Volume 15

Spring

2019

djim.management.dal.ca |

Digital Distrust: Assuring Security and Trust in Egovernment

Christopher Fernandes and Francesca Patten

School of Public Administration, Dalhousie University

Abstract

As we enter the Anthropocene for digital information, governments are constantly seeking new ways to 'plug-in' populations and promote ease of access of government services. Dubbed 'e-governance', this concept uses Information and Communicative Technologies (ICT) to create and expand e-channels of service access to populations through the transformation and improvement of technology (Bannister & Connolly 2012). In doing so, however, the ability for government to connect with populations poses both technical and normative challenges surrounding assurance, security, and trust. Although the Government of Canada, for example, states explicitly that encryption and secure-sending of data should provide citizens with an adequate assurance of protection, this relationship is dependent upon the trust of the citizenship it serves (Immigration and Citizenship Canada 2018). What should happen, however, if the government is seeking to provide this service to a group with which it is not perceived to have a fully-established trust relationship with? Can the government 'create' trust through e-governance by highlighting access and transparency? This paper explores the theoretical frameworks of mutual trust and assurance which currently dictate the terms of Canadian e-government. Specifically, we explore both the normative elements of trust between marginalized groups and the government, as well as how policymakers use e-governance not only as a means of efficacy, but for explicit trust-building as well.

Introduction

One of the primary functions of government is to be universally and equally available to all citizens. When the systems of government are established and organized, they must consider this mandate in their actions. The emergence of the internet, and its integration into government, has dawned a new era of communication, characterized by its speed, both operationally and in its ability to innovate. The rapid adoption of this so-called Information Communication Technology (ICT) has revolutionized how governments and citizens interface with each other. While scholarship has struggled to maintain pace with the rapid emergence of issues in e-governance, changes to structures and systems continue to arise in drastic and unpredictable ways. As systems change and develop rapidly, the full weight of this cultural and organizational shift is thrust upon governing structures and forces them to make accommodations. In order to encourage full citizen utilization of e-government, governments must adapt to rapidly changing technology and conceptions of identity by establishing trust through meaningful assurance. To do so, however, will require both organizational restructuring as the current systems of governance do not have the organizational capacity to properly accommodate effective additional measures of doing so, and work within current systems of offline culture.

Definitions of Trust

Trust is a complex and multi-dimensional concept; it is both difficult to define and highly context-specific. In the terms of e-government, a great deal of research has already been done in pursuit of an accurate definition, which will hopefully lead to more effective social transaction between parties, both online and offline. There is great value in reviewing the available definitions of trust and establishing commonalities among those which are pre-existing, as establishing trust between government and citizens is essential to the proper functioning of e-government. A definition must include the who, how, and why of establishing citizen-e-government trust. To begin, universal across all definitions of trust are that it must involve both a trustor and a trustee to conduct the transaction (Papadopoulou, Nikolaidou &, Martakos, 2010; Colesca, 2009). The government and citizens can act in both of these roles, as the government must trust that citizens will use the services that they provide in the way that they are intended, or they will no longer supply the service. On the other hand, citizens must also trust that their governments are using their personal information in an appropriate way, or they will not use them. Additionally, the matter of purpose must factor into any working definition, which, in the case of e-government, requires creating the proper conditions for universal access to and use of e-government services (Papadopoulou et al., 2009). Not all people trust government equally, which has a definite impact on their use of government services. If there is no universal trust in government, then there can be no universal provision of services by the government, and thus they will be inefficient in their universal provision of service.

Trust is not homogeneous, meaning it cannot be built with only one approach. As such, understanding the various types of government trust required for e-government allows for a more thorough approach to establishing it. Papadopoulou, Niolaidou, and Martakos explain in their comprehensive typology of trust in e-government that citizens can have trust in stored data, services, information, systems, transactions, government organizations, and institutions (Papadopoulou et al., 2009). Each of these so-called 'types' are also accompanied by various dimensions such as reliability, confidentiality, and predictability. The dimensions, then, must be met in order to ensure trust in the various types. For many individuals, the various types represent different unique risks, which are emphasized by their various identity factors which already impact how much they trust the government. There is fundamentally "a 'trust tension': between the need to collect data on individuals as the basis for providing services," which means that people's identities are, now more than ever, disclosed to the government (Dutton, Guerra, Zizzo, & Peltu, 2005, p. 13). This matter is complicated by the fact that many people do not trust the government with their data, even offline, and by the added element of cyber risk. So, although some of these types share common dimensions, they are all unique contributors to e-government distrust and require unique solutions.

Factors and Dimensions of Trust in e-government

Although trust and assurance have been major topics of literature, trust is seen as a vital element of successful e-government policy. The great diversity of governments currently implementing ICTs to some degree also represents a wide variety of approaches, philosophies, and assumptions implicit in new programs and innovations. While this represents a large portion of data, the majority of current e-government programs are optional alternatives to traditional offline interfaces. As such, participation in many e-government programs has been optional, thus requiring trust for participation. This has impacted current literature, as it has assumed that trust is necessary for the proper functioning of e-government, an assumption which is also adopted for the purpose of this paper. There are a number of technical elements which apply to trust, including that physical cues which would indicate deceit being absent online, and the quality of the service and information which is available through e-government operations (Dutton et al., 2005). Additionally, in situations from a normative perspective, studies have shown that various factors of identity can have a notable impact on levels of trust as well. All factors have either a positive or negative relationship with trust, meaning that as positive factors increase, so too does the individual’s trust in e-government. Just the same, as a negative factor increases the level of trust decreases. Positive factors involve gender, education level, years of internet experience, trust in technology, and perceived trust-level in the government’s organization, quality perception, and perception of usefulness (Colesca, 2009). Negative factors include levels of concern with privacy, level of perceived risk, age, and gender (Colesca, 2009). Each of these factors then has an effect on citizens’ perceptions of the government’s willingness and ability to protect their identity data, including any data that is publicly accessible, relating to demographics, or highly personal information (Beldad, 2011). Identity management is the basis of trust between citizens and their governments. It must be done appropriately so that the many elements which influence trust can be managed and encouraged, and certainly not threatened by the risk of mismanagement.

Elements of individual’s identity influence how they trust government, and, in some cases, those identity markers also make them hesitant to disclose their personal information to the government, thus dissuading them from participating in e-governance at all. So, is there a way for e-government to act in a way that will encourage participation, rather than simply accepting technology as a further deterrent of service use? Certainly, there is a mainstream optimism that e-government creates “new and better government,” (2007, p. 375) as Bekkers and Homburg describe it, by reimagining the administrative responsibilities of government in a way that is “responsive, client oriented, and cohesive.” (2007, p. 375). From a technological perspective, ensuring that identity is protected appears to be paramount in establishing trust, through trustworthy authentication processes and systems for identification (Dutton et al., 2005). Trust cannot be purely technically established, however, as it must also address the normative elements which were previously mentioned. The aforementioned factors which influence trust are only a few elements of many, including personal experience. It is worth looking at one such experience to understand how trust can influence a demographic’s experience of government, and the considerations which must be made going forward.

Thus, the establishment of trust will require a multi-faceted approach by government when creating new e-government initiatives or transitioning existing functions and services online. This is the case because, although the creation of e-government is revolutionary in the sense that it changes what government does and, therefore, what government is, it still functions within the traditional power dynamics and frameworks which exist in offline government systems. As such, for e-government to be legitimately effective in revolutionizing government, it must be cognisant of the differing dimensions and characteristics of trust or e-government will fail to create the wider access to services which makes it useful.

Assurance of e-Governance: Quality and Identity Assurance

Assurance, as a factor of organizational design in identity management, can be primarily organized into two different 'branches': quality assurance and identity assurance. The latter is concerned primarily with security, the former with delivery, implementation and continuous development of e-government programs. The concept of identity management has already been touched upon, but it remains to be seen why assurance is necessary to assuring trust. Simply put, the government's investment in identity management, which is vital to its ability to function effectively, is pursued in order to create a relationship with its citizens, a process which is the "starting point of trust and confidence in interactions" (Stefanova, Kabakchieva, & Borthwick, 2010, p. 24; "Treasury Board Secretariat", 2013). Functionally, establishing this relationship is dependent on how organizations respond to the challenges associated with ensuring identity is managed appropriately and ethically when delivering e-government services to a population. If they are not proactive in this management, then citizens will feel that their concerns are not being heard, and they will have a more difficult time establishing trust in the future after it has been lost. Both quality and identity assurance have normative and technical dimensions and offer challenges to implementing effective yet efficient e-government services.

Quality assurance is "the ongoing, continuous process of evaluating, monitoring and improving the quality of a higher education system, institution, or programme ("Governance and Quality Assurance", p. 2). Specifically, governments are concerned with their e-government structures being both accessible, ergo, able to actually access the service, and proactive, so that citizens will want to access the service again independently (Lucia, Aquino, Tokairim, Torres, & Barbarian, 2004). Within the Canadian context, having a reliable program that can attain both of these criteria can have two main broader implications. Firstly, amidst a declining trust in government, robust e-government systems are seen as offering a potential solution (Myeong, Kwon, & Seo, 2014; Tolbert & Mossberger, 2006). Having a universally trusted, tested, and developed program that works under the pressures of public use can incentivize e-government and encourage governments to develop and enhance these programs. Alternatively, such programs can also have catastrophically negative results when they are not developed properly and can serve as counterproductive. The Phoenix pay system is an excellent example of poor organization design quality assurance (Simpson, 2018). Although it may have passed quality assurance expectations from a technical perspective, the failure of the government to execute their program will likely contribute to a decline in trust of the Canadian government to manage e-government programs. When a large program like Phoenix not only cannot operate, but the government also fails to respond to the issue in a timely manner, it becomes an ongoing stain on their credibility to conduct service delivery. As the vast majority of the online content which citizens access comes from private organizations, rather than government, the standard of quality that the government must adhere to in order to maintain usage is quite high, and so are citizens' expectations of it. Secondly, a failure to provide the necessary checks and balances to uphold the integrity of the program can also strain e-governance from a quality assurance standpoint. Checks can be performed as audits from several organizations such as the internal agencies or external companies ("Ernst & Young", 2018). In both situations, organizational collaboration, which is already a challenge within public-private partnerships, is strained. To combat this tension, considering either departmental, interdepartmental or inter-organizational problem-solving is required to ensure that quality in technical, as well as organizational, expectations are met ("Ernst & Young", 2018).

On the other side of assurance and management is identity. Identity assurance is "a measure of certainty that an individual, organization or device is who or what it claims to be. Identity risk is the risk that an individual, organization or device is not who or what it claims to be" ("Treasury Board Secretariat", 2016). The government and the people now act in a reciprocal manner of assurance when it comes to identity verification; the government assures that our identity will only be used by us, whereas the people assure that when using any ICT through e-government that they are truthful and honest with the identity they are accessing. In both situations, management of identity is crucial to the security in delivery of programs where service and delivery meet. For example, identity theft from the business sector often has policy implications, as those policies govern identity management (Colbert, 2017). Although, by definition, any activity impersonating the identity of another is considered fraud in the criminal code, questions of responsibility and accountability arise when identity assurance is compromised ("Bill C-46", 1985). Are the standards which private companies are held to the same as those which apply to the government? For the sake of responsible and ethical governance, this cannot be the case, as citizens are not customers for the government, and the trust which they have in government is not established in the same way.

Expectation and Reality: e-Governance and Assurance

Should identity that is compromised by the private sector, such as banking, result in policy changes by the government? As was previously mentioned, trust is complicated by the added technological element which it poses, and people's impressions are influenced by their experiences as customers with private enterprises online. Within e-governance, the use of technology is important in identity assurance. The use of technologies such as biometrics propose solutions for security, but challenges as well. Storage of data, indexing of metadata and retrieval of identity are just some of the many challenges that organizations must face when using technology in data management. One such challenge is answering the invasiveness that technology may pose; often, populations feel that biometric technologies are intrusive or invasive to personal privacy (Jackson, 2009). Storage of data, indexing of metadata and retrieval of identity are just some of the many other challenges that organizations must respond to when using technology in data management (Baldwin, Mount, Beres, & Shiu, 2008).

To bridge the technical challenges, the government can use robust and secure ICTs for e-governance to also meet the normative challenges of people's reprehension towards government. With the ever-growing interest in ICTs by governments, they must assure citizens that their identities are managed effectively and efficiently but also ethically (Meijer, 2015). ICTs give governments tools to design and implement structures of assurance through technological advancements, but if marginalized populations have no assurance in the power or faith of the government itself, the 'governance' part of e-governance fails. The government can continue to use the e-government system to extend its power, but the governance itself fails. Consequently, as the government increases the usage and tools of e-governance, marginalized populations, who are often unable to access ICTs, are left out of the presumed benefits (Hill, 2015). Although assurance in its purest form is a relationship between the government and people, e-Governance must overcome normative challenges of inherent identity formation that is resultant of governmental action; if one's experiences of the government is negative, then the person will either refrain from accessing e-Governance, or the challenges of implementing effective e-Governance through technical capabilities must address normative barriers.

Marginalized Populations and Challenges in e-Governance

As mentioned above, there are certain factors that can lead to a change (increase or decrease) when it comes to trust in the government (Colesca, 2009), yet some factors of trust can be attributed to the historical and political contexts of certain populations in Canada and their history with the government. For e-governance to work, that is the practice of government and ruling of populations through the medium of technology, there must be a reciprocity of acceptance of such governance with the government's trust of the good intentions of the people. If there are historical and political contexts that create an imbalance of power, or continued instances of violence towards a group, the legacies of such trauma may create a resistance or lack of trust in the government, rendering e-government and identity management obsolete.

In 2015, the Canadian government proposed Bill C-51, anti-terror legislation that would expand the powers of police and spy agencies (Shulman, 2015). Although the government proposed the legislation to combat the rising threat of terrorism, there were some who felt that the government could use this legislation as a legal way to "spy on political activists and movements" (Shulman, 2015, para. 10). Canada's extremely complex history has proved examples of the government actively monitoring and surveillance of citizens based on factors such as political identity, race and organizational affiliation. The internment of Japanese in Canada (whom many had been legal Canadian citizens) during World War II is an example of the government using legal methods of population displacement and deportation, many to a land not familiar (Sugiman, 2005). Additionally, the revelation of Project SITKA, a report undertaken by several Canadian agencies such as the RCMP and CSIS that provides "a snapshot of individual threats associated with Aboriginal public order events for the year" (Livesey, 2017, para. 27). Fundamentally, these examples are some among many that highlight how the Canadian government since Confederation has been concerned about identity management and surveillance. As Canada seeks to use more e-government services, can it repair the mismanagement of identity and rebuild trust amongst marginalized populations?

With the introduction of Bill C-59 adding changes to the oversight capabilities of CSIS and the Communications Securities Establishment (CSE) (which oversees Canada's cyber and signal intelligence), the ever-changing growth of technology produces complex problems that require policy intervention (Roach, Carvin, & Focese, 2017). However, if the government has mismanaged identity or proven itself to abuse the trust given by the citizens through democratic legitimacy, growing e-government proves itself a challenge through access. Marginalized populations may voluntarily refrain from using e-government services for personal reasons, creating fundamental gaps and opportunities for government identity management. If there is a growing use of e-government services (either from a perceived sense of efficacy or governments seeking to shift services online for greater access), marginalized populations may lose the capability to decide on voluntary government identity management. Policy decisions from all levels of governments must account for legacies of abuse of power in marginalized communities when creating, changing or implementing e-government.

Collaboration in Service Delivery of e-Governance

As Canada explores different options to promote e-governance as a method for delivering services, the critical role of the government in providing services by promoting methods of efficiency in an innovative environment is occurring alongside the constant changing nature of electronic technologies. Given that the Government of Canada recognizes a need to think differently in the face of changing technologies, it must look towards innovating the public sector and service delivery as a response to the rapid development of technology ("Canadian Digital Service", 2017). This reflectiveness and necessity for innovative development reflects in Canada's creation of the Canadian Digital Service, a project that borrows 'ways-of-thinking' from the private sector from leading start-ups such as Shopify and brings their talents to the public sector ("Canadian Digital Service", 2017; Ireton, 2017). Ideally, the government is attempting to shape the public sector and service delivery by borrowing such tools as innovative method development and efficient processes service delivery ("Canadian Digital Service", 2017). Knowing that the public sector faces challenges such as innovative service delivery means that the public sector can integrate certain strengths found in the private sector through collaborative efforts (Schuurman & Tõnurist, 2016). On one hand, innovation is key for private-sector businesses as it aims to improve efficiency and improve products (Cankar & Petkocesk, 2013). On the other hand, recognizing that the public sector is not a business and concerned with profits, innovation through service delivery is underexplored (Schuurman & Tõnurist, 2016). Given that a primary objective of e-governance is service delivery, and given that our understanding that people's experiences of e-governance is shaped through experiences in the private sector, it is reasonable to suggest that the Canadian government use talent and innovative thinking that prospered in the private markets to produce 'better' e-government service delivery. By creating zones of innovative thinking (whether it's the Canadian Digital Service or innovation hubs), the ability to use private-sector practices to strengthen service delivery in the public sector is an experiment that will provide interesting results in the future.

Organizational Design and E-Government: Future Issues

To this point, it has been argued that the current systems of e-government trust and assurance are attempts by the government to adapt to the massive changes necessitated by the emergence of new technologies on the current organizational design. For a number of reasons, the current system is not equipped to deal with these changes. To begin, the creation of the majority of e-government systems have been created by the private sector, for private sector purposes. As the government is not currently in the position of innovating itself, it is currently adapting systems which are at odds with its own function. By using systems which were developed for the private sector for public sector functions, the current systems face a value and organizational conflict in their nature. Secondly, the creation of the internet is a vast new medium, often ungovernable by organizations and constantly changing. The new medium favours radical, or at least rapid, change. The government is accustomed to incremental change, and thus cannot fully operate under the same conditions as the internet necessitates. As government organization is unable to change radically and quickly, e-government will pose significant problems in its future impacts on government structures.

References

Baldwin, A., Mount, M.C., Beres, Y., & Shiu, S. (2018). Assurance for Federated Identity Management. HP Laboratories, 1-29.

Bekkers, V., & Homburg, V. (2007). The Myths of E-Government: Looking Beyond the Assumptions of a New and Better Government. The Information Society, 25 (5), 373-382.

Beldad, A., de Jong, M., & Steehouder, M. (2011). I Trust Not Therefore it Must be Risky: Determinants of the Perceived Risks of Disclosing Personal Data for E-Government Transactions. Computers in Human Behavior, 27, 2233-3342.

Bill C-46. (1985). An Act respecting the criminal law. Retrieved from https://laws-lois.justice.gc.ca/eng/acts/C-46/section-380.html.

Caldwell, N. D., Roehrich, J.K., & George, G. (2017). Social Value Creation and Relational Coordination in Public-Private Collaborations. Journal of Management Studies, 54(6), 906-28.

Canadian Digital Service. (2017). What We Do - Canadian Digital Service. Retrieved from https://digital.canada.ca/what-we-do/

Cankar, S.S., & Petkovsek, V. (2013). Private And Public Sector Innovation And The Importance Of Cross-Sector Collaboration. Journal of Applied Business Research, 29(6), 1597-606.

Colbert, Y. (2017). Identity-theft Victim Says Thieves Have It Easy and Federal Rules Must Change. CBC News. Retrieved from https://www.cbc.ca/news/canada/nova-scotia/identity-theft-mail-forwarding-fraud-canada-post-1.4193216.

Colesca, S. E. (2009). Understanding Trust in e-Government. Inzinerine

Ekonomika-Engineering Economics 3, 7-15.

Dutton, W., Guerra, G.A., Zizzo, D.J., & Peltu, M. (2005). The Cyber Trust Tension in E-government: Balancing Identity, Privacy, Security. Information Polity, 10(1-2), 13-23.

Assurance. (n.d). Ernst & Young. Retrieved from https://www.ey.com/ca/en/industries/government---public-sector/government-and-public-sector_assurance.

Filgueiras, L., Aquino, P., Tokairim, V., Torres, C., & Barbarian, I. (2004). Usability Evaluation as Quality Assurance of E-Government Services. IFIP Advances in Information and Communication Technology, 77-87.

Hill, W. C. (2015). E-Governance: Silencing Vulnerable Populations. Procedia Engineering, 107, 181-85.

Ireton, J. (2017). Canadian Digital Service Takes Startup Approach to Building Better IT for Government. CBC News. Retrieved from https://www.cbc.ca/news/canada/ottawa/canadian-digital-service-recruiting-it-brains-prevent-phoenix-1.4445010.

Jackson, L. A. 2009. Biometric Technology: The Future of Identity Assurance and Authentication in the Lodging Industry. International Journal of Contemporary Hospitality Management, 21(7), 892-905.

Livesey, B. (2017). Spies in Our Midst: RCMP and CSIS Snoop on Green Activists. National Observer. Retrieved from https://www.nationalobserver.com/2017/05/05/news/spies-our-midst-rcmp-and-csis-snoop-green-activists.

Meijer, A. (2015). E-governance Innovation: Barriers and Strategies. Government Information Quarterly, 32(2), 198-206.

Myeong, S., Kwon, Y., & Seo, H. (2014). Sustainable E-Governance: The Relationship among Trust, Digital Divide, and E-Government. Sustainability, 6(9), 6049-6069.

Papadopoulou, P., Nikolaidou, M., & Martakos, D. (2010). What is Trust in E-Government? A Proposed Typology. Proceedings of the 43rd Hawaii International Conference on System Sciences, 1-10.

Roach, K., Carvin, S., & Forcese, C. (2017). We Need Real, Honest Debate on Bill C-59. The Globe and Mail. Retrieved from https://www.theglobeandmail.com/opinion/we-need-real-honest-debate-on-bill-c-59/article37175837/.

Schuurman, D., & Tõnurist, P. (2016). Innovation in the Public Sector: Exploring the Characteristics and Potential of Living Labs and Innovation Labs. Proceedings of the OpenLivingLab Days 2016, Montreal, Canada, 78-90.

Shulman, M. (2015). Demonstrators Across Canada Protest Bill C-51. CTVNews. Retrieved from https://www.ctvnews.ca/politics/demonstrators-across-canada-protest-bill-c-51-1.2279745.

Simpson, K. (2016). Conservatives Took Payroll Training Responsibilities Away from Phoenix Creator IBM. CBC News. Retrieved from https://www.cbc.ca/news/politics/conservatives-took-phoenix-training-away-from-ibm-1.3779917.

Stefanova, K., Kabakchieva, D., & Borthwick, L. (2010). Innovative Approach to Identity Management Solution Development for E-government at EU Level. Journal of Telecommunications and Information Technology, 8(2), 24-31.

Sugiman, P. (2005). 2. Memories of Internment: Narrating Japanese-Canadian Women’s Life Stories. Diaspora, Memory, and Identity, 48-80.

Tolbert, C. J., & Mossberger, K. (2006). The Effects of E-Government on Trust and Confidence in Government. Public Administration Review, 66(3), 354-369.

Treasury Board Secretariat. (2016). Guideline on Identity Assurance. Retrieved from https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678§ion=HTML.

Treasury Board Secretariat. Standard on Identity and Credential Assurance. Retrieved from https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678§ion=HTML.

Governance and Quality Assurance. Paris: UNESCO International Institute for Educational Planning. Retrieved from http://www.iiep.unesco.org/sites/default/files/brochure_higher_education.pdf.