Know Your Audience

How can public sector organizations ethically collect data on and about their publics?

MCM Capstone

Anthony Petrielli

Email: petriela@mcmaster.ca

Phone: 416-710-2684

Submitted to: Professor Dave Scholz, APR

Program: Master of Communications Management

Department of Communications Studies and Multimedia

Faculty of Humanities, McMaster University

Table of Contents

Abstract

Data collection is becoming a bigger part of people's and organization's everyday lives. Organizations are trying to find ways to better understand their publics by collecting data on them and making informed decisions through using this information, and public sector organizations are no different. As the race to collect and analyze data only expands, public sector organizations are trying to sort out how they too can collect and use this type of information to better serve their publics. Through a series of in-depth interviews with subject-matter experts and a general public survey, this capstone study examined how and to what extent public sector organizations can ethically collect data from their publics. This study puts forth a framework for ethical data collection that includes the entirety of the data lifecycle span and focuses on informed consent and transparency between organization and publics, data collection methods and a plan for the data once it is collected. Further research on educating publics and obtaining informed consent is recommended in order to build trust to advance data collection and usage practices.

Keywords: Data collection, trust, public sector organizations, organization-public relationships, government, informed consent, data lifecycle

Introduction

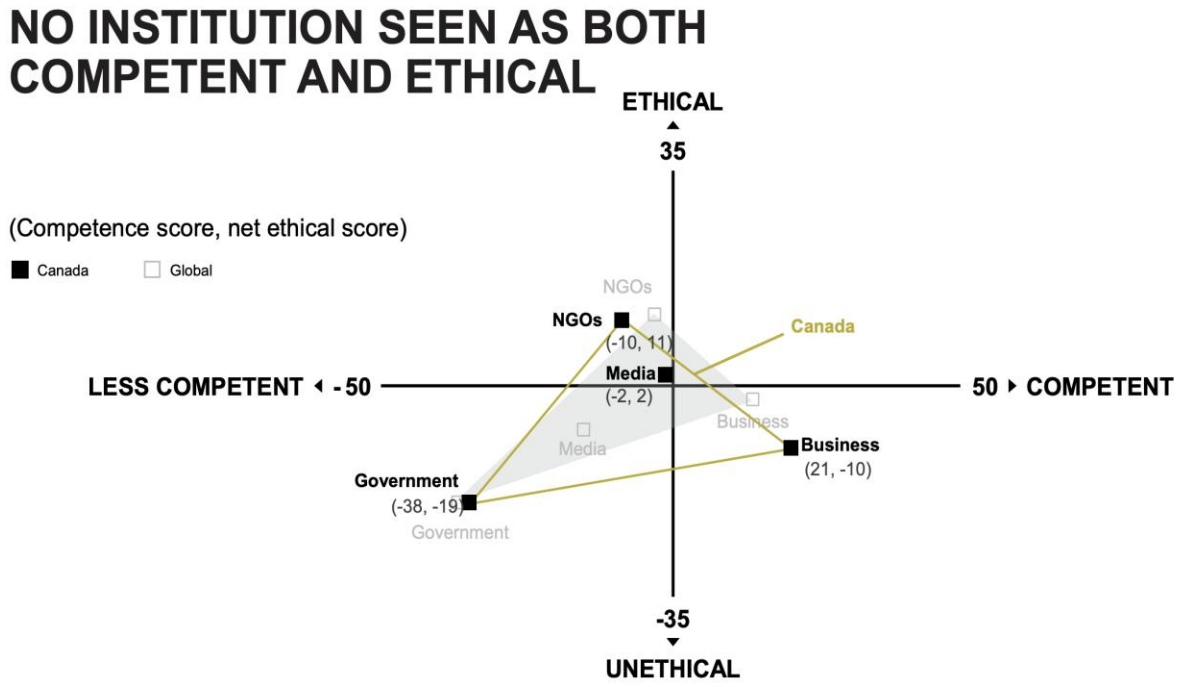
Public sector organizations are facing an issue the Canadian Minister of Digital Government, Scott Brison, succinctly described as, “We can’t have citizens feeling that Netflix understand their needs better than the government” (Greenwood, September 7, 2018). With the advancement of disruptive new technologies in recent years, there has been a considerable focus on collecting data and tailoring messages and information to specific audience groups in order to facilitate user engagement. An article in the Harvard Business Review noted, “In a future in which customer data will be a growing source of competitive advantage, gaining consumers’ confidence will be key” (Morey, Forbath and Schoop, 2015, para. 4). As data collection becomes more prevalent in the business landscape, “Companies that are transparent about the information they gather, give customers control of their personal data, and offer fair value in return for it will be trusted and will earn ongoing and even expanded access” (Morey, Forbath and Schoop, 2015, para. 4).

The idea of transparency and trust in data collection was supported by a study by the Office of the Privacy Commissioner of Canada that found the vast majority of Canadians are worried they are losing control of their personal information with 92 per cent expressing concern, and 55 per cent of Canadians indicating that they trust the government to respect their privacy (Office of the Privacy Commissioner of Canada, 2019). This is a critical time for government organizations, as Edelman’s Canada Trust Barometer 2020 found that government ranked last in trust among businesses, NGOs and media, by the mass population (2020 Edelman trust barometer, February 19, 2020).

Not only did government rank low in trust, but they also ranked low in ethics and competence across the board in Edelman's study (2020 Edelman trust barometer, February 19, 2020).

Figure 1

Trust is Built on Competence and Ethics



Note: Edelman Trust barometer

Similarly, 65 per cent of Edelman respondents believed government does not understand emerging technologies enough to regulate them effectively (2020 Edelman trust barometer, February 19, 2020).

In May of 2019, the Honourable Navdeep Bains, Minister of Innovation, Science and Economic Development, launched Canada's new Digital Charter. Bains stated that, "We are building a Canada where citizens have confidence that their data is safe and privacy is respected, unlocking the kind of innovation that builds a strong economy that works for everyone" (Innovation, Science and Economic Development Canada., May 21, 2019). From a public relations standpoint, this is a twofold issue of obtaining data to understand and segment their publics, and to ensure that data collection is being done properly so as to build and maintain trust with their audience. As Bains further noted, "Canadians' trust in the digital world is shaken. But in this new age, Canada's competitiveness will depend on our ability to use digital innovation to harness the power of data" (Innovation, Science and Economic Development Canada., May 21, 2019).

The Toronto Police Service (TPS), Canada's largest municipal police service, acknowledged in early 2020 that they "informally tested" a powerful data surveillance tool to collect information on citizens (Cardoso & Freeze, February 13, 2020). Facial recognition software is now regularly used by police services across Canada in limited capacities. The criticism that came from this latest information caused TPS to halt all use and contact Ontario's Information and Privacy Commissioner and the Ministry of the Attorney-General to review the technology. Michael McEvoy, British Colombia's privacy commissioner, said of this information that, "I think it is very questionable whether it would conform with Canadian law" (Allen & Gillis, February 20, 2020).

Canada's Digital Charter lists 10 principles that aim to provide the framework for continued Canadian leadership in the digital and data-driven economy. This charter is attempting to protect Canadians' privacy and personal data but also leverage Canada's unique talents and strengths in order to harness the power of digital and data transformation.

Brenda McPhail of the Canadian Civil Liberties Association said, "It sounds hyperbolic, it sounds dystopian — but the reality is that we live a lot of our lives online" (CBC News, February 14, 2020). This creates a number of data points and information that can be used by organizations, such as those in the public sector, to inform them on their publics. Ann Cavoukian, the executive director of the Global Privacy and Security by Design Centre stated, "More digital memories are going to be appearing and if we don't address these issues in terms of preventing non-consenting access to this data, we're going to lose the game" (Pringle, February 1, 2020).

Given the current climate, questions abound about data collection. How can public sector organizations ethically collect data? What methods should be used to collect data? What is the future of data collection? With the wealth of data that is now available for companies to utilize, it is important that companies are acting ethically in how they obtain this information on their publics. Due to how rapidly the landscape of technology and data has evolved, little research has been conducted on the ethical collection of data for public sector organizations.

Research Problem: Significance and importance of the study

This study seeks to understand how and to what extent can data be collected ethically by public sector organizations. Through this research, it also wants to examine how can public sector organizations understand their publics in a manner that meets their needs, protects their publics and follows legislation? As a new and emerging field, this area of research has yet to be properly explored creating an opportunity to establish an important case study in this field. This is a growing area of public interest, heightened by the incident with Facebook and Cambridge Analytica, and as evidenced by the development of Canada’s first ever Digital Charter, an area of interest that public sector organizations are and will be delving into further.

To properly examine this topic, the purpose of this study is to first, determine how public sector organizations can ethically collect data on their publics to make informed decisions. The second purpose of this study is to explore the legislation surrounding data collection on publics. The final purpose of this study is to understand how members of the public feel about their data being collected and how to build trust through this process.

This case study seeks to create a framework for public sector organizations to follow to create methods for ethical data collection. The findings will serve as a reference point to confirm appropriate ways for public sector organizations to collect information on their publics.

Literature Review

Data Collection in Canada and Surveillance States

In order to look at data collection, one must first define data and what is being collected. Merriam-Webster defines data as, "factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation" (Merriam Webster, 2019). When it comes to measuring and analyzing data, organizations often use data referred to as "'Big Data'. The most commonly used definition of Big Data was created by Gartner Inc., who stated, Big data "is high-volume, -velocity and -variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making" (Sicular, 2013, para. 3). When discussing data collection, it is important to keep these terms in mind, as the data being collected is factual information used as a basis for decision-making, and the datasets being collected are often Big Data.

Data collection and mining is described as, "a technique of using special software to sift through large databases in order to derive information that is implicit but not explicit in the data" (De George, 2011, p. 470). Data collection then serves as a means by which organizations can understand their audience(s), creating an opportunity to tailor messaging and advertising to specific segments.

Yuval Noah Harari gave Big Data the name, “Dataism” (Harari, 2016). One of the key components of Dataism is that, “we should willingly give all of the data pertaining to ourselves to Google and other tech companies because they will then know more about ourselves than we possibly can. They will therefore make ‘better’ decisions for us!” (Mitroff, 2019, p. 58). Data, then, can be described by some corners as a tool to create efficiencies and increase quality of life. Organizations, such as Google described here or in the case of this paper public sector organizations, can view data as a means by which to improve services to publics.

Data collection in Canada is governed by the Communications Security Establishment (CSE) whose mission is to, “To provide and protect information of national interest through leading-edge technology, in synergy with our partners” (Government of Canada, 2014, August 8). The mandate of the CSE is outlined in the National Defence Act and requires the CSE to do three things:

- to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
- to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada;
- to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. (Government of Canada, 2019, August 1).

However, the CSE is prohibited by law from targeting Canadians or anyone in Canada without a judicial warrant (Weston, 2014, January 31). In a general sense, data is protected through the

Canadian government and unless otherwise consented to, data collection does not happen other than for security purposes.

There are legislative Acts across Canada that cover specific data collection and use. For example, Ontario is governed by Freedom of Information and Protection of Privacy Act (FIPPA) and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) while Alberta is overseen by the Alberta's Freedom of Information and Protection of Privacy Act (FOIP). Further examples include Quebec’s Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information and British Colombia’s Freedom of Information and Protection of Privacy Act. These acts put rules and guidelines in place for data collection as well as a right of access to the information after it has been collected, which are consistent within each province, but not across the country of Canada as a whole. There is also the Privacy Act, which relates to information the Government of Canada collects and holds on people.

Ontario's privacy commissioner Ann Cavoukian says there has to be, "greater openness and transparency because without that there can be no accountability. This trust-me model that the government is advancing and Communications Security Establishment Canada is advancing – 'Oh just trust us, we're doing the right thing, don't worry' — yes, worry! We have very good reason to worry" (Weston, 2014, January 31). The question therein lies, what data is being collected and what is being done with it when it is?

While data is becoming increasingly available and collected, Giroux (2015) raises concerns of a “social order in which new surveillance technologies grant the state a degree of power unthinkable to past generations – exceeding in reach and complexity even the totalitarian state imagined in Orwell's dystopian account, 1984” (Giroux, 2015, p. 108). Surveillance in this sense is defined by Merriam-Webster as, “close watch kept over someone or something” (Merriam-Webster. (2019b); in the case of this paper, the close watch is public sector organizations over their publics.

As an example, the Ontario Government even acknowledges these concerns, noting that a risk of digital or e-Government is surveillance and loss of privacy. They implicitly state that, “Surveillance in public places, the home, and the workplaces can compromise individual’s right to privacy and can infringe on people’s ability to communicate, organize and associate freely” (Ontario Government, 2019, July 30, p. 7). In the United States, the Edward Snowden disclosures suggest strongly that, “Big Data practices are skewing surveillance even more towards a reliance on technological ‘solutions,’ and that this both privileges organizations, large and small, whether public or private, reinforces the shift in emphasis towards control rather than discipline and relies increasingly on predictive analytics to anticipate and pre-empt” (Lyon, 2014, p. 1). As datasets continue to grow and be collected, what organizations, particularly public sector organizations, are doing with this data is a question that will often arise. Lyon (2014) goes one step further by stating, “Big Data practices in consumer surveillance are (now literally!) co-travelers with those of state surveillance and together produce the kinds of outcomes around which ethical debates should now revolve” (p. 1).

Ethics

Ethics is defined as a, “systematic attempt to make sense of our individual and social moral experience, in such a way as to determine the rules that ought to govern human conduct, the values worth pursuing and the character traits deserving development in life” (De George, 2010, p. 13). Furthermore, “The virtue school stresses that to be ethical means possessing the right set of attributes, for example, honesty, trustworthiness, and strength of character" (Mitroff, 2019, p. 59).

Breaking down "ethics" further, there are three phases of ethical study to note and they are descriptive ethics, normative ethics and metaethics. Descriptive ethics, "consists of studying and describing the morality of a people, culture or society" (De George, 2010, p. 13). Normative ethics, "seeks to uncover, develop, and justify the basic moral principle or principles, or the basic moral values, of a moral system, found in a given society, and more generally and ideally in human society as a whole" (De George, 2010, p. 14). Metaethics, "is the study of normative ethics, and, to some extent, both normative and descriptive ethics involve some metaethical activity" (De George, 2010, p. 14).

Bowen's (2010) research led to a discussion of "authentic ethics" whereby the values that are enacted through organizational decision-making represent the core of the organization. Further work also indicates a link between ethical values and the authenticity of an organization (Bowen, et al., 2006). In essence, ethics guide a series of decisions that organizations make that their publics then judge them on to understand their values and authenticity. Mitroff (2019) notes, "the major schools of ethics in Western societies were formulated when ethics was principally a matter of the rightful conduct between a small number of individual actors or agents with clearly foreseeable benefits versus disbenefits" (p. 65). Due to the complexity of today's world, including technology, Mitroff (2019) states ethics, "requires the ability to see and to acknowledge the intended and unintended consequences of one's actions. In short, it requires the ability to make connections" (p. 65).

These connections also span to levels of ethics and responsibilities. Mitroff (2019) outlines an ethical belief of "passing the ethical buck" onto someone else, whereby someone else takes the blame and is responsible for an action being unethical, so even if an individual performed the unethical action they are not to blame. Mitroff (2019) states that this passing of the buck, "is one of the cornerstones of the Technological Mindset" and something seen in the digital world, including data collection. (p. 60). Additionally, research has indicated that a company has additional social and moral responsibilities beyond what is mandated by law (De George 2010). In this scenario, companies have an ethical responsibility to not just meet the letter of the law, but to act ethically beyond that.

In this sense, there are variances in business, where there are three different types: ethics in business, business ethics as a movement and business ethics as part of the general field of ethics (De George, 2010). De George (2010) explains that when it comes to business ethics, "there is not separate or esoteric set of norms that apply to business and do not apply elsewhere" (p. 9). This means that societal norms apply in the business world just as they would in any other facet of the world. De George (2010) further explains that, "the business ethics movement is thus a social phenomenon with academic, business, social and governmental aspects" (p. 11). In this sense, business ethics has been happening for decades now, including events such as worker rights and codes of conduct. In the area of business ethics, it often runs parallel to ethical issues faced by individuals. De George (2011) notes, "we have seen business ethics is not a separate ethics that constrains business in a way that other human and social endeavors are not constrained" (p. 12).

When it comes to data collection and ethics specifically, De George (2011) states that, "While the search for such information about an individual [that the individual did not want revealed] might be unethical, that is not the purpose of data mining by most companies" (p. 471). That said, he further goes onto explain that, "every company has an obligation to determine that any system containing confidential records is secure and that employees with access to such files are informed of, and trained in, security procedures" (De George, 2011, p. 471).

Trust

According to Merriam-Webster's dictionary, trust has been defined as, "Assured reliance on the integrity, veracity, justice, friendship or other sound principle, of a person or thing; confidence; faith; belief" (Merriam-Webster, 2019c). This definition focuses on having faith and reliance within a defined situation, which requires a level of trust. A separate, yet, commonly cited definition of trust courtesy Mayer, Davis and Shoorman (1995), describes trust as, "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (p. 712). In this sense, there is an element of vulnerability and even risk, which is cause for a level of trust.

To further this notion, there is research of trust that describes its existence only to come when there is an element of risk present (Adams, 1995; Coleman, 1990; Luhmann, 1989). Risk is further explored in relation to trust because, "Risk causes uncertainty and insecurities, whereas trust is an effective instrument to deal with them. It is important to mention that trust does not eliminate the risk itself. Rather it helps to overcome risk by changing its perception" (Akkaya, Wolf, Krcmar, 2010, p. 1).

Following this theme of trust and risk. Luhmann (2000) notes trust is directly linked to an individual's conscious decision to choose between two or more alternatives (ex: choosing between two wealth advisors - one may perform better than the other). Luhmann concludes, "Trust is only required if a bad outcome would make you regret your action" (Luhmann, 2000, p. 3).

Giddens (1990) explored a different aspect of the term trust, saying, “Trust is related to absence in time and in space. There would be no need to trust anyone whose activities were continually visible and whose thought processes were transparent, or to trust any system whose workings were wholly known and understood” (p. 33). He goes on further to suggest trust is attributed to reliability; an important component rooted in trust when facing multiple outcomes (Giddens, 1990).

Thomas (1998) identifies three broad conceptions of trust: ‘‘(a) fiduciary trust, which is notable for asymmetric relationships and attendant opportunities for malfeasance; (b) mutual trust, which develops between individuals who repeatedly interact with one another; and (c) social trust, which is embedded within institutions we know in common and take for granted’’ (p. 170).

Trust also ties into relationship maintenance strategies that result in the building of relationship outcomes: control mutuality, commitment, satisfaction and trust (Bowen & Gallicano, 2013). This is further explained by Bowen and Gallicano (2013) stating, “Being able to know and understand the organization allows publics to build expectations of it. When the organization meets those expectations, trust begins to form” (p. 195). Earlier work by Bowen falls in line with this research as he found that building trust and sustaining relationships is based on ethical consistency (Bowen, 2010). In relation to government, Welch, Hinnant and Jae Moon (2004) state, “citizen trust in government is built upon expectations conditioned by some type of social context or interaction” (p. 376).

Bowen and Gallicano (2013) argue that when it comes to relationship outcomes, “trust is the most pervasive and important factor, akin to the ‘backbone’ of the relationship” (p. 195). Organizations that value trust as well as credibility project these traits through their corporate reputation (Fombrun & van Riel, 1997). This ties trust in further to corporate reputations and how organizations are viewed, as corporate reputations are defined as, “a collective representation of a firm’s past actions and results that describes the firm’s ability to deliver on multiple outcomes” (Fombrun & van Riel, 1997, p. 10).

Welch, Hinnant and Jae Moon (2004) also studied trust in relation to e-government and concluded that, “electronic government strategies—transaction, transparency, and interactivity—are important factors that directly affect e-government satisfaction and indirectly affect trust” (p. 371). Nelson (1997) has identified five problems for building trust in cyberspace: security and reliability, identity and authentication, confidentiality, verification, and jurisdiction. Teo et al., (2008) argue that trust is key for retaining online relationship between the online service providers and the users. Additionally, researchers (Gefen et al., 2004; Pennington et al., 2003) have found trust as a factor that is a crucial enabler of e-commerce transactions, and extends this argument to e-government context (Teo et al., 2008). The trust factor also plays a critical role in the use and application of e-government services and adoption (Mahmood et al, 2014, p. 15).

It is also important to note that, trust and confidence have been examined without taking into account the differentiation that could exist among the various types of trust citizens can have and that could be influenced by e-government experience (Morgeson et al., 2011).

Public and Publics

The term *public* is a debated term in the fields of public relations, political science, psychology, marketing and advertising (Vasquez & Taylor, 2001). Price (1992) goes as far to say that no other term has caused so much social concern, academic interest or intellectual discussion. Public, “generally refers to common access or matters of concern, especially in matters of office and state” (Vasquez & Taylor, 2001, pp. 140/2). In relation to public relations, the term is more refined to mean, “a situational collection of individuals who emerge and organize in response to a problem” (Vasquez and Taylor, 2001, p. 140/2).

According to Grunig’s (2013) research, the first of three segments for practicing excellence in public relations is, “Identifying and segmenting stakeholders and publics and the issues they create” (p. 11). Ehling (1975) defines a public as a group of people that arises within a community around a controversial issue. Dewey (1938) outlined three factors 1) face a similar indeterminant situation 2) recognize what is indeterminant – problematic – in that situation and 3) organize to do something about the problem. Grunig (2013) furthered this by defining three stages in the evolution of a public: latent, aware and active.

Leichty and Warner (2001), posit that, “publics often exist prior to and independent of the organization” (p. 61). This serves as a key distinction to other definitions by stating the organization does not actually play into the forming of publics. Organizational publics grant legitimacy to the organization and make the organization dependent on them in this respect (Metzler, 2001).

To identify these publics, the Situational Theory of Publics is commonly used. Grunig (2013) writes that, “The situational theory of publics provides a sophisticated method of identifying different types of publics and for planning strategies to communicate with them” (p. 12). This tool is used to help segment and isolate publics to then develop methods to communicate and build relationships with them. However, some (Cozier & Witmer, 2001; Vasquez, 1993; Vasquez & Taylor, 2001) have countered the assumption of the Situational Theory that publics develop due to problems in life, and instead called for a more social theory of publics.

Ultimately, there is value in understanding publics, as Heath (1997) notes, “the identification, monitoring, and analysis of key publics’ opinions that can mature into public policy and regulative or legislative constraint” (p. 6). By knowing their audiences, organizations can then in turn work to appease them and/or tailor specific messages to them that will resonate and provide value.

With the advancement of disruptive new technologies in recent years, there has been a considerable focus on collecting data and tailoring messages and information to specific audience groups to facilitate user engagement (El-Haddadeh, Weerakkody, Osmani, Thakker, & Kapoor, 2019). This goes hand-in-hand with how organizations view, segment and build relationships with their publics.

e-Government

In a research paper, on the definition of e-Government, “The field of e-government deals with the major initiatives involving using multi-ways, taken by all levels of governments to enhance the services quality and security on behalf of public and business as a new key approach or strategy” (Hu, Pan, Lu and Wang, 2009, p. 980). This definition hinges on the belief that e-Government consists of dynamic elements that span a number of sectors but are tied together by the core belief of improving service quality and security (Hu et al, 2009). In earlier definitions, E-government is described as, “utilizing the Internet and the World-Wide-Web for delivering government information and services to citizens” (UN, 2002). In addition to the internet, it can also include “database, networking, discussion support, multimedia, automation, tracking and tracing, and personal identification technologies” (Jaeger, 2003).

Further definitions of e-Government include different angles or focuses on specific aspects of what is happening or being delivered. Tung and Rieck (2005) focus on what e-

Government delivers by asserting in their definition that, “E-government is believed to lead to better delivery of government services, improved interaction with business and industry, citizen empowerment through access to information, or more efficient government management” (p. 417). Conversely, it has also been defined in terms of how it operates, with Fountain (2001) stating, “‘E-government’ is a government that is organized increasingly in terms of virtual agencies, cross-agency and public-private networks whose structure and capacity depend on the internet and web” (p. 156). Gil-Garcia and Pardo (2005) related it to democracy by asserting, “E-government as the intensive or generalized use of information technologies in government for the provision of public services, the improvement of managerial effectiveness, and the promotion of democratic values and mechanisms” (p. 188). This serves as a definition whereby government uses technology in order to continue democratic practices and values through technology.

There are also a number of definitions that focus on e-Government as a means to disseminate information through technology. World Bank (2003) defines e-Government as “the use by government agencies of information technologies (such as wide area networks, the internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government”. Similarly, Jaeger and Thompson (2004) define e-Government as, “the provision of government information through the internet to citizens and businesses and among government agencies” (p. 95).

The definitions view e-Government, generally speaking, as a means to an end for communicating to audiences. Al-Kubaisi (2018) asserts that, “The strategic goal of e-government is to support and streamline government services to all stakeholders, including; government, citizens and business” (p. 4). While definitions have varied throughout time, they generally incorporate the belief that it is a means by which government is able to communicate and message their publics. Schelin (2003) notes that, "one context for examining e-government centers on recognition that e-government is more than just a shift in communication patterns or mediums. At least potentially, it involves a transformation of the organizational culture of the government" (p. 125).

As technology continues to evolve, so too will the definition and meaning of e-Government. Kim and Ni (2013) note that, "As many social institutions and individuals migrate their activities to the computer-mediated, digitalized, networked community, many new phenomena have arisen" (p. 138). Ontario, and Canada as a whole, has followed other large countries around the world such as the UK, USA and Australia by creating digital government teams. The Ontario Government (2020, January 20) defines "digital" as:

> Digital is a means to an end, not an end itself. Digital creates better value for investments and enables more efficient services. It's a different way of thinking and working to solve human problems and produce better outcomes in an era where computers are widely used, the internet exists, and people have come to expect speed, convenience, and simplicity.

The Ontario Government further states that by becoming digital, their aim is to provide more efficient services, and solve human problems in an era where the internet exists, and computers are widely used. Tom Loosemore, co-founder of the Government Digital Service, defined digital as, "Applying the culture, practices, processes & technologies of the Internet-era to respond to people's raised expectations" (Loosemore, 2016, May 10).

These definitions and outlines come together to define e-Government as a means by which governments, specifically in Canada in this case, provide levels of service and communication through technology.

Research Questions

To understand how public sector organizations can ethically collect data, this case study will focus on two research questions:

Research Question 1: How and to what extent can data on publics be collected in an ethical and legal manner? The purpose of this question is to intersect what the law and ethics say about collecting data to understand commonalities between the two. It is important to conduct a literature review on the legislation regarding data collection and then cross reference it with ethics theory. For this research, ethics is defined as a, "systematic attempt to make sense of our individual and social moral experience, in such a way as to determine the rules that ought to govern human conduct, the values worth pursuing and the character traits deserving development in life" (De George, 2010, p. 13). This study seeks to establish a baseline foundation for data collection according to the law and ethics.

Research Question 2: How and to what extent can data on publics be collected whereby publics are comfortable with the method(s)? The purpose of this question is to determine ways in which data can be collected from publics in ways that they are okay with, instead of just complying with the law. Research has indicated that that a company has additional social and moral responsibilities beyond what is mandated by law (De George 2010). In order to build trust, four maintenance strategies have been highlighted: control mutuality, commitment, satisfaction and trust (Bowen & Gallicano, 2013). It is further noted that trust is the foundational element of those four that must be present as all other outcomes are undermined if trust does not exist. This study seeks to serve the purpose of exploring ways to collect data from publics with mutual benefits where trust can be maintained.

Methodology

According to Yin (2014) there is a twofold definition of a case study as it, “investigates a contemporary phenomenon in its real-world context” and it “points to case study design and data collection features, such as how data triangulation helps to address the distinctive technical condition whereby a case study will have more variables of interest than data points” (p. 2). For research to be categorized as a “case study” there are three types of criteria that must be met: the researcher must ask and answer how and why; the researcher must have no control over actual behaviour events that take place; and must focus on current events (Yin, 2014). Furthermore, an explanatory methodology, described as “a case study whose purpose it is to explain how and why some condition came to be” (Yin, 2014, p. 238) was used to determine how data can be ethically collected by public sector organizations.

A McMaster Research Ethics Board (MREB) application was prepared, revised and approved as part of the research process. There were two distinct methods of collecting information, each of which required separate letters of consent (reference Appendix C and D). The first method of this data collection was done through a survey that was open to anyone that lives in Canada and is over the age of 18. In order to understand the public’s view on data collection, the survey was administered through social media to roughly 1,500 people (Reference Appendix A for the full survey). There were 104 total responses by Canadian residents over the age of 18. Participants had to click through a consent notice page, that provided details on what their information would be used for. The second method of this data collection was the in-depth interviews. In-depth interviews, “like all qualitative research methods, provides rich detail and the ability to understand what the individual being interviewed really thinks about something” (Stacks, 2017, p. 196). In order to protect the individuals, the author secured their informed consent, which included noting that the interviewees identity would not be disclosed through the paper. The consent form also outlined steps being taken to minimize potential harm as well as protect their privacy and confidentiality (Yin, 2014). Once the interviews were complete, responses were analyzed and categorized according to themes that provide insights into this study as well as future research opportunities.

To conduct this case study, the research triangulated a literature review, conducted in-depth interviews with subject matter experts and surveyed the general population. The researcher interviewed five individuals in-depth; these individuals spanned a wide range of expertise including legal, communications and information technology. The survey was distributed to a wide age range of publics within Canada. The goal was to solicit 100 responses; the final number of responses was 104. Similarities and connections between these information sources was analyzed to determine a framework for public sector organizations to collect data.

Professor Dave Scholz was the supervisor for this capstone, and his feedback provided guidance and leadership throughout the process.

Participants

Participants for this study are broken into two groups. The first is survey respondents, which is a general group that can include anyone over the age of 18 that lives in Canada. The second group consisted of subject-matter experts related to ethical data collection by public sector organizations, including public relations, information technology, information and records management as well as lawyers. These individuals worked across a number of public sector organizations such as municipal government, provincial ministries, education and a crown corporation owned by a provincial government.

Results

Survey Results

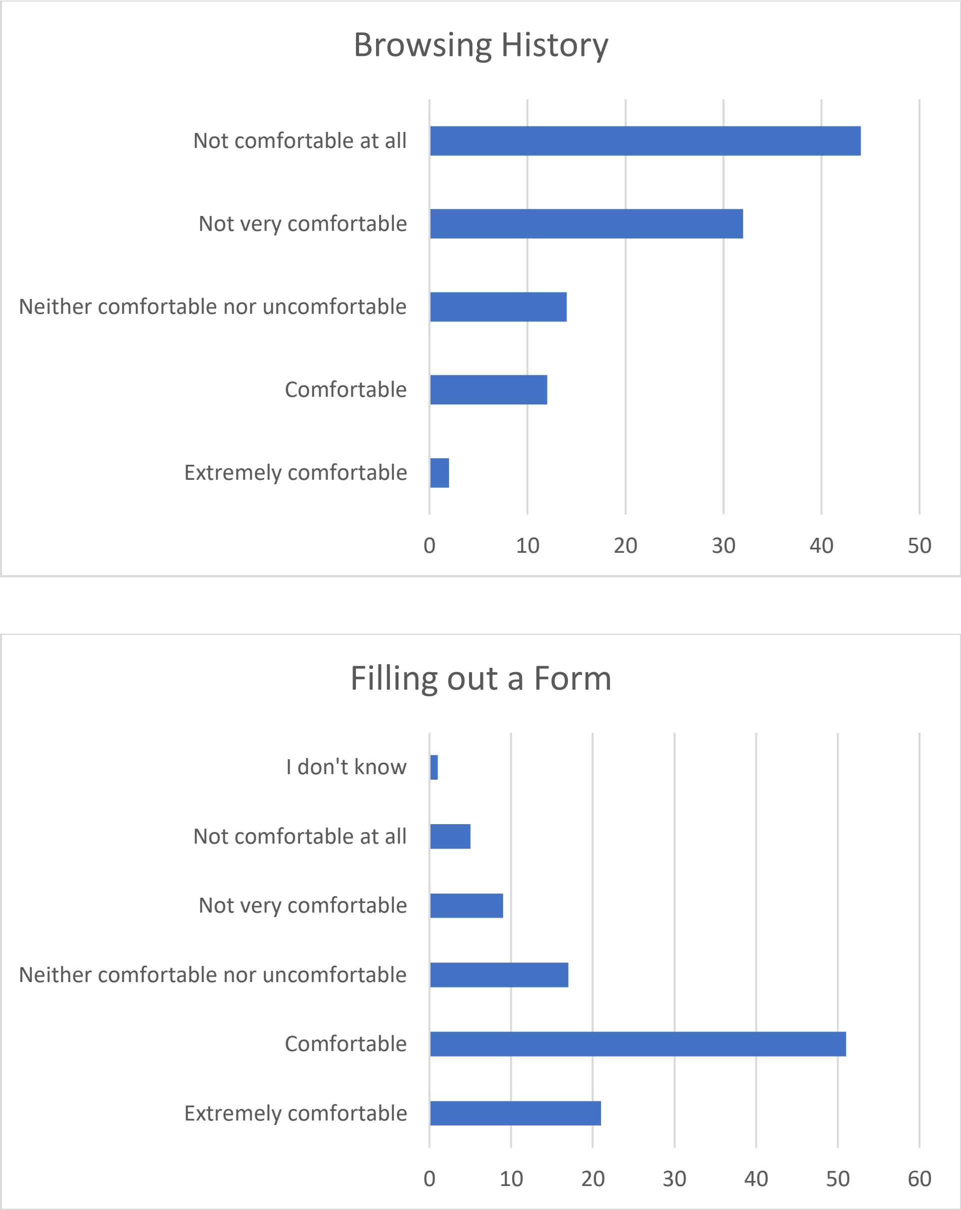
The breakdown of responses by age groups were 7 per cent between the ages of 18 and 25 years old, 39 per cent between 26 and 35, 16 per cent between 36 and 45, 26 per cent between 46 and 55 and 12 per cent between 56 and 65. There were no responses over the age of 65.

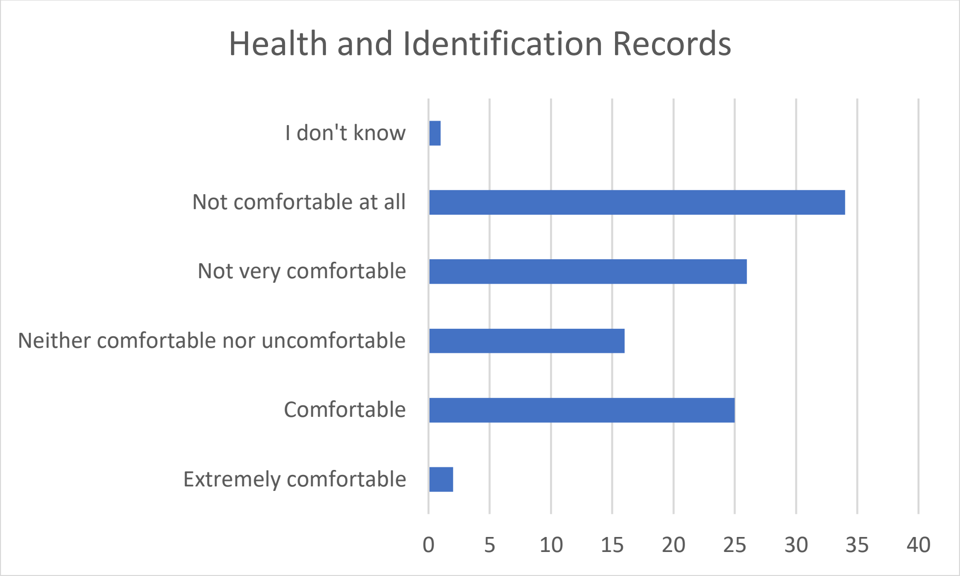
The survey results indicate that, predominantly, 40 per cent of people were "maybe" okay with public sector organizations collecting data on them. In response to whether they would like to receive personalized offers, 43 per cent of people responded no.

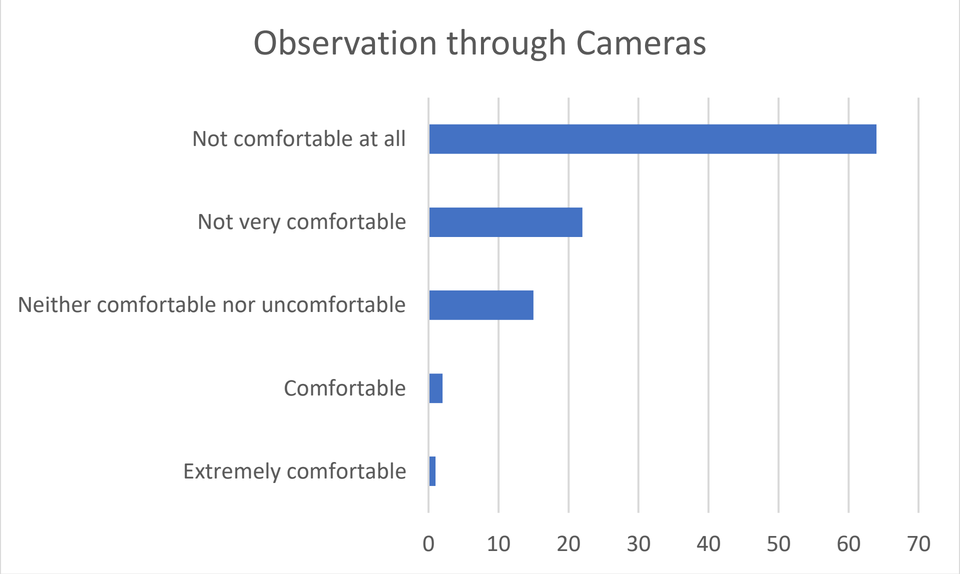
A series of likert scale questions were then asked about methods of data collection and how comfortable respondents would be about them. The primary responses for each question prompt showed that 42 per cent of people would not be comfortable at all if their internet browsing history was used, 49 per cent would be comfortable with filling out a form, 33 per cent would not be comfortable at all with their health and identification information being used, 62 per cent would not be comfortable at all with observation through camera, 51 per cent would be comfortable with mailed questionnaires and 35 per cent would be comfortable with a phone survey. The method with the highest level of comfort indicated, which was extremely comfortable, was filling out a form. The methods respondents were most divided on were healthy and identification records where 25 per cent said they were not very comfortable with this, 24 per cent said they were comfortable, 33 per cent said not at all and 15 per cent said they were neither comfortable or uncomfortable. Respondents were also divided phone surveys as 35 per cent said they were comfortable, 24 per cent said they were not comfortable, 19 per cent said they were not comfortable and 15 per cent said they were neither comfortable or uncomfortable. The method that received the least amount of extremely comfortable and comfortable votes combined was observation through cameras at 2 per cent combined. The highest combined vote for extremely comfortable and comfortable was mailed questionnaires. View Figure 2 for full responses.

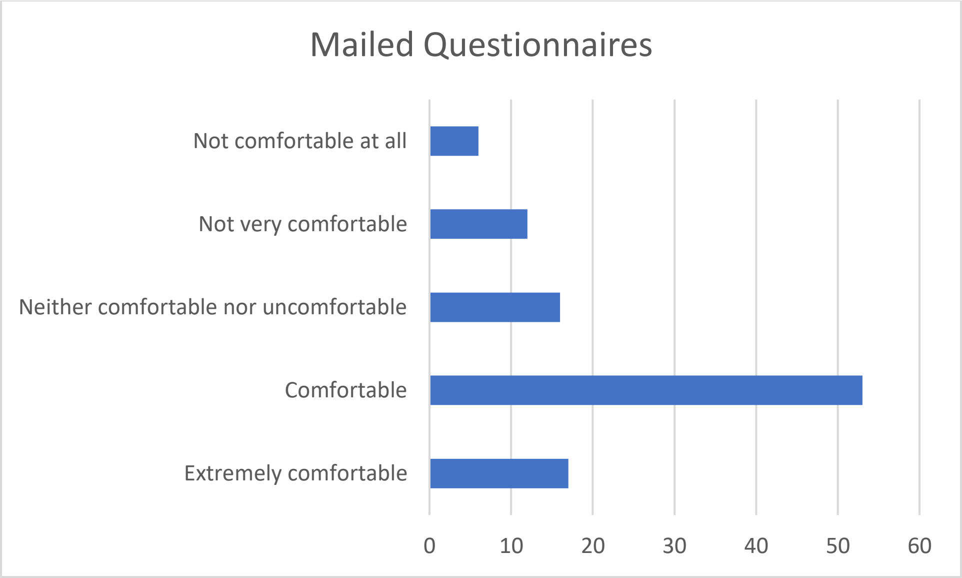
Figure 2

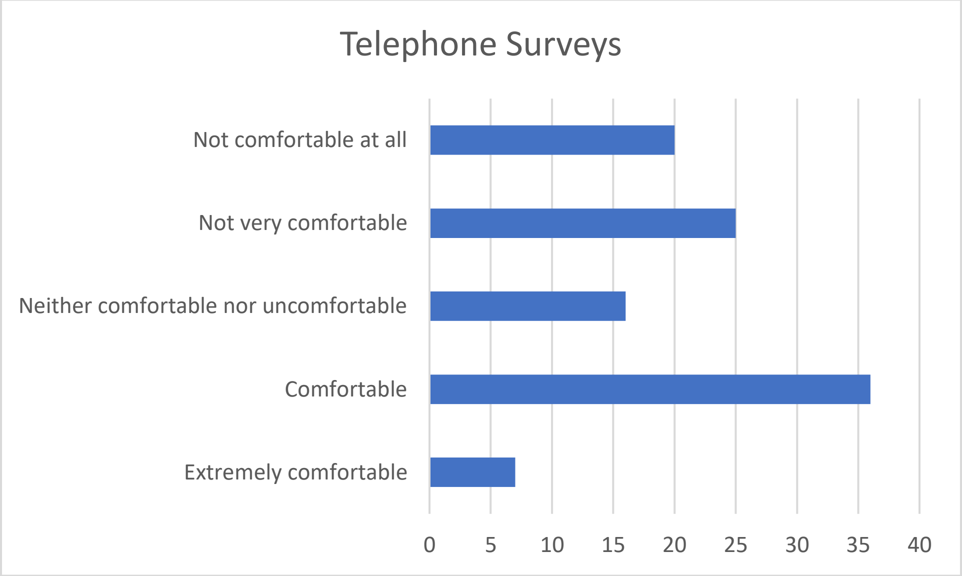
Full Responses Charted Out




Health and Identification Records
I don't know
Not comfortable at all
Not very comfortable
Neither comfortable nor uncomfortable
Comfortable
Extremely comfortable
0
5
10
15
20
25
30
35
40


Observation through Cameras
Not comfortable at all
Not very comfortable
Neither comfortable nor uncomfortable
Comfortable
Extremely comfortable
0
10
20
30
40
50
60
70





Note: Responses indicate full responses from all survey participants.

n = 104.

When specifically asked what methods they would prefer public sector organizations used to collect data on them, results were mixed. Roughly 65 per cent of respondents noted it will need to be done with their explicit consent and/or permission and done willingly. Examples provided by respondents included online forms, questionnaires, and phone surveys. There were

15 per cent of people that said quite clearly that they would prefer their data not be collected at all. The most common word used in reply, beyond words that were also seen in the question itself, was “consent.”

As a follow-up question, respondents were asked what they would prefer public sector organizations doing with the information collected on them. Similar to the previous question, roughly 10 per cent of responses stated to some degree that information should not be collected on them. One of the most common words across all responses was, “better” and this was in relation to improving services, tailoring information to individuals, and ease of use for inputting data between various agencies (such as health, program registration, etc.). The next most common theme was security and confidentiality of the data, as respondents wanted to be assured that their data information was private, and, for some, anonymized.

Respondents concluded the survey by asking whether they think public sector organizations should be allowed to collect and store information on them at all, and 79 per cent indicated that yes, they should, but only to some; 19 per cent said no.

Interview Results

In a series of in-depth interviews, participants answered questions regarding ethical data collection by public sector organizations through sharing their insights and observations.

Research Question 1: How and to what extent can data on publics be collected in an ethical and legal manner?

When asked how they would collect and store information on their audiences today, every participant noted having a purpose for the data at the very beginning of the process to help inform the data collection process. Participant two stated, “start with justification for this in the first place so that you’re collecting information just for the purpose of the study or survey.” Participant one added that organizations need to, “be clear on what we’re trying to do” and noted the use of a privacy impact assessment that includes, “what should be collected, what’s the purpose and how will it be collected.” For participant three it was important that, “we are doing something where I can take the data and do something with it.” Participant four added, “evaluate the types of data I’m collecting to understand harms and consequences to safeguard information.” While participant five concluded, “all of the things that go can go wrong relates to the data you are handling, so I think we first need to ask, do we really need to collect this data? Is there a legitimate business purpose?”

Participants varied in how they would collect data from their publics. Three of the five participants noted that they would acquire data through the use of technology. For participant three, it came down to doing so by way of, “generally electronic because it’s easy to manipulate,” and through the power of technological data collection, it could then be useful and worth the participants time and ethical in its use of their efforts to gather their information in the first place. Participant two noted that if a technological solution is used then there’s a need to account for, “cyber security and a log with access and authorization.” Participant four took a different direction by noting, “you need to know who your audience and be strategic about how to get that information across to them to collect the data.” Participant five stated that it, “depends what you’re trying to achieve with the data.”

When the topic shifted to ask how data can be ethically collected, every participant noted obtaining consent. Participant three noted that, “in the public sector, the only requirement is notice collection. What we tend to do is something to get you to consent to use of information.” Participant four stated one should, “ask their permission to do that I would design the method in a way to get informed consent." In terms of what should be included, participant two outlined whether it was full or partial consent required, letting publics know how their information can be removed after they've submitted it, and contact information for publics to follow-up with should they have any questions, concerns or want to withdraw. Participant one summed it up by noting, "as long as people are aware and have the ability to opt out, and that it's by choice not automation." Participant three also added a question, asking, "if someone isn't reading the terms and conditions, is that really ethical?" Participant five added that beyond disclosure and consent, ethical data collection is, "more than just the law and the contract. Data privacy means not only protecting the data but respecting the data and that means respecting the people you are collecting data on."

Beyond obtaining consent, participants outlined how data collection can be deemed unethical or illegal in its collection. Responses boiled down to not obtaining informed consent as well as not using the data for its intended purpose. Participant five noted that it is unethical to, "bury the terms of your privacy notice (through legalise language or writing a notice that's much longer than necessary) or deceive your audience in the terms." Participant three noted that it is unethical if you, "use it for something I didn't know or could have reasonably anticipated, or if you took it out of context and used it for something I didn't know about." In addition, participant one added that it can be unethical if the data was used to influence you without your awareness, anything that can be used against them, using data from another collection where consent was not granted to allow them use it for further purposes as well as buying data. Three of the five participants noted, without prompt, that the data cannot cause more harm than good for those giving up their information.

There were also a number of times where those surveyed mentioned that data collection is only a piece of the puzzle to consider and that everything has to work together. Participant four noted, “ethical collection and use of data is an aspect of data life cycle. You can’t talk about collection and use without discussing storage, consent, destruction and so on.” Every participant noted a need to justify the use and purpose of the data, and that you can’t just collect data for the sake of collecting data on people. Participant five stated, “organizations collect more data than they reasonably to. While they disclose it and you acknowledge it, I would not consider it ethical.” Participant three added, “do you really need all of this information or are you just collecting it? I think we over collect data and a lot of times people don’t know what they need to know.”

Research Question 2: How and to what extent can data on publics be collected whereby publics are comfortable with the method(s)?

When discussing how data can be collected whereby publics are comfortable with the method(s), participant one stated the need to, “being open and transparent, including what you’re doing with the data, what you’re collecting and why, plus the ability to opt-out.” Participant two also noted an opt-out and added providing a contact person to follow-up with, in regard to understanding what is happening with the data or if any future opt-out is desired by the respondent. Participant four boiled it down to asking for their permission stressing the importance of, the individual or group of people know what they are getting into by releasing their information, and the organization honestly upholds what they are saying they will do with it, they should be comfortable. Participant five broke it down to “active” and “passive” collection whereby in active collection the participant willingly provides their information to the organization while passive collection walks the line of ethical as they are not always aware that information is being collected for them. The example provided by the participant was someone visiting a website and all the information automatically collected on them without their consideration, such as their browser, time of day visiting the website and so on.

The participants all noted that when it came to making publics comfortable with data collection it depended on what data was being used, who is the target audience and what is the purpose. They were not concerned with specifically how to collect the data in order for publics to be comfortable. Instead the responses centered on how to obtain informed consent. Participant five noted, “to get an opinion, ask them directly. The difficult part is people aren’t always interested in talking.” Participant three stated that, “the gap to me is nobody is reading anything. You can ask for consent, but people aren’t reading. You can call people and they don’t know what’s actually happening.” Participant two noted that, “the method does not matter, you have to be comfortable with the organization you’re giving it to.” Participant four added that, “people are pretty well-versed on regulations and we are well-placed to move towards informed consent, but it’s going to vary based on context.” Participant four also continued to say that the gap between legal and ethical data collection is technical consent versus informed consent and that organizations have a responsibility to clarify information and make sure people know what they are agreeing to when they provided their personal data.

Without prompt, four of the five participants shifted the conversation from ethical data collection to data security in order to make publics comfortable. Participant three noted, “nobody cares about the collection, people only care when something goes wrong with the data after it has been collected.” Participant two stated, “we are one major data breach away from realizing what we do is likely insufficient. We need to teach staff the legal ramifications of dealing this type of information.” Participant four noted any discussion of ethical data collection has to include the data life cycle including storage, protection and destruction of the data at some point. Participant five added that, "everything that could go wrong stems from the actual data collection and why you are doing it so you need to put a lot of thought into it right from the start." It was clear from the responses that data collection is only one component of handling and using data, and that even if it is done correctly, it does not matter if the other parts – handling, practical use, storage, destruction, to name a few – are not done properly.

Moving forward in data collection, participants noted the need for further transparency and anticipation of data use. Participant one argued for a "universal standard and built-in standard to share data across all levels of government with a centralized understanding of individuals information and rights." Participant three also said that, "there will be more requests for data within the public sector and for data to start moving between different public sector organizations." To this end, participant two called for, "the role of the privacy commissioner will need to increase, and we should see that role become more prominent in lower levels of government." Participant four stated that more foresight in the consent process will save organizations time so that they don't have to go back to individuals to ask for further consent in order to use their data for something else. Participant five called for more careful consideration from the beginning with the goal of minimizing the data collected in order to protect both the organization from having too much "unnecessary" information, and the individual from not giving up more information than they reasonably need to.

Discussion

This capstone study examined ethical data collection by public sector organizations, how it can be achieved, and what methods can be pursued in order to ethically collect data. The interview results indicated a number of considerations for ethical data collection, including informed consent, transparency in the use of the data and understanding the data life cycle as a whole. Meanwhile, the survey respondents demonstrated mixed results on the comfort level of data being collected on them and used, as well as a certain level of comfort in submitting their data to public sector organizations by way of surveys, questionnaires and surveys.

Consent and Transparency

Each interview participant focused on informed data consent throughout their answers, noting the need to educate their publics on why they are collecting information on them and what they plan on doing with it. Conversely, 40 per cent of survey respondents said they were "maybe" okay with public sector organizations collecting data on them. This brought to mind Mayer, Davis and Shoorman's (1995) definition of trust where one party is willing to be vulnerable to the actions of another party. When asked what they would prefer a public sector organization doing with the information collected on them, one survey participant stated, "everything comes down to consent. If I know what it's being used for or has the potential to be used for and I agree, no problem." Survey respondents as a whole were most concerned with whether or not they understood data collection was taking place and what consent they have provided. From there, they in turn noted whether or not the data collection would be used for the greater good, with one survey respondent directly writing that data collection should be, "using it on an aggregate basis to help improve the economy or wellbeing of Canadians." Tying this in with Mitroff's (2019) assertion that "Dataism" can help organization's make better decisions for individual's, there is a connection between consenting to use information, understanding why it's useful and the potential benefits to everyone involved.

Consent to collect data therein was tied to the use of the data and whether or not it was "worth it" for publics to willingly give up their information. One survey respondent stated, "I would prefer if public sector organizations took data collected on me to improve services and make a positive change/impact. For example, improving customer service." The concept of using data collected to improve customer service and programs offered was a regular theme among survey respondents, and it tied into the interview results where every participant noted the need for meaningful data collection that provided value to publics and the organization. Mitroff (2019) noted that when the term of ethics arose, particularly in Western societies, it centred around the concept of benefits outweighing disbenefits combined with the ability to foresee intended and unintended consequences. Corporations that use data collection for good can not only receive tangible benefits, but a boost in corporate reputation and trust as well (Fombrun & van Riel, 1997). Participant four specifically noted the need for organizations to understand the harms and consequences of the data collection in order to properly plan and strategize it in the first place. Using the Situational Theory of Publics (Grunig, 2013), can help organizations identify commonalities among different stakeholders to develop a consensus around data collection benefits and uses.

The concept of foresight in the consent process was constant among interview subjects and was also echoed by survey respondents stating their overwhelming desire to consent to data collection. Participant four called for a, "layered consent process to continually get people's information and attention about what's happening." As Ontario's privacy commissioner, Ann Caovoukian (Pringle, February 1, 2020), discussed, there is a need for greater openness and transparency in order to hold organizations accountable. This can come in the original consent phase as well as a tiered approach that keeps the impacted publics updated on what is happening with their data. The idea of "layered consent" communicated an idea that survey respondents and interview subjects referenced across the board as a format that helps to meet everyone's needs.

Survey respondents clearly noted that they wanted to be informed on what was happening with their data. It is a potential lens into Kim and Ni’s (2013) assertion that new phenomena will arise as organizations build digitized, networked communities emerge.

Participant three wondered about how data can be shared across different levels of governments seamlessly and gave an example of flooding whereby important information can be relevant to a number of levels of public sector organization, and that it is beneficial to everyone if it is shared properly. The consent required for that type of scenario should ideally be thought of in advance of the original data collection and built into the consent process from the beginning. When organizations act with moral rectitude and reflexiveness, trust and credibility are enhanced (Bowen & Gallicano, 2013). Organization’s should be aware of this and plan their actions and strategies accordingly so as to gain that trust and strong decision-making processes that allow them to ask for further consent to use data collected to help make decisions or provide services that go beyond the initial use of that data collection. For public sector organization’s to ethically collect data and utilize it, it will be vital to prioritize trust and transparency in the process to advance their efforts. As seen through Edelman’s trust barometer (February 19, 2020), trust in government organizations is low in Canada and through Fombrun and van Riel’s (1997) research, an organization’s corporate reputation is a collective response to their past actions. Instances such as the Toronto Police Service’s being caught testing a data collection tool “informally” come into question in this scenario, placing even more of an emphasis on building trust and being transparent in this process.

Data Lifecycle

The beginning of the data collection process had similar responses from interview subjects as they noted the need to acquire consent. Participant three discussed how a collection notice was generally the only legislative requirement for organizations to follow. While survey respondents noted that their consent prior to the actual act of data collection in response to the question, “What would you prefer public sector organizations doing with the information collected on you?” One survey participant noted that public sector organizations can use their data and do, “Whatever they want as long as I give permission.” This falls in line with the Ontario Government’s view on data collection, by which they note that if it is collected through unknown surveillance, it infringes on publics rights to act freely (Ontario Government, 2019, July 30). This is a key and meaningful portion of the data lifecycle as proper consent not only allows for proper collection in the first place, but it can inform what you can do with the data after you get it. That includes storage, use, retention and destruction.

Every interview subject referenced that data goes beyond collection and includes components such as storage, use, access and destruction. Each one noted, without prompt, that you could not look at one component of data in pure isolation without considering other factors involved. At the same time, survey respondent’s answers varied significantly when presented with different data collection methods while many also indicated concerns over data security and protection. One survey respondent, for example, stated that, “I’d like organizations to make every effort to protect my data and store it securely.” This falls in line with the 10 principles listed in Canada’s Digital Charter, which includes Data and Digital for Good, Control and Consent, Safety and Security as well as Transparency, Portability and Interoperability among other principles.

Among potential risks brought up in regard to data collection, survey respondents were most concerned with their data and information being compromised or breached. Participant five noted that any data collected represents an opportunity for data to be hacked so organizations should be debating if it is even worth it in the first place. Participant four also discussed how potential benefits have to outweigh the potential risks in any data collection and that safeguarding information needs to be a priority. Many of these potential risks are known, as evidence by the Ontario Government admitting the risk of loss of privacy through e-government, where the vast majority of data is collected and stored. Participant two discussed putting in place a formal data access system with levels of approval and formal data management training to ensure that data is stored and maintained safely in a regulated manner. This line of thinking bridges the trust of publics and organizations together as defined by assured reliance on matters such as integrity and justice (Trust, 2019). As Luhmann (2000) noted, trust is only required if there is potential for a bad outcome to occur. In this case, it is evident there is fear from both the organizations and publics as to potential concerns and it is a strong consideration in the data collection process.

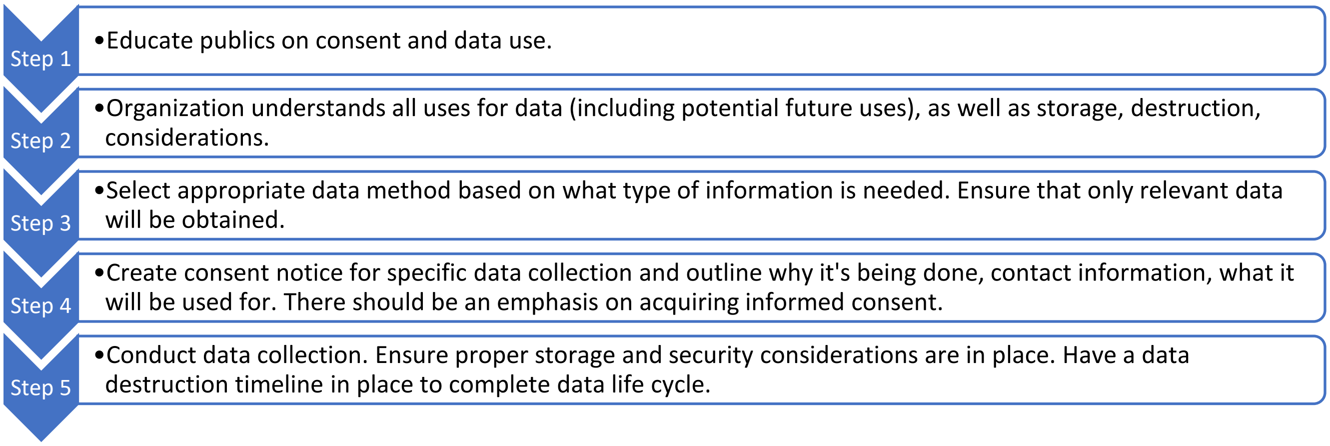
There are also legal ramifications to consider for the data lifecycle. Participant three noted that they “only” had to follow the specific Act to their province and from there had to collect the information with an information collection notice as well as understand freedom of information, yet also noted, “it’s not a lot to govern the whole process.” However, public sector organizations have to be ready to identify and release certain information upon request as noted through Acts specific to their province. Participant five lamented the different laws between each province which can be, “confusing and take time to learn each one, moving from province to province.” This can cause complications across the country whereas, previously noted, 92 per cent of Canadians expressed concern over losing control of their personal information and 55 per cent indicated they trust the government to respect privacy (Office of the Privacy Commissioner of Canada, 2019). Across the board there are a number of intricacies between Acts, for example, the Privacy Act overseeing the Government of Canada and The Personal Information Protection and Electronic Documents Act (PIPEDA) have different definitions of personal information. In order to create an environment for informed consent and transparency, consistency throughout the country, across different levels of government can be further explored. This should encompass all levels of the data lifecycle. As Canadians in this study, and others, have indicated, they lack trust in public sector organizations handling their data, and part of that can be attributed to not even knowing the rules or regulations that apply to them in the first place.

Ethical Data Collection Trust/Framework

This study examined ethical data collection and results indicated a further need from all angles to educate all stakeholders in informed consent. As one component of the overall data collection process, and based on the findings and participant insights, an ethical data collection framework was developed to demonstrate a method and model to ethically collect data for public sector organizations.

Figure 3

Ethical Data Collection Framework



Step 1	• Educate publics on consent and data use.
Step 2	• Organization understands all uses for data (including potential future uses), as well as storage, destruction, considerations.
Step 3	• Select appropriate data method based on what type of information is needed. Ensure that only relevant data will be obtained.
Step 4	• Create consent notice for specific data collection and outline why it's being done, contact information, what it will be used for. There should be an emphasis on acquiring informed consent.
Step 5	• Conduct data collection. Ensure proper storage and security considerations are in place. Have a data destruction timeline in place to complete data life cycle.

Note: Framework describes sequential steps to take for ethical data collection.

There is still trepidation from publics when it comes to data collection, as evident by the 79 per cent of survey responses that indicated they think public sector organizations should be allowed to collect data on their publics, but only some. There is an opportunity to further educate publics on data collection, why it can be of use to them, what they are consenting to and how it benefits both organization and publics. This process is seen as the first step in order to bridge the gap between organization use and building trust with publics in a two-way symmetrical communications model that focuses on mutual understanding and respect to achieve a set of objectives.

The second step in Figure 3 is for the organization to understand all their data uses from the outset. This would help avoid having to ask for further permissions and consent from publics after a data collection has taken place. As participant four noted, “you want to get it right the first time so that you don’t have to go back and ask again for further uses.” This can also help bridge the gap for inter-public sector use of information as noted by interview subjects. One organization can collect data that can be of use to a separate public sector organization in the future. This should be understood and outlined in the consent process from the beginning. Plans and processes should also be in place to store the data, have access controls, and to understand how and when it will be deleted.

The third step takes into account reaching your relevant publics based on what data you are attempting to collect. As interview subjects noted, what you are trying to do should inform how you are trying to go about it. At the same time, when it comes to selecting the method for data collection, it is recommended to be aware of what survey respondents indicated they are most comfortable with. When building out the data collection method, questions should also be rigorously scrutinized to ensure that only necessary information is being collected so as to ensure there is not information collected that provides no value related to the purpose of the data collection in the first place. This ties into participant five's assertion that organizations need to respect individuals and their data.

Once the consent education and data collection structure as well as information gathering methods have been created, public sector organizations can then work towards creating a consent notice and focusing on informed consent. Three of five interview participants explicitly noted that even if there is a consent notice, it is not ethical if the individual or group of people agreeing to it are not actually aware of what they are agreeing to. Survey respondents also indicated that they are willing to provide information in scenarios where they understand why it is happening.

Finally, step five outlines having a plan that goes beyond the act of data collection. As participant four noted, "ethical data collection goes beyond the act of collecting data as it includes the whole process which means, storage, access, use and destruction." Survey respondents also identified a fear of having their data breached, which goes beyond the act of the actual data collection itself. This indicates that organizations need to account for the whole data lifecycle from the outset in order to ensure that data is not only collected ethically, but that it is managed ethically as well.

This is a framework whereby future research can be built.

Recommendations for Communications Professionals

Collecting data on audiences is only becoming more prominent for organizations, including the public sector. This will impact communications professionals in a number of ways, including how to ensure this is done legislatively through the use of tools such as surveys, and how it can be done ethically so as to not damage the relationship between the organization and their public. After all, as the Public Relations Society of America notes, "Public relations is a strategic communication process that builds mutually beneficial relationships between organizations and their publics" (Public Relations Society of America, n.d.). In this sense, communications professionals will have a leadership role to play in ensuring that not only is data collected ethically, but it is explained to publics so that they can maintain trust. When it comes to trust and ethics, De George (2011) and Mitroff (2019) offer preliminary research and insight to read up on.

It is imperative that communications professionals thoroughly understand legislative requirements when it comes to data collection. This includes the practical application of understanding the legislature and knowing the language required in information collection notices, how to format collection tools and properly explaining where the data will go and how it will be used, or not used. Recommended reading includes Canada's Communications Security Establishment as well as relevant literature depending on the level of government; for example, municipal governments can look to the Municipal Act. In order to collect data ethically, communications professionals will have to understand not only consent, but how to ensure informed consent from their publics. Professionals can study tactics and strategies that cover how to inform their publics of consent. For publics to feel comfortable "giving up" their personal information, they will need to understand what it is being used for, how it is being used, stored, etc. and communication professionals can work with internal and external stakeholders to educate about consent and data use.

The implementation of consistent, ethical data collection processes across public sector organizations does not appear integrated through the various divisions and departments. For example, marketing differs in their data collection processes as they attempt to understand their audience for sales and advertising purposes compared to finance, collecting information on taxpayers and ensuring finances are properly calculated. This approach is not user friendly for publics, having to consistently re-enter the same information across various divisions and departments that all work for the same funnel, while it is costly and inefficient for the organizations themselves. There is an opportunity for Communications professionals to audit their organizations to ensure consistent, ethical data collection is being practiced while seeking opportunities to explain to their public what and why it's happening, as well as create trust in this process between organization and public. A plan will also have to be created both internally and externally in order for this to happen. Responsibilities will need to be sorted out through the organization to establish who owns the various components of data collection and working with the public to build and maintain trust in the process.

Finally, as evident by the responses through the survey, there is a legitimate fear of data privacy, breach and mismanagement. Communicators will have to ensure transparency and openness in this process, as well as assist in ensuring that data is properly handled and maintained. It is recommended to read the work conducted on e-government to date that discusses its uses, including Hu et al (2009), Tung and Rieck (2003) and Al Kubaisi (2018). As seen through the data collected for this paper, the purpose of the data can help to inform the level of consent required, as well as the method by way the data is collected in the first place. Understanding this process and following it in the correct order can help ensure that communications professionals and their organizations are ethically collecting data in a manner that their publics feel comfortable with.

Recommendations for Future Research

This study serves as an introduction to a topic that is only expanding and becoming more prominent in its application. The results demonstrate that there is still a lot of research, education and practice that has to take place on this subject. Based on survey responses, there are many opportunities to further research, including whether public sector organizations should be collecting data from their publics at all, what is the best medium/tool to collect data from publics and how to break this down through various age groups. When it comes to the interview responses, future research can also look at how to best bridge the gap between data collection and various agencies so that everything can be centralized in one location and how public sector organizations can better educate publics on their data use practices.

Preliminary suggestions include:

- Conducting research on specific public sectors, including municipal, provincial and federal government, as well as other sections such as health and education. Each sector may have unique results based on their publics and organizational goals.
- Further research can also be done to breakdown the study by age. There was nobody over the age of 65 that responded to the survey and the vast majority of respondents were either between 26 and 35 or 46 and 55. There is an opportunity to focus in on specific age groups to understand their feelings and thoughts towards data collection by public sector organizations and what can be done to appease them.
- Set up experiments based on Luhmann's (2000) framework on trust that looks at various data collection methods to determine the impacts of specific methods of data collection and how they alter levels of trust with publics.
- In addition, a study of what specific data publics would disclose can be looked at to pair with this study. For example, does the answer change if it is health records vs home address and phone number.

- Next steps beyond this research can aim to study and understand what public sector organizations should do with the data collected, how it should be stored and how as well as to who access should be provided to employees. It will also be imperative to research how public sector organizations can use data collected to better serve the public and make informed decisions.

Limitations

There are a number of limitations in this study including a small sample size of survey participants (104) This led to a notable sampling error where, “the sample drawn from a population does not accurately reflect that population” (Stacks, p. 224). Further, among those that did respond, various age groups were not equally represented. There was also limited access to subject-matter experts as only five were interviewed.

Survey respondents were based on the researcher’s network, through either personal connections or friends of friends, known as a snowball sample (Stacks, p. 375). As Stacks (2017) notes, “snowball sampling, like all forms of nonprobability sampling, cannot be generalized to the larger population” (p. 228). Subject-matter experts were also, in part, chosen based on their interest in the study, availability and overall timing. There is potential for some measurement error, described as “the amount of random error found in any measure” (Stacks, p. 234), regarding the concept of data and information collection, and how survey respondents understood and answered these questions.

References

2020 Edelman Trust Barometer: Canada. (2020, February 19). Retrieved from https://www.edelman.ca/sites/g/files/aatuss376/files/2020-02/2020 Edelman Trust Barometer Canada - FINAL.pdf

Adams, J. (1995). Risk UCL Press, London.

Akkaya, C., Wolf, P., and Krcmar, H. (2010). "The Role of Trust in E-Government Adoption: A Literature Review" AMCIS 2010 Proceedings. 297. http://aisel.aisnet.org/amcis2010/297

Al-Kubaisi, A.S. (2018). Enhancing the Adoption of E-Government Systems through Open Government and Open Government Data (OGD) Initiatives in Qatar. *Journal of Information Engineering and Applications*. Vol. 8, No. 1.

Allen, K., & Gillis, W. (2020, February 20). Privacy watchdogs weigh probe of facial recognition technology. Retrieved from https://www.pressreader.com/article/281547997913548

Bowen, S. A., Heath, R. L., Lee, J., Painter, G., Agraz, F. J., McKie, D., & Toledano, M. (2006). The business of truth: A guide to ethical communication. San Francisco, CA: International Association of Business Communicators.

Bowen, S. A. (2010). The nature of good in public relations: What should be its normative ethic? In R. L. Heath (Ed.), *The Sage handbook of public relations* (2nd ed., pp. 569-583). Thousand Oaks, CA: Sage.

Bowen, S. A. & Derville Gallicano, T. (2013). A philosophy of reflective ethical symmetry. In K. Sriramesh, A. Zerfass, & J.N. Kim (Eds.), Public relations and communication management: current trends and emerging topics. (pp. 93-107) New York: Routledge.

Cardoso, T., & Freeze, C. (2020, February 14). Toronto police chief orders officers to stop using Clearview AI software. Retrieved from https://www.theglobeandmail.com/canada/toronto/article-toronto-police-chief-orders-officers-to-stop-using-clearview-ai/

CBC News. (2020, February 14). Police use of facial recognition program breaks 'trust relationship' with public, privacy expert says. Retrieved from https://www.cbc.ca/news/canada/toronto/clearview-ai-toronto-police-ccla-privacy-1.5463823

Coleman, J.S. (1990). Foundations of social theory Belknap Press, Cambridge

Cozier, Z. R., & Witmer, D. F. (2001). The development of a structuration analysis of new publics in an electronic environment. In R. Heath & G. Vasquez (Eds.), Handbook of public relations (pp. 615–623). Thousand Oaks, CA: Sage.

De George, R. T. (2010). *Business ethic*s (7th ed.). Englewood Cliffs, NJ: Prentice Hall.

Dewey, J. (1938). Logic: The theory of inquiry. New York: Henry Holt.

Ehling, W.P. (1975). PR administration, management science, and purposive systems. *Public Relations Review*,1, 15–42.

El-Haddadeh, R., Weerakkody, V., Osmani, M., Thakker, D., & Kapoor, K. K. (2019). Examining citizens' perceived value of internet of things technologies in facilitating public sector services engagement. *Government Information Quarterly*, *36*(2), 310-320. https://doi.org/10.1016/j.giq.2018.09.009

Fombrun, C., & Riel, C. van. (1997). The reputational landscape. *Corporate reputation review*, 1–16.

Fountain, J.E. (2001). Building the Virtual State: Information Technology and Institutional Change, Brookings Institution Press, Washington, DC, pp. 155-89.

Giddens, A. (1990). The consequences of modernity. Retrieved from http://voidnetwork.gr/wp-content/uploads/2016/10/The-Consequences-of-Modernity-by-Anthony-Giddens.pdf

Garson, G.D. (1999). "Information systems, politics, and government: leading theoretical perspectives", in Garson, G.D. (Ed.), Handbook of Public Information Systems, Marcel Dekker, New York, NY, pp. 591-605.

Gefen, D., Benbasat, I., & Pavlou, P. (2008). A research agenda for trust in online environments. Journal of Management Information Systems, 24(4), 275-286.

Gil-Garcia, J.R. and Pardo, T.A. (2005). "E-government success factors: mapping practical tools to theoretical foundations", Government Information Quarterly, Vol. 22 No. 2, pp. 187-216.

Giroux, H. A. (2015). Totalitarian Paranoia in the Post-Orwellian Surveillance State, Cultural Studies, 29:2, 108-140, DOI: 10.1080/09502386.2014.917118

Government of Canada. (2019, August 01). What we do and why we do it. Retrieved from https://www.cse-cst.gc.ca/en/inside-interieur/what-nos.

Government of Canada. (2014, August 08). Mission, Vision and Values. Retrieved from https://www.cse-cst.gc.ca/en/about-apropos/vision-mission.

Grunig, J. E. (2013). Furnishing the edifice: Ongoing research on public relations as a strategic management function. In K. Sriramesh, A. Zerfass, & J.-N. Kim (Eds). *Public relations and communication management: Current trends and emerging topics* (pp. 1 – 26). New York: Routledge.

Harari, Y. N. (2016). Homo Deus: A Brief History of Tomorrow. Print.

Heath, R. I. (1997). *Strategic Issues Management*. Thousand Oaks, CA: Sage.

Hu, G., Pan, W., Lu, M. and Wang, J. (2009). "The widely shared definition of e-Government", The Electronic Library, Vol. 27 No. 6, pp. 968-985. https://doi.org/10.1108/02640470911004066 Download as .RIS

Innovation, Science and Economic Development Canada. (2019, May 21). Minister Bains announces Canada's Digital Charter. Retrieved from https://www.newswire.ca/news-releases/minister-bains-announces-canada-s-digital-charter-839625460.html

Jaeger, P.T. (2003). "The endless wire: e-Government as a global phenomenon", Government Information Quarterly, Vol. 20 No. 4, pp. 323-31.

Jaeger, P.T. and Thompson, K.M. (2004). "Social information behavior and the democratic process: information poverty, normative behavior, and electronic government in the United States", Library & Information Science Research, Vol. 26 No. 1, pp. 94-107.

Leichty, G. & Warner, E. (2001). Cultural topoi: Implications for public relations. Handbook of public relations. 61-74.

Loosemore, T. [@tomskitomski]. (2016, May 10). *Digital: Applying the culture, practices, processes & technologies of the Internet-era to respond to people's raised expectations*. Twitter. https://twitter.com/tomskitomski/status/729974444794494976.

Luhmann, N. (2000). 'Familiarity, Confidence, Trust: Problems and Alternatives', in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, chapter 6, pp. 94-107, Retrieved from http://www.sociology.ox.ac.uk/papers/luhmann94-107.pdf

Luhmann, N. (1989). Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität, Enke, Stuttgart.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society. https://doi.org/10.1177/2053951714541861

Mahmood, M, Osmani, M. & Sivarajah, U. (2014). The role of trust in E-government adoption: A systematic literature review. 20th Americas Conference on Information Systems, AMCIS 2014.

Mayer, R.C., Davis, J.H., and Shoorman, F.D. (1995). An Integrative Model of Organizational Trust, Academy of Management Review, 20, 3, 709-734.

Merriam-Webster. (2019a). Data. In Merriam-Webster.com. Retrieved from https://www.merriam-webster.com/dictionary/data

Merriam-Webster. (2019b). Surveillance. In Merriam-Webster.com. Retrieved from https://www.merriam-webster.com/dictionary/surveillance

Merriam-Webster. (2019c). Trust. In Merriam-Webster.com. Retrieved July 22, 2019, from https://www.merriam-webster.com/dictionary/trust

Metzler, M. S. (2001). The centrality of organizational legitimacy to public relations practice. In R. L. Heath (Ed.), *Handbook of public relations* (pp. 321-334). Thousand Oaks, CA: Sage.

Mitroff, I. I. (2019). *Technology run amok crisis management in the digital age*. Cham, Switzerland: Palgrave Macmillan.

Morey, T., Forbath, T., & Schoop, A. (2015, October 11). Customer Data: Designing for Transparency and Trust. Retrieved from https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

Morgeson, F. V., VanAmburg, D., & Mithas, S. (2011). Misplaced trust? Exploring the structure of the egovernment-citizen trust relationship. Journal of Public Administration Research and Theory, 21(2), 257-283.

Michael Nelson (1997) Building Trust in Cyberspace, International Information & Library Review, 29:2, 153-157, DOI: 10.1080/10572317.1997.10762423

Office of the Privacy Commissioner of Canada. (2019, May 9). Canadians concerned about privacy online; want more control over their personal information: poll. Retrieved from https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_190509/

Ontario Government. (2019, July 30). Promoting Trust and Confidence in Ontario's Data Economy. Retrieved from https://engage.ontario.ca/sites/default/files/discussion_paper1_eng_final.pdf

Ontario Government. (2020, January 20). Start with users. Deliver Together. Retrieved from https://www.ontario.ca/page/start-users-deliver-together

Pennington, R., Dixon, W.H. & Grover, V. (2003). The role of system trust in business-consumer transactions. Journal of Management Information Systems, 20,(3), 197–226.

Price, V. (1992): Public Opinion, Newbury Park, CA, Sage.

Pringle, R. (2020, February 1). Controversial Clearview AI app could 'end privacy.' So, what now? | CBC News. Retrieved from https://www.cbc.ca/news/technology/clearview-app-privacy-1.5447420

Public Relations Society of America. (n.d.). About Public Relations. Retrieved from https://www.prsa.org/about/all-about-pr

Schelin, S. H. (2003). E-Government: An Overview. In G. Garson (Ed.), *Public Information Technology: Policy and Management Issues* (pp. 120-138). Hershey, PA: IGI Global. doi:10.4018/978-1-59140-060-8.ch006

Stacks, D. W. (2017). *Primer of public relations research*. New York: The Guilford Press.

Teo, T. S., Srivastava, S. C., & Jiang, L. (2008). Trust and electronic government success: an empirical study. Journal of Management Information Systems, 25(3), 99-132.

Thomas, C. W. (1998). Maintaining and restoring public trust in government agencies and their employees. Administration and Society 30 (2): 166–93.

Tung, L.L. and Rieck, O. (2005), “Adoption of electronic government services among business organizations in Singapore”, Journal of Strategic Information Systems, Vol. 14 No. 4, pp. 417-40.

UN. (2002), “Benchmarking e-government: a global perspective”, available at: http://unpan1.un.org/intradoc/ groups/public/ documents/ UN/UNPAN021547.pdf

Vasquez, G. M. (1993). A homo narrans paradigm for public relations: Combining Bormann’s symbolic convergence theory and Grunig’s situational theory of publics. *Journal of Public Relations Research*, 5, 201–216.

Vasquez, G. M., & Taylor, M. (2001). Research perspectives on the public. In R. Heath & G. Vasquez (Eds), *Handbook of public relations* (pp. 127–138). Thousand Oaks, CA: Sage.

Welch, E., & Hinnant, C., & Jae Moon, M. (2005). Linking Citizen Satisfaction with E-Government and Trust in Government. Journal of Public Administration Research and Theory. 15. 371-391. 10.1093/jopart/mui02l.

Weston, G. (2014, January 31). CSEC used airport Wi-Fi to track Canadian travellers: Snowden documents | CBC News. Retrieved from https://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881.

World Bank (2003), “Definition of e-government”, available at: www1.worldbank.org/publicsector/egov/.

Yin, R. K. (2014). Case study research: Design and methods (5th Ed.). Thousand Oaks, CA: Sage Publications.

Appendix A

Survey

Question 1:

Please select whether you are a resident in Canada:

- I am a resident
- I am not a resident
- Prefer not to disclose

Question 2:

Please select your age:

- Under 18
- 19 – 25
- 26 – 35
- 36 – 45
- 46 – 55
- 56 – 65
- 66+
- Prefer not to disclose

Question 3:

Please select whether you are okay with public sector organizations collecting data on you:

- Yes
- Maybe
- No
- I don’t know

Question 4:

Please select whether you would agree to public sector organizations using information they have about you to send you personalized offers that match your interests:

- Yes
- Maybe
- No
- I don’t know

Question 5:

Please indicate your level of comfort to the following methods for collecting your data:

	Extremely comfortable	Comfortable	Average	Not very comfortable	Not comfortable at all	Don’t know
Internet browser history						
Filling out a form						
Health and identification records						
Observation through cameras						
Mailed questionnaires						
Telephone surveys						

Question 6:

How would you like public sector organizations to collect data on you?

Question 7:

What would you like public sector organizations doing with the information collected on you?

Question 8:

Do you think public sector organizations should be allowed to collect and store any information on you at all?

- Yes to all information
- Yes but only to some information
- No
- I don’t know

Appendix B

Question 1:

If you were going to collect and store information on your audience today, how would you go about doing so?

Question 2:

What does ethical data collection mean to you?

Question 3:

What would you consider ethical data collection?

Question 4:

What would you consider unethical data collection?

Question 5:

In your opinion is there a gap between how public sector organizations can legally collect data, and what is an ethical way to do so?

Question 6:

In your best opinion, what is the best method for collecting information on/about you?

Question 7:

What do you think the future holds for data collection for public sector organizations?

Question 8:

Is there any additional information you'd like to share regarding ethical data collection for public sector organizations?

Appendix C

LETTER OF INFORMATION / CONSENT - INTERVIEWS

A Study about ethical data collection for public sector organization

Principal Investigator:

Dr. Dave Scholz

Department of Humanities

McMaster University

Hamilton, Ontario, Canada 647-233-4682 E-mail:dscholz@avenue.cllmcmaster.ca

Student Investigator:

Anthony Petrielli

Department of Humanities

McMaster University

Richmond Hill, Ontario, Canada

(416) 710-2684

E-mail: petriela@avenue.cllmcmaster.ca

Purpose of the Study

You are invited to take part in this study on how public sector organizations can ethically collect data. I want to help create a framework for public sector organizations to follow. I am hoping to learn how public sector organizations can ethically collect information on their publics. I also hope to find out what publics are comfortable with when it comes to data being collected about them. I am doing this research for my capstone project.

What will happen during the study?

I will be asking you a series of questions about ethical data collection for public sector organizations in order to get your opinion(s) on this topic. This should take approximately 30 – 45 minutes. Questions include how you would ethically collect data and what would you consider unethical data collection to be.

With your permission I would like to take handwritten notes supplemented by audio-recording the interview.

Are there any risks to doing this study?

The risks involved in participating in this study are minimal. You may feel uncomfortable with answering questions related to ethics and collecting personal information. You may find it stressful to answer these questions at times.

You do not need to answer questions that you do not want to answer or that make you feel uncomfortable. I describe below the steps I am taking to protect your privacy.

Potential Benefits

The research will not benefit you directly. I hope to learn more about ethical data collection by public sector organizations. I hope that what is learned as a result of this study will help us to better understand how public sector organizations can collect information on their publics. This could help create a framework for these organizations to collect this information to better understand their publics.

Confidentiality

You are participating in this study confidentially. I will not use your name or any information that would allow you to be identified. No one but me will know whether you were in the study unless you choose to tell them.

The information/data you provide will be kept on a computer that is protected by a password. Once the study has been completed, the data will be destroyed.

What if I change my mind about being in the study? Your participation in this study is voluntary. It is your choice to be part of the study or not. If you decide to be part of the study, you can stop (withdraw), from the interview for whatever reason, even after signing the consent form or part-way through the study or up until March 31, 2020 when I expect to be submitting my capstone.

If you decide to withdraw, there will be no consequences to you. In cases of withdrawal, any data you have provided will be destroyed unless you indicate otherwise. If you do not want to answer some of the questions you do not have to, but you can still be in the study. In order to withdraw after the interview is completed, email the researcher directly at petriela@avenue.cllmcmaster.ca.

How do I find out what was learned in this study?

I expect to have this study completed by approximately March 31, 2020. If you would like a brief summary of the results, please let me know how you would like it sent to you.

Questions about the Study:

If you have questions or need more information about the study itself,

please contact me at: 416-710-2684.

This study has been reviewed by the McMaster University Research Ethics Board and received ethics clearance. If you have concerns or questions about your rights as a participant or about the way the study is conducted, please contact:

McMaster Research Ethics Secretariat

Telephone: (905) 525-9140 ext. 23142

C/o Research Office for Administrative Development and Support E-mail: ethicsoffice@mcmaster.ca

CONSENT

☐ I have read the information presented in the information letter about a study being conducted by

Anthony Petrielli of McMaster University.

☐ I have had the opportunity to ask questions about my involvement in this study and to receive additional details I requested.

☐ I understand that if I agree to participate in this study, I may withdraw from the study at any time

or up until March 31, 2020

☐ I have been given a copy of this form.

☐ I agree to participate in the study.

☐ I agree that the interview can be audio [video] recorded. [ ]Yes [ ]No

____

Anthony Petrielli – Letter of Information /Consent [version 4, December 15, 2019]

Signature: ______________________________________ Date: ________________________

Name of Participant (Printed) ___________________________________

SUMMARY OF RESULTS

[ ] Yes, I would like to receive a summary of the study's results.

Please send them to me at this email address ______________________________________ Or to this mailing

address:____

[ ] No, I do not want to receive a summary of the study's results.

Appendix D

Knowing Your Audience: How can public sector organizations ethically collect data?

This survey is administered by Anthony Petrielli, Department of Humanities at McMaster University. The purpose of the survey is to help understand how the general public feels about their data being collected by public sector organizations. Information gathered during this survey will be written up as a capstone project. What we learn from this survey will help us understand how public sector organizations can ethically collect data.

To learn more about the survey and the researcher's study, particularly in terms of any associated risks or harms associated with the survey, how confidentiality and anonymity will be handled, withdrawal procedures, incentives that are promised, how to obtain information about the survey's results, how to find helpful resources should the survey make you uncomfortable or upset etc., please read the accompanying letter of information.

This survey should take approximately 10 minutes to complete. People filling out this survey must be 18 years of age or older.

This survey is part of a study that has been reviewed and cleared by the McMaster Research Ethics Board (MREB). The MREB protocol number associated with this survey is MREB# 2379.

You are free to complete this survey or not. If you have any concerns or questions about your rights as a participant or about the way the study is being conducted, please contact:

McMaster Research Ethics Secretariat

Telephone 1-(905) 525-9140 ext. 23142

C/o Research Office for Administration, Development and Support (ROADS)

E-mail: ethicsoffice@mcmaster.ca

The “Consent to Participate” Statement:

Having read the above, I understand that by clicking the “Next” button below, I agree to take part in this study under the terms and conditions outlined in the accompanied letter of information.

Acknowledgements

I would like to express my thanks and gratitude to all those in my personal and professional life that not only made my time in the Master of Communications Management (MCM) program so enjoyable but helped pushed me to get to the end of the finish line. Perhaps a bit naïve, I did not know how much work and dedication this would truly take but I am proud of the journey it took to complete the program. I learned a lot about myself in this time, but also about how amazing my friends and family are.

To my parents, Lisa and Vince – thank you for always believing in me and supporting my goals. I can't think of two people I admire more. You both work so hard, yet to manage have fun and enjoy all life has to offer. I hope to follow in your footsteps.

To my MCM11 cohort – I joined this program for a degree, but I came away with much more. I learned something from each and every one of you. The group chat will live forever.

To my friends and family – your support and time has been incredible, and I truly believe I have the best friends and family in the world. Thank you for encouraging me along this road and always being there for me when I needed support.

To my bosses – Meeta Gandhi, Carol Moore and Kathleen Graver, and my work colleagues, thank you for believing in me and providing me opportunities to complete the program. You were all so supportive and caring. It means more than I can ever express.

Finally, I would like to express my thanks to my capstone supervisor, Dave Scholz, and program directors Alex Sevigny and Terry Flynn. You all pushed me, taught me in and out of the classroom and supported my curiosity. Thank you for teaching us to shoot the puck.

Anthony (Tony). March 17, 2020.