studies from Open Knowledge International discusses whether the use and collection of data in the smart city approach would be beneficial and widely accepted by society as a whole (About, Open Knowledge Foundation). By having businesses and citizens participate in the smart cities approach, it would create a more inclusive society, more transparency, and more accountability. Many scholars that support the smart cities approach argue that with better data, governments can design better public policies and address social, economic, and environmental issues. For instance, Anthony Townsend explains government could address traffic congestion in cities, housing issues, pollution, and other current issues by the use of digital technology and information technology (Townsend, 2014, p. xii, 8). Townsend discusses the benefits of data in the smart cities approach, but is also very worried about the challenges of the data collection and the use of data in communities (Townsend, 2014, p.17).

Carlo Ratti and Matthew Claudel noticed that people in the communities already supply data information about the cities or towns through apps that report pothole areas, fallen trees, traffic, and other data about their surroundings (Ratti and Claudel, 2016, p.52). Ratti and Claudel both agree the society needs to change the way it collects and uses data because right now, the control of data information is a top-bottom approach (Ratti and Claudel, 2016, p.53). Ratti and Claudel support the idea of a bottom-up approach to data collection and the use of data because it gives the public control over how data is being used and will benefit society overall (Ratti and Claudel, 2016, p.55). For instance, Google collects and uses data from their clients (users of Google) in exchange the client gets free Google services from email to Google search engine (Ratti and Claudel, 2016, p.55). However, some researchers are in favor of giving people control over who they want to give their data, in exchange for receiving benefits or keeping their data private (Ratti and

Claudel, 2016, p.55). Many kinds of literature I reviewed support the idea of giving people more control over their data rather than just a small hand full of influential groups. This is because, with more people who have a say in how to use and collect data, they would be able to create communities that are smarter and more efficient.

The overview of what the smart cities approach is, in the paragraphs above, will assist the reader in understanding the in-depth complexity of smart city approaches, especially with regards to data collection and use of data. In this section, we explore a different kind of smart cities approach definition, but all of the definitions have a common theme that using technologies and data leads to making better decisions. Some countries are more focused on the human-centric of the smart cities approach while other countries are more focused on the technological efficiency the smart city projects can bring to the community. In the data ethics section of the literature review, it explains the importance of a more human-centric smart cities approach, especially with the on-going discussion of the Toronto Waterfront Project.

3.3 Data and Privacy Laws

In Canada, there are two federal privacy laws: The Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA). The Privacy Act's purpose is "to extend the present laws of Canada that protect the privacy of the individual with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information" (Privacy Act, 2018, p.1). The PIPEDA's purpose is to "set out the ground rules for how businesses must handle personal information in the course of their commercial activity" (PIPEDA legislation and related regulations, OPC). In the PIPEDA context, personal information consists of: "name, opinions about the individual, birth date, income, physical description, medical history, gender, religion, address, political affiliations and beliefs, education, employment, and visual image such as photographs, and videotape where individuals may be identified" (Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts, OPC). Moreover, some provinces have a similar privacy act as the PIPEDA such as BC, Alberta, and Quebec which may be applied instead of the PIPEDA (Summary of Privacy Laws in Canada, OPC). Municipalities in Canada are under the jurisdiction of the provincial government so that privacy laws would be under the provincial government (Summary of Privacy Laws in Canada, OPC).

In the PIPEDA, there is the ten "fair information principles":

- Accountability
- Identifying purposes
- Consent
- Limiting collection
- Limiting use, disclosure, and retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging Compliance (PIPED Fair Information Principles, 2018, OPC)

The Privacy Commissioner of Canada oversees the two federal privacy laws (Office of the Privacy Commissioner of Canada, Summary of privacy laws in Canada). The Privacy Commissioner of Canada's objective is to protect and promote privacy rights in Canada (Office of the Privacy Commissioner of Canada, About the OPC). On April 24, 2018, Canada's federal privacy guardian along with the provinces and territories' privacy guardians have sent an open letter to the Minister of Infrastructure Canada and Communities to be aware of the privacy and the security of personal information when selecting the winning municipalities for the Smart Cities Challenge (Office of the Privacy Commissioner of Canada, Joint Letter to the Minister of Infrastructure and Communities on Smart Cities Challenge). The Open Letter from federal, provincial, and territorial privacy guardians has considered the privacy risks in the smart cities approach and mitigating controls.

Some of the privacy risks they discuss in the Letter were smart technologies such as using and collecting data from sensors or personal devices that could be difficult for someone who wants to opt out from it (OPC, Joint Letter to the Minister of Infrastructure and Communities on Smart Cities Challenge). They are also concerned with the volume of data being collected that could enable privacy-invasive activities such as surveillance or profiling (OPC, Joint Letter to the Minister of Infrastructure and Communities on Smart Cities Challenge). The Letter stated that "the more points of data collection, processing and access, the greater the risk of a security failure" (OPC, Joint Letter to the Minister of Infrastructure and Communities on Smart Cities Challenge). Since public trust is one of the fundamental components to having a successful smart cities initiative, the mitigating control needs to be well thought out (OPC, Joint Letter to the Minister of Infrastructure and Communities on Smart Cities Challenge).

The Open Letter from all the provincial and territorial privacy guardians has indicated six privacy and security measures in the smart cities approach:

"**Data-minimization –** systems must not collect, use or disclose personal information unless it is necessary to do so to achieve the outcomes of the initiative. In all cases, where the goals can be achieved using less privacy invasive alternatives, those alternatives should be pursued.

De-identification – systems must endeavor to de-identify personal information at the earliest opportunity and include measures to mitigate the high risk of re-identification that is inherent with connected devices. As well, systems should only retain, use and disclose de-identified information.

Data governance and Privacy Management program – initiatives must be supported by policies that address privacy and security requirements including appointing a privacy lead, monitoring and auditing for compliance, and breach response. There must also be contractual protections and accountability for all of the diverse parties involved in the initiative. This is especially important given that the department is encouraging communities to develop proposals in conjunction with other partners.

Privacy impact assessments and threat risk assessments – these are widely recognized as important tools to help ensure that privacy and security risks are identified and adequately addressed in the design of new technologies and programs. In some jurisdictions, they are required.

Community engagement and project transparency – communities must ensure full transparency of the information practices of their initiatives to help community members understand how they might be affected. Transparency is reflected in Canadian provincial and federal access and privacy laws.

Consent – systems must ensure individuals' meaningful consent where required by law, including the opportunity to opt out of participation, where feasible." (OPC, Joint letter to the Minister of Infrastructure and Communities on Smart Cities Challenge)

Since the smart cities approach is still a very recent government policy, understanding the benefits and challenges may be different for different countries. Canada has started the Smart Cities Challenge, and there are many information unknowns, such as if municipalities have the capacity and resources to implement their smart cities approach. Moreover, whether municipalities are prepared to mitigate data breaching, cyberattacks, and use their collected data effectively to make future policies. Many applicants to the Smart Cities Challenge do not clearly outline if privacy issues were part of their smart cities design (Participating Communities, Impact Canada Challenge Platform). Moreover, many applicants' smart cities approach did not mention data sharing between communities or within municipal departments (Participating Communities, Impact Canada Challenge Platform). The expert interview questions about privacy, data ethics, cybersecurity, and resources will help municipalities to implement the smart cities approach in their community. The information in this research paper includes many government documents, journal articles, expert interviews, and other kinds of relative literature that will provide valuable information to help municipalities when they are implementing their smart cities approach.

The Centre for International Governance Innovation, which is an independent and non-partisan think tank organization, published the report "In the Data Governance in the Digital Age: Special Report of 2018", where many scholars and IT experts advocate for a National Data Strategy in Canada. One of the scholars in the Report is Teresa Scassa, a Canadian lawyer that specialized in Information Law and advocates for a National Data Strategy in Canada to address data and privacy issues. In the smart cities approach on data, governments tend to collaborate with the private sector on stalling and operating sensors around the community to collect huge volumes of data and process it at high speed (Data Governance in the Digital Age: Special Report, 2018, p.6). Governments and the private sector can collect data and use data to drive innovation and efficiency, but at the same time it may foster high levels of risks and harm to the public such as cyberattacks, data breaching, data discrimination, loss of autonomy, and dignity (Data Governance in the Digital Age: Special Report, 2018, p.7). Scassa argues that the current system does not fully view data as a resource and laws have not adapted to protecting individual data rights from being exploited (Data Governance in the Digital Age: Special Report, 2018, p.7). Scassa states that "the blurring of public and private – in particular around data – as well as the deeply interwoven challenges raised by big data, AI, and machine learning, make it problematic to silo issues in this way" (Data Governance in the Digital Age: Special Report, 2018, p.7). Also, as the Internet of Thing (IoT) becomes more sophisticated in collecting data, it increases the possibility of collecting more private and personal information (Data Governance in the Digital Age: Special Report, 2018, p.9). By having fragmented methods to address the issue around data, it causes complexity and inefficiency (Data Governance in the Digital Age: Special Report, 2018, p.7).

When developing a solution to address data issues, one needs to keep in mind data justice which consists of fairness, transparency, and equity (Data Governance in the Digital Age: Special Report, 2018, p.11). Algorithmic transparency is a key component in data justice because many governments and private sectors make a decision based on the data and the algorithms it uses to process the data (Data Governance in the Digital Age: Special Report, 2018, p.11). Moreover, when the government uses data to make decisions, it must not create social inequalities (Data Governance in the Digital Age: Special Report, 2018, p.11).

The PIPEDA, one of the Federal privacy laws, is weak in protecting personal information where companies collected, used, and disclosed data (Data Governance in the Digital Age: Special Report, 2018, p.9). It is a problem that PIPEDA does not see data as a crucial economic asset because in a digital economy data is a resource to create innovation and revenue (Data Governance in the Digital Age: Special Report, 2018, p.9). On the other hand, in the European Union, it recently implemented the General Data Protection Regulation (GDPR) where it has better data protection than any data related protection law (Data Governance in the Digital Age: Special Report, 2018, p.9). The GDPR has unified the flow of data from one country to another within the European Union because data can flow smoothly from one jurisdiction to another (Data Governance in the Digital Age: Special Report, 2018, p.9). Therefore, it would be effective for unified data regulation to protect an individual's data right. Canada could learn from the EU's experience in implementing the GDPR.

In Canada, there are two federal acts that govern data and privacy, the Personal Information Protection and Electronic Documents Act (PIPEADA) and the Privacy Act (Privacy laws in Canada, 2016, Office of the Privacy Commissioner of Canada). According to the privacy laws in Canada, "PIPEDA is the federal privacy law for private-sector organizations, and it sets out the ground rules for how businesses must handle personal information in the course of commercial activity" (Summary of Privacy laws in Canada, 2018, Office of the Privacy Commissioner of Canada). The Privacy Act is "a person's right to access and correct personal information that the Government of Canada holds about them and applies to the Government's collection, use and disclosure of personal information" (Summary of Privacy laws in Canada, 2018, Office of the Privacy Commissioner of Canada). Moreover, each province and territory has its privacy law when it comes to government handling personal information (Summary of Privacy laws in Canada, 2018, Office of the Privacy Commissioner of Canada). When looking at personal data law, Estonia is leading the way with data collection and the use of data. Canada can learn from Estonia's Personal Data Protection Act when implementing the smart cities approach because Estonia gives its citizens more control over their data (Herlihy, 2013, Government Digital Service). Estonia has built itself as a leader in digital society by providing municipal and state services delivery 99% online through a single state portal system (We have built a digital society and so can you, E-Estonia). Estonia has been using Blockchain since 2008 to decrease cyberattacks because in 2007 Estonia had a cyber attack that shut down all their government websites, but the data was not lost (We have built a digital society and so can you, E-Estonia). Estonia acknowledges that creating a digital society needs effective cybersecurity and is essential to protect it from being vulnerable to cyber attacks (We have built a digital society, and so can you, E-Estonia). Estonia recognizes the importance of continuous experimentation and learning from their mistakes because it helps to grow a strong and feasible data-driven government (We have built a digital society, and so can you, E-Estonia). Estonia's experience in data collection, the use of data, privacy protection, and cybersecurity would help Canada address data and privacy issues in the implementation of the smart cities approach across the country.

One of the key challenges of data collection and use of data in the smart cities approach is the concern of privacy laws and regulations not keeping up with technological development. In an open letter to the Minister of Infrastructure and Communities, all provincial and territorial privacy guardians voiced their concerns about individual privacy, surveillance activities, consent, privacy impact assessment, community engagement and other issues with the implementation of the smart cities approach. It is important that provinces and territories are raising their concerns about these challenges listed above to the Minister

because it may push the federal government to revise the PIPEDA or create a new privacy regulation to address the privacy issues with data-related smart city projects.

EUROPEAN UNION STANDARD DATA

This paper will look at the GDPR as a case study on how the EU protects an individual's privacy and data in the context of the smart cities approach. In the European Union, the General Data Protection Regulation (GDPR) "regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU" (European Commission, What does the General Data Protection Regulation (GDPR) govern?). The GDPR unifies the data protection regulation in Europe (Andrews, 2018, How the EU's new data laws will affect Smart City development). In May 2018, the GDPR was enforced to unify the data protection law in Europe Union countries since more than 90% of citizens wanted unified data protection right across the European Union (European Commission, Data Protection in the EU). The core component to GDPR is that it protects individual data by giving more power for the individual if they consent in sharing their data to a third party (Andrews, 2018, ITU News). According to Jamie Cudden, a Smart City Program Manager in Dublin states that the GDPR builds trust between the data custodian and the public as well as giving people more power in protecting their data (Andrews, 2018, ITU News).

Moreover, Cudden argues that cities need to be more transparent in how they collect and use data to benefit the citizens or cities (Andrews, 2018, ITU News). Under the GDPR, any smart city project would need to address personal data management risks before starting (Andrews, 2018, ITU News). Moreover, GDPR would push companies to improve their anonymization algorithms when collecting, using, and disclosing data (Andrew, 2018, ITU News).

The GDPR in the context of the smart cities approach would be a good case study for Canada to understand their success and challenges. By looking at the EU's GDPR, it would help Canada amend its privacy law or create a new privacy law that addresses cybersecurity and data breaching in the smart cities approach in Canada. In the interview results section of the paper, it will consist of Scassa, an expert in privacy and information law in Canada who will share her expert opinions about the GDPR and the other two Federal privacy laws. Furthermore, in the case study section of this paper, Estonia's experience in being a digital society is a good case study for Canada to learn from.

In the previous section on privacy laws in Canada, it discusses that PIPEDA is not protecting individual privacy enough. This section on EU's GDPR explains that the GDPR has a stronger and more updated version to address privacy concerns, especially for data-related smart city projects. In the interview section, I interviewed with Scassa to explain about privacy laws and regulations in the context of the smart cities approach. Also, the interviewing with Scassa provided recommendations to address the privacy laws and regulations issued in Canada.

TYPES OF DATA PRIVACY

When discussing data privacy, need to distinguish the different types of data privacy. According to Kitchin, a smart cities scholar, there are six types of data privacy:

1.) "Identify privacy (to protect personal and confidential data)
2.) Bodily privacy (to protect the integrity of the physical person)
3.) Territorial privacy (to protect personal space, objects and property)

4.) Locational and movement privacy (to protect against the tracking of spatial behaviour)
5.) Communications privacy (to protect against the surveillance of conversations and correspondence)
6.) Transactions privacy (to protect against monitoring of queries/searches, purchases and other exchanges)" (Kitchin, 2016, p.5)

Furthermore, Kitchin outlines a table below that shows possible privacy breaches when it comes to collecting, processing, and disclosing data using smart technologies in the community. The table below illustrates the possible privacy breaches and how these privacy breaches are triggered.

The diagram/table that illustrates the taxonomy of privacy breaches and harm (Kitchin, 2016, p.6):

TABLE 1: TYPES OF DATA PRIVACY

The Diagram/table that illustrate the taxonomy of privacy breaches and harm (Kitchin, 2016, p.6):

Domain	Privacy Breach	Description
Information Collection	Surveillance Interrogation	• "Watching, listening to, or recording of an individual's activities" • "Various forms of questioning or probing for information"
Information processing	Aggregation Identification Insecurity Secondary use Exclusion	• "the combination of various pieces of data about a person" • "linking information to particular individuals" • "carelessness in protecting stored information from leaks and improper access" • "use of information collected for one purpose for a different purpose without the data subject's consent" • "failure to allow the data subject to know about the data that others have about her and participate in its handling and use, including being barred from being able to access and correct errors in that data"
Information Dissemination	Breach of confidentiality Disclosure Exposure Increased accessibility Blackmail Appropriation Distortion	• "breaking a promise to keep a person's information confidential" • "revelation of information about a person that impacts the way other judge her character" • "revealing another's nudity, grief, or bodily functions" • "amplifying the accessibility of information" • "threat to disclosure personal information" • "the use of data subject's identity to serve the aims and interests of another" • "dissemination of false or misleading information about individuals"
Invasion	Intrusion:	• "invasive acts that disturb one's tranquility or solitude"

	Decisional interference:	• "incursion into the data subject's decisions regarding her private affairs"

By being aware of the different data privacy issues, it helps to address the problem based on the privacy breach and the stage of the data (collection, process, and disclose). This privacy chart above would be helpful to understand how different stages of the data life cycle could cause harm. There are many data privacy concerns when implementing the smart cities approach. However, Kitchin argues that as a society we should not give up using data science and smart technology because of possible ethical harm when using the technology to collect, use, and disclose data (Kitchin, 2016, p. 5). He argues that the government should establish incentives to lower these privacy risks (Kitchin, 2016, p. 5).

Kitchin's table illustrates clearly the types of data that could be collected, used, and disclosed in a smart city project. The table outlines in each stage of the data, what are the possible privacy breaches and the description of how the privacy breach occurred. Having an explicit table on data privacy helps the reader to understand how collecting, using and disclosing data could have privacy concerns. Furthermore, it also allows them to comprehend how data privacy problems are interconnected with the critical challenges in the smart cities approach to data such as data ownership, data sovereignty, data ethics, cybersecurity, and municipal resources.

DATA OWNERSHIP

When municipalities collect, use, and disclose data from the smart technologies they implement, there is an important discussion on who owns the data. Some municipalities would collaborate with the private sector when it comes to the implementation of the smart cities approach in their community. Some companies may want part ownership of the data collected.

Kurtis McBride, a co-founder and chief executive officer of Miovision, a smart city technology company that specialized in traffic data, argues that data collected by cities should be the one to own that data because if another stakeholder owns that the data, cities would not be able to use the data for the benefit of the public (Data Governance in the Digital Age: Special Report, 2018, p.45). If cities or the country do not have a robust governance standard on data, influential tech companies would have an advantage over the public sector (Data Governance in the Digital Age: Special Report, 2018, 46). There has been a shift in having data be the product of intellectual property, to having data as a tool to create intellectual property (Data Governance in the Digital Age: Special Report, 2018, p.45). When private sectors collaborate with cities, they use legal ownership and technical architectures as ways to own city data (Data Governance in the Digital Age: Special Report, 2018, p.45). Furthermore, cities should be the ones owning the data being collected because the public infrastructure collecting the data is funded by tax dollars (Data Governance in the Digital Age: Special Report, 2018, 46).

Moreover, for Indigenous communities implementing the smart cities approach in their community, they should also be the owner of their data. If Canada plans to develop a national data strategy, Indigenous people should be able to voice their opinion on a Nation-to-Nation discussion (Data Governance in the Digital Age: Special Report, 2018, p.60). According to the British Columbia First Nations Data Governance Initiative, the three levels of government are managing Indigenous data poorly, with the following issues:

1.) “Methods and approaches used to gather, analyze and share data on Indigenous communities have reinforced systemic oppression, barriers and unequal power relations;

2.) Data on Indigenous communities have typically been collected and interpreted through a lens of inherent lack, with a focus on statistics that reflect disadvantage and negative stereotyping;

3.) Data on Indigenous communities collected by nation-state institutions has been of little use to Indigenous communities, further distancing Nations from the information;

4.) Data on Indigenous communities collected by the nation-state government has been assumed to be owned and therefore controlled by said government

5.) With a lack of meaningful Nation-to-Nation dialogue about data sovereignty” (Data Governance in the Digital Age: Special Report, 2018, p.60).

Many Indigenous leaders have voiced their concerns over data sovereignty because data sovereignty is a core component of self-government (Data Governance in the Digital Age: Special Report, 2018, p.11).

Data ownership is one of the challenges of data collection, and the use of data in the smart cities approach because with public institutions collaborating with private tech sectors the tension of who owns the data would be contested. McBride supports municipalities owning the data instead of the private tech sector because the data collected is using taxpayers’ money to do it. Also, throughout the Data Governance in the Digital Age: Special Report, many of the authors support the idea of having a national data strategy to address data issues such as data ownership, privacy, data sovereignty, and other data issues.

SMART GOVERNANCE

In this research, smart governance means a government that uses technology to engage with residents by having discussions in real-time and providing digital services to residents similar to e-Estonia. Moreover, to create an efficient departmental operation where government departments break communication silos and have an adequate data management system and/or cloud-based file sharing system to make a decision based on data collected by smart technologies (sensors, government services apps, etc.). When municipalities implement the smart cities approach in their communities, municipalities would need to change their governance structure into smart governance. The following documents discuss the types of smart governance models and how to reform “traditional governance” to “smart governance.”

TYPES OF SMART GOVERNANCE MODEL

According to Vinod Kumar, smart governance is about “participatory decision making, transparent corrupt free Governance, best public and social services and above all well thought out political strategies, and perspective by the inhabitants” (Vinod Kumar, p.22). The four smart governance models discuss by Vinod Kumar are developed in the context of the Indian government structure (Vinod Kumar, p.35-6). However, the models could be customized or use as a case study to understand how Canadian municipalities can implement “smart governance.”

Vinod Kumar explains that there are four types of models for smart governance:

Model 1: No Transformation of Government Structure and Processes

Model 2: Innovation in Decision-Making Process and Implementation

Model 3: Creation of Smart Administration

Model 4: Rearranging Governance as Dictated by Smart Cities (Vinod Kumar, p.35-40).

Model 1: No Transformation of Government Structure and Processes

The first model is where the municipality makes no government structure and process changes when implementing smart city projects in their communities (Vinod Kumar, p.36). If the government has opportunities for residents to voice their opinions and provide good public service with an excellent administrative operation, it may not need a governmental structural transformation (Vinod Kumar, p.36).

Model 2: Innovation in Decision-Making Process and Implementation

The second model is not a full governmental structural reform but emphasizes using more innovative ways or tools to be incorporated in the decision-making process (Vinod Kumar, p.36). For instance, they are using the Decision Support System (DSS) for participatory decision-making (Vinod Kumar, p.37). Another example is using the Geographic Information System (GIS) or Spatial Decision Support System (SDSS) could assist in the decision-making process for the municipal government (Vinod Kumar, p.37). Schuurman D, Baccarne B, De Marez L, and Mechant P describe this type of smart governance focus as "the process of collecting all sorts of data and information concerning public management by sensors or sensor networks" (Vinod Kumar, p.37). As a result, by using data, the government can make better decisions (Vinod Kumar, p.37).

Model 3: Creation of Smart Administration

The third model focuses on developing "smart administration," where the change is a more internal restructuring of the organization (Vinod Kumar, p.37-8). For model 3, the creation of smart administration needs to be more "digital-based" (Vinod Kumar, p.38). For instance, sending documents electronically, with self-generated date stamps on all documents, and other digital tools (Vinod Kumar, p.38).

Model 4: Rearranging Governance as Dictated by Smart Cities

The fourth model of smart governance focuses on "rearranging the position of government within the urban system as dictated by the urban system itself" (Vinod Kumar, p.39). To achieve this, the municipality needs to interact not only within their smart city but interact with other external smart cities as well (Vinod Kumar, p.39). This model is pro-active and connects governance structure where its objective is to address public policy issues by connecting with other smart cities in the country or around the world (Vinod Kumar, p.39-40).

Analysis of the Four Smart Governance Models

Vinod Kumar argues that it is challenging to endorse one particular model for all smart cities because each municipality have their unique challenges and context, but still will share some similar challenges as well (Vinod Kumar, p.41). Vinod Kumar explains that Model 1 and Model 2 are relatively easier to implement

than Model 3 and Model 4 (Vinod Kumar, p.41). Vinod Kumar argues that when a municipality become very mature in their smart cities phase, Model 3 and Model 4 are more appropriate models to use (Vinod Kumar, p.41).

The four models Vinod Kumar presents give the reader a general understanding of what kind of models are out there for smart governance. The analysis from Vinod Kumar lets the reader understand there is no universal model for municipalities to implement; it all depends on the context of the municipality.

Smart Governance: Five Key Operational Areas to Improve

The next author Beth Blauer will discuss five key operational areas in municipal governments they could implement to achieve "smart governance" or "more responsive government" (Blauer, p.154). Blauer is an Executive Director of the Centre for Government Excellence (GovEx) at Johns Hopkins University, where the organization assists with over 100 cities on building better data-driven cities (Blauer, p. 152). Data has been beneficial for cities and small communities to make decisions based on the information collected to provide better services for the public. For instance, in London, there are chips in transit cards which collect data from the user. The city planner uses the data collected to make changes in the transit system to optimize efficiency (Blauer, p.152). Blauer argues that municipal governments need to provide a more proactive service delivery than reactive city service (Blauer, p.153). With the use of data in communities, municipal governments should be able to change their service delivery to the public more proactively, more productively, and more efficiently.

Blauer proposed five key operational areas in municipal governments that can transform the municipal government into a more responsive government (Blauer, p.154). The five key operational areas for municipal governments to improve are: cultural transformation, data management, modernized performance management, the capacity to leverage advanced analytics, and networks (Blauer, p.154).

In the literature review and the case study sections, smart governance is discussed. Blauer supports the "smart governance" concept but has five recommendations for municipalities to work on to use data most effectively within the context of government administration structure. In the next five subsections of the smart governance sector, it will clearly explain how and why these five recommendations are essential for municipalities to implement.

Cultural Transformation

There is a need for cultural transformation in the government bureaucratic system because the current attitude in public service is pessimistic about changing cultural operation in the bureaucratic system (Blauer, p.154). According to the "What Works Cities" organization, it found that bureaucratic cultural barriers were one of the core issues that hinder municipalities from implementing a data-driven community (Blauer, p.154). Moreover, the municipalities that were successful in achieving a data-driven community were able to do so by having pilot projects to see if it works and then scale up the project (Blauer, p.154). Senior leadership needs to take a more proactive role and have a clear vision in the organization if the government wants to change the bureaucratic system into a more data-driven organization (Blauer, p.155). From municipal to federal departments, there is a silo effect that causes inefficiency and makes it challenging to implement a data-driven bureaucracy (Blauer, p.155-6). This shows implementing a smart city approach in communities and municipal governments needs to address communication silo or silo effects within its departments. For instance, one municipal department could collect the data and the other municipal

department would find that data collected useful, but have no idea that data was received by the other department already (Blauer, p.156). To ultimately achieve the smart cities approach, municipal departments need to break the silo effects and share their knowledge and data. Using data to address social, economic, and environmental issues involves different departments collaborating. Blauer states that to resolve the silo effect, municipal departments need to create a multidisciplinary approach to department operation and organizational planning (Blauer, p.156). However, the most significant barrier for data-sharing across departments is legal issues (Blauer, p.156). There are many laws in place to protect privacy, but it may hinder municipal departments from sharing their data (Blauer, p.156). Moreover, there needs to be reform on how municipal-level, provincial-level, and federal-levels share data by eliminating barriers (Blauer, p.156).

Public servants should have the opportunity to experiment with new ideas by providing safe spaces for creativity (Blauer, p.156). Blauer advocates that municipalities would benefit significantly if there is an "innovation lab" (Blauer, p.157). Similar in Vancouver, there is an innovation lab called City Studio, where students, city staff and residents come together to address social, economic, and environmental issues (About CityStudio Vancouver, City Studio). City Studio has been collaborating with many municipalities across Canada and bridging students, city staff, and residents on finding a new and creative solution (About CityStudio Vancouver, CityStudio). A few municipal governments in the US, such as Boston have collaborated with universities to provide technological and analytical development training programs for public servants to update their technical and analytical skills (Blauer, p.157).

The first recommendation Blauer suggests is to change the public service work culture that supports innovation in the workplace, to have more proactive senior leadership, and to break communication silos. If a strong communication silo exists within a department or between departments, it is most likely the information being used is not precise or misunderstood. Strong and proactive leadership may help push the innovation agenda in the government to promote better data strategies for public service. By establishing a better public service culture that incorporates these three changes: innovation, proactive leadership, and breaking silo effects would the government be able to become more effective in using data.

DATA MANAGEMENT

Data management is one of the key elements in implementing the smart cities approach in municipalities across Canada. There is a misconception that data governance is only about open data, but open data is one part of the data governance (Blauer, p.157). Moreover, by having concrete and unified data governance in place in municipal government, it would be more productive when municipal departments share data (Blauer, p.157). As a result, the decision made with the cooperation of different municipal departments would be more holistic (Blauer, p.157-8). To maintain strong data governance in municipalities, municipalities would develop data policies that outline the creation, maintenance, and disclosure of data internally and externally (Blauer, p.158). Many cities focus on using data for Open Data but do not have a concrete plan on how to use the data for internal use or decision making (Blauer, p.158). According to Welch, Feeney, and Park research on data sharing within governments, between governments and external institutions it found that coercive, persuasive and technically competent environments increase the likelihood of governments sharing their data (Blauer, p.158). In the research, a coercive climate means regulations, laws, or policies become the tool that push governments to share data (Blauer, p.158). The study defines a persuasive environment as a partnership between departments or external institutions on a

project or program (Blauer, p.158). A technically competent environment means whether the government is open to using cloud-based systems to store their data or using social media to connect with their residents or using open-source technologies (Blauer, p.158).

Many municipalities are unwilling to share their data within their municipal government or external governments because of fear, cost, ownership, and differing priorities (Blauer, p.159). By not sharing data within government and between government it creates a "data management silos" (Blauer, p.159). As a result of the mismanagement of data in government, it creates inefficiency because many junior public servants are the ones inputting information between data systems (Blauer, p.159). This type of work could be resolved by centralizing the data system or technology that transfers their data to other data systems electronically.

According to GovEx research, there are five approaches municipalities can take to improve their data management without spending a tremendous amount of money on IT.

1.) Data inventory

2.) Create a governance committee

3.) Invite the right people by including people outside of IT and making it inclusive

4.) System Inventory

5.) Decision-making Authority (Blauer, p.159-160)

Blauer's second recommendation is to have a better data management plan that promotes data sharing, where the process of data sharing is effective. To achieve better data management, there are five suggestions: to have a data inventory, to create a governance committee, to invite the right people by including people outside of IT and make it inclusive, to have system inventory, and to have structural decision-making authority. To use data effectively and efficiently, a better data management plan is needed as well as modernized performance management.

MODERNIZED PERFORMANCE MANAGEMENT

The third key operational area is modernized performance management. Having a performance management system that monitors performance in real time would help city planners to see how their designs align with the outcomes they want to achieve (Blauer, p.160). It is essential to have a performance management system when implementing the smart cities approach across Canadian communities because municipalities could adjust or keep the smart technology design based on the data it shows in the performance management system. However, performance management as a tool may not be used effectively since some people may have vague or poorly scoped request for data from data producers (Blauer, p.160). Therefore, other government employees need to be more specific in their data requests and need to think about the volume of requests the data team can get. When short-term reports become too focused on "executive attention and resources on strategic priorities" it would result in non-productive work and not used for decision-making because people would not trust the data (Blauer, p.161).

The third recommendation from Blauer is to modernize the performance management plan to reduce reporting fatigue because if the performance management is poorly used it may not be able to achieve its

original objective of having performance management in the first place. By not having effective performance management, the municipal department may not be able to plan or revise the smart city projects they implemented. Also, data has a significant role in the development of performance management, so the data collected must be accurate.

ADVANCED ANALYTICS

The fourth operational area is to use the data in the most effective way by having advanced analytics help municipalities to use the data for decision-making. Municipalities need data science tools such as machine learning, artificial intelligence, and predictive modeling to make a decision. However, using these data science tools are "high-risk high-reward" because the tools optimize service delivery, but there is a high chance of privacy concerns and algorithmic bias (Blauer, p.162).

By using advanced analytics in the smart cities approach in municipalities, there would be algorithmic bias in the data. Before data is processed, the algorithm needs to be examined for biases to prevent biased results that are used for decision-making (Blauer, p.163). Municipal governments who are implementing the smart cities approach must be aware and have a plan for protecting marginalized people from the algorithmic bias (Blauer, p.163). If government data contained biases that disadvantaged marginalized people, the residents may start to distrust the data (Blauer, p.163). Later in the data ethics section, it will provide more information about data biases and how to address them.

Moreover, when it comes to addressing data privacy issues, municipalities should provide proper training for public servants to use the data and understand privacy concerns (Blauer, p.162). On the other hand, residents need to be aware of how the data system works in their municipalities (Blauer, p.162). By having residents knowing how the data system collects, uses, and discloses data, it can hold the municipal government accountable. Blauer is in favour of having municipal governments have an "opt-out" system for the resident who does not want their data to be used (Blauer, p.162).

Blauer's fourth recommendation is to use advanced analytics to assess the data collected. Moreover, to resolve or at least minimize the data bias from data collection and advanced analytics. Since humans were the ones that designed these advanced analytics, it most likely would contain biases when analyzing the data. Blauer acknowledges the privacy concerns when using advanced analytics, so it is vital to be aware of it and mitigate it.

NETWORKS

Lastly, networks from philanthropy organizations and the private sector can help governments implement a data-driven decision-making government (Blauer, p.163). For example, the Civic Analytics Network (CAN) helps municipal governments in the US on data analytics and data management by providing best practice to municipalities (Blauer, p.163). The Data-Smart City Solutions organization has multiple projects, including the Civic Analytics Network (About, Data-Smart City Solutions). Their office is at the Ash Centre for Democratic Governance and Innovation at Harvard Kennedy School (About, Data-Smart City Solutions). The Civic Analytics Network (CAN) provides a shared site for data visualization and analytics for all municipalities which are part of the Civic Analytics Network (About the Civic Analytics Networks, Data-Smart City Solutions). The Civic Analytics Network becomes the centre point for all municipalities to share their data and experience when they are using data and smart technologies to make policy and service decisions (About the Civic Analytics Networks, Data-Smart City Solutions).

The last recommendation from Blauer is for municipalities to have an organized network to share best practices with other municipalities. By having a network where municipalities can collaborate and share information will help their municipalities to improve their data strategies or smart city projects. In the interview section I interviewed with Mr. Entwistle from the City of Kelowna, where he claims that municipalities in British Columbia (BC) share information through a collaborative platform similar to the Civic Analytics Networks.

The connection between "smart governance" and data ethics is crucial to understand because data itself is used to make decisions which affect data ethics. The "smart governance" structure is where the implication of data ethics should be implemented. Blauer discusses advanced analytics that can contain biases where it could harm communities, especially marginalized communities. This is an example of a data ethics issue that needs to be discussed at the beginning of the smart cities approach implementation process. Many of the data ethics considered in the next section, and the interview section will outline correlation between "smart governance" and data ethics.

DATA ETHICS

When there is a discussion about the collection, the usage, and the disclosure of data, data ethics is one of the main components to debate about, mainly when an unethical data scandal occurs. For instance, the Facebook Data Analytics Scandal had triggered a public discussion about data ethics, data breaching, data collection, and the use of data (Anderson, Facebook privacy scandal explained). This has caused people to be more aware of how data is being collected and used and how it affects peoples' privacy. The Internet of Things (IoT) are technological devices such as smartphones and sensors being connected to the internet by collecting, exchanging, and using data (Morgan, A Simple Explanation of 'The Internet of Things'). The use of IoT has increased over the years, from 500 million in 2003 to 8 billion users in 2017 (Hanna and Isaak, 2018, p. 57). There is a prediction that by 2020, there would be 50 billion IoT users (Hanna and Isaak, 2018, p.57). The data mining and data analysis political consulting firm, Cambridge Analytica used a psychological profile app they created to get Facebook users' information and their other Facebook friends to collect their data and to influence how they vote in elections (Anderson, Facebook privacy scandal explained). The users' Facebook data was being used for analysis by Cambridge Analytica without the users' consent (Anderson, Facebook privacy scandal explained). As a result, Facebook responded by limiting the app' ability to access Facebook users' events, restraining apps to look at the member list and group content, and terminating for people to search for other Facebook users by a phone number or email address (Anderson, Facebook privacy scandal explained). When data breach or cyber attacks occur, institutions such as tech companies and governments react by changing their practices to regain users' or citizens' trust again.

Furthermore, up until now, the rules and norms of data economy have mostly been influenced by significant private sector companies such as Google, Amazon, and Uber than by governments (Data Governance in the Digital Age: Special Report, 2018, p.21). However, with the implementation of the EU's GDPR, it has influenced how the data economy is being regulated (Data Governance in the Digital Age: Special Report, 2018, p.21). Data and the algorithms to process the data could have conscious and unconscious biases (Data Governance in the Digital Age: Special Report, 2018, p.21). For instance, the algorithm for image recognition created by Google mislabeled gorillas as "black people" (Data Governance in the Digital Age: Special Report, 2018, p.21). Another example is where a financial AI system gives a lower interest rate to

Asians or whites than to blacks or Latinos (Data Governance in the Digital Age: Special Report, 2018, p.21). Therefore, it is crucial to be aware of conscious and unconscious biases in algorithms because it is very dangerous to have data that disadvantage a group of people based on their ethnicity, gender, socio-economic status, and sexual orientation. When a municipal (or state or federal) government uses algorithms to assess and evaluate the data collected by smart technologies, it needs to be aware of algorithm biases.

Correspondingly, Haggart argues that it is the government's responsibility to make legislation, regulation, investment, and have moral conscious when addressing issues of the data economy (Data Governance in the Digital Age: Special Report, 2018, p.22). The government could implement better regulation on data that protects individuals' privacy rights because the government has a higher incentive than the private sector to act in the interest of the public due to its accountability to its citizens (Data Governance in the Digital Age: Special Report, 2018, p.22). The private sector would put social responsibility as the one of the core values of their companies only if consumers would advocate the companies to do so (Data Governance in the Digital Age: Special Report, 2018, p.22).

Similar to other authors in the Data Governance in the Digital Age: Special Report, Obar and McPhail advocated for a national data strategy. In Obar and McPhail's article, it reminded people to think about the idea of "should we" collect this and use this data before rushing towards creating and using the algorithmic data process (Data Governance in the Digital Age: Special Report, 2018, p.56-7). We are living in a digital economy at the moment where decisions and processes are made quickly that may not fully capture the consequence or harm of those decisions and processes. Obar and McPhail proposed that the municipalities and other stakeholders using data to ask these questions in their work:

1.) Should we collect these data?

2.) What are the benefits and possible harms?

3.) Who does it benefit or harm? (Data Governance in the Digital Age: Special Report, 2018, p.56-7)

According to Virginia Eubanks's research, it found that "across the country, poor and working-class people are targeted by new tools of digital poverty management and face life-threatening consequences as a result. Automated eligibility systems discourage them from claiming public resources that they need to survive and thrive. Complex integrated databases collect their most personal information, with few safeguards for privacy or data security, while offering almost nothing in return. Predictive models and algorithms tag them as a risky investment and problematic parents. Large complexes of social service, law enforcement, and neighborhood surveillance make their every move visible and offer up their behaviour for government, commercial, and public scrutiny" (Data Governance in the Digital Age: Special Report, 2018, p.57).

Likewise, data discrimination and data bias disadvantage vulnerable and marginalized groups such as low-income households, children, the elderly, disabled, Indigenous communities, lesbian, gay, bisexual, transgender, queer, two-spirited (LGBTQ2), ethnic minorities, and other disadvantaged communities (Data Governance in the Digital Age: Special Report, 2018, p.57). Obar and McPhail provide numerous recommendations to prevent big data discrimination by having a national data strategy that consists of:

1.) Addressing Discriminatory Data Sets

2.) Acknowledging the challenge of biased data sets

3.) Addressing Discrimination by Design

4.) Acknowledging the challenge of biased algorithms

5.) Acknowledging the challenge of biased individuals

6.) Addressing the oppression of Indigenous Nations

7.) Respecting the rights of Indigenous Nations

8.) Addressing Consent Failures

9.) Acknowledging the challenge of consent failure (Data Governance in the Digital Age: Special Report, 2018, p.58-61).

To understand data biases, people need to understand that data set and data are not new information, but many current data set systems to contain historical data sets such as health, financial, public safety and so on (Data Governance in the Digital Age: Special Report, 2018, p.58). Those historical data may contain biases that are transferred to the current updated data set systems (Data Governance in the Digital Age: Special Report, 2018, p.58). There is a challenge in addressing biased data sets because it is embedded in historical and new data sets. Obar and McPhail recommend that regulations should make it mandatory for people using data sets to be held accountable for their decision-making process (Data Governance in the Digital Age: Special Report, 2018, p.59). Not only is there bias in data sets, but also biased algorithms. Obar and McPhail understand that it is challenging to develop unbiased algorithms, but when there is a biased algorithm processing data it usually affects poor and marginalized people the most (Data Governance in the Digital Age: Special Report, 2018, p.59). To address the biased algorithms, there should be a national strategy that includes auditing and eliminating bias algorithms in data processing (Data Governance in the Digital Age: Special Report, 2018, p.60). Obar and McPhail supported an "algorithmic accountability bill" that was passed in New York City as an oversight tool for data bias (Data Governance in the Digital Age: Special Report, 2018, p.60).

CONSENT

When using the smart cities approach, such as using smart technology or sensors to collect and use data in a community, there is always a discussion about consent. At the heart of privacy laws in Canada, consent requirement is a mechanism to protect against inappropriate use of citizens' data (Data Governance in the Digital Age: Special Report, 2018, p.61). However, the consent requirement of big data discrimination has two major flaws (Data Governance in the Digital Age: Special Report, 2018, p.61). First, individual consent and privacy agreement such as a terms and conditions online agreement where people do not read the document and/or do not understand the document (Data Governance in the Digital Age: Special Report, 2018, p.61). However, people still click "I agree" because they want to quickly use their services and the online agreements are often take too long to read (Data Governance in the Digital Age: Special Report, 2018, p.61). This type of consent is not sufficient or genuine, but it is merely a check in a box that may only have a minimum privacy protection for the individual. Second, the consent agreement may be vague or legal in its language on keeping and using data collected because entities may not have a clear plan in the

beginning when they are first collecting the data (Data Governance in the Digital Age: Special Report, 2018, p.61). This means the individuals would not have control what their data is being used for and there are limited ways to contest it since individuals agreed to the consent agreement they gave (Data Governance in the Digital Age: Special Report, 2018, p.61). When a community sets up smart technologies across the community to collect data for future policy planning or improve efficiency in the community, the citizens most likely do not receive a consent request from the city or town.

Obar and McPhail's suggestion to improve the current consent model by "strengthening purpose specification requirements for data use and ensuring lawful data use in all consequential data-driven decision-making processes, including eligibility determinations" (Data Governance in the Digital Age: Special Report, 2018, p.61).

Data ethics is one of the key themes discussed in this research and to reduce unethical activities in the realm of data should be a high priority for municipalities when implementing smart city projects. Data ethics is increasingly at the forefront of the smart cities approach discussion, and the idea of consent has been a challenge in these discussions. The nine recommendations to prevent big data discrimination by having a national data strategy listed above by Obar and McPhail would help municipalities to think about collecting, using, and disclosing data in the smart cities approach. The next two subsections of the data ethics checklist and the Toronto Waterfront project will give the reader a more in-depth understanding of data ethics issues, especially in how it hinders our democracy.

DATA (ETHICS) CHECKLIST

FIVE CS FRAMEWORK

In Loukides, Mason, and Patil's journal article, they are advocating for the implementation of ethics in technical education and corporate culture because it would reduce unethical results in collecting, using, and disclosing data (Loukides et al., p.22). Loukides, Mason, and Patil proposed five key frameworks to help data scientists to build data products that consider data ethics (Loukides et al., p.8). The five Cs frameworks are consent, clarity, consistency, control (transparency), and consequences (harm) (Loukides et al., p.8). Firstly, obtaining consent to collect the data and to use the data are essential to building trust (Loukides et al., p.8). Trust is the building block for collecting, using, and disclosing data, and without trust, people would not trust the data product. Secondly, clarity is also an important element to build a data product because the public needs clarity in what they are consenting to (Loukides et al., p.9). Most consent documents are lengthy and difficult to understand (Loukides et al., p.9). Thirdly, consistency is crucial because if the consent message is not consistent, it will break the trust (Loukides et al., p.11). Fourthly, it gives more control of the data to the people whose data is being collected (Loukides et al., p.11). Lastly, data scientists need to understand what are the consequences and the potential risks of the data product they developed (Loukides et al., p.13). The five Cs framework is supposed to ensure that the data products produced should "do no harm" (Loukides et al., p.14).

CHECKLIST

The authors have recommended a few options to increase better data ethics. One of the recommendations is to have a checklist to guide data scientists when developing data products (Loukides et al., p.17). Loukides, Mason, and Patil argue that by having a checklist, it would reduce unethical errors similar to having a checklist for doctors in surgery (Loukides et al., p.17). According to the Fairness, Accountability,

and Transparency in Machine Learning group, they suggest that data scientists should evaluate the social impact of their data product in the designing phase, pre-launch phase, and post-launch phase (Loukides et al., p.17). By having a checklist in these phases, it may decrease unethical behaviours, bias algorithms, and unethical data collection (Loukides et al., p.17).

Ethics in the whole organization

Another recommendation is to construct ethics in the whole organization and not just as an individual responsibility (Loukides et al., p.18). For instance, Toyota and W. Edwards Deming created a management system in the production line where anyone in the organization has the right to pull the Andon cord if one saw a problem (Loukides et al., p.18). When the cord is removed, the production line operators would discuss with senior managers about the issue and restart the production by implementing the solution that was considered (Loukides et al., p.18). This example shows that it is essential to empower everyone in the organization because by having more eyes in the organization, it could increase the efficiency of due diligence in the organization. The author argues that data-driven organizations should allow people to voice their concerns without the fear of retaliation (Loukides et al., p.19).

Moreover, in the hiring process in the organization, it needs to contain an ethical challenge component, so the hiring committee could understand what the candidates think about ethical and security choices (Loukides et al., p.19). The authors also advocate for teams in the organization that reflect different thought processes, experiences, ethnicities, and backgrounds (Loukides et al., p.20). The organization should be transparent about their principles (Loukides et al., p.20). This would result in a better organization to identify and reduce unethical data decision and behaviours.

Regulation

There are many situations in which ethical standards have improved by the enforcement of law and regulations (Loukides et al., p.21). For instance, the Nazi atrocities enforced the development of the Nuremberg Code (Loukides et al., p.21). Another example is the GDPR which has pushed for a uniform data policy in the EU on data (Loukides et al., p.21). Loukides, Mason, and Patil argue that it is impossible for data and privacy-related regulations to keep up with technological development (Loukides et al., p.21). Moreover, the development of policy tends to lack technical experts in data science (Loukides et al., p.21). There are two sides of the argument to have data scientists or not in policy development (Loukides et al., p.21). Sometime data scientists may be too focused on "what technology wants" (Loukides et al., p.21). On the other hand, non-data scientists may not be well informed in the technological field of public policy (Loukides et al., p.21-2). Therefore, there needs to be a balance between a data scientist, public policy experts, and other multidisciplinary experts related to data when developing or revising data and privacy regulations.

The discussion above of the 5C's (consent, clarity, consistency, control, and consequences), the checklist, and regulations are topics to discuss in the data ethics field. Also, the 5C's, the checklist, and regulations are recommendations from Loukides, Mason, and Patil to reduce the unethical data activities in an organization. The discussion of regulation to address privacy concerns and to protect individual privacy was discussed in the privacy law section of the literature review and will be addressed again in the interview section. As the reader can see, the key themes are interconnected. Throughout the research, many experts are advocating for stronger or updated regulations to address privacy, ethics, cybersecurity, and other data-related smart city projects.

TORONTO WATERFRONT PROJECT - DATA ETHICS

BACKGROUND: TORONTO WATERFRONT

The Toronto Waterfront Project (also known as Sidewalk Toronto) is not part of the Smart Cities Challenge, but the Federal government, the Ontario government, and the Toronto municipal governments are collaborating with Sidewalk Labs, an Alphabet company (Google) to make the Toronto Waterfront a data-driven community (Sidewalk Toronto, About). Quayside is where the Toronto Waterfront Project is located, and its goal is to improve the residents' and users' quality of life by making it a data-driven and technological community where it addresses social, economic, and environmental issues (Sidewalk Toronto, About). The Toronto Waterfront Project is considered a "smart city" project and does contain many concerns and challenges such as privacy (Levinson-King, Google's 'secret' smart city on Toronto's waterfront sparks row, BBC). Privacy, security, and the ethics of data are discussed throughout this research, literature review documents, and interviews where it does raise similar questions as those of privacy experts on the Toronto Waterfront Project. The former Ontario privacy commissioner, Ann Cavoukian resigned last year over the concerns of privacy, data collection, and use of data in the Toronto Waterfront Project ('Not good enough': Toronto privacy expert resigns from Sidewalk Labs over data concerns, CBC News). Cavoukian supports the "stripping any given data point of all personally identifiable details right away using well-established techniques, as there is no opportunity for people to consent to the collection of the information" ('Not good enough': Toronto privacy expert resigns from Sidewalk Labs over data concerns, CBC News). Sidewalk Labs proposed that data would not be owned by one entity, but it will be in a 'civic data trust', but Cavoukian states that there is no mandatory requirement for the company to de-identify the data collected, only "encouraged" ('Not good enough': Toronto privacy expert resigns from Sidewalk Labs over data concerns, CBC News). There are many challenges and concerns especially about privacy and data that the Toronto Waterfront Project has not addressed or does not have concrete plans to mitigate the problems (Sidewalk Lab's Waterfront Project Under Fire From Industry Leaders, Toronto Storeys).

URBAN SPACE AND DEMOCRATIC GOVERNANCE

Bianca Wylie, a Centre for International Governance Innovation (CIGI) senior fellow and co-founder of Tech Reset Canada wrote an article that raises concerns about the Toronto Waterfront Project and the challenges of the "smart cities approach" (Wylie, Searching for the Smart City's Democratic Future, Centre for International Governance Innovation). Wylie argues that the core flaw with the smart cities approach is "corporations are seeking to exert influence on urban spaces and democratic governance. And because most governments don't have the policy in place to regulate smart city development – this presents a growing global governance concern" (Wylie, Searching for the Smart City's Democratic Future, CIGI). Wylie states that the idea of "smart cities" is marketing from tech companies that claim that they provide many benefits to the public from better urban living to economic development for the city (Wylie, Searching for the Smart City's Democratic Future, CIGI). Furthermore, Wylie claims that the Toronto Waterfront agreements does not "impose baseline requirements around control of public data and publicly owned digital infrastructure" (Wylie, Searching for the Smart City's Democratic Future, CIGI).

Wylie explains that the procurement process of awarding the contract to build the Toronto Waterfront Project was not transparent at all (Wylie, Searching for the Smart City's Democratic Future, CIGI). In a City of Toronto report, it outlines that six applicants competed for this contract and that only three applicants

made it to the final stage (Wylie, Searching for the Smart City's Democratic Future, CIGI). However, the report did not outline the criteria in how they made their decision to determine who won the contract (Wylie, Searching for the Smart City's Democratic Future, CIGI). In the nine months during the procurement process, the public was not involved, and there was little to no transparency in the request for proposal (RFP) process (Wylie, Searching for the Smart City's Democratic Future, CIGI). Wylie argues that there needs to be public engagement during the procurement process of awarding the contract because the public could raise concerns and questions about the procurement process (Wylie, Searching for the Smart City's Democratic Future, CIGI). Wylie supports an open procurement and contracting process where public consultations and public education are occurring at the same time (Wylie, Searching for the Smart City's Democratic Future, CIGI).

Wylie explains that the public consultation of the Toronto Waterfront project has been concentrated on urban issues from mobility to housing (Wylie, Searching for the Smart City's Democratic Future, CIGI). It does not focus on the idea that "a smart city is a political issue and not a technology issue" (Wylie, Searching for the Smart City's Democratic Future, CIGI). This could defer the concentration of the social and democratic framework of the Toronto Waterfront project (Wylie, Searching for the Smart City's Democratic Future, CIGI). Wylie raises the idea that people are not focused on the idea that a big technology company is involved in the Toronto Waterfront Project and it is not just a government project to "improve quality of life" for its citizens (Wylie, Searching for the Smart City's Democratic Future, CIGI). It is important to have public awareness of these privacy, data, and democratic issues with the Toronto Waterfront project (Wylie, Searching for the Smart City's Democratic Future, CIGI). Wylie argues that it is possible to build a democratic and just smart city by addressing these challenges and concerns from privacy to surveillance (Wylie, Searching for the Smart City's Democratic Future, CIGI). Wylie provides some recommendations in the next section to address these challenges and concerns.

WYLIE'S RECOMMENDATIONS

The five recommendations Wylie suggests:

1.) To ensure an open procurement and contracting process
2.) To develop an intensive public education and consultation
3.) To have civic data governance as a government responsibility
4.) To have smart cities as a political issue, not a technology issue
5.) To implement an agile policy-making process (Wylie, Searching for the Smart City's Democratic Future, CIGI).

In the following sections of this research, there will be discussions and analysis of other experts on data ethics of Wylie's perspective of the smart cities approach. The Toronto Waterfront Project shows the many challenges in privacy, ethics, and democracy in the smart cities approach.

In the Canadian context of an ongoing smart city project is the Toronto Waterfront Project where it has been getting much publicity in its privacy, ethics, and democratic concerns with the way data are collected, used, and disclosed. Wylie wants the government and all involved stakeholders to understand the potential harm that smart city projects can have in a community. The five recommendations that Wylie suggests could help municipalities to implement a just and democratic smart city. The privacy, ethics, and democratic

process of a smart city project are discussed in the interview section under data ethics, especially with Millar.

3.4 Data Sovereignty

To have strong data sovereignty is a crucial element to address data privacy in the smart cities approach. The municipalities who implement the smart cities approach will use smart technologies to be connected to the internet to collect, use, and disclose the data called the Internet of Things (IoT) (Adler, 2015, The Urban Internet of Things). The Internet of Things (IoT) is "the use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical objects" (Understanding the Internet of Things, p.1). The smart cities approach consists of using IoT as a tool to collect data, and the data is connected to the internet. Therefore, the internet infrastructure, especially how the data flows on the internet is an important security measure.

Andrew Clement, an expert in the social significance of information infrastructure and information society, explained that Canada's internet infrastructure relies on the American's internet infrastructure because many communication and data flows in Canada would mostly pass into the US network system (Data Governance in the Digital Age: Special Report, 2018, p.26). When Canadians' data and the information crosses the US border, the data and information would not be protected under the Canadian legal system, but would be subject to the American legal system (Data Governance in the Digital Age: Special Report, 2018, p.28). Those data going through the US would be subject to NSA surveillance (Data Governance in the Digital Age: Special Report, 2018, p.28). Clement argues that "the current heavy reliance of Canadian internet routing on US digital infrastructure, for both domestic and international communications, put personal and corporate data at risk while impairing the efficiency and quality of Canadian internet services" (Data Governance in the Digital Age: Special Report, 2018, p.29). Moreover, the substantial reliance of the US in the realm of digital infrastructure deteriorates Canada's digital sovereignty and bilateral bargaining powers (Data Governance in the Digital Age: Special Report, 2018, p.29).

Moreover, trade policy has to affect data sovereignty because some trade agreements have rules to require that data must be kept in the country or data collecting in one country must be able to transfer to another country (Data Governance in the Digital Age: Special Report, 2018, p.10). For instance, the Trans-Pacific Partnership agreement "prohibits data localization requirements unless they fall within a limited exception" (Data Governance in the Digital Age: Special Report, 2018, p.10). By prohibiting data localization in trade agreements, it gives the private sector and other governments the authority to access valuable data. When the municipality uses smart technologies to collect, use, and disclose technology, it needs to be aware of how the data is flowing.

Clement advocates for "data localization," which mean Canadian data should be kept in within Canada (Data Governance in the Digital Age: Special Report, 2018, p.31). "The Federal government and two provinces have taken modest steps in this direction by demanding personal data collected by public bodies be stored within Canada, but there is not yet a similar requirement with internet routing" (Data Governance in the Digital Age: Special Report, 2018, p.31). Clement provides nine recommendations:

1.) "develop and promote the use of public IXPs in Canada;

2.) build up and open access to Canada's long-haul internet backbone, especially for interconnecting IXPs;
3.) require public bodies to peer openly at local IXPs where feasible;
4.) promote open peering at IXPs in procurement and other policies;
5.) require greater transparency and accountability of Canadian internet carriers in relation to their internetworking practices;
6.) enforce greater transparency and equivalent protection in data exchange under the Personal Information Protection and Electronic Documents Act, as they apply to internet carriers operating in Canada;
7.) evaluate the privacy risks for Canadians' data when exposed to US jurisdiction in light of NSA mass surveillance;
8.) require greater transparency and accountability on the part of Canadian security and intelligence; and
9.) reconsider Canada's role in the Five Eyes security alliance in light of the Snowden revelations and the policies of the current US administration" (Data Governance in the Digital Age: Special Report, 2018, p.33).

When data is flowing through the internet, data sovereignty would be part of the discussion on the implications of data collection and use of data. Data flowing or stored outside the Canadian border is concerning because it hinders our privacy, sovereignty, and democratic institutions, especially if a foreign country is intercepting the data for surveillance purposes.

3.5 Cybersecurity

CYBERSECURITY LIFE CYCLE

To protect the smart cities' data and privacy from cyber attacks, the development of the cybersecurity plan is crucial. Communities across the world have started to implement an advanced information and communication technology (ICT)-based solution to deliver better services for residents (Barik, Sengupta, and Mazumdar, p.392). This type of solution is what the smart cities approach is about. However, the security of resources and privacy of residents' data are core issues in the smart cities approach that needs to be addressed (Barik et al., p.392). In some smart cities approaches, their digital infrastructure is interconnected, which means when one system gets an attack, it may hinder the other system because both systems are connected in the same digital infrastructure (Barik et al., p.392). It is important to develop a risk assessment for the smart cities approach and evaluate the security risks because it could assist to prevent, detect, and recover from cyber-attacks (Barik et al., p.392). Since the development of cybersecurity is not a one-time event, it needs constant improvement because while new infrastructures would be built, there would be new threats, and new vulnerabilities may occur (Barik et al., p.392). Therefore, Barik, Sengupta, and Mazumdar recommend a life-cycle approach to cope with the cybersecurity in the smart cities approach (Barik et al., p.392). The cybersecurity life-cycle approach includes:

1.) "The establishment of scope and boundaries of the proposed security implementation.
2.) The identification of security requirements, keeping in mind applicable laws and regulations and specific concerns and expectations of various stakeholders.
3.) Risk assessment is performed to identify and comprehend the risks that can potentially breach the cyber security of the smart city.
4.) The identified risks are then prioritized, and a detailed risk mitigation strategy is designed.

5.) This would comprise of identification of security controls and measures that can reduce the risks to an acceptable level.
6.) It includes the formulation of cyber security policies and procedures and a selection of appropriate software and hardware security tools.
7.) The measures are then implemented, configured, and adopted to mitigate the identified risks
8.) After implementation of security measures, continuous monitoring is undertaken to check whether the implemented controls are able to satisfy the identified security requirements.
9.) Such monitoring is usually based on log records and generates several metrics that help to understand the security posture of the smart city.
10.) Depending on the monitoring results, corrective actions, if required, are planned and implemented to address specific concerns." (p.392-3)

A cybersecurity plan tries to balance between system efficiency, security expense, and data protection (Barik et al., p.398). The smart cities data system needs to be efficient, but it also needs to protect the data, and to protect the data, there is a certain amount of security expense it would be able to spend. The cybersecurity plan is not a one-time event, but it requires constant improvement in the cybersecurity system because it tends to have new vulnerabilities in the system, sprouting new threats, changes in laws and regulations and other evolving elements that influence the cybersecurity to be updated (Barik et al., p.398). There are eight stages to the cybersecurity life cycle in the smart cities approach:

1.) Scope and Cyber security policy formulation
2.) Cyber security requirements identification
3.) Risk management
4.) Detailed security policy formulation
5.) Security measures implementation
6.) Cyber Security incident management
    Service continuity management and disaster recovery
7.) Cyber Security metrics generation
8.) Audit and compliance checking (Barik et al, p.399)

SCOPE AND CYBER SECURITY POLICY FORMULATION:

The first stage of the cyber security life cycle is to analyze and scope what is the cyber security's objective, the intended outcomes, and the risk control (Barik et al., p.398).

CYBER SECURITY REQUIREMENTS IDENTIFICATION:

In the second stage, the municipality should identify the critical assets, which are primary assets and supporting assets (Barik et al., p.400). The primary assets include smart services and information assets (Barik et al., p.400). The supporting assets include hardware, software, network, personnel, site, and city's structure (Barik et al., p.400). Smart Services means the service the municipality provides by using smart technology to collect, use, and disclose data to deliver smart services for residents such as smart transportation (Barik et al., p.393).

Risk Management:

In the third stage, the risk assessment would be calculated based on analyzing the service value, vulnerabilities in the system, and the likelihood of those vulnerabilities being exploited (Barik et al., p.400). In this context, service value means that the security requirements would calculate the risk of maintaining the weaknesses of smart services (Barik et al., p.400). Vulnerabilities in a system could be technical, but also managerial (Barik et al., p.400). Technical vulnerabilities are present when software and hardware in a system have weaknesses (Barik et al., p.400). Managerial vulnerabilities are limited policies and procedures in managing the system (Barik et al., p.400). The municipality who is implementing the smart cities approach would need to build a set of risk acceptance criteria (Barik et al., p.401). This means what are the risks the municipality could accept and what are the high risks that must be addressed (Barik et al., p.401). Many risks can be solved by the implementation of controls, which would entail the use of resources such as infrastructure, time, money, knowledge, and administrative resources (Barik et al., p.401).

Detailed Security Policy Formulation:

In the fourth stage, the municipality would develop security manuals, cybersecurity policies, cybersecurity guidelines, cybersecurity procedures, and templates for the enactment of the cybersecurity plan (Barik et al., p.401). There need to be records of all activities related to cybersecurity because the records could be used to trace if a data breach occurs, for audit purposes, and compliance checks (Barik et al., p.399, p.401).

Security Measures Implementation:

In the fifth stage, the municipality should allocate tasks to each employee who would be responsible for a specific activity in the cybersecurity plan (Barik et al., p.401). The municipality needs to provide security awareness and an education program on cybersecurity issues for residents (Barik et al., p.401). Periodically, the municipality must notify its residents of the latest security issues and the mitigation plan should a security breach occur (Barik et al., p.401). Since technology develops at a fast pace.

Cyber Security Incident Management:

In the sixth stage, there are two components: the cybersecurity incident management and the service continuity management and disaster recovery (Barik et al., p.401-2). The municipality must develop cybersecurity incident management as having a smart cities approach cybersecurity plan would not eliminate vulnerabilities (Barik et al., p.401). For cybersecurity incident management, there must be a controlled and organized approach. For instance, the municipality should have a system to detect, report, and assess cybersecurity incidents when implementing the smart cities approach in their community (Barik et al., p.402). In the cybersecurity incident management plan, it would be beneficial to have controls for prevention, reduction, and restoration from the cyber-attack (Barik et al., p.402). For each cyber-attack, the municipality could use the experience as a lesson learned and develop preventative measures to address that specific cyber-attack in the future (Barik et al., p.402).

Service Continuity Management and Disaster Recovery:

The municipality must develop a service continuity management, and disaster recovery; in the event of a disruption to the data system from cyber attacks or disasters there should be a plan for the continuity and restoration of smart services (Barik et al., p.402). Also, there needs to be a continuity of management of smart services by performing impact analysis and risk assessments (Barik et al., p.402).

CYBER SECURITY METRICS GENERATION:

In the seventh stage, it is essential for the municipality to analyze the performance of the cybersecurity by developing a cybersecurity metrics to assess the current cybersecurity reality in the community (Barik et al., p.403). By having cybersecurity metrics, it would help the municipality to plan to update or provide other further investments (Barik et al., p.403).

AUDIT AND COMPLIANCE CHECKING:

The last stage of the cybersecurity life cycle in the smart cities approach is to perform an audit and compliance check on the cybersecurity (Barik et al., p.403). The findings and outcome of the audit and compliance check should be used for the continuing improvements to the cybersecurity plan (Barik et al., p.403). By having the audit and compliance checks in place, it would ensure safety, accountability, and transparency to the residents, businesses, and government and that data and other municipal services are well managed (Barik et al., p.403). The cyber security life cycle does not just stop in the audit and compliance checking; it goes back to the first stage again (Barik et al., p.399). The cyber security life cycle continues incrementally and never stops as long as the municipal data system is running.

The framework for this research will focus on existing research on privacy law, data security, privacy concerns, and data ethics. Moreover, it will consist of case studies and interviews that would aid in understanding the implications of data collection and the use of data in the smart cities approach and how it affects the citizens, businesses, and society. The research would consist of the SWOT (strength, weakness, opportunity, and threat) analysis to analyze the information from the interview and the literature materials. As Canada begins to implement the smart cities approach, it would be helpful to understand how data affects the operation of the municipality and how to develop mitigation measures to lower the risk of a massive security breach privacy concerns. The benefits of using data to manage the communities outweigh the disadvantages. However, it does not mean that the issues with using data in communities are not insignificant. It implies that the municipality needs active mitigation and control measures during the implementation process of the smart cities approach.

3.6 Summary of the Literature Review Findings

As Canada prepares to implement the smart cities approach in some municipalities, provincial and territorial privacy guardians have voiced their concerns about privacy implications when implementing smart city projects. There is room to improve the Canadian privacy and data regulations such as PIPEDA to keep up with the technological development use in the smart cities approach. The EU's GDPR would be a case study for Canada to learn to improve its data and privacy regulations. To enhance data and privacy regulation, knowing the types of data privacy would assist in identifying the problem and creating mitigation to address every kind of data privacy.

There are several privacy and security challenges with the implementation of the smart cities approach in Canadian communities. The dispute between the municipal government, citizens, and private companies on who owns the data creates many difficulties as all the stakeholders want to own all or partially own the data for future use. The municipal government intends to own the data to protect individual privacy from companies misusing their data without the consent from the community. The citizens want to own the data, so the government and the private companies would not misuse the data by sharing the data with other third

parties without the consent from the citizens. The private companies want to own the data to use the data for other projects in which they are invested.

Moreover, private companies may use legal tactics and in the user's agreement to own the data. Therefore, before municipal governments sign contracts with vendors to implement their smart city project, they need to discuss data ownership; if it is not considered properly, it may cause complexity and privacy violations.

It is not just data ownership that can cause complexity with the implementation of the smart cities approach, but also data sovereignty. When the Internet of Things (IoT) are used in the communities to collect data, it is linked to the internet where data is flowing through Internet Exchange Point (IXP) where large quantities of Canadian data are leaving Canada to the US. Once the data to the Canadian IXP travels to another foreign IXP, the foreign country's intelligence agency could access the data. With many smart city projects collecting vast amounts of data about the community, it could provide a foreign country power from surveillance on our residents to leverage on establishing trade agreements. Municipal governments not only need to worry about data flowing out of the country but also about data that is stored outside the country. Once the data leaves Canada, it is not in the jurisdiction of the Canadian government, but it is under the jurisdiction of the country to which the data flows or is stored. The nine recommendations from Clement would help address data sovereignty concerns.

With IoT applied across the communities collecting data and having the data process with machine learning or AI in the data system, it attracts hackers to break into the system to steal valuable data. This can cause significant harm and privacy concerns to the community. Therefore, cybersecurity concern is also a top priority for the municipality to develop a mitigation strategy to protect the data system from being hacked. Having a cybersecurity life cycle plan would facilitate a structure to balance between security, efficiency, and resources. The cybersecurity life cycle plan is not a one-time affair, but a constant adjustment of the cybersecurity life cycle plan. For instance, it is modifying the security scope or risk management based on the new technological developments that triggers new vulnerabilities to the data system. Security and privacy are not the only challenges with data collection, but also how to use the data for correct decision-making.

With the implementation of the smart cities approach, governments need to become "smarter." There has been a marketing influence on the idea of "smart governance" for smart cities. "Smart governance" in this context means a government uses data and technologies to make decisions while having efficient governmental administration operation. Blauer's article identified five essential governmental administration areas to improve. First, to have a cultural transformation in how the public service operates. A multidisciplinary approach with proactive leadership from senior executives will help reduce communication silos within and between departments. Also, by providing safe spaces for public servants, it could generate innovation and creativity needed in the design and implementation of the smart cities approach. Second, to have an efficient data management plan because it would make it more efficient to organize, use, and share the data collected. Having a weak data management system for data sharing can create inefficiency in the administration because junior public servants would waste their time inputting information from another department's data system into their data system. If the data are shared efficiently without manually re-inputting the data, it could save time and taxpayers' money. Blauer argues it is also essential to have a concrete plan on how to use the data collected for internal use such as decision making, and designing public policies and programs. Third, to have modernized performance management where

the request for using the data collected would be concise and specific to reduce reporting fatigue for public servants who are working on the performance management team. Fourth, to have advanced analytics such as machine learning, AI, and predictive modeling to assist civil servants to analyze the data so that the information could be effectively used for decision making. However, using advanced analytics, it is "high-risk high-reward" because since there are huge privacy and security concerns and data biases. Fifth, to have networks to collaborate with the municipalities to share best practices. In the Finding section, it will consist of two case studies: Estonia and Somerville on "smart governance," and it will aid Canadian municipalities to improve their governance and administration processes.

Security and privacy play a major role in the smart cities approach, so considering data ethics in the design and implementation process of smart city projects is constructive. By remembering these three questions when designing and implementing smart city projects, the team would pay more attention to the ethics of the project:

1.) Should we collect these data?

2.) What are the benefits and possible harm?

3.) Who does it benefit? (Data Governance in the Digital Age: Special Report, 2018, p.56-7)

By asking these questions, the team would reconsider their smart city projects to see if it is ethical to collect these data and to see who benefits from it. Also, the team would consider the possible benefits from collecting the data and the potential harm or disadvantage from collecting the data.

In the literature review section, the reader gains knowledge on the key themes: privacy law, types of privacy, data ownership, smart governance, data ethics, data sovereignty, and cybersecurity from government documents to reports. However, there are still unknown questions about these issues. The two case studies, Estonia and Somerville, and the interview with the seven experts could answer some of these questions. Example of some unanswered questions are:

1.) How do you protect your data?
2.) Is a checklist a feasible solution to addressing data ethics?
3.) How does privacy laws and regulations work for data-related smart city projects in Canada?

Research on the implication of smart cities are very active, and the discussion about privacy in smart cities is becoming more discussed in society. The interviews with experts give the reader a better insight of the issue compared to the literature review documents because the recommendations from the experts take considerations of the Canadian context of the implementation of the smart cities approach in Canadian municipalities. Moreover, the two case studies focus on the issue of "smart governance," and they show how "smart governance is applied in reality.

4.0 Case Studies

4.1 Introduction

The finding section will consist of two case studies, Estonia and Somerville. The Estonia and Somerville case studies provide actual best practices on the "smart governance" needed in the implementation of smart city projects. Estonia is one of the leading countries on digital government, where the majority of the services for citizens are online instead of paper-based (e-Governance, e-Estonia). Somerville uses technologies to improve their administrative process and public engagement to deliver better smart city projects and government services to the public. The result of the four interviews will be presented and analyzed in the findings. There are five categories in the interview component: Privacy law, data infrastructure, data ethics, cybersecurity, and municipal resources. The case studies, interviews, and the works of literature that follow, will help shape the recommendations in this research.

4.2 Estonia – Smart governance and Data

It is central to learn from Estonia's experience in becoming a leader in the digital government because to implement the smart cities approach; the municipal governments need to update their governance structure into smart governance that incorporates digital technology and data-driven decision making. Having smart governance is one of the key elements of the smart cities approach. By doing so, within two decades, Estonia has become a leader in digital government (Success Stories, e-Estonia). For Estonia, their government service delivery for residents is 99 percent online, which means the Estonian government can reduce time to process documents and save residents' time (e-Governance, e-Estonia). This also means saving taxpayers' money by reducing bureaucratic expense. One of the online services that the Estonian government provides is e-tax, which is where Estonians can file their taxes in three to five minutes online (e-tax, e-Estonia). By providing easy instructions and a user-friendly online tax system, residents can easily submit their taxes online each year and the government can receive approximately 95 percent of all tax declarations (e-tax, e-Estonia). By having an efficient, online system, it makes it easier for businesses to invest in the country. It only takes a company a few hours to register online in Estonia compared to a few days elsewhere (Business and Finance, e-Estonia).

Moreover, the Estonian government has a State e-Services Portal (eesti.ee), which is a website that links to hundreds of online services provided by numerous government departments (e-governance, e-Estonia). Therefore, each year, Estonia saves around 800 years of working hours (e-governance, e-Estonia). One of the elements of the smart cities approach is to provide efficient services to citizens. By having a centralized online service system for citizens to receive government services, it makes it easier and more efficient for both the citizens and the government. Moreover, the data would be centralized for the public servants to access for policy and program planning. However, by concentrating data, it means if the system gets hacked, all the data would be available to the hackers.

For the e-governance system in Estonia, they also provide a government cloud system, i-voting (online voting), and e-cabinet (e-governance, e-Estonia). All government data in Estonia is stored in a government cloud system that helps to break IT infrastructure silos because the government cloud system forces departments to share the data and resources (e-governance, e-Estonia). The Estonian cloud system meets the national IT Security Standard (ISKE), which means data is stored safely and handled with discretion (e-

governance, e-Estonia). For the government cloud system, the Estonian government collaborates with technology companies such as Cybernetica, Dell EMC, Ericsson, OpenNode, and Telia (e-governance, e-Estonia). Each technology company provides a specific component in the operation of the government cloud system (e-governance, e-Estonia).

E-GOVERNANCE

In 2005, Estonia was the first country to implement online voting by using ID-cards (e-governance, e-Estonia). The e-Cabinet is a multi-user database that gives real-time information (e-governance, e-Estonia). Before each e-Cabinet meeting, the ministers review the information and check a box to show if they agreed or disagreed with a decision (e-governance, e-Estonia). A decision without differ would move forward without discussion in the meeting, and those decisions with objections would be discussed in the conference (e-governance, e-Estonia). As a result, an average cabinet meeting in Estonia is around 30 to 90 minutes, compared to before e-Cabinet where it had taken four to five hours (e-governance, e-Estonia). The e-Cabinet meeting is an excellent example of how smart governance should be used because technology becomes a tool to implement a more efficient way in the governance process. Without technology, it would be challenging to achieve this kind of format. To implement smart governance in the smart cities approach, it would be effective to implement the e-Cabinet technology in committee meetings in municipal departments. The municipal departments' committees would use data collected from smart technology to develop a decision, and the decision process would use e-cabinet technology. This would speed up the decision-making process as well as keeping the decision-making process centralized. As municipalities implement the smart cities approach, they would also need to implement smart governance to match the speed and efficiency.

BLOCKCHAIN, SECURITY, AND SAFETY IN ESTONIA

Estonia knows that by having a digital government, it would be prone to cyber-attacks (Security and Safety, e-Estonia). In 2007, Estonia experienced many cyber-attacks on its government system (Security and Safety, e-Estonia). The 2007 cyber-attacks triggered the Estonian government to use Blockchain technology to protect government data and the government system (Security and Safety, e-Estonia). Currently, Estonia is the leading country with excellent cyber security experts (Security and Safety, e-Estonia). The Estonian government uses Blockchain technology in its data system to protect the data from being changed or manipulated by anyone (Security and Safety, e-Estonia).

Blockchain is a decentralized technology where there is no one central place to store the information, but multiple users that are holding a copy of the information (Rosic, What is Blockchain Technology? A Step-by-Step Guide for Beginners). The Blockchain technology used in the Estonian government is "digital defense dust," where it protects all data and smart devices from being exploited (Estonian Blockchain Technology, p.1). When the data is changed, the Blockchain technology can detect it (Estonian Blockchain Technology, p.1). The Estonian government does not store data in the Blockchain, but it works similar to a speed camera that detects driving violations (Estonian Blockchain Technology, p.1). Moreover, the use of Blockchain technology does not prevent cybercrime itself, but the government can detect the cyber breach 100 percent of the time (Estonian Blockchain Technology, p.2). Using the Blockchain protects data by having the original data as digital fingerprints (also known as "hash values"), so even obtaining the digital fingerprints it would still be challenging to know what the data is about (Estonian Blockchain Technology, p.2). According to FireEye, a leading cybersecurity vendor, research found that without Blockchain

technology it would take an average of seven months to detect a data breach, compared to an immediate detection of data breaching with using the Blockchain (Estonian Blockchain Technology, p.3).

Estonia understands that cyber threats and data breaches are part of the challenges of implementing the smart cities approach in becoming a digital society. However, Estonia believes in the continuous experimentation and lessons learned to address problems such as cyber threats, and data breaches (We have Built a Digital Society and So Can You, e-Estonia). Estonia has increased its cybersecurity plan these past few years by including "intrusion detection and protection systems, practiced cooperation with both public and private institutions, significantly contributed to the awareness of users, and is participating in an intensive international cooperation" (We have Built a Digital Society and So Can You, e-Estonia).

DATA EMBASSY

Estonia has created a data embassy outside its borders, but the data is still under Estonian government control (We have Built a Digital Society and So Can You, e-Estonia). Estonia opened its data embassy in Luxembourg (Estonia to open the World's first Data Embassy in Luxembourg, invest in Estonia). The advantage of storing a backup data outside Estonia's borders is that in case of data centres in Estonia ceasing to work, or if there is a disruption from a natural disaster, massive cyber attack, or other alarming catastrophes (We have Built a Digital Society and So Can You, e-Estonia). Moreover, the physical data embassy in Luxembourg is still under Estonia's sovereign which means data store in these embassies will always be under Estonia's control and ownership (Estonia to open the World's first Data Embassy in Luxembourg, invest in Estonia). This means that the data stored in the embassy outside Estonia's border will not be controlled by a foreign country. The data embassy pilot project in Luxembourg started in 2018, and the experience of the pilot project will be an example for other countries who want to store their data outside their borders (Estonia to open the World's first Data Embassy in Luxembourg, invest in Estonia). Storing data outside their borders would help if there is a huge cyber attack or natural disaster that caused the data to be lost, but could be recovered from the backup data stored outside the borders.

ESTONIA'S DIGITAL AGENDA 2020

The digital transformation of urban services and infrastructure in Estonia improve the livelihood of citizens. In the implementation of the Estonian Information Society Strategy 2013, they were able to increase basic Information and Communication Technology (ICT) skills (Digital Agenda 2020 for Estonia, p. 6). For example, the private sector organized a digital literacy program called "Come Along!" for the public sector (Digital Agenda 2020 for Estonia, p. 6). Moreover, the development of e-governance in Estonia benefits both the citizens, the public sector, and private sector (Digital Agenda 2020 for Estonia, p. 7). For instance, anyone can create register a company in less than 20 minutes within their own home (Digital Agenda 2020 for Estonia, p. 7). One of the surveys in 2012, found that 76 percent of businesses and 67 percent of individuals are satisfied with the government e-services system (Digital Agenda 2020 for Estonia, p. 7). Therefore, the majority of businesses and citizens approve and are content with the e-service in Estonia. By having smart technology to create smart governance, it provides many benefits to everyone, and taxpayers' money is well spent. The smart cities approach should not just think about the benefits of the citizens, but also other institutions such as the private sector and non-profit sector.

Even though there is an improvement in digital literacy in Estonia, but there is still a lot of work that can be done to improve digital literacy for the public. One of the challenges is to improve people's skill in protecting their data (Digital Agenda 2020 for Estonia, p. 10). Moreover, the public sector still has not

optimized the use of ICT due to some e-services are poorly implemented because the department did not customize the technology for its intended purpose (Digital Agenda 2020 for Estonia, p. 10). Another government administration issue in smart governance is to integrate the government across jurisdictions and departments (Digital Agenda 2020 for Estonia, p. 10). Most of the time, the best solution to address this issue is to centralize administration functions and consolidate the ICT solution (Digital Agenda 2020 for Estonia, p. 10). The benefit of centralized administration function is that the operation is consistent and data are easy to transfer from one department to another. Nonetheless, a complex customize IT solution may "increase the vulnerability of ICT systems and increase their security risks; raise, in the long term, operation costs; and reduce the flexibility of ICT-solution" (Digital Agenda 2020 for Estonia, p. 10).

In 1993, Estonia created a Principles of Information Policy which outlines what Estonia's digital society should be (Digital Agenda 2020 for Estonia, p.18). There are two sections in the Principle of Information Policy that highlight security:

1.) "The development of information society will not undermine the users' sense of security. The mitigation of non-acceptable risks in information and communication systems will be guaranteed and security requirements will be taken into account when designing the systems and throughout their life cycle.

2.) The protection of fundamental freedoms and rights, personal data and identity will be ensured. Individuals are the owners of their personal data and will have an opportunity to control how their personal data are used."

The Principle of Information, specifically the security components, are crucial to have when implementing the smart cities approach because having a policy that protects individual privacy rights may help reduce unethical data activities.

When looking at personal data law, Estonia is leading the way with data collection and the use of data (Herlihy, 2013, Government Digital Service). Canada can learn from Estonia's Personal Data Protection Act when implementing the smart cities approach because Estonia gives its citizens more control of their data (Herlihy, 2013, Government Digital Service). Estonia has built themselves as a leader in digital society by providing municipal and state services delivery 99% online through one state portal system (We have built a digital society and so can you, E-Estonia). Estonia has been using Blockchain since 2008 to decrease cyberattacks because in 2007, Estonia had a cyber attack that shut down all the government websites, but the data was not lost (We have built a digital society and so can you, E-Estonia). Estonia acknowledges that creating a digital society requires effective cybersecurity to protect it from cyber-attacks (We have built a digital society, and so can you, E-Estonia). Estonia recognizes the importance of continuous experimentation and learning from their mistakes because it helps to grow a reliable and feasible data-driven government (We have built a digital society, and so can you, E-Estonia). Estonia's experience in data collection, the use of data, privacy protection, and cybersecurity would help Canada address data, and privacy issues in the implementation of the smart cities approach across the country.

4.3 Somerville: Smart Governance

SMART GOVERNANCE

In Okner and Preston's journal article, they argue that to build smart governance, the municipality must include citizen engagement as its top priority along with smart technologies (Okner & Preston, p. 346). The

authors have raised that the public sector has been lagging behind the private sector in incorporating digital technologies (Okner & Preston, p.347). During the planning phase of the smart governance, the municipal government could use information and communication technologies to provide communication outlet for residents where the municipality could see the discussion in real-time (Okner & Preston, p.348). By focusing on citizen engagement with the use of information and communication technologies, citizens can be empowered to raise an innovative solution that could help improve their neighbourhood (Okner & Preston, p.348).

THE CASE STUDY: SOMERVILLE

The author looked at Somerville as a case study for a municipality that had limited resources, but used smart technology in the community and build smart governance in their municipality (Okner & Preston, p.350). Somerville has a data-driven performance management system called SomerSTAT, where it uses financial, personnel, and operational data to assist decision making in the municipality (Okner & Preston, p.351). For instance, when managers and other leaders from different municipal departments hold a meeting, they use SomerSTAT data to see where the opportunities for amelioration are (Okner & Preston, p.351). When a decision or a plan is made, they record and track the development (Okner & Preston, p.351). The SomerSTAT team in Somerville integrates with all municipal departments (Okner & Preston, p.351). This would break down some communication silos between municipal departments.

Another municipal digital program is the ResiSTAT, which is a data-driven decision-making program that uses SomerSTAT's data to present the data in community meetings (Okner & Preston, p.351). Moreover, the City of Somerville has an online community platform to promote active engagement with the residents so that the residents can voice their opinion of municipal policies (Okner & Preston, p.351). It is not just technology that makes smart governance, but also how to organize and structure the municipal departments. The Somerville by Design (SBD) team is an excellent example of how municipal departments could have one team that focuses on the integration of different departments in a municipal government. The SBD team is an urban planning team in the Somerville government that redesigned the municipal departments' structure when it comes to engagement between departments (Okner & Preston, p.352). This means breaking down silos by creating different teams to work together to tackle multidisciplinary issues for each neighbourhood in Somerville (Okner & Preston, p.352). Since each neighbourhood may have different problems from other neighbourhoods, it would be useful to have one team in each department to collaborate with other teams from different departments who are also focusing on the same neighbourhood (Okner & Preston, p.352).

Nevertheless, technology still has played a massive role in smart governance. The Somerville by Design (SBD) team uses Dropbox, a cloud-based file sharing service where other teams in municipal departments or anyone who needs access to the file could use Dropbox to get access to that information (Okner & Preston, p.362). Dropbox is a platform to store and share information, but also a collaborative space for users' discussions (Dropbox business, Work Better, Safer, Together). This breaks down the communication silos between departments (Okner & Preston, p.352). To have smart governance, the municipality would need to continuously improve their process and be able to adapt quickly (Okner & Preston, p.354).

Somerville also collaborates with the private sector in making their community smarter. Somerville works with Gehl Architects, an urban research and design firm where they collect data in the community and recommend ways to improve the community by focusing on people and how they interact with public space

(Okner & Preston, p.364). By collaborating with the private sector, Somerville ensures that all data is owned by the municipality and not the private sector (Okner & Preston, p.365). This shows that Somerville understands that the municipality has a responsibility for securing the safety and privacy of the data collected, used, and disclosed since one of the main elements of Somerville's smart governance is a community-led planning approach where it gives residents a platform for public dialogue to voice their ideas and concerns (Okner & Preston, p.365).

Somerville provides a good case study for other municipalities who want to implement the smart cities approach. There are ten components to Somerville's smart governance and smart cities approach:

1. A need for a continuous process of urban planning in the community
2. To respect and protect authenticity in placemaking
3. To understand the multifaceted web of people's life and action in the community
4. To have quantitative analysis in all municipal departments
5. To have residents' engagement in the planning processes
6. Use low-cost technology to increase public engagement by reaching diverse neighbourhoods
7. To have multidisciplinary teams in municipal departments
8. To engage with neighbourhoods to get local insight since one size fits all approach are not effective
9. To aim high and set goals
10. To be holistic, resilient, and sustainability (Okner & Preston, p.365).

4.4 Summary of the two Case Studies

The two case studies: Estonia and Somerville, focus on how to improve the government administration and governance to become "smarter" by using technologies to improve service delivery for their residents. Both Estonia and Somerville show that technologies and the way the government structures their administration operation could steer the government to become more efficient and effective. For Estonia, they centralized their online service system where residents can receive government service online where it can save both residents and the government time and money. Moreover, the ID cards for residents to use are linked to the centralized online service system. Also, the way Estonia structures their cabinet meeting with multi-user database technology for members to review meeting agenda with recommendations in real-time information and having a checkbox for a member to click agree or disagree with the advice given. The Estonian cabinet meeting structure and the technology used could be implemented in municipal departments' committee meetings when implementing smart city projects. The Estonian cabinet meeting example could be an excellent case study for Canadian municipalities to implement as part of becoming a "smarter" government. Compared to the Somerville case study, where Somerville focus on using technologies to improve public engagement by making it more accessible for all. Also, Somerville emphasizes how the municipal departments are structured and operate in particular, having a team to integrate and be a bridge to all the other teams working on the smart city projects. Besides, Somerville stresses using data collected to make

decisions, so by having a data team member in all committee meetings to assist in the discussions. The objective of having "smart governance" is to operate in a data-driven administrative operation efficiently and effectively where communication silos are at the minimum. Both of the case studies could help Canadian municipalities when they implement their smart cities approach. The reform of the municipality governance and administrative operation would be crucial when designing and implementing smart city projects in the communities because if the municipal government is not operating at the maximum efficiency, it may miscalculate the design and implementation of the smart city projects. In the literature review section under smart governance, the journal article written by Blauer outlines a few recommendations for municipalities to become "smarter" in administrative and governance operation. Some of Blauer's recommendations are implemented in Estonia and Somerville. For example, both Estonia and Somerville changed their data management and public service culture by restructuring the administration operation and the way they deliver government services to the residents.

Estonia's government advertise the use of Blockchain is helpful to identify cyber attacks, but in the cybersecurity interview with Kerschbaum disagrees with the effectiveness of Blockchain as part of a cybersecurity strategy for Canadian smart city projects. The discussion of the cybersecurity life cycle in the literature review section is similar to Kerschbaum's recommendation in having a Security Plan. However, the cybersecurity life cycle or the Security Plan are not mentioned or recommended in Estonia's cybersecurity strategy. In the interview with Kerschbaum, the reader will understand why Estonia markets the idea of Blockchain as part of their cybersecurity strategy.

Smart Cities: Apps & Data

When the municipality implements the smart cities approach, some neighbourhoods may be at a disadvantage or rarely use smart technology to its advantage (Townsend, p.190). The Researchers notice poor neighbourhoods with huge minority residents tend not to use municipal services or municipal smart system compared to Native English speakers' neighbourhoods (Townsend, p.190). For instance, New York City and Vancouver provide municipal services in other languages, but poor neighbourhoods with huge minority residents use the services less than other neighbourhoods (Townsend, p.190). The reason of this is not well understood, but there are a few presumptions such as unaccustomed with interacting with government in this form or different cultural norms on how to interact with government (Townsend, p.190). As a result, Native English speakers' neighbourhoods tend to have more resources to address their issues because they use the municipal system more (Townsend, p.190).

It would be challenging for municipalities to dispatch resources in neighbourhoods that use little of the municipal services or system because they would not have enough data to make a smart decision. Not only would municipality need to be aware of algorithm bias that might disadvantage poor minority neighbourhoods, but also how to get more disadvantaged neighbours to use the municipal smart services. There needs to be better citizen engagement and research on different neighbourhoods, especially the poor neighbourhoods that use little of the municipal services. The municipality should research on why poor neighbourhoods tend to use less of the municipal services and how to create an inclusive solution to address this issue. Also, when municipalities try to implement the smart cities approach in their community, they may have to make a tough spending choice because the smart technologies tend to be expensive which may push municipalities to cut services (Townsend, p.192). These municipal services would be crucial for working poor neighbourhoods because working poor tend to focus more of their resources on basic needs,

and municipal services assist them (Townsend, p.192). It is essential for the municipal government to take consideration of service cuts and how it will affect the disadvantaged groups. The data collected should help indicate the consequence of each municipal's decision, such as service cuts and how it affects the public.

In 2008 Washington, DC created an app contest called Apps for Democracy, to have data scientists to develop a product that uses government data to provide useful government services for residents and local businesses (Townsend, p.200-1). The data scientists were using government data that was already in open data, but the data were distributed in different government websites (Townsend, p.201). One example of a successful municipal app is the public transportation app where it provides real-time data about public transit to residents (Townsend, p.204). On the other hand, the Apps for Democracy app contest gave the data scientists the power to identify what the problems are at the expense of excluding residents to participate (Townsend, p.202). The Apps for Democracy did not connect data scientists with residents in the community, so the product of the apps was serving privileged residents who have a smartphone (Townsend, p.204). Also, the app contest did not consider ethnic minority neighbourhoods and multiple languages services for residents who would benefit these services (Townsend, p.204). Therefore, if municipal implement an app contest, there are many components to take considerations such as making it inclusive for everyone in the community.

Since the municipal data-driven system is being used to make decisions, the data in the system could be distorted because people could change the criteria in how to collect the data (Townsend, p.211). For example, the New York City Police Department's CompStat, a data-driven management system, where police officers record the crime to make a strategic plan to reduce crime rates (Townsend, p.210). The data show there was a decrease in crime rate, but the data was distorted because of the method of collecting the data (Townsend, p.210). The police officers were classifying the crime committed lower than it should be and discouraging residents from reporting the crime (Townsend, p.210-1). Therefore, the data shows a reduction in the crime rate due to the distorted ways of collecting the data (Townsend, p.210-1). When designing the data-driven system, there need to be some clear criteria of how data is collected, what data needs to be collected, and what data should not be collected. There should be ethical workshops on how to handle data and the danger of unethical practices for all municipal employees in their training program.

There are many companies that private help services for municipalities when they are implementing the smart cities approach. For instance, there is a start-up company called, CityMart that provides cities with ideas of the smart cities approach and cities can purchase smart technologies from their local start-up companies or other smart technology companies around the world with CityMart (Townsend, p.246-7). This start-up company provides smart cities service that can help the municipality on the implementation of the smart cities approach, and the municipal government can also support their local businesses that provide jobs for the residents. On the other hand, the collaboration between the municipal government and the private sector comes with challenges as well. Townsend argues that companies that collaborate with cities want ownership of the data it collects (Townsend, p.292). Many municipalities have difficulties in negotiating who controls the data collected on the residents (Townsend, p.293). This means municipalities need to be more prepared in how to negotiate contracts with companies. Furthermore, municipalities need to have regular audits on public data generated by residents to see if there is any unethical use, collect, and disclose data (Townsend, p.293).

5.0 Interviews

5.1 Introduction

In the case study section, it focuses mostly on smart governance and a little on cybersecurity. This research contains six interviews, and the interviews are based on a specific field concerning data. The four categories of the interviews are privacy law, data ethics, cybersecurity, and cyber-attacks, data infrastructure (data ownership and data sovereignty), and municipal resources. The interview questions are in the appendix section, and the interview sections below would contain the answers in each category. The interviews discuss and challenge the ideas outlined in the literature review and case studies, so it would help assist in the development of the recommendations. Furthermore, the interviews with experts tend to be intertwined with different key themes. For instance, Scassa specialized in information and privacy laws, but in the interview with her, she also discusses data ethics as well. Since the key themes are interconnected, the discussion tends to overlap with each other.

The table below illustrates the hypotheses and some of the key findings. To understand the findings in more detail, the interview conducted with each expert illustrates their expertise.

Table 2: Expert Interviews: Hypotheses and Findings

Expert Interview	
Hypotheses	Findings
Privacy Law **Canada's privacy law not sufficient in keeping up with technology development when it comes to data collection and the use of data (data mining)**	Privacy Law PIPEDA not sufficient for regulating data-related smart city projects PIPEDA needs to be amended by having stronger penalty Regulations are the best way to protect individual privacy
Data Ethics **Yes, checklist would help to reduce unethical data collection and the use of data** **Yes, increase digital literacy education for the public would create a more aware public on ethical issues in data collection and use of data**	Data Ethics Clement disagrees with having a checklist as the resolution for data ethics concerns Millar explains a checklist could be helpful, but it cannot be a generic checklist for all smart city projects. Millar recommends governments should focus more on process if the decision was made democratic or not in how, why, and should the data be collected

	Millar argues that to have digital literacy training is not for residents to stop unethical data collection because the big tech companies have a lot of resource to fight back. With digital literacy training, the residents have a better basic knowledge to challenge what data should be collect, how the data should be collect, and so on.
IT Data Experts **Government tends to have more challenges in updating technology compared to private sector is because the government needs to think about accountability, transparency, and the level of approval time is longer.** **Blockchain would help protect the information, but not prevent getting the "digital fingerprint" of the information.** **To update your cybersecurity continuously since technology evolves all the time**	IT Data Experts Clement argues that it is not only the government fault when the implementation of technology does not go well. It is also the responsibility of the private sector who created the product for the government to use. Kerschbaum disagree with the effectiveness of using Blockchain for municipalities as part of their cybersecurity strategy. A Privacy Impact Assessment and the Security Plan are more effective than using Blockchain Kerschbaum and Fung agree that there needs to be a constant revision of the security strategy the development of technology and cyber threats are not static
Local Government – resources **Yes, the public would need more digital literacy to take advantage of the smart cities approaches such as residents may use municipal apps to check the air quality, the traffic/traffic accidents, paying municipal bills, and so on.** **Yes, public servants would need to increase their digital literacy in order to implement smart governance** **The smaller municipalities would have more challenge than the bigger municipalities to implement a data driven government** **Top 5 challenges for local government to implement smart cities approaches:** **1.) Privacy** **2.) Data breaching and cybersecurity** **3.) Digital literacy workforce (smart governance)**	Local Government – resources Adcock explains that digital literacy workshops or training needs to be equitable for all residents There is a platform called MISA Canada, where municipalities can collaborate and share best practices Challenging to get the skill sets needed to implement smart city projects Millar states that some people may be responsible for a project in the municipality, but do not have the skill sets to work on the project effectively. Limited resources, so municipalities would only focus on the top priority projects Uses Privacy Impact Assessment (PIA) Top 5 Challenges (two common themes between Vancouver and Kelowna): Limited resources and

4.) **Who owns the data (government, tech companies, both?)** 5.) **The level of acceptance from the public**	Skill sets challenges/changing work culture (generation gap)

5. 2 Privacy Law

It was crucial to interview a lawyer who specialized in information and privacy law because the development of using, collecting, and disclosing data in the smart cities context is relatively recent with many challenges. The interview with Teresa Scassa, a University of Ottawa Professor in the Faculty of Law who specialized in information and privacy law, was very insightful. Scassa discusses that as technology rapidly develops, privacy becomes a significant concern. Individual privacy is considered a human right, and it should be protected. However, Scassa argues that Canadian privacy laws are not sufficient in keeping up with technology development when it comes to collecting, using, and disclosing data. At the Federal level in Canada, there are two privacy laws: The Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA), but only PIPEDA would be applied in the smart cities approach. Scassa explains that PIPIEDA, provincial/territorial privacy laws, and municipal jurisdiction would be the laws that govern the privacy and data aspect of smart cities approach in municipalities. However, Scassa expresses that privacy laws in smart cities are a very complicated situation, and it depends on what kind of "smart city technologies or data methods" the municipality is doing. Scassa gave an example of the Toronto Waterfront project if it put sensors in the waste management to collect data, would the data be owed by the private companies or by the municipality. The private companies would argue that it is on their private property, so the data is privately own. On the other hand, waste management is under municipal jurisdiction, so municipality argues that the municipal government should own the data. This kind of discussions is still ongoing because laws and regulations are not very clear and not keeping up with the development of technology.

When PIPEDA was created, the economy was collecting data for the marketing purpose of selling the product, but now, the information or data is the product. Scassa argues that there needs to be an update or modification on the PIPEDA to match the current data and privacy issues. The collaboration between the municipal government and private sector to implement the smart cities approach is most likely inevitable. According to Scassa, private companies provide products to the municipal government to implement the smart cities approach want part ownership or full ownership of the data collected. Scassa explains that some companies may charge more for the product if the company cannot have part ownership or full ownership of the data collected because if the company has part ownership or full ownership of the data, it may use the data for other commercial use that would generate revenue for the company. Therefore, the company can give a lower price rate for the municipality. For instance, by having companies have partial ownership of the data collected from sensors on buses or public transit, smart cards could mean lower costs for public transit for the public. Some people may be comfortable with the data being collected and part ownership from the private sector because it means cheaper public transportation. Since municipal governments already have a low budget to start with but have a long list of services they need to provide to the public, it may be economically more manageable for the municipal government to collaborate with companies where

companies can have part ownership of the data. Scassa also raises that sometimes it is difficult for the municipality to have full ownership of the data. For instance, Scassa states that there is an Ontario municipality, Innisfil, which collaborated with Uber where the Innisfil government subsidizes the ride for residents instead of purchasing buses and saves millions of dollars a year. However, the data of any Uber ride in Innisfil is be owned by Uber even though the municipal government subsidizes it. This example shows that it is challenging for municipalities to own all the data being collected.

Many governments have started to study the GDPR in the EU and what they can learn from it, so they can tailor similar data privacy regulation in their country. Scassa discusses that Canada is still looking at the GDPR by seeing what is the lesson learned so far and may adopt some of GDPR to the Canadian context. Scassa argues that the significant benefit of GDPR is that it strengthens data privacy. Also, Scassa notes that the fines in GDPR are high, so it gives companies incentive not to break any GDPR rules. However, Scassa argues that with higher fines, small to medium-sized businesses may not be able to survive or be willing to take the risk because of the penalties. This may give big companies the advantage because big companies tend to have more resources and can survive the fines.

Nevertheless, Scassa states that it is still too early to tell what the limitations of GDPR are because GDPR has only been implemented for less than a year. She explains that GDPR contains a stronger consent component than PIPEDA which brings benefits to other countries outside the EU such as Canada and the US, because companies who want to maintain a business in the EU, cannot have a high standard of personal data protection in the EU and another lower standard on data protection outside of the EU. Most companies should be consistent with having the GDPR standard on protecting personal data across their entire operations because it is currently the highest data protection regulations. Therefore, companies operating outside the EU would benefit the data and privacy protection of GDPR.

Moreover, Scassa pointed out that the judicial system is more focused on data protection in smart cities than focusing on the surveillance aspect of data collection in smart cities. Scassa explains that the moment you step out of your home, there are many Internet of Things (IoT) in the city that collect data about you, and even when you are back home, you may have IoT collecting data about you, such as heat sensor. The primary concern is that data collected in the city, and your own home could be used as a surveillance tool for National Security agencies. To protect data and privacy is not just having regulations for the private sector to follow, but also the concern of people accessing the data to surveillance other people. In the data infrastructure interview, Andrew Clement will discuss this.

Many people believe that by de-identifying the data or making the data anonymous in the smart cities approach, it would protect individual privacy and data. However, Scassa raised a concern that even with de-identified the data, the data can still be analyzed for human behaviour. It means the data collected in one community can be analyzed for their human behaviour, and this information could be used to decide who gets what resources and benefits. Scassa also stated that in one mall in Canada, they have started to implement cameras and sensors on the shopping centre digital directory boards to collect information about the shoppers' gender, age and how they look at the directory boards. The company argues that it is not collecting personal data on shoppers because the data collected are de-identified.

On the other hand, privacy experts argue the data are not de-identified because they are collecting information such as gender and age, which is personal information. This case is still being reviewed by the

Privacy Commissioner. When Scassa was explaining about this shopping centre digital directory board case study, she emphasized that data and privacy issues are very challenging and complex to resolve, especially with the current data and privacy laws in Canada.

The privacy and data laws in Canada need improvement, especially for municipalities, when they implement the smart cities approach in their communities. Scassa strongly recommends that the PIPEDA be revised by having stronger enforcement such as a stronger penalty. Scassa argues that the current system in PIPEDA penalty is too soft, and most companies pay the penalty, but it does not incentivize them not to collect data in an unethical way. By studying the EU's GDPR, it may help Canada to revise the PIPEDA to address the outstanding data privacy issues.

To understand the privacy and data laws are essential to the implementation of the smart cities approach in Canadian municipalities. Having a lawyer specialized in information law to explain how the current privacy and data laws work in smart cities provides very valuable context. Scassa also provided insightful information on EU' GDPR and how the GDPR has a stronger regulation on penalty compared to Canada's PIPEDA. Also, Scassa strongly recommends the amendment of PIPEDA to keep up with technological development and protect individual privacy.

The discussion about privacy laws and regulations in Canada and the EU are helpful to understand how laws and regulations are not equipped to handle the design and implementation of data-related smart city projects. However, businesses are still proceeding without the amendment of the privacy laws and regulations in Canada. Since there are many uncertainties with the development of technologies and the data component of smart city projects, it makes it challenging to address privacy issues. It is essential to understand that privacy laws and regulations have a significant role in resolving or minimizing the harm of unethical collection, usage, and disclosure of data.

5.3 Data Infrastructure (Data Sovereignty and Data Ownership)

Reading the journal article from Andrew Clement, an information infrastructure expert from the University of Toronto, it was critical to interview him on data infrastructure. It is a common discussion about why government tends to have more challenges in updating technology or using technology compared to the private sector. Clement clarifies that governments and public institutions operate in a different ground compared to the private sector, where governments have more stakeholders to engage with compared to the private sector such as start-up tech companies who report to the shareholders. Moreover, Clement explains that people need to use governmental systems, and any problems can have a major impact. Therefore, Clement expresses that government tends to be more conservative compared to the private sector. However, when the government implements technology that causes major issues such as the Phoenix system, it seems that the government is the only stakeholder at fault, and less blame falls on the private companies that created the Phoenix system. Clement argues that in the Phoenix system, both the government and the private sector that created the Phoenix system are at fault and should be held accountable. Clement explains that the private sector also makes mistakes, but the consequences are not felt the same as when governments make a mistake. Clement clarifies that the challenges in the public sector tend to be more visible compared to the private sector. Governments hold a lot of responsibilities and mistakes in governments can have damaging consequences.

CENTRALIZING VS. DECENTRALIZING SYSTEMS

The debate of centralized versus decentralized system (integrating data system or not) has been a long discussion, and there are advantages and disadvantages in centralizing or decentralizing the data system. By centralizing the data system, it creates efficiency in data sharing, but it also increases the vulnerability of hackers taking all that data in one centralized location. Clement claims that there is a lot of contingency when it comes to the idea of centralizing or decentralizing data system. Clement explains that municipality that has an integrated system, it may be they integrated separate systems or a vendor that sells a more integrated system. However, Clement states that for more prominent institutions such as the Federal government created systems for each department separately because they were probably using different vendors that offered tools that they need that are different from other departments. Clement argues that the objective to integrate systems is for data to flow easier from one department to another, but to construct it, it is more difficult to achieve in practice. To incorporate all departments into one data system is exceptionally challenging because Clement argues that they would need to change their work practices that can be very disruptive. The question is "who will need to change their work practice and how would it be changed". Centralizing or decentralizing is a very fraught issue, and there is no simple answer. Clement claims that the tech sector argues that they have the resource and expertise to protect public institutions' data. However, by storing massive data in one area, people would be tempted to hack into the system because the valuable data it contains.

TRADITIONAL GOVERNANCE TO "SMART GOVERNANCE"

As technology plays a significant role in our society, people have been discussing the idea of "smart governance." Clement is skeptical of the term "smart governance" because he argues it is a marketing tactic from tech vendors to sell public institutions this idea that their products can make their governance "smart." Clement notes that government institutions need to be aware of what is happening in the tech sector and what kind of new services they are offering that would be helpful for governments to deliver public services to citizens. For instance, as a society, we are more relying on the smartphone to do our daily activities, and governments should look at if they can provide public services in smartphone apps.

In this research, smart governance means to use technology to engage with residents by having discussions in real-time and providing digital services to residents similar to e-Estonia. Smart governance in this research also mean to create an efficient departmental operation where government departments break communication silos and have an effective data management system and/or cloud-based file sharing system to make decisions based on the data collected by smart technologies such as sensor, government services apps, and other IoT. Clement expresses that it is good that the government uses new technology to engage with the public, but some groups such as older people may not use those new technologies to engage with the government. The older generation may prefer traditional in-person public engagement. Clement warns that the government should not leave behind those who are not adapting to the new digital public engagement. Clement questions on who benefits from this "smart governance" concept since it is most likely that some people would be at a disadvantage from this "smart governance."

UNETHICAL ALGORITHM

Clement questions the idea of "unethical algorithms" because an algorithm cannot be unethical. It is the management of the organization and programmers that develop the algorithm or software design it to have unethical outcomes. Clement states that by calling ethics, it tends to put emphasized on individual such as

programmers or developers and question if they are acting ethically or not on developing algorithms. It seems that algorithms, especially in AI and machine learning, are somehow treated independent and autonomous actors for ethical judgment, but Clement disagree with this idea. He argues it is not the algorithms that are ethical or unethical. Clement explains that institutions and actors who develop and make decisions on the design of the algorithm or software should be held accountable. Clement argues that by using the term "unethical algorithm" is a deflection from where the issues of responsibility and accountability for being ethically is appropriately situated. According to Clement, people should be asking "who has the power, who is benefiting, who has a say, and who suffer the consequences." Clement gave an example of the recent incident, the Boeing 737 MAX, where the management and/or engineers approved the engine of the Boeing 737 MAX airplane that was not properly tested, but it is not the engine of the airplane is at the heart of the accountability lies. The ethicality applies to the management and/or engineers that agreed the airplane was safe, and they should be held accountable, not the airplane itself. Clement recommendations the importance of having someone accountable for making a decision in order to minimize unethical decision or activities in algorithms. By having someone or a group of people from management to be held accountable for their decisions may reduce unethical decisions or activities in algorithms. I raised the idea of a checklist for data scientists when designing the algorithms in a system based on the recommendation from DJ Patil's article. In our interview discussion, Clement argues that by having a checklist for data scientists it pushes ethical responsibility in the front line while letting those responsible for the deployment to be off the hook.

DATA SOVEREIGNTY

The two concerns for Canada when it comes to data sovereignty, especially with the implementation of smart cities in Canadian municipalities are privacy and security concerns. Clement gave a current example of data sovereignty being a challenge in the Sidewalk Lab (also known as Toronto Waterfront Project or Sidewalk Toronto) in Toronto where the public is advocating for data being stored within the Canadian border. The concerns are that the data collected would flow through outside Canada through the US routing hubs where foreign jurisdiction such as the NSA can intercept the data. If Canada continues to rely on the US routing hubs, it puts risk on individual Canadians and to Canadian democracy. This shows that Canada's data sovereignty is being more economically and technically depend on the US. Clement has two recommendations: to insist that data be stored within Canada and have data centre connecting to Canada's internet exchange point. However, Clement is aware that it is hard to 100 percent guarantee no data flow outside of Canada, but those two recommendations would help minimize the threat of Canada's data sovereignty.

The interview with Clement provided insightful information on data sovereignty because data collected by IoT may flow to a foreign IXP where it could be subjected to a foreign intelligence agency. Since smart city projects tend to collect may information about the community and the residents, foreign intelligence agency could use the data as part of the surveillance of that municipality. Also, data should be stored within Canada and not abroad because the data would not have the protection of the Canadian government. It is crucial for municipalities to have an appropriate strategy on where to store the data and how the data flow within the Internet. Moreover, Clement's perspective of a checklist to minimize unethical behaviour such as unethical or biases algorithm used to assess the data collected is pushing the responsibility only to the programmers or developers and not having senior executive or senior management to take part of the responsibility.

Furthermore, Clement challenges the idea of "smart governance" because it is indicating that the governance of the government has not been "smart," and it needs these technologies to improve their governance practice. Clement argues that the idea of "smart governance" is a marketing strategy from the technology vendors to sell their products to municipalities. The expertise from Clement would support the analysis and recommendations of this research paper.

The discussion of who is responsible for the ethics of collecting, using, and disclosing data is very contentious. Some experts argue that the private sector is responsible while others argue the public sector or mix of both. However, it is essential to keep in mind how well humans are protected from the systematic collection of information from the private and public sectors. Having a basic layout on where the responsibility lies is essential, but if the system cannot protect or minimize humans from harm, it may become an exercise or a checkbox for senior management to complete.

5.4 Data Ethics

It is essential for municipalities to think about data ethics and have a concrete strategy to address data ethics issues in the smart cities approach. The interview with Benjamin Fung, a Computer Science Professor from McGill University was very insightful about the privacy, security, and ethics of data collection and the use of data. Fung explains that unethical data collection and unethical use of data focus on the idea of consent of the participants. Fung defines unethical data collection, and unethical use of data is collecting and using data without the consent from participants. Moreover, Fung argues that currently, many consent agreements are unethical as well because they are too vague, too long, and challenging for participants to understand. Fung states that in the data collector's perspective, they want to collect as many data as possible. Also, Fung claims that in the smart cities context, data collectors may not know 100 percent how they would use the data at the moment they collect the data. Therefore, they would create the consent agreement vague to give themselves more flexibility since they do not know what to do with the collected data.

Fung questions the idea of ethics expert participating in the development of the data system. Would the ethics expert be from within the data development companies, or from government institutions, or a non-profit organization? However, Fung does agree that it would be beneficial to have ethics and privacy experts involved in the data processor of the smart cities approach. It is important to know if the ethics experts would have any conflict of interest in participating in the design and implementation of the smart cities approach.

According to Fung, a checklist would not be the most effective way to address data ethics issues. Fung argues that one checklist would not be applicable to all the smart city projects because different projects would have or needs different requirements. Furthermore, Fung explains that the checklist is not for data collection, but for data sharing for a third party and disclosure of data because the checklist would able to remind what attributes should be shared to the third party or what characteristics would be disclosed publicly.

Fung supports the idea of drawing a boundary of what data should be collected, but also agrees it would be challenging in drawing that boundary in practice. By drawing the boundary, it will most likely compromise the smart city projects. Also, Fung explains that it will be challenging in how to draw that boundary because different smart city projects have different objectives, so it is hard to draw a consistent boundary.

Furthermore, Fung clarifies the challenges of drawing the boundary and creating a checklist are similar because the development of smart city projects cannot be static and universal for all communities. Fung explains that one should not think about data collection in a binary mode as in collecting the data or not collecting the data because it is possible to collect data in a Privacy-Preserving manner.

PRIVACY-ENHANCING TECHNOLOGIES (PET)

Fung states that Privacy-Enhancing Technologies (PET) would help reduce privacy concerns when collecting and using data in smart cities. The PET has many privacy-preserving techniques. One example of a PET is the Privacy-Preserving Data Mining (PPDM) technique. The Privacy-Preserving Data Mining (PPDM) techniques "are designed to guarantee a certain level of privacy while maximizing the utility of the data to allow for effective data mining" (Mendes and Vilela, 2017, p.10564). Fung explains that PET is useful because you can add some noise such as randomization in the data while collecting data in real-time so that it can protect the privacy of people. Fung argues that by using PET, the data collectors need to think about the trade-offs between privacy and the data quality or data accuracy.

Fung gave an example of how PET is used. There are seven cars on the road, and each car is using GPS. Traditionally, we need to know the location of these seven cars, but we need a unique ID for each car. In the privacy-preserving data collection technique, there is a technology called Mixnets. Mixnets would immediately mix the data it is collecting. Those seven cars in this one region using GPS would have their signals send to Mixnets, and their data would be mix before sending it to the GPS service provider. The GPS service provider would only see the seven dots, but they do not know which cars are which. However, the service provider can still reply to the user by sending the information back to Mixnets, where Mixnets would distribute the information to the correct car. Fung states that this is an example of how we can still collect the data we need without compromising our privacy. Fung argues that technology does exist in protecting our privacy when collecting data, it is whether if people use it or not.

Furthermore, Fung claims that there is no intention for companies to use it because the technology is costly. Fung clarifies that this is not a black and white problem, but we need to view the privacy and data collection issues as somewhere in between. According to Fung, there are many examples of how to mitigate privacy concerns by using PET already. However, people are not using these solutions because there is no motivation in using it. There is no intention for the company to use this, unless the consumer raises its voice, otherwise why the company will change.

According to Fung, Privacy-Preserving Data Publishing (PPDP) technique is used for when data are being published and when data collectors are sharing data without compromising individual privacy. This technique would be helpful for smart cities because different municipalities may want to share their data or different departments within a municipality may want to share data where it protects individual privacy.

Differential privacy (DP) is a privacy model used in PPDP and PPDM. According to Fung, in the last ten years, differential privacy has become a tool to protect individual privacy. Even if someone has access to the information, they would not be able to pinpoint who are the people. Apple has already implement differential privacy in their data system. Fung recommends that differential privacy is a useful tool to implement in real life. Fung explains that data can transform it into a differential privacy dataset before the organization shared their data. Therefore, privacy is preserved. Fung states that during the data collection

phase, the injection of noise to the dataset is not injected randomly, but it follows a specific method. This method would help satisfy the privacy protection one wants.

LINKING DATABASES TOGETHER

Another danger of not receiving consent from participants is sharing data between two databases without the consent from participants. Fung explains that this makes it easy to identify the person even if the data is anonymous. Moreover, Fung argues that the objective of the smart cities approach is to link different databases together and it is unethical for data collectors to link up one database to another database without the consent of the participants. According to Fung, the biggest data privacy concern is not what one data collector can get from participants, but what is dangerous is linking this database to other databases. Fung describes that once the database is linked to another database, an individual becomes "unique," which means it would be easier to identify a person or a group of people even though if the data is anonymized. Fung gave an example of how two databases link can quickly identify a person. If Database A contains the information of 10 professors in Montreal who is working in engineering and Database B includes medical information such as people who have asthma. By linking Database A and Database B, it may show within the ten professors in Montreal, only one of them have asthma. Therefore, by combining databases, it becomes easier to identify people even if the data is anonymized.

Furthermore, Fung argues that major data privacy issues are linking databases together because someone could link up to these databases and could use the data to restructure people's routine. Fung states that it is not just how they use the data, but linking the data without consent is a major concern as well. Currently, many companies do link databases together without the consent of the participants. Fung explains that this is precisely the difficulty of smart cities projects because smart cities projects are about linking databases together. This is the exact conflict between smart cities projects and privacy concern projects. However, Fung claims that the privacy-preserving data technique for this scenario is already considered and there are ways to link up databases without compromising privacy too. The solution already exists, but it is a complex solution, which means it would cost a lot. Sometimes is not just money that can help get the solution. Fung explains that there is a conflict between privacy protection and data utility (also known as data accuracy). The data collector wants accurate results from smart cities, but it is often a trade-off between privacy and data accuracy. Fung describes if there is high-level privacy protection, the accuracy will drop, but when it is high accuracy, the data collector needs it would lower the privacy protection. Fung states that when using PET, it is about finding the trade-off that as a society, we can accept to achieve reasonable accuracy without compromising privacy. Fung gave an example by explaining if the data collector does not think about privacy concerns and collect data it would be at 90% accuracy on the raw data. After adding some noise such as changing the age in the database, the accuracy will drop to 86%. As a result, it is a 4% drop and a 4% drop in the price for achieving some privacy requirements. Fung argues that there is no "free lunch here," we need to sacrifice some accuracy to achieve some privacy. Even if you have access to all raw data, it would not be 100% accurate on every recommendation. Fung gave an example on the recommendation items function in the Amazon website for the user to purchase other items based on their data search. However, the recommended items from the Amazon website is not 100% accurate on what the user will buy, but it would generate some accurate items the user will buy. Fung argues that we are working in an imperfect world anyways, we need to sacrifice a couple of more accuracy, and we can get the privacy we want.

PRIVACY BY DESIGN

Fung recommends municipalities should use the Privacy by Design (PbD) framework at the beginning of the first stage of the smart cities plan because it can help municipalities create a well-planned privacy design plan in their data systems. Privacy by Design is "building privacy into the design, operation, and management of a given system, businesses process, or design specification" (Privacy by Design: Setting a new standard for privacy certification, p.2). The PbD will give municipalities a structural framework to keep in mind of privacy throughout the smart cities plan. There are seven foundational principles of PbD, and they have listed the chart below (Privacy by Design: Setting a new standard for privacy certification, p.2).

Table 3: Seven Foundational Principles of Privacy by Design (PbD)

7 Foundational Principles of Privacy by Design (PbD)	
Principles	Meaning of the Principles
1.) Proactive not reactive – preventative not remedial	To have a plan to prevent incidents to happen and not have a reactive approach
2.) Lead with privacy as the default setting	To have an automatically protected personal data plan in all data systems and operational practices
3.) Embed privacy into design	The system should fully incorporate privacy controls and not as an add-on
4.) Retain full functionality (positive-sum, not zero-sum)	There should be no unnecessary trade-off between privacy and security
5.) Ensure end-to-end security	To have a data lifecycle security in the data system from collecting the data to retaining the data to destroying the data if data is not needed
6.) Maintain visibility and transparency – keep it open	To be transparent to all stakeholders in how the data system is operating and have independent verification
7.) Respect user privacy – keep it user-centric	To have the system be user-centric meaning keeping individual privacy interest in mind

DIGITAL LITERACY:

Fung agrees that having more digital literacy it would help the public push companies to change their privacy practices. However, it is challenging to educate the public about the fine prints of the consent agreements. Fung raises that people who want to use the service are willing to sacrifice their privacy. Similar to what the public transit example from Scassa. Fung argues that there is no easy solution and that the digital literacy provided to the public or school may not be enough.

FUNG'S RECOMMENDATIONS

Throughout the interview with Fung, he recommends many mitigations and controls to reduce the tension between privacy concerns and data collection. Fung recommends municipalities who are implementing the smart cities approach to use PET to protect privacy. The municipalities need to think about the trade-offs between the level of data accuracy and the level of privacy protection they want when using PET. The second recommendation from Fung is for municipalities to think about privacy in the life cycle of the data

by thinking about privacy in the first stage of the data collection. This approach is called Privacy by Design. The third recommendation is for municipalities to be more aware of the privacy concerns with linking different databases together and prepare a mitigation plan.

In this research, the interview with Fung contributes significantly to the discussion of privacy, security, data ethics, and efficiency. Fung recommends privacy enhancing technologies (PET) and Privacy by Design (PbD) to address privacy concerns when municipalities implement their smart city projects. His recommendations for the municipalities are feasible to implement and would provide mitigation for privacy issues. Municipalities would need to consider the trade-offs between privacy requirements and data accuracy when using PET. Fung argues that municipalities are not using PET or tech vendors are not promoting PET because there is not enough strong regulations and laws to push municipalities to use privacy enhancing technologies. Therefore, it goes back to reforming data and privacy laws in Canada to ensure better privacy protection for residents. Also, Fung warned the dangers of linking different databases because it could violate many privacy concerns. However, Fung pointed out that the smart cities approach is about linking different databases to make better-informed decisions, so municipalities need to be very aware of this problem to create mitigation to address this problem.

The second data ethics expert interviewed for this research was Jason Millar, a University of Ottawa Professor who specialized in Computer Science Ethics. Millar explains that to define unethical data collection and use of data; one needs to think about the process of how the decision was made to collect that type of data or not in the first place. He argues it is difficult to say what would be ethical or not because different groups of people have different values of judging what the right thing to do is. Millar supports the idea of creating the process for decision making in what data to collect or not. The process needs to outline a fair practice that includes a clear accountability and governance structure.

Millar agrees that it is a good idea to use Privacy Enhancing Technologies (PET). Millar argues that the question is not whether you to use PET to minimize privacy concerns, but it is should municipalities be collecting the data in the first place. He explains that the ethical question is not answered by just using PET because PET only helps with providing security and privacy. PET does not assist in the decision of how does the municipality go about deciding whether or not to collect that type of data in the first place. Millar suggests that municipalities to think about these questions if the municipality agrees to collect these data:

How did the municipality get to that decision?

Was it a fair process?

Was the process transparent?

Was the process democratic?

Why was the process democratic?

CHECKLIST

According to Millar, a checklist similar to decision trees or flow charts or decision-aid is one tool to use to think through the ethical dimension of data collection. However, Millar argues that it is important to know how the checklist is constructed because if the checklist were created in exclusivity, it most likely would

not work well. The creation of the checklist must be well constructed by including people who are involved with the specific smart city projects. Millar argues that the checklist should not be a general one because different smart city projects demand certain stakeholders. Therefore, there should be checklists for different types of smart city projects. Moreover, a checklist needs to have governance and accountability structures to make the checklist more effective.

MISUSE DATA

Millar argues that institutions misuse data not because there is a motive behind the misuse of data. It is sometimes the people working in these institutions have a lack of awareness in unethical data collection and use of data. He clarifies that some people in the municipal government may be given the responsibility for this project, but the person may be unaware of the consequences of the decision they made on collecting or using the data. Millar agrees that having stronger regulations and more accountability mechanisms would help minimize unethical data collection and use of data. The regulations and laws on data and privacy need to be effective to address these data and privacy concerns because, without effective laws, it will not protect the public from these harms.

DIGITAL LITERACY

Millar agrees that providing digital literacy for the public and public servants is helpful, but it is not the core solution to address the data ethics concerns. Millar explains that there is a huge power imbalance between the private tech companies (data scientists) and the public and public servants. By viewing digital literacy as a core solution to address the data ethics concerns, it puts the whole ethical responsibility to the public to push back these big influential tech companies where the tech companies have considerable resources to fight back. It is costly and inefficient to make everyone an expert in data. Moreover, it may not have the outcome people expect it to because it is very challenging to achieve this in the first place. The core solution to address data ethics concerns is to have regulations where it gets implemented when there is a political will to do so.

According to Millar, by having digital literacy education for the public and public servants will helps keep institutions accountable. Millar explains that digital literacy would demystify technology because when people think of technology similar to "magic," it becomes a major problem. Millar compares the current challenge to what happens in Europe in the 15th century where priests and people with resources had all the power over average citizens because the citizens did not know how to read and write and believe what priests tells them. When the printing press became predominant, and people learned how to read and write, they started to question people in power. Millar explains that the data scientists or programmers are similar to the priest that held power in the past. In the current context, it is where the average citizens are now in a state with minimum to no computer science skills that believe data scientists and programmers would make decisions in the best interest of the public. Millar argues that by having the public and public servants more digital literacy education, it will help challenge these data scientist and programmers why are they collecting data this way and not that way. Digital literacy education could provide a basic understanding of what data is and what computer science is for the public. For instance, if a data scientist said that they are not able to anonymize the data collected, the people with the digital literacy education could challenge them because the public now knows it is possible to anonymized the data. Millar states that to understand and learn about social implication takes time to learn, and sometimes, people with the technical skills may not have the training on the social implication in a product they produce.

MILLAR'S RECOMMENDATIONS

Millar has two recommendations for municipalities to implement when designing and implementing the smart cities approach: Algorithmic Impact Assessment (AIA) and Canada's Directive on Automated Decision-Making. There are five key components to the AIA:

1.) The institution using automated decision systems need to assess how their automated decision systems affect the communities in terms of justice, bias, fairness, or other socio-economic issues
2.) The institution needs to collaborate with external researchers to assess the life cycle of the automated decision systems
3.) The institution needs to publicly publish on what is an automated decision system and include relative researchers' assessment of the system before implementing the system in the institution.
4.) The institution needs to answer or clarify any questions and comments from community members
5.) The institution need to construct a plan to address communities who are affected by the automated decision systems due to biases or other issues not addressed by the institution's mitigation plan. (Reisman, Schultz, Crawford, and Whittaker, 2018, p.4)

Canada's Directive on Automated Decision-Making is a guide for Federal departments and agencies who are using automated decision systems in their programs to deliver services for Canadians (Directive on Automated Decision-Making, TBS, 2019). The Directive requires the department or agency to complete the Algorithmic Impact Assessment (AIA) and the responsibility would be under the Assistant Deputy Minister (ADM) or an individual who was appointed by the Deputy Head to be in charge of the program that is using automated decision systems (Directive on Automated Decision-Making, TBS, 2019).

The interview with Millar provides a different perspective and recommendation from Fung. Millar focuses on the ethical side of resolving privacy and security concerns. On the other hand, Fung concentrates on the technical side of protecting the community's privacy and security. Millar focuses on how the social impact of data collection and use of data is most likely not thought about from data scientists. Therefore, it is crucial to bring people from different expertise to work together in the design and implementation of the smart cities approach because many multidisciplinary issues need to be addressed as a team.

Millar's interview brings a different perspective than Fung. Millar's data ethics perspective is similar to Wylie's perspective, who wrote a critique on the Toronto Waterfront Project. Both Millar and Wylie are concerned with the democratic process of what data to collect or not. Millar has similar opinions as Fung, Clement, Scassa, Loukides, Mason, and Patil on the idea of having stronger privacy laws and regulations to address many of the data-related smart city projects that hinder individual privacy, democracy, and cybersecurity.

5.5 Cybersecurity & Cyberattacks

The smart cities approach uses many Internet of Things (IoT) to collect data and uses machine learning or AI to assess the data in their data system. Cyber attacks are a major threat to municipalities when they implement the smart cities approach. However, the opportunities for municipalities are to design well-planned cybersecurity. Therefore, it is important to have a cybersecurity expert to explain how to protect a system from cyber attacks and data breaches. Florian Kerschbaum, a Computer Science Professor from the University of Waterloo, explains that there are five ways to defend against a cyber threat: prevent, deter,

deflect, detect, and recover. Kerschbaum recommends reading his Module 7 PowerPoint from one of his Computer Security and Privacy courses at Waterloo and the book, Security in Computing.

THE SECURITY PLAN

The security plan is to "explains what the security goals are, how they are to be met, and how they will stay met" (p.9). The security plan consists of "the current state of the security of an organization, as well as a plan for improvement" (p.10). There are seven parts of the security plan: policy, current state, requirements, recommended controls, accountability, timetable, and continuing attention (p.10). Kerschbaum argues that having a security plan is the best method to protect the data system in a municipality.

POLICY

The first component in the security plan is the policy where it outlines the purpose and intent of the security plan (C. Pfleeger, S. Pfleeger, Margulies, and Prentice-Hall, 2015, 10.1 Security Planning). Kerschbaum explains that the policy stage is where it clearly states the goal, responsibility, and commitment. In the goal section of the policy stage, it needs to think about confidentiality, integrity, availability, and priorities such as securing data or serving customers (p.11). In the responsibility section of the policy stage, it needs to outline where the security responsibility lies (Pfleeger et al., 2015, 10.1 Security Planning). The last section of the policy stage is the organization's commitment to security (Pfleeger et al., 2015, 10.1 Security Planning). In the policy stage, Kerschbaum emphasizes that there needs to be a discussion of trade-offs in the security plan. To think about the trade-offs in the early stages of the Plan, it ensures a structural system that contains a cost-benefit analysis.

CURRENT STATE

The second component is the Assessment of Current Security Status, which means to analyze and understand the vulnerability the system might be exposed to (Pfleeger et al., 2015, 10.1 Security Planning). The organization would conduct a risk analysis by identifying the assets and controls in the data system, the vulnerabilities of the current system, and possible situations that the system can go wrong (Pfleeger et al., 2015, 10.1 Security Planning). However, it is still possible to have vulnerabilities that are not identified in the security plan due to new technology or the system progresses (Pfleeger et al., 2015, 10.1 Security Planning). Kerschbaum stresses that a risk analysis is crucial for the security plan, and it should be completed carefully. According to Kerschbaum, the Threat Analysis would be helpful for municipalities when they implement the smart cities approach. Kerschbaum explains that the Threat Analysis would identify and assess the possible threat in the system. The Threat Analysis would be conducted at the Assessment of the Current Security Status in the Security Plan.

REQUIREMENTS

The third component of the security plan is security requirements, which are known to be the heart of the Plan (Pfleeger et al., 2015, 10.1 Security Planning). The requirements tend to contain "the functional or performance demands placed on a system to ensure a desired level of security" (Pfleeger et al., 2015, 10.1 Security Planning). It will be beneficial for the organization to contain these seven components in the security requirements:

- **"Correctness:** Are the requirements understandable? Are they stated without error?
- **Consistency:** Are they any conflicting or ambiguous requirements?
- **Completeness:** Are all possible situations addressed by the requirements?

- **Realism:** Is it possible to implement what the requirements mandate?
- **Need:** Are the requirements unnecessarily restrictive?
- **Verifiability:** Can test be written to demonstrate conclusively and objectively that the requirements have been met? Can the system or its functionality be measured in some way that will assess the degree to which the requirements are met?
- **and traceability:** Can each requirement be traced to the functions and data related to it so that changes in a requirement can lead to easy re-evaluation?" (Pfleeger et al, 2015, 10.1 Security Planning).

Moreover, budget, schedule, performance, policies, and governmental regulation may also shaped the control of the security plan (Pfleeger et al., 2015, 10.1 Security Planning).

Recommended Controls

The fourth component is the Recommended Controls, which is a list of recommended controls that meets the security requirements in the security plan (Pfleeger et al., 2015, 10.1 Security Planning). The developer of the Plan could use the risk analysis to develop a structure that identifies the vulnerabilities to create the controls for the data system (Pfleeger et al., 2015, 10.1 Security Planning).

Accountability/ Responsibility for Implementation

The fifth component of the Security Plan is Accountability. The document for this section would outline each in the organization on their responsible and accountable for different parts of the security plan (Pfleeger et al., 2015, 10.1 Security Planning). When the requirements are not met, or there is an error in the implementation of the security plan, the documentation would clearly state who is responsible and who is held accountable (Pfleeger et al., 2015, 10.1 Security Planning). Therefore, when it is outline which role in the organization is responsible and accountable for what, it ensures trust between individuals in the organization. When responsibility and accountability are unclear, individuals in the organization would blame others and not take responsibility.

Timetable

The sixth component is a timetable for the implementation of the security plan. It would be challenging and ineffective to implement the whole security plan at once (Pfleeger et al., 2015, 10.1 Security Planning). It is recommended that organizations should implement a part of the Plan pieces by pieces by having set milestones, so the senior management could see the process and make adaptation if needed (Pfleeger et al., 2015, 10.1 Security Planning). The timetable of the security plan needs to be flexible for adjustment because new threats may occur and it may need new equipment to address the issue by creating or revising the control (Pfleeger et al., 2015, 10.1 Security Planning).

Continuing attention/ Plan Maintenance

The last component of the security plan is continuing attention or plan maintenance. This means that there is a need to regularly review and update the security plan (Pfleeger et al., 2015, 10.1 Security Planning). The major reason to be continuously attentive to the Plan is that the world is constantly changing and it needs to keep up with the security development. Data systems must constantly adapt to the new environment and improve the system (Pfleeger et al., 2015, 10.1 Security Planning). As the world changes, new vulnerabilities will occur, and the current controls in the Plan may not be applicable in the near future

(Pfleeger et al., 2015, 10.1 Security Planning). Therefore, organizations need to improve their security plan and data system constantly.

PRIVACY IMPACT ASSESSMENT

Kerschbaum explains most organization collecting data would use the Privacy Impact Assessment. It is a standard practice in government institutions and the private sector. The Privacy Impact Assessment (PIA) "is a process that helps determine whether government initiative involving the use of personal information raise privacy risks; measures, describes and quantifies these risks; and proposes solutions to eliminate privacy risks or mitigate them to an acceptable level" (Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada, OPC). Moreover, Kerschbaum explains that the PIA identifies the privacy impact, and it is not identifying countermeasures. Once you identified the privacy impact assessment, you can rank it with effects. Then you decide on which kind of Privacy Enhancing Technology (PET) you want to use to protect the assessed impact. The PIA is not always in the Security Plan. PIA focuses on privacy, while Security Plan focuses on security. If you are a very revolved organization, you do both the PIA and security plan. Sometimes there are different departments, one responsible for the privacy and another responsible for privacy.

Kerschbaum states that there is no standard PIA, and organizations can adjust or customize the PIA to their needs and objectives. According to the Privacy Act in section 3, all government institutions that touch some privacy issues must complete a PIA for new programs or modified programs (Privacy Impact Assessments: Frequently asked questions, OPC). Moreover, Kerschbaum suggests municipal governments should learn from other municipal governments or organizations on how to develop its own PIA. The PIA needs to have experts in law, privacy, information technology, and other relative digital experts (Privacy Impact Assessments: Frequently asked questions, OPC). Moreover, different provincial governments have their template of the PIA for their municipalities and government department to use, such as British Columbia's Office of the Information and Privacy Commissioner (OIPC). In the next interview on municipalities, both municipalities I interviewed used the PIA for their smart cities plan.

BLOCKCHAIN – ESTONIA

Kerschbaum argues that the Blockchain system used in Estonia would not be effective in protecting the data and individual privacy. Kerschbaum states that Estonia's Blockchain system is not addressing the security needs in a smart cities approach. Kerschbaum clarifies that Blockchain would not help minimize the security threats in a smart city system such as personally identifiable information collected by IoT and tampered traffic lights. Kerschbaum explains that a blockchain is not sufficient to detect a hack because one cannot control the new data going into the Blockchain. Also, Kerschbaum describes one can only detect the data already in the blockchain system and not the new data going in.

Furthermore, Kerschbaum claims that there is existing technology to provide the same level of protection Estonia is claiming for Blockchain. Kerschbaum gave an example of TripWire, where it takes a "hash" of each file and stores it outside the computer, and this tool has the same effect as Estonia claim for Blockchain. The practice of TripWire has been used for over 20 years now. Therefore, Kerschbaum does not see the additional advantage of using Blockchain in a smart cities approach. On the other hand, Kerschbaum does see the advantage of Estonia using Blockchain because Estonia is afraid of Russians hacking their system again, so by convincing other people outside the country to store a copy of their information through Blockchain, Estonia would not lose their data if they ever get a massive hacking

incident. Kerschbaum explains since more users in Estonia's Blockchain system, the more copies of the information are out there, meaning easier to recover the information if Estonia ever gets hacked. Overall, Estonia's Blockchain is a marketing scheme to sell this idea to secure Estonia's data in case of another Russian cyber attack that happened in 2007.

The interview with Kerschbaum on cybersecurity is very helpful because he provides strong recommendations on how municipalities could improve their cybersecurity strategy. Kerschbaum strongly recommends municipalities to implement the Privacy Impact Assessment (PIA) and have a Security Plan to mitigate security concerns. Moreover, Kerschbaum argues that the Blockchain used in Estonia would not be helpful in the smart cities context because there are already technologies such as TripWire that provides similar results as Estonia claims. Kerschbaum provides expert recommendations on cybersecurity that is challenging to find in social science journal articles because many social scientists may not have the computer science knowledge to explain cybersecurity concerns in a smart city context.

5.6 Interview – Municipal Resource

There are many municipalities across Canada working to implement the smart cities approach in their communities. It was crucial to conduct interviews with municipal experts on their experience in working for a municipal government. The two expert interviewees are Rob Entwistle, an Information Services Manager, from the City of Kelowna and Jessie Adcock, a Chief Technology Officer, from the City of Vancouver. The city of Vancouver is one of the finalists of the Smart Cities Challenge. The city of Kelowna entered the $10 Million category and the City of Vancouver with the partnership with City of Surrey for the $50 Million category. The interviews consist of questions about digital literacy to data privacy to challenges municipalities have to implement the smart cities approach.

KELOWNA

DIGITAL LITERACY

Rob Entwistle states that the broader public may not need a more detailed digital literacy, but for the communities who are engaged in the implementation of the smart cities plan such as government institutions, the business sector, universities, the tech industry, and other stakeholders. Entwistle explains that for the general public, the residents want to know how the smart city plan benefits them then going into detail how it works in a digital framework. Entwistle argues that the objective of the smarter cities approach is to work more collaboratively together. For instance, when Kelowna was designing their smart city plan, the city consulted with the public on what kind of projects the communities envision for the smart cities approach.

Moreover, there were workshops with industries, businesses, educators, and other sectors to understand problems in Kelowna and what kind of solutions would be possible to implement. Entwistle gave an example in Kelowna downtown, where there is an Okanagan Innovation Centre to bridge different stakeholders to collaborate. The Okanagan Innovation Centre has been partnering with the City of Kelowna and other start-up companies to collaborate and implement projects that benefit the community.

Entwistle agrees that there is a need to have more digital literacy training for public servants to implement the smart city plan in municipal government. One of the purposes of the smart cities approach is to improve services for the public, especially customer service delivery. Entwistle argues that currently, the residents

go to city hall to get this service and go to the provincial government to get that services, but it would be more efficient to provide cohesive services for the residents. To achieve this, it all starts with collaborating with different stakeholders and re-thinking how to do things. Entwistle supports the idea to have digital literacy training for public servants taught by both IT industries and universities to ensure city employees to understand digital service delivery.

5.6.1.2 Resources

Municipal governments tend to have limited resources to use to deliver services for residents. Entwistle argues that the collaboration between the city and stakeholders would provide many benefits such as increased resources to implement municipal services for residents. Before the municipal government would tax people to generate revenue than have a budget to engage with the service provided. However, the approach now is to collaborate with different stakeholders to identify the problem and figure out how to share a budget across various jurisdictions such as health, education, and the private sector to try to resolve problems. Entwistle clarifies municipalities do have limited resource, but municipalities also have strong resources in base funding and human capital. Entwistle recognizes municipalities have limited resources and to address this issue; municipalities will analyze all the priorities and act on the higher priorities. It is best for collaboration between different stakeholders, then individual institutions trying to resolve the issue individually because it would be more cost-effective. Entwistle explains that municipalities do share data, but now, many government data are available through Open Data for other governments to use. Moreover, municipalities not only share data, but they also share best practices through MISA Canada, a platform to share ideas at the municipal level.

Entwistle states that when it comes to collaboration and data sharing, discussion on data ownership is agreed upon early on before the implementation of the project. To decide who owns the data, it may be determined based on who benefits from the data. For example, Entwistle explains if citizens movement is collected as data, then the data is owned by the citizens and not the municipality or the vendors that supply the technology.

Data Privacy Tools

The primary data privacy tool the Kelowna is using is the Privacy Impact Assessment (PIA). Also, Entwistle states that Kelowna tries to keep data within Canada as well and not in a data centre located outside of Canada. Furthermore, more sensitive data would not be published on Open Data. Entwistle gave a bike sharing data example of information that should not be on Open Data. The data on bike share in Kelowna was not published on Open Data because there was too many detail information. Even though the information is anonymized, it still shows the personal information of the cyclist, such as where they live and where they travel.

Top 5 Challenges

Entwistle states the top five challenges to implement the smart cities approach are:

1.) Awareness in municipal government wanting to collaborate with the community
2.) Developing a collaborative culture beyond the municipality, but collaborating with the community more
3.) Limited resources – Prioritizing projects with multiple stakeholders and community members
4.) Changing culture of the workforce – Training

5.) Smart cities bandwagon: To identify which tech vendors are helping the community and which tech vendor just want to make a huge profit without considering what the community needs.

VANCOUVER

DIGITAL LITERACY

Adcock explains that smart cities are changing the business model, moving from paper-based manual processes to data-based processes. Adcock claims that the shift has already been made in other sectors such as banking and retail. As technology is transforming cities, cities are starting to transform their service delivery to the public, according to Adcock. Adcock argues that municipal service delivery will never be the same maturity as Amazon.

Adcock argues that there needs to be an equitable amount of digital literacy for the community because some people may still not have internet access, struggling with accessibility and disability, and not having access to tools to connect to the internet. Adcock supports digital literacy, but as a society, it needs to be aware of digital equity as well because if digital equity is not in mind, it may make the digital divide a lot worse.

Adcock explains that the "smart governance" would be different depending on the city, the country, the project, and the program the government is implementing. Moreover, Adcock explains that there are many factors of designing a different "smart governance" such as what technology is being used, what technology the government has, and what kind of budget the government have as well. Adcock argues that there is no one sides fits all "smart governance" or a universal governance model. Nonetheless, Adcock agrees that investing in people in skill set who can understand and have the competency to implement the smart cities projects would be very beneficial. Additionally, Adcock discusses the importance of having people with different skills set other than specific knowledge about "smart cities," such as understanding planning and engineering. Different skills set in the municipal government would contribute to a variety of government services for the public.

RESOURCES

Adcock also agrees with limited resources in municipal government is a challenge, but the municipal government needs to categorize their top priorities and act on the top priorities. Adcock recognizes it is impossible to digitalized or deploy technology in all government services to the public because of scarce resources in the government. Adcock suggests resolving this scarce resource problem in government; the government needs a strong business model for business case analysis to understand where to deploy the resources. Also, having "smart decision making." You are only able to do the top priorities. It is impossible to digitalized or deploy technology in support of all services. You never have the luxury for doing that. Challenging is the older ways of doing things. Need a strong business model for business case analysis to understand where to deploy the resources. It requires "smart governance" or "smart decision making" and a real appreciation of priorities and business case.

DATA PRIVACY TOOL

Adcock discusses the City of Vancouver uses the Privacy Impact Assessment (PIA) to assess the privacy impact in all their smart city projects, including non-technology based projects as well. The PIA used in Vancouver is laid out by the Office of the Information and Privacy Commissioner (OIPC) for British

Columbia (BC). Adcock states that the City of Vancouver has completed a preliminary PIA even before selecting the projects for their smart city plan, and the Federal government set this requirement in the Smart Cities Challenge. Adcock clarifies that PIA is the primary tool for assessing privacy impact in their smart city plan, but it is open to using other data privacy and security tools for more complex smart city projects if implemented in the future.

TOP 5 CHALLENGES

Adcock's top five challenges to the implementation of the smart cities approach are:

1.) Budget funding
2.) Privacy
3.) Cybersecurity
4.) Skills (workforce to implement the projects)
5.) Resources

The two interviews with two experts from Kelowna and Vancouver offer a local government perspective, which is vital to know to develop recommendations that could be helpful to municipalities. Both interviewees provided great insight when it comes to digital literacy, resources, security, and privacy. By understanding the challenges, municipalities face when implementing a smart cities approach, other levels of government could help ease the problems as an example of giving more resources to the municipality. It is excellent to know that municipalities are thinking about privacy and cybersecurity concerns because those issues are one of the most alarming. However, data ethics and democracy are not raised in both municipal interviews as the top five challenges to implement the smart cities approach in their communities. Since there are many high priorities municipalities need to address, it seems they are more focused on administration function challenges in implementing the smart city projects.

Table 4: Summary of Literature Review, Case Studies, and Interviews

What is known	What is unknown	Case Study	Interview
Privacy Laws and Regulations in Canada Privacy laws and regulation would regulate collecting, using, and disclosing data PIPEDA regulates private companies' data collection and use of data	Is the privacy laws and regulations in Canada keeping up with the development of smart city projects in communities? What jurisdiction's privacy laws and regulations would be in play for smart city projects?	N/A	Scassa recommends PIPEDA to be reformed Scassa states that depending on what the smart city project is, it would be under different jurisdiction: municipal, provincial, and federal
Data Ownership Collaboration between municipal government and private sector on data collection and use of data Data ownership is an important component to clearly define before collecting and using data Some private companies may want to own the collected data on other activities	Are municipalities thinking about data ownership? Who should own the data? What are the challenges with owning the data?	N/A	Data ownership is talk about in Vancouver and Kelowna smart city projects Scassa states that sometime private companies would charge cheaper if private companies to own part of the data. Municipalities may be tempted because they have limited resources Kelowna: it depends on what the smart city projects is and who should own it (municipal, citizens, or private companies)
Smart Governance Data collected from IoT are used to make better decisions Data collected assess by AI and machine learning 5 operational area to improve administrative operation (smart governance)	What types of smart governance is there? How is having "smart governance" beneficial? Do Canadian municipalities share best practice with each other?	Estonia: Effective and efficient digital services by centralized majority of government services Somerville: Use data and technologies to make public engagement more inclusive. Focus more on citizen-centric approaches to smart cities	Both Vancouver and Kelowna only implement top prioritize projects because of limited resources Adcock (Vancouver): no one size fits all smart governance Entwistle (Kelowna), municipalities use MISA Canada, a platform for municipalities to share smart practices on information and communication technology (ICT) related issues.
Data Ethics Consent is not clear Data biases Discriminatory data set	How to protect individual privacy? Is there any technology to protect privacy while collecting the data?	N/A	Fung: Using Privacy Enhancing Technologies (PET) to protect privacy. However, it is a trade-off between privacy requirements and data accuracy.

Checklist to mitigate unethical data collection and unethical use of data Include data ethics course in Computer Science program	What are some methods to address data ethics? Is digital literacy to address data ethics? Is having digital literacy for the public and public service a good tool to address data ethics issues?		Fung, Millar, and Kerschbaum argue that PET and differential privacy are good tools to protect privacy Millar: It is not whether the municipality uses PET or not to protect privacy. The question is in the ethics lens, "Should municipality collect that data?" Millar recommends to Municipality if they are using automated decision technologies such as AI and machine learning to assess the data collected, it would be wise to use Algorithmic Impact Assessment (AIA) and Canada's Directive on Automated Decision-Making
Data Sovereignty Internet of Things (IoT): data flow through the internet Keep data stored and flow within Canada border Data flow outside or stored outside, foreign intelligence agency can access the data. (surveillance)	In the context of smart city, how data sovereignty plays a role?	N/A	Clement explains that when Internet of Things (IoT) collects data, the data flows into the Internet system where it could flow outside the Canadian border to the US and come back in to Canada later. Clement also recommends data should be stored within the Canadian borders because once it is outside the border it is no longer under the protection of the Canadian government.
Cybersecurity Cybersecurity life cycle for municipalities implementing the smart cities approach	How to protect data system from cyberattacks? How to set up a good cybersecurity plan?	Estonia uses Blockchain technology to detect cyberattacks or recover data if it gets a massive cyberattack or natural disaster	Kerschbaum recommends implementing: A Security Plan, and Privacy Impact Assessment (PIA) as part of municipalities' cybersecurity strategy

			Kerschbaum argues that implementing Estonia's Blockchain
Municipal Resources Municipal limited resource Digital literacy	What are the top 5 challenge issues? Are municipalities ready for cybersecurity? Is digital literacy the way to address data collection and use of data issues? What data privacy tools are municipalities using?	N/A	Both Vancouver and Kelowna use the Privacy Impact Assessment (PIA) as part of the requirement from the Smart Cities Challenge Both Vancouver and Kelowna share two similar top 5 challenges: limited resources and skill sets

All the interviewees provided valuable insight and different perspectives on an interdisciplinary public policy. The smart cities approach is an interdisciplinary public policy where different skill sets are needed at the table to address challenges and concerns. The focus on collecting, using, and disclosing data in a smart city approach touches different challenges from data ownership to data privacy laws to cybersecurity of the data system. There are different kinds of smart cities approach. The case studies show different municipality or country can focus on different ways of using data and technologies to provide services for their residents. Furthermore, both case studies focus on "smart governance," and there are different "smart governance" approaches. The "smart governance" section in the literature review gives possible recommendations for municipalities to implement "smart governance" while the two case studies provide real-life examples of how it is achieved.

Nevertheless, both the case studies and literature reviews do not provide enough information about cybersecurity issues and ways to protect privacy and security. Since cybersecurity is in the computer science field, it was crucial to interview experts in computer science. There are little journal articles on smart cities that discuss cybersecurity because there is little collaboration between social science experts and computer science experts. This research brings together social science experts, computer sciences experts, and municipal public servants on the implication of data collection and use of data in the smart cities approach.

The journal articles collected for the literature review section have little to no cybersecurity strategy to address privacy and security concerns because the collaboration between social science experts and computer science experts are very low. Also, both case studies did not provide feasible recommendations on how to protect the privacy and security in their data system. The interviews complement and challenge the two case studies on cybersecurity, which helps to understand what are the options to protect data or detect cyber attacks other than Blockchain. The Somerville case study did not include a cybersecurity strategy but only focus on the benefits of using technologies to make public engagement more inclusive and how improving administration operation can have positive outcomes and benefits to the residents. The

Estonia case study provided some security suggestions such as using Blockchain, but Estonia did not provide recommendations similar to Fung and Kerschbaum. For instance, having a Security Plan or using Privacy Enhancing Technologies. Kerschbaum questions the use of Blockchain as part of a security strategy because it does not adequately detect cyber attacks. Kerschaum recommends implementing a Security Plan, which includes a risk assessment and the Privacy Impact Assessment. Therefore, the interviews with Fung and Kerschbaum provided a very descriptive explanation of cybersecurity and privacy strategies that are not found in the literature review documents and the two case studies.

In the literature review section under privacy law, it outlines the privacy laws in Canada and the EU's GDPR. The interview with Scassa, a lawyer, specialized in information law, gave her professional experience and analysis on PIPEDA and GDPR. By reading the information on PIPEDA and GDPR in government, websites do not provide information such as how effective is the regulation and were in the regulation can be improved. Scassa provided useful information such as the penalty in PIPEDA is not effective enough to protect privacy. To implement the smart cities approach in municipalities, municipalities need to be aware of laws and regulations related to data and privacy.

Moreover, other experts have raised the suggestions by having stronger regulation to protect the privacy and security because the current privacy and data regulation is not doing enough. Most experts believe regulations and laws are the keys to hold tech companies and governments accountable to the public when it comes to what kind of data should be collected and how data can be protected. Also, Millar argues that it will be challenging to make everyone an "expert" in data and privacy because the big tech companies have a lot of resources to fight the consent arrangement and privacy requirements since the regulations are weak. Therefore, the reform of privacy regulations needs to be at the forefront of the implementation of smart city projects.

Both the case studies do not discuss privacy laws and regulations on data, but the literature review and the interview with Scassa contain the discussion of Canadian privacy laws and EU's GDPR. The interview with Scassa offered information about data and privacy in the context of the smart cities approach that was missing in the literature review documents. Scassa explains that to apply privacy laws and regulations on a smart city project may not be black and white because there are many components and unclear interpretations of the law.

The case study of Estonia focuses on "smart governance" and cybersecurity. The Somerville case study focuses on participatory "smart city" and smart governance. Some experts in the interview challenge some of the information from these case studies, while some experts agree and add on more details about the specific issue. For instance, Kerschbaum challenges the effectiveness of using Blockchain in the context of protecting or detecting cyber attacks. Nonetheless, the interview with municipal experts, Adcock, and Entwistle both discuss the importance of engaging with the public and being as inclusive as possible. It is similar to how Somerville's smart governance operates where civic engagement is at the core of smart governance.

The two case studies provide an excellent example of how "smart governance" can achieve and what kind of outcome it can bring to residents. On the other hand, the two case studies did not provide or discuss data ethics or data ownership and the other key themes discussed in this research. Since Somerville put civic

engagement as an important component to smart governance, but it did not expand the idea of a possible democratic threat from smart city project that Wylie discussed the Toronto Waterfront Project.

The seven interviews contributed greatly to this research because they provided expertise in their field and interconnect some of the key themes discussed throughout this research. Some of the findings from the interviews were very interesting. For example, both of the municipal experts, Adcock and Entwistle did not have data ethics issues or democracy challenges or transparency as one of the top five challenges with implementing the smart cities approach. Both experts are focus on the lack of skill sets needed to implement smart city projects. Nonetheless, it is good that both Adcock and Entwistle agreed that inclusivity is important in the implementation of smart city projects. It is also good to hear that Adcock voiced that privacy issues and cybersecurity issues are also part of the top five challenges to implementing the smart cities approach. When it came to discussing cybersecurity issues in the interview sections, it gave a general understanding of what technologies could be used to protect data. However, the experts did not go too much in detail because of the complexity of explaining the technical issue to someone who does not have a strong background in computer science. Nevertheless, the cybersecurity and data ethics component of the interviews provided information that was not discussed in many social science journal articles on smart cities. Overall, the literature review, case studies, and interviews comprise a holistic understanding, and discussion around the implication of data collection and use of data in the smart cities approach.

6.0 Discussion and Analysis

6.1 SWOT Analysis

It would be valuable to apply the SWOT analysis in this research because it structures the research into the four categories: Strengths, Weaknesses, Opportunities, and Threats. This discussion and analysis section will comprise of the SWOT analysis and a summary of key themes of the discussion raised in previous sections. There are many implications of data collection and the use of data in the smart cities approach because of the challenges such as privacy and security, which affect citizens, businesses, and the civil society as a whole (Sali, 'Web of data' collected by smart city tech stokes privacy fear). The research discusses key themes such as "smart governance," privacy laws, data ethics, data infrastructure, cybersecurity, and municipal resources because these key themes outline the implication of data collection and use of data in the smart cities approach. The citizens receive many benefits, such as digital services.

On the other hand, the citizens are at a disadvantage if the smart city projects are designed and implemented poorly due to violating unethical data collection or weak cybersecurity strategy. Data ethics, data ownership, data sovereignty, and cybersecurity are significant issues that affect citizens the most because it affects their privacy and sense of security. If data are not collected and used ethically, it can severely harm citizens because programs created by these data could disadvantage marginalized citizens. Moreover, if the data system processing the data contain certain biases, it will most likely hurt marginalized people the most. Even the process involving what data to collect and deciding who gets to decide what data to collect needs to be done with transparency and accountability. There are many complex issues and questions when it comes to using and collecting data in a smart city approach. The discussion and analysis section along with other sections above will help to understand the recommendations to address the issues of collecting and using data in smart cities and how to protect citizens, businesses, and civil society as a whole.

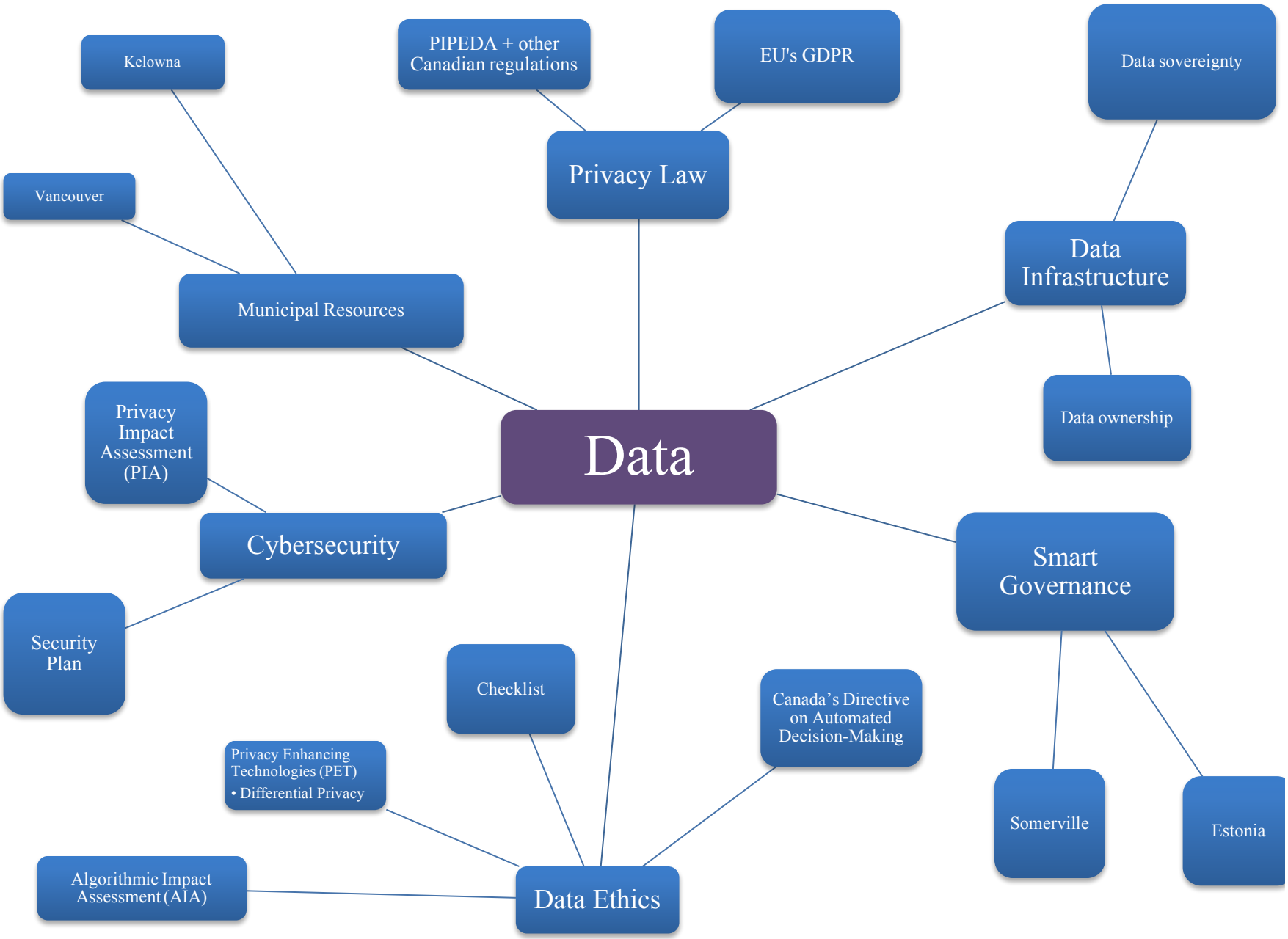
Table 5: The chart below outlines the SWOT analysis, including the key themes in this research

Strength	Weakness	Opportunity	Threat
What are the strength of data collection and the use of data? Increase efficiency Provide better services Increase innovation **[Sub-Question #3: benefit]**	What are the weakness of data collection and the use of data? Data biases Privacy issues Slow regulation/law development Limited resource to implement data-driven communities **[Sub-Question #2]**	What are the opportunities of data collection and the use of data? Smart governance Make better public policies Increase efficiency in government services for the public **[Sub-Questions #1]**	What are the threats of data collection and use of data? Cyberattacks Data breaching Ownership of data Data sovereignty Democracy (Urban Space and democratic governance)

			[Sub-Question #3: challenge/threat]

In the next page, it outlines the key themes in a cloud diagram to illustrate the research in a holistic approach.

Figure 1: Cloud Diagram of the Key Themes


Kelowna
PIPEDA + other Canadian regulations
EU's GDPR
Data sovereignty
Vancouver
Privacy Law
Data Infrastructure
Municipal Resources
Data ownership
Privacy Impact Assessment (PIA)
Data
Cybersecurity
Smart Governance
Security Plan
Checklist
Canada's Directive on Automated Decision-Making
Privacy Enhancing Technologies (PET)
• Differential Privacy
Somerville
Estonia
Algorithmic Impact Assessment (AIA)
Data Ethics

STRENGTHS

There are many strengths in using, collecting, and disclosing data in the smart cities approach. Some of the strengths are increasing efficiency in government operation (smart governance) and community functions such as autonomous vehicles, transit apps, shared bikes, environmental sensors, and other smart cities designs (City of Melbourne, 2018). By collecting, using, and disclosing data from the Internet of Things (IoT) and using advanced analytics to assess the data, it can help the government to provide better public services for citizens (Eggers and Shah, The government CDO: Turning public data to the public good, Deloitte Insights). The data collected can increase innovation in the public sector and private sector, similar to Estonia's experience of having data shared with the private sector and open data. Having more data implies more information for municipalities to analyze and develop better public policies and programs for residents.

The two case studies, Estonia and Somerville show that there are many benefits of "smart governance." Estonia's case study outlines that when the government provides digital services for residents, it can cut administrative costs and save time for both the government and the residents (e-Governance, e-Estonia). Moreover, Somerville's case study shows that a municipality can use technology to make public engagement more inclusive to those unable to attend the public discussions in-person (Okner & Preston, p.365). By improving public engagement, Somerville was able to develop projects that included diverse opinions (Okner & Preston, p.365). The City of Somerville restructured their administrative operation to break communication silos by having a team to integrate other teams who are designing and implementing smart city projects (Okner & Preston, p.352). Some smart governance strategies address the weaknesses of the smart cities approach when it comes to collecting, using, and disclosing data. For instance, how the administrative structure operates in the municipality to address communication silos, accountability, approval process, and other governmental administration. Having an excellent and functional administrative system is crucial because smart city projects are already very complex, so the process of decision-making, accountability, and other administrative functions are important for the design and implementation of smart city projects.

Smart governance is not only strength but also an opportunity for municipalities who are starting to design and implement smart city projects in their communities. The municipal interview with Entwistle shows that municipalities are sharing smart practices through organizations or networks. By having municipalities network with each other, it increases the flow of creativity and smart practices with each other so municipalities can learn from other municipalities' successful smart city projects and avoid or modify unsuccessful smart city projects. In the literature review section under smart governance, one of Blauer's recommendations was networks and how in the US there is a network called Civic Analytics Network for American municipalities to engage with each other by sharing ideas (Blauer, p.163). The strength of sharing ideas and smart practices with different municipalities provide many benefits. Data collection and use of data in the smart cities approach provide many benefits and opportunities, but also many weaknesses and threats.

WEAKNESSES

The smart cities approach on data collection, and the use of data contains many weaknesses that need to be understood in order to mitigate and create controls to address these weaknesses. The five major weaknesses

are data bias, unethical data collection, privacy issues, limited municipal resources, and the slow development of data and privacy regulations and laws.

As discussed in the literature review and interview on data ethics, it is essential to address data bias, and data ethics in the smart cities approach because if data are used to disadvantage certain groups, it fails the objective of a smart city. It will result in surveillance of the public, especially the disadvantaged groups. The data that is collected should not be used for giving more resources to affluent communities at the expense of underprivileged communities.

Obar and McPhail, in one of the literature review documents, focus on the dangers of data bias and data discrimination when using data to make decisions (Data Governance in the Digital Age: Special Report, 2018, p.57). When developing algorithms and using the smart cities method in communities, designers and programmers need to think about data discrimination and data bias. There can be conscious and unconscious data discrimination and data bias. For unconscious data discrimination and data bias in the smart cities approach, there should be an active response to the problem and the problem could be a lesson learned moment for all stakeholders collaborating with the community. Also, to create preventive measures, so in the future, this problem would not occur again. It is similar to a policy analyst designing a policy for a community to address an issue, but the policy design is not perfect. There is room for improvement, and the policy analyst keeps on improving the policy. Society keeps on changing and developing; the policy cannot stay still but needs to keep on changing and improving. For the algorithm data process, there will always be a need to improve and adapt to the current issues.

Moreover, the idea of what data should and should not be collected regardless of the data can protect individuals or group privacy using Privacy Enhancing Technologies (PET). The question is, is it is ethical to collect this information from this community and what is the harm of collecting these data from this community? It is challenging to draw the line on what is ethical and what is not ethical to collect data on. Not only is it challenging to draw the line, but it is even more challenging to collaborate and receive consent from most stakeholders on what to collect data or not. In the interview with Millar, he emphasizes that there should be a clear structure on the process of deciding what data to collect or not because it holds the people who made the decision accountable for it. Also, by having a clear structure on the process of deciding what data to collect or not, it helps revise the process. For instance, if the process does not include enough public engagements or lack of structure on who approved this smart city project. The discussion of data ethics in smart city projects would take some time for the municipality to create a strategic plan on which type of data collection it wants to collect in their smart city projects.

When discussing data ethics on data collection and use of data, the topic of consent is discussed. In the interview with Fung, he mentions that consent tends to be unclear and vague, and that could impact the privacy protection for individuals' data being collected and used. On the other hand, Fung understands why the consent is ambiguous because sometimes, data analysts do not know what data collected are useful, so data analysts want to collect as much data as possible. In a few of the literature review documents, other authors have raised the issue of unclear and vague consents. Some argue that it is unethical to have ambiguous and ambiguous consent because if the individual or group does not understand what they are consenting to, it defeats the whole purpose to have consented. It is essential that municipalities address unclear and vague consent when implementing data-related smart city projects in their communities.

In addition to this, the development of privacy and data laws and regulations are not keeping up with technological progress. In the interview with Scassa, she talked about how there are many "grey areas" to interpret the privacy and data laws with the current technological advancement and smart city projects. Furthermore, Scassa discusses the challenge of which privacy laws and regulations, each smart city project is under because depending on what the project is, it may fall under federal, or provincial, or municipal jurisdiction. Scassa also states that sometimes data collection and use of data could be a mixture of two jurisdictions. Scassa recommends reforming PIPEDA, the federal privacy law by having a stronger penalty to protect individual privacy because the current penalty is not strong enough to reduce privacy violations from private companies. If a privacy policy, regulation, or law does not have the mechanism to prevent companies and governments not to collect and use data in an unethical way, it will cause poor decision-making when it comes to policies and programs for the community. Scassa argues that it is not effective to have a privacy regulation or law that has a weak penalty if companies violate the rules because companies would pay up the small fine since it does not hurt their bottom line to do so. On the other hand, Scassa explains the penalty cannot be too high because small start-up companies would not be able to compete with the big tech companies for those smart city project contracts. The penalty will need to be strong enough to deliver better privacy protection for the public, but the penalty cannot be too overpowering that it disadvantages market competition.

However, for any changes in laws and regulations, it needs the political will to push the agenda forward. Many experts in my interview advocate for better laws and regulations to manage the data collection and use of data in smart city projects because that is the most effective way to protect individual privacy. Fung argues that municipalities are not using privacy enhancing technologies (PET) to protect privacy because many companies do not have the incentive or the mandatory requirement to use PET due to the high cost of using these technologies. Fung recommends that regulations that require the usage of PET in smart city projects would help increase individual privacy. Thus, the reform of privacy laws and regulations are a crucial component for a successful implementation of data-related smart city projects.

Furthermore, municipalities tend to have a budget constraint, so the implementation of the smart cities approach would be costly, and some municipalities may not be able to afford it. Scassa explains with the limited resources that municipalities have, they may sign agreements with vendors who can provide a "cheaper" price for the smart technologies in return for partial data ownership. This may weaken the privacy protection for the public. In the interview with Entwistle, from Kelowna and Adcock from Vancouver discuss how municipalities do have a budget constraint, but their strategy is to pick the top priorities to work on. By working on high priorities, they can achieve some smart city projects while doing other smart city projects in later years when they have the budget to do so. The design and implementation of data-related smart city projects are a very long process and requires a well-thought-out strategy. It should not be designed and implemented as quickly as possible but set on a reasonable timeline for the design and implementation of these projects.

There are many smart cities marketing schemes, from what "smart" technologies to use to how to implement the smart cities approach that would provide the most benefits for communities. Clement argues that even putting the word "smart" in front of the word cities or governance or technology tend to be a marketing technique for the organization to sell a product to another organization. Two of the interviewees, Clement, and Kerschbaum both have raised the issue of marketing techniques from tech companies and other countries about how the tech companies and other countries sell the implementation of smart technologies

for increasing efficiency. This can be misleading for municipalities to implement the smart cities approach. However, in this paper, "smart governance" means using technology to make better decisions and improve administration function. Also, "the smart cities approach" in this paper means to use data and connected technologies to achieve beneficial outcomes for residents by having openness, integration, transferability, and collaboration as the main components to the smart cities approach. It is important for municipalities to be aware of the marketing scheme of smart cities and not just quickly jump on the bandwagon.

OPPORTUNITIES

The implementation of the smart cities approaches especially the data collection and use of data provides many opportunities for the municipalities. The two greatest opportunities would be "smart governance," this includes the increase of government administration efficiency through the use of technologies in government services to the public. In the previous section on Somerville's experience in "smart governance," it shows that it provides many opportunities for the municipal government to improve their public engagement with their residents (Okner & Preston, p.365). Moreover, residents of Somerville had the opportunity to participate in the development of city policies and programs (Okner & Preston, p.365). By using the data collected by smart technologies, policy analysts could design better public policies because of real-time data and a large amount of data being collected. It provides many opportunities for the government and the private sector to be more innovative in providing services that are helpful and cost-effective to the public as one sees with Estonia's experience and with Innisfil, Ontario, which Scassa discussed in the interview.

Estonia and Somerville are fascinating case studies for Canadian municipalities to learn best practices from. Both Estonia and Somerville focus on "smart governance" and how to use data to assist in decision-making and provide better digital services. In the interview with Millar, he recommended municipalities to implement Algorithmic Impact Assessment (AIA) and Canada's Directive on Automated Decision-Making to address automated decision-making technologies such as AI and machine learning. With the implementation of "smart governance," municipalities may use advanced analytics such as machine learning to make automated or part automated decision-making. It is important to assess automated decision-making with the AIA and use Canada's Directive on Automated Decision-Making as a guide.

Also, the EU's GDPR would be a good case study for the Canadian government to study the strengths and weaknesses of the regulation. One of the most effective government tools to address data and privacy issues using the smart cities approach is to have regulations and laws. According to Scassa, it is still too early to assess the limitations and weaknesses of the GDPR because it has only been implemented for a little over a year. It will take some time until there are enough of GDPR cases to assess the effectiveness of the regulation. Nevertheless, the implementation of GDPR has provided many benefits to other non-EU countries to have similar data privacy protection because companies who operate in the EU and in other non-EU countries tend to be consistent in their privacy protection plan by implementing the GDPR standard. This may give opportunities for Canada and other non-EU countries to reform their data privacy laws and regulations.

THREATS

There are many strengths and opportunities with data collection and use of data in the smart cities approach. Nevertheless, there are significant threats to the smart cities approach when it comes to collecting, using, and disclosing data. The top four threats on data collection and the use of data in smart cities are cyber

attacks, data breaching, ownership of data, and data sovereignty. To address cyber attacks and data breaching in the smart cities approach, municipalities would need to design their cybersecurity life cycle to minimize the threats. Municipalities would have many partnerships with vendors, who supply the smart technologies and they may want part ownership of the data collected. However, municipalities could sign contracts with vendors that state municipalities would have full ownership of the data collected. In the interview with Scassa discussed above, it is sometimes challenging for municipalities to have full ownership of the data collected.

On the other hand, Scassa clarifies that some smart city projects' data may not be 100 percent owned by the municipality or the residents. The example Scassa gave was Innisfil, an Ontario municipality who subsidized Uber to provide transportation services for their residents and this plan saved a lot of money for the municipality compared to purchasing buses and operating them. In this case, Uber would own these data collected in these rides. Smart city projects are challenging to decide on who owns the data. If data ownership is not clearly defined, the tech companies may reuse the data for other activities without the consent from the municipality or their residents.

Besides ownership of data, Clement discusses that data sovereignty is also a major threat for municipalities because with the use of Internet of Things (IoT) in communities the data collected would most likely flow outside the Canadian border to the US border in their Internet Exchange Points (IXPs). In the interview with Clement discussed above, data sovereignty is significant to data privacy. Clement explains that when data flow outside the Canadian border to the US border, the US intelligence agency can access the data collected. Depending on what kind of data is collected by the municipality, some of the information could be very sensitive. In the worst-case scenario, a foreign intelligence agency could use the data as a surveillance tool for Canadian municipalities.

Another major threat in privacy when it comes to the smart cities approach is linking multiple databases together. In the interview with Fung, he explains the dangers in linking databases together and how it can be easy to identify a person even when the data is anonymized. When municipalities implement the smart cities approach in their communities, they need to be aware and cautious when linking different databases together. Fung explains that one of the primary functions of the smart cities approach is to collect different kinds of data and link databases together to assist in policies and programs the municipal government wants to implement to address problems in their communities. Nevertheless, Fung mentions that there is a Privacy Enhancing Technology (PET) that can address the linkage of multiple databases and still protect some privacy. Fung states that it is costly to implement the PET to address the linking multiple databases issue. Therefore, Fung argues that putting the requirement to use PET in data-related smart city projects as a regulation mechanism could protect individual privacy in the case of linking multiple databases.

Throughout the design and implementation of the smart cities approach, municipalities need to think about the trade-offs between privacy and accuracy in collecting, using, and disclosing data, especially using PET in their smart city projects. Municipalities are already in a position of scarce resources, so implementing security plan and privacy controls may be costly for the municipality to implement. However, municipalities could collaborate with their provincial government and/or federal government to fund part of the total cost of implementing the security plan and privacy mitigation. Fung explains that it is impossible to achieve 100 percent privacy and security in the smart cities approach, but the municipality could mitigate the risk by putting in controls to reduce the threat. Thus, Kerschbaum argues that having a security plan in

the smart cities approach for municipalities would be beneficial for municipal governments to think about how they are going to protect people's privacy and data, but at the same time provide good services for the public to use.

These threats need to be addressed when municipalities are implementing the smart cities approach. However, these threats could be a good lesson learned for municipalities and may promote municipalities to share their lessons learned with other municipalities. In the recommendation section, there will be a few recommendations for municipalities to address these weaknesses and threats when it comes to using, collecting, and disclosing data in the smart cities approach. The recommendations in this paper would help assist addressing some of these challenges, such as protecting citizens privacy by building a robust security plan and use privacy enhancing technology.

7.0 Recommendations

Throughout the research, it shows the implementation of smart cities approach in the municipality especially in collecting, using and disclosing data is very complex, but there are many opportunities to use the data effectively and responsibly. The significant issues with the gathering, using, and disclosing data are privacy and cybersecurity concerns. Moreover, municipalities need to ensure effective and efficient governmental administration (smart governance) to implement the smart cities approach in their communities. There are ten recommendations to address privacy and cybersecurity issues when it comes to data collection and use of data in the smart cities approach. The table below outlines the hypothesis and questions where the data collected from literature review documents, case studies, and interviews shaped the ten recommendations.

Table 6: Linking Research Question to the Ten Recommendations

Research Question: What are the implication of data collection and the use of data in smart cities and how it affects citizens, businesses, and civil society as a whole?		
Hypothesis/Questions	Data collected	List of Recommendations
Sub-Question: What government tools and approaches can Canada learn from other countries when it comes to data collection and the use of data in smart cities?	Baluer's article on smart governance (5 recommendations) 2 Case studies, Estonia and Somerville Vinod Kumar's four types of smart governance model	Recommendation #1: Government administration ("Smart Governance")
Sub-Question: What are the benefits and problems of data collection and the use of data that the government needs to be aware of when implementing the smart city approach? (Address the problem in this recommendation)	Interview with Fung discussion of PET Interview with Millar, and Kerschbaum agree with using PET in smart city projects	Recommendation #2: Privacy Enhancing Technologies (PET)
Hypothesis: Blockchain would help protect the information, but not prevent getting the "digital fingerprint" of the information. Hypothesis: To update your cybersecurity continuously since technology evolves all the time	Interview with Kerschbaum: Security Plan, Privacy Impact Assessment (PIA)	Recommendation #3: Security Plan
Hypothesis: Canada's privacy law not sufficient in keeping up with technology development	Interview with Scassa Kitchin's Types of Privacy	Recommendation #4: Reform PIPEDA

when it comes to data collection and the use of data (data mining) Sub-Question: How does privacy policies impact smart cities data collection and the use of data?	Wylie's perspective on Toronto Waterfront Project	
Sub-Question: What are the benefits and problems of data collection and the use of data that the government needs to be aware of when implementing the smart city approach? (Address the problem in this recommendation)	Interview with Fung about privacy issues. Fung recommends Privacy by Design (PbD)	Recommendation #5: Privacy by Design (PbD)
Sub-Question: What are the benefits and problems of data collection and the use of data that the government needs to be aware of when implementing the smart city approach? (Address the problem in this recommendation)	Interview with Adcock, City of Vancouver, and Entwistle, City of Kelowna	Recommendation #6: Having a diverse skill sets
Hypothesis: Yes, increase digital literacy education for the public would create a more aware public on ethical issues in data collection and use of data Hypothesis: Yes, the public would need more digital literacy to take advantage of the smart cities approaches such as residents may use municipal apps to check the air quality, the traffic/traffic accidents, paying municipal bills, and so on. Hypothesis: Yes, public servants would need to increase their digital literacy in order to implement smart governance	Interview with Millar on digital literacy education Interview with Adcock and Entwistle	Recommendation #7: Invest in digital literacy
Hypothesis: To update your cybersecurity continuously since technology evolves all the time	Barik, Sengupta, and Mazumdar's Cybersecurity life cycle	Recommendation #8: cybersecurity life cycle
Sub-Question: What are the benefits and problems of data collection and the use of data that the government needs to be	Interview with Clement on data sovereignty	Recommendation #9: Keep data within the Canadian Borders

aware of when implementing the smart city approach? (Address the problem in this recommendation)		
Hypothesis: Yes, checklist would help to reduce unethical data collection and the use of data	Interview with Millar Loukides, Mason, and Patil's 5 C's and checklist Wylie's perspective on Toronto Waterfront Project	Recommendation #10: Data Ethics Guideline

7.1 Recommendation 1: Government administration ("Smart Governance")

The first recommendation is to ensure government administration function is prepared to implement the smart cities approach effectively and efficiently. Estonia's digital government and Blauer's article gave concrete examples and recommendations to improve governmental administration. When applying the smart cities approach, municipal departments need to break communication silos within their departments and other departments they collaborate with by having an integrating team to bridge other teams together similar to Somerville's SomerSTAT team. There needs to be a bureaucratic cultural change to construct a "safe space" for creativity and opportunity to experiment with new ideas because they may reduce the fear of workplace retaliation. Having a good data management system and performance management system would help the municipality to evaluate and analyze the data collected. Also, having a good data management system and performance management system it makes it more efficient and effective in sharing data within and outside the department.

Moreover, to have collaboration and sharing data, committee meetings should be structured similar to the Somerville committee meeting or Estonia's e-Cabinet meeting. Estonia's e-Cabinet meeting provides an excellent example of how to make a committee meeting in the municipal department more effective by using technology to reduce the committee meeting time yet have a concrete decision-making process. The committee meeting will have an agenda for each session where they are a proposed recommendation, and if all members of the committee agree with the advice, the advice would not need to be discussed in the committee meeting. The recommendations that have a disagreement will be discussed during the meeting. All recommendations by the committee will be recorded and signed for approval. Therefore, there will be clear transparency and accountability in who approved the recommendation. It is essential to have clear evidence in who approved the decisions and recommendations to ensure accountability and a tool to improve administration function. Furthermore, in each municipal department committee meeting, they can have a few members from the data team to attend the meeting to assist in the data and how that decision is backed up with the data collected similar to Somerville's committee meetings.

In addition, municipal governments can use technologies to improve their interaction or engagement with their residents comparable to the City of Somerville. In the smart cities context, technologies are not just for collecting, using, and disclosing data, but to become more inclusive and accessible for residents to participate in what kind of smart city projects are important to their community. The municipality can

collect a lot of data from public engagement with residents, that may be challenging to collect by placing IoT across the communities. It makes the process of developing smart city design more democratic when municipalities include residents' perspective.

Key Considerations

To implement smart governance there would be a need to invest in technology where it could be very costly for municipalities to purchase especially for the medium to small sized municipalities. To implement smart governance would be beneficial for all level of governments. This recommendation promotes municipalities to use technology to engage with a wider public who normally cannot attend the public consultation in person, yet still keep having public engagement in person for those who do not use many technology in their daily life.

7.2 Recommendation 2: Privacy Enhancing Technologies (PET)

The second recommendation is to use Privacy Enhancing Technologies (PET) when collecting, using, and disclosing data. When municipal governments are using PET, it should have computer science experts who understand how to use PET in the smart cities context. The PET could help mitigate privacy concerns when municipal governments are collecting more sensitive data. Using PET, municipalities need to decide the trade-off between privacy requirements and the accuracy of the data. It is impossible to get 100 percent high privacy and high accuracy. The municipality needs to find a balance between the top priority privacy requirements and the level of accuracy they need.

Key Considerations

For municipalities to implement PET, it would be challenging due to the high cost of the technology. Since municipalities especially the small to medium sized municipalities have limited funding and resources, it might be impossible to implement this technology based on their financial resource.

7.3 Recommendation 3: Security Plan

The third recommendation is to have a Security Plan to address cybersecurity issues. By having a Security Plan that contains the seven components: Policy, current state, requirements, recommended controls, accountability, timetable, and continuing attention, it would provide structure for the organization to handle any cybersecurity issues. The Security Plan is a constant working process because the development of technology and societies are not static.

Key Considerations

To implement a Security Plan, it would be challenging for some municipalities especially the ones with less financial resource and inability to attract high skilled workforce (eg: data scientist and cyber experts) to work for their government. For medium to small municipalities who are unable to attract and afford to employed a high skilled employee with computer science background may be more vulnerable for cyberattacks or unable to implement a successful Security Plan. To implement the Security Plan would be costly and there may be some municipalities who cannot afford it.

7.4 Recommendation 4: Reform PIPEDA

The fourth recommendation is to reform PIPEDA to ensure stronger enforcement such as stronger penalties when companies violate privacy requirements. Also, to have stronger incentives and regulations on collecting, using, and ethically disclosing data. Depending on what the smart city project is the data privacy laws under different jurisdictions (Federal jurisdiction or Provincial jurisdiction or Municipal jurisdiction). To reform the PIPEDA, it may be helpful to study the EU's GDPR to see if there are any components in the regulation could be implemented in Canada. It is crucial to have effective regulations to regulate collecting, using, and disclosing data in all smart city projects because that is the most effective way to protect individuals' privacy.

Key Considerations

To reform PIPEDA, it would require political will at the Federal level and privacy experts to successfully amend the Act. Also, the process to reform a legislation would take a substantial time and the regulation may not keep up with the technological development.

7.5 Recommendation 5: Privacy by Design (PbD)

The fifth recommendation is to have the Privacy by Design (PbD) in all smart city projects because it will ensure people working on the smart city projects to keep in mind the privacy components of all smart city projects. The PbD consist of seven principles to guide the smart city projects from design to implementation.

Key Considerations

To implement a Privacy by Design (PbD), it would be challenging for some municipalities especially the ones with less financial resource and inability to attract high skilled workforce (eg: data scientist and cyber experts) to work for their government.

7.6 Recommendation 6: Having a diverse skill sets

The sixth recommendation is to ensure diverse skill sets in the municipal government when designing and implementing the smart cities approach. It is crucial to have a team with various skill sets from computer science to program implementation to privacy law because the smart cities approach is interdisciplinary work that requires many different skill sets. Since the design and implementation process of the smart cities approach is still a very new public policy there are many unanswered challenges. Therefore, having a team with diverse skill sets will help develop tangible solutions to problems.

Key Considerations

For bigger municipalities such as Toronto, Montreal, and Vancouver may be easier to attract a diverse workforce with multi-disciplinary skill sets, but it would be very challenging for medium to small municipalities to attract these workers.

7.7 Recommendation 7: Invest in digital literacy

The seventh recommendation is to invest in digital literacy for the public and the public service. As technology processes, it is necessary for the public and the civil service to keep up with technological advancement. There should be appropriate digital literacy training for the public service to implement the smart city projects across their communities and improve or make the governmental administration process "smarter." This is important since most people in civil service experienced fast-growing technological change and may not have the digital skill sets needed to implement smart city projects. Moreover, they must ensure the delivery of digital literacy for the public to be equitable across the different socio-economic background, gender, age, special needs, sexual orientation, visible minorities, and Indigenous communities. By having basic digital literacy training, the citizens can better inform their decisions and hold the government accountable.

Key Considerations

To invest in digital literacy for the public and the public service (all level of government) would be expensive. The provincial governments and the federal government in Canada would be able to afford to invest in digital literacy for their public service compared to municipal governments because municipal governments tend to have limited resources. Also, to invest in digital literacy for the public may be also challenging to achieve and may be very costly. To invest in digital literacy is not to make the public responsible to push the agenda for better privacy protection from tech companies, but to be able to question the municipal government and tech companies' smart city project proposal.

7.8 Recommendation 8: Cybersecurity Life Cycle

The eighth recommendation is to have the Cybersecurity Life Cycle in place for municipalities who are implementing the smart cities approach that contains a substantial data component to their smart city projects.

Key Considerations

To implement a Cybersecurity Life Cycle, it would be challenging for some municipalities especially the ones with less financial resource and inability to attract high skilled workforce (eg: data scientist and cyber experts) to work for their government. For medium to small municipalities who are unable to attract and afford to employed a high skilled employee with computer science background may be more vulnerable for cyberattacks or unable to implement a successful cybersecurity life cycle. To implement the Cybersecurity Life Cycle would be costly and there may be some municipalities who cannot afford it.

7.9 Recommendation 9: Keep data within the Canadian Borders

The ninth recommendation is to ensure data collected are stored and flow within the Canadian border. It is crucial for data to be in place within the Canadian borders because if the smart cities data is stored and flow outside the border, it is outside Canadian jurisdiction. This means the Canadian government cannot protect the data from being intercepted by a foreign Intelligence Agency when the data leaves the Canadian border through internet exchange points (IXP) or data stored in a data centre outside of Canada.

Key Considerations

To ensure data collection and flow of data to be kept within the Canadian borders would be challenging because it may involve many stakeholders especially telecommunication companies' collaboration to achieve it. This may be a long process and may take a substantial time to achieve.

7.10 Recommendation 10: Data Ethics Guideline

The tenth recommendation is to have a data ethics guideline that includes multiple checklists based on the type of smart city projects and an algorithmic impact assessment (AIA). Having a data ethics guideline that outlines the structure of decision-making on what data to collect or not and other data ethics concerns should be included in the data ethics guideline. The development of the data ethics guideline needs to incorporate diverse skill sets and inclusivity. It is essential to have the data ethics guideline aware of the data bias and data discrimination in data collection and use of data. The data ethics guideline needs to have some mitigation for reducing data bias and data discrimination. In addition to this, the guide ought to include these three questions raised by Obar and McPhail:

1.) Should we collect this data?
2.) What are the benefits and possible harm?
3.) Who does it benefit? (Data Governance in the Digital Age: Special Report, 2018, p.56-7)

Also, the data ethics guide should include Millar's suggestions on municipalities to think about these questions when municipalities agree to collect these data:

1.) How did the municipality get to that decision?
2.) Was it a fair process?
3.) Was the process transparent?
4.) Was the process democratic?
5.) Why was the process democratic?

Moreover, the guideline should include who is responsible for approval of each decision and the multiple checklists should include a signature in each approval step. This would make it clear on who is accountable for that decision and it is easier for auditors to audit the smart city projects. The municipality should use the algorithmic impact assessment (AIA) in data-related smart city projects where it uses automated decision-making technology to assess the data to make recommendations for the municipality. The AIA would assess the impact of using that algorithm in assessing and analyzing the data collected. In addition, the data ethics guideline should have a clear consent policy on how the consent should be, how to receive consent, and who should develop the consent.

Key Considerations

To have a well designed and implemented data ethics guideline would create a structure or standard for smart city projects. This recommendation would be the best to start for municipalities. To create a data ethics guideline would not cost as much as the other recommendations. However, municipalities would

need to hire public servants that have the knowledge of data ethics in the context of the smart cities approach.

8.0 Conclusion

There are many challenges and opportunities with data collection and use of data in the smart cities approach. The key themes discussed in this research provide many opportunities for municipalities to deliver better services for their residents. Nevertheless, there are many challenges and complexities for municipalities to address when implementing data-related smart city projects. The research looked at the challenges of data collection and use of data in the smart cities approach with a holistic framework where it covers key themes such as privacy law, data ethics, cybersecurity, data infrastructure (data sovereignty and data ownership), and municipal resources. The research analysis was structured in a SWOT analysis to outline the opportunities and challenges the municipality would encounter. The case studies and interviews provided great insight into the key themes discussed throughout this research. The case studies would inspire municipalities to implement a "smart governance" that focus on public engagement and administrative efficiency to handle smart city projects. The interviews provided information that was helpful to craft the ten recommendations. Each expert provided some recommendations to address a specific key challenge with data collection and use of data in the smart cities approach. Therefore, the ten recommendations discussed in the last section was developed by the literature review documents, case studies, and interviews to help mitigate or reduce these risks.

Since the implication of data collection and use of data in the smart cities approach is complex, the design and implementation process should be thoroughly considered at each step of the way. The implementation of smart city projects should not be rushed because of problems that may occur if data-related smart city projects are not planned out properly. The challenges of data collection and use of data in the smart cities approach seems frightening, but at the same time, it gives an amount of excitement to the possibilities municipalities can achieve with their residents. It is important to keep in mind the major harm that privacy concerns and cyber threats can have on a society. The approach to design and implement these smart city projects needs to have a democratic process, transparency, and accountability. Without these key elements, the smart city projects would not be supported by residents or produce the outcome the government wants. The smart cities approach is not a static one, it is always evolving, so the challenges and solutions need to be innovative and creative.

9.0 References

"About." Open Knowledge Foundation, okfn.org/about/.

"About." Sidewalk Toronto, Sidewalk Toronto, sidewalktoronto.ca/.

"Created by Cities, for Cities." World Council on City Data (WCCD), www.dataforcities.org/wccd.

Adler, L. (2015, August 31). The Urban Internet of Things. Retrieved February 10, 2019, from https://datasmart.ash.harvard.edu/news/article/the-urban-internet-of-things-727

Albrice, D. (2016). Current State Analysis. Retrieved 2019, from http://www.assetinsights.net/Glossary/G_Current_State_Analysis.html

Anderson, M. (2018, April 6). Facebook Privacy Scandal Explained. CTV News. Retrieved April 8, 2018, from https://www.ctvnews.ca/sci-tech/facebook-privacy-scandal-explained-1.3874533

Andrews, J. (2018, August 7). How the EU's new data laws will affect Smart City development. ITU News. Retrieved August 15, 2018, from https://news.itu.int/eu-gdpr-smart-cities/

ANZSOG (2018, April 3). Better Data the Key to Improving Indigenous Disadvantage: Professor Ian Anderson. Retrieved April 10, 2018, from https://www.anzsog.edu.au/resource-library/news-media/better-data-indigenous-disadvantage-ian-anderson

Barik, M. S., Sengupta, A., & Mazumdar, C. (2017). Managing the Cyber Security Life-Cycle of Smart Cities. Smart Cities: Foundations, Principles and Applications, 391-406. Retrieved July 12, 2018.

Benay, A. (2018). Government Digital: The Quest to Regain Public Trust. Toronto, ON: Dundurn Press.

Blauer, B. (2018). Building the data city of the future. The ANNALS of the American Academy of Political and Social Science, 675(1), 151-165. doi:10.1177/0002716217746359

Canadian Internet Registration Authority (n.d.). Canada's Internet Infrastructure: Made-in-Canada Internet Exchange Points (IXPs). Retrieved March 3, 2019, from https://cira.ca/canada%E2%80%99s-internet-infrastructure-made-canada-internet-exchange-points-ixps

Centre for Cities. (2014, May 29). Smart Cities. Retrieved May 15, 2019, from https://www.centreforcities.org/reader/smart-cities/what-is-a-smart-city/1-smart-cities-definitions/

Cheung, Rachel. "Smart cities: are we sleepwalking into a Big Brother future of constant surveillance in the name of improved efficiency and safety?" South China Morning Post, 15 Aug. 2018, https://www.scmp.com/lifestyle/article/2159810/smart-cities-are-we-sleepwalking-big-brother-future-constant-surveillance

City of Melbourne. (n.d.). Melbourne as a Smart City. Retrieved March 8, 2018, from https://www.melbourne.vic.gov.au/about-melbourne/melbourne-profile/smart-city/Pages/smart-city.aspx

CityStudio. (n.d.). About CityStudio Vancouver. Retrieved November 20, 2018, from https://www.citystudiovancouver.com/what-we-do/

Computer Security and Privacy: Module 1 Introduction to Computer Security and Privacy [PowerPoint]. (2019). Retrieved May, 2019, from https://crysp.uwaterloo.ca/courses/cs458/S19-material/Module1.pdf

Computer Security and Privacy: Module 7: Non-technical Aspects [PowerPoint]. (2019). Retrieved May, 2019, from https://crysp.uwaterloo.ca/courses/cs458/W19-material/Module7.pdf

Data Governance in the Digital Age: Special Report (pp. 1-125, Rep.). (2018). Waterloo, ON: Centre for International Governance Innovation. Retrieved November 5, 2018, from https://www.cigionline.org/sites/default/files/documents/Data Series Special Reportweb.pdf

Data-Smart City Solution. (2016, May 4). About the Civic Analytics Network: A Network of Leading Chief Data Officers. Ash Center for Democratic Governance and Innovation. Retrieved December 10, 2018, from https://datasmart.ash.harvard.edu/news/article/about-the-civic-analytics-network-826

Data-Smart City Solution. (n.d.). Our Mission. Ash Center for Democratic Governance and Innovation. Retrieved December 10, 2018, from https://datasmart.ash.harvard.edu/about/data-smart-city-solutions

Dropbox Business. (n.d.). Work better, safer, together. Retrieved January 16, 2019, from https://www.dropbox.com/business

E-Estonia (n.d.). Security and Safety. Retrieved June 15, 2018, from https://e-estonia.com/solutions/security-and-safety/

e-estonia. (n.d.). Business and Finance: e-tax. Retrieved March 15, 2018, from https://e-estonia.com/solutions/business-and-finance/e-tax/

E-Estonia. (n.d.). E-estonia. Retrieved June 15, 2018, from https://e-estonia.com/

e-estonia. (n.d.). e-governance. Retrieved March 15, 2018, from https://e-estonia.com/solutions/e-governance/

E-Estonia. (n.d.). Estonian Blockchain Technology. Retrieved June 15, 2018, from https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf

Eddy, Max. "How Companies Turn Your Data Into Money." PC Magazine, 10 Oct. 2018, www.pcmag.com/article/364152/how-companies-turn-your-data-into-money.

Estevez, Elsa, et al. "Smart Sustainable Cities: Reconnaissance Study." International Development Research Center (IDRC), www.idrc.ca/sites/default/files/sp/Documents EN/smart-cities-report.pdf.

Estonia's Ministry of Economic Affairs and Communication. (2018). Digital Agenda 2020 for Estonia (Rep.). Retrieved September 15, 2018, from Ministry of Economic Affairs and Communication website: https://www.mkm.ee/sites/default/files/digital_agenda_2020_estonia_engf.pdf

European Commission. (n.d.) Data protection in the EU. Retrieved April 13, 2018, from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

European Commission. (n.d.). Smart Cities. Retrieved May 15, 2019, from https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en

European Commission. (n.d.). What does the General Data Protection Regulation (GDPR) govern?. Retrieved April 13, 2018, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

Getting to the Open Smart City (Rep.). (2018, October). Retrieved November, 2018, from https://futurecitiescanada.ca/downloads/2018/Getting_to_Open_Smart_City.pdf

Glaeser, Edward L., et al. "How Companies Can Use the Data They Collect to Further the Public Good." Harvard Business Review, 16 May 2018, hbr.org/2018/05/how-companies-can-use-the-data-they-collect-to-further-the-public-good.

Government of Canada. (2019). Directive on Automated Decision-Making. Retrieved May 22, 2019, from https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

Habib, Mamun, Bishwajit B. Pathik, and Hafsa Maryam. Research Methodology-Contemporary Practices: Guidelines for Academic Researchers. Cambridge Scholars Publishing, Newcastle upon Tyne, England, 2014.

Herlihy, P. (2013, March 31). 'Government as a data model': What I learned in Estonia. Retrieved March 10, 2018, from https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/

Impact Canada (n.d.). Process. Retrieved April 25, 2018, from https://impact.canada.ca/en/challenges/smart-cities/process

Impact Canada (n.d.). The Challenge. Retrieved April 25, 2018, from https://impact.canada.ca/en/challenges/smart-cities/challenge

Impact Canada. (November 2017). Smart Cities Challenge: Applicant Guide. Retrieved March 15, 2018, from https://impact.canada.ca/sites/default/files/2017-11/SCC_Applicant_Guide.pdf

Impact Canada. (November 2017). Smart Cities Finalist Guide. Retrieved March 15, 2018, from https://impact.canada.ca/en/challenges/smart-cities/finalist-guide

Infrastructure Canada, "Smart Cities Challenge: Spotlight on Finalists." Smart Cities Challenge: Spotlight on Finalists, June 2018. www.infrastructure.gc.ca/alt-format/pdf/cities-villes/spotlight-vedette-eng.pdf.

Invest in Estonia. (2017, June). Estonia to Open the World's First Data Embassy in Luxembourg. Retrieved June 15, 2018, from https://investinestonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/

Kitchin, R. (2016). The ethics of smart cities and urban science. Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences, 374(2083), 20160115. doi:10.1098/rsta.2016.0115

Levinson-King, Robin. “Google's 'Secret' Smart City on Toronto's Waterfront Sparks Row.” BBC News, 23 Mar. 2018, www.bbc.com/news/world-us-canada-43493936.

Life in the smart city. (2018). Retrieved June, 2019, from https://worldin2019.economist.com/lifeinthesmartcity

Loukides, M., Mason, H., & Patil, D. (2018). Ethics and Data Science (Rep.). O'Reilly Media. Retrieved November 20, 2018, from https://learning.oreilly.com/library/view/ethics-and-data/9781492043898/

McDonald, John. “The Internet of Things Requires Machine Leaning and AI.” Internet of Things Blog, IBM, 20 Mar. 2019, www.ibm.com/blogs/internet-of-things/iot-the-internet-of-things-requires-machine-learning/.

McKinsey Global Institute. (2018, June). Smart cities: Digital solutions for a more livable future (Rep.). Retrieved June, 2019, from McKinsey & Company website: https://www.mckinsey.com/~/media/mckinsey/industries/capital projects and infrastructure/our insights/smart cities digital solutions for a more livable future/mgi-smart-cities-full-report.ashx

Mendes, R., & Vilela, J. P. (2017). Privacy-preserving data mining: Methods, metrics, and applications. IEEE Access, 5, 10562-10582. doi:10.1109/ACCESS.2017.2706947

Mindtools. (n.d.). SWOT Analysis. Retrieved December 2018, from https://www.mindtools.com/pages/article/newTMC_05.htm

Ministry of Housing and Urban Affairs. (n.d.). What is Smart City. Retrieved May 15, 2019, from Government of India website: http://smartcities.gov.in/upload/uploadfiles/files/What%20is%20Smart%20City.pdf

Morgan, J. (2014, May 13). A Simple Explanation of 'The Internet of Things'. Forbes. Retrieved April 10, 2018, from https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#33344f581d09

“'Not Good Enough': Toronto Privacy Expert Resigns from Sidewalk Labs over Data Concerns.” CBC News, 21 Oct. 2018, www.cbc.ca/news/canada/toronto/ann-cavoukian-sidewalk-data-privacy-1.4872223.

Office of the Privacy Commissioner of Canada. (2018). Joint Letter to the Minister of Infrastructure and Communities on Smart Cities Challenge. Retrieved May 5, 2018, from https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/let_sc_180424/

Office of the Privacy Commissioner of Canada. (n.d.). Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada. Retrieved April 10, 2019, from https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_201103/

Office of the Privacy Commissioner of Canada. (n.d.). PIPEDA fair information principles. Retrieved March 10, 2018, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

Office of the Privacy Commissioner of Canada. (n.d.). PIPEDA in Brief. Retrieved March 10, 2018, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

Office of the Privacy Commissioner of Canada. (n.d.). PIPEDA legislation and related regulations. Retrieved March 10, 2018, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/

Office of the Privacy Commissioner of Canada. (n.d.). Privacy Impact Assessments: Frequently Asked Questions. Retrieved April 10, 2019, from https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/02_05_d_33/

Office of the Privacy Commissioner of Canada. (n.d.). Provincial legislation deemed substantially similar to PIPEDA. Retrieved March 10, 2018, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/

Office of the Privacy Commissioner of Canada. (n.d.). Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts. Retrieved March 10, 2018, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_26/

Office of the Privacy Commissioner of Canada. (n.d.). Summary of Privacy Laws in Canada. Retrieved March 10, 2018, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

Office of the Privacy Commissioner of Canada. (n.d.). The Privacy Act. Retrieved March 10, 2018, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/

Okner, T., & Preston, R. (2017). Smart Cities and the Symbiotic Relationship between Smart Governance and Citizen Engagement. Smart Cities: Foundations, Principles and Applications, 344-372. Retrieved July 12, 2018.

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in computing (Fifth ed.). Upper Saddle River, NJ: Prentice Hall.

Pringle, Ramona. "'Data Is the New Oil': Your Personal Information Is Now the World's Most Valuable Commodity" CBC News, 25 Aug. 2017, www.cbc.ca/news/technology/data-is-the-new-oil-1.4259677.

Privacy Act (n.d.). Department of Justice. Retrieved March 10, 2018, from https://laws-lois.justice.gc.ca/eng/acts/P-21/

Privacy by Design: Setting a new standard for privacy certification (Rep.). (n.d.). Retrieved April 25, 2019, from Deloitte website: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF

Ratti, C., & Claudel, M. (2016). The City of Tomorrow: Sensors, Networks, Hackers, and the Future of Urban Life. Yale University Press.

Reisman, D., Schultz, J., Crawford, K., & Whittaker, M. (2018, April). Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability (Rep.). Retrieved May, 2019, from AI Now website: https://ainowinstitute.org/aiareport2018.pdf

Rosic, Ameer. "What Is Blockchain Technology? A Step-by-Step Guide For Beginners." Blockgeeks, 2016, blockgeeks.com/guides/what-is-blockchain-technology/.

Sali, David. "'Web of Data' Collected by Smart City Tech Stokes Privacy Fears." Ottawa Business Journal, 19 Mar. 2019, obj.ca/article/web-data-collected-smart-city-tech-stokes-privacy-fears.

Scassa, Teresa. "Why Canada Needs a National Data Strategy." Policy Options, 15 Jan. 2019, policyoptions.irpp.org/magazines/january-2019/why-canada-needs-a-national-data-strategy/.

Sen, Rana, et al. "Building the Smart City with Data, Digital, and Design." Deloitte, Deloitte Center for Government Insight, www2.deloitte.com/us/en/pages/public-sector/articles/smart-city-big-data.html.

Shah, Sonal, and William D. Eggers. "The Government CDO: Turning Public Data to the Public Good." Deloitte Insight, 12 Oct. 2018, www2.deloitte.com/insights/us/en/industry/public-sector/chief-data-officer-government-playbook/government-cdo-turning-public-data-to-the-public-good.html

Statistics Canada. Population. (2018). Retrieved June, 2019, from https://www150.statcan.gc.ca/n1/pub/12-581-x/2018000/pop-eng.htm

Statistics Estonia. More births and smaller emigration increased the population figure. (2019, May 9). Retrieved June, 2019, from https://www.stat.ee/news-release-2019-053

Toronto Storeys. "Sidewalk Lab's Waterfront Project Under Fire From Industry Leaders." Toronto Storeys, 6 June 2019, torontostoreys.com/2019/06/sidewalk-labs-waterfront-project-privacy/.

Townsend, A. M. (2014). Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia. New York, N.Y.: W.W. Norton & Company.

U.K. Department for Business for Innovation & Skills. (2013, October). Smart Cities: Background Paper (Rep.). Retrieved May, 2019, from Department for Business Innovation & Skills website: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246019/bis-13-1209-smart-cities-background-paper-digital.pdf

Understanding the Internet of Things (IoT) (Rep.). (2014, July). Retrieved June, 2018, from GSM Association website: https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf

Vinod Kumar, T. M., and SpringerLink (Online service). E-Governance for Smart Cities. Springer Singapore, Singapore, 2015; 2014;, doi:10.1007/978-981-287-287-6.

Wylie, Bianca. "How to Build a Democratic Smart City." Centre for International Governance Innovation, 13 Aug. 2018, www.cigionline.org/multimedia/how-build-democratic-smart-city.

Wylie, Bianca. "Searching for the Smart City's Democratic Future." Centre for International Governance Innovation, 13 Aug. 2018, www.cigionline.org/articles/searching-smart-citys-democratic-future.

Zhou, S., Anderson, S., Gui, B., & Zhang, S. (2017). Smart Cities and Social Governance: Guide for Participatory Indicator Development (Rep.). Retrieved May 15, 2019, from UNDP China website: https://www.undp.org/content/dam/china/docs/Publications/Smart Cities and Social Governance-EN.pdf

Appendices

Appendix 1: Interview Questions – Law & Privacy

1.) How would you define individual privacy rights?

2.) Is Canada's privacy law sufficient in keeping up with technology development when it comes to collecting, using, and disclosure of data (data mining)?

3.) What are the benefits and limitations of the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA) when it comes to data collection, the use of data, and the disclosure of data in smart cities?

4.) Should Canada implement similar privacy law such as General Data Protection Regulation (GDPR) in the European Union (EU)?

5.) What are the benefits and limitations of GDPR?

6.) How would provincial/territorial and federal privacy law work in the implementation of the smart cities approach?

7.) How does privacy laws in Canada impact data collection and the use of data in the smart cities approach?

8.) What are some of recommendations or areas of improvement in privacy laws in Canada that could be improve?

Appendix 2: Interview Questions – Data Infrastructure (Data Sovereignty and Data Ownership)

1.) What are the advantage and disadvantage in centralizing the data system? Does centralize the data system makes it easier to hack the system?

2.) Is there a need to change government operation from traditional governance to smart governance?

3.) Why do governments tend to have challenges in updating technology in their institutions compared to the private sector?

4.) How to minimize unethical algorithms used in smart cities?

5.) Canada relies on the United States (US) internet infrastructure because many Canadians' data flow through the US internet infrastructure and cloud services.

a.) What are significant concerns for Canada when it comes to data sovereignty especially with the implementation of smart cities in Canadian municipalities?

b.) Is there any solutions or recommendations for Canada to become more independent or more control over the flow of the data on the internet?

Appendix 3: Interview Questions – Cybersecurity

1.) What are ways to minimize cyberattacks on data systems?

2.) The Estonian government uses Blockchain as a tool for their cybersecurity plan where it can detect cyber-attacks and identify any modifications of data in the system. Would using Blockchain be the best way to protect data?

3.) According to the article, "Managing the Cyber Security Life-Cycle of Smart Cities" by Mridul S. Barik, Anriban Sengupta, and Chandan Mazumdar: Cybersecurity life cycle consist of 8 steps: Scope and Cyber security policy formulation, Cyber security requirements identification, Risk management, Detailed security policy formulation, Security measures implementation, Cyber Security incident management & Service continuity management and disaster recovery, Cyber Security metrics generation, and Audit and compliance checking.

a.) Would a cybersecurity life cycle minimize cyberattacks and data breaching in the system?

b.) What are ways to build up the cybersecurity plan (e.g.: cybersecurity life cycle plan), so it would protect the data in the system?

4.) Would creating a checklist on what data can be collected and used and what data should not be collected and used help lower the unethical data collection and use of data in smart cities approach?

a. If creating a checklist is a good idea, who should be involve in creating the checklist? IT experts? Ethics experts? Policy Analysts? Program Analysts? Public consultation with the public?

b. If yes, should the checklist only be used for data scientists? Or should checklists be used for any teams who are involved with the implementation of the smart cities approach?

Appendix 4: Interview Questions – Data Ethics

1) How would you define unethical data collection and unethical use of data?

2) Would creating a checklist on what data can be collected and used and what data should not be collected and used help lower the unethical data collection and use of data in smart cities?

a.) If creating a checklist is a good idea, who should be involve in creating the checklist? IT experts? Ethics experts? Policy Analysts? Program Analysts? Public consultation with the public?

b.) If yes, should the checklist only be used for data scientists? Or should checklists be used for any teams who are involved with the implementation of the smart cities approach?

3) In general, the public are concern with institutions misuse of data being collected and used for unethical motives.

a. Should institutions draw a boundary in what data to collect, using, and disclose? Why or why not?

b. In the smart cities context, what are some feasible actions to minimize unethical data collection and use of data? Stronger regulations? More accountability?

4) By having more digital literacy education for the public, would it help keep institutions accountable and protect the public from unethical data collection and use of data?

5.) In the smart cities context, do you have any data ethics recommendations for municipalities to implement?

Appendix 5: Interview Questions – Municipal Resources

1.) Is there a need to have more digital literacy for the public to understand and take advantage of how the smart cities approach work?

2.) Is there a need to have professional development for public servants on digital literacy to implement smart governance?

3.) Municipal governments tend to have limited resources. What are the challenges with implementing the smart cities approach when the municipal government has scare resources? Does it affect the outcome the municipality sets out?

4.) What kind of data privacy tools is the municipal government using when implementing the smart cities approach? What are the mitigation measures for protecting privacy when collecting, using, and disclosing data?

5.) What are the top 5 challenges for municipal governments when they implement the smart cities approach?