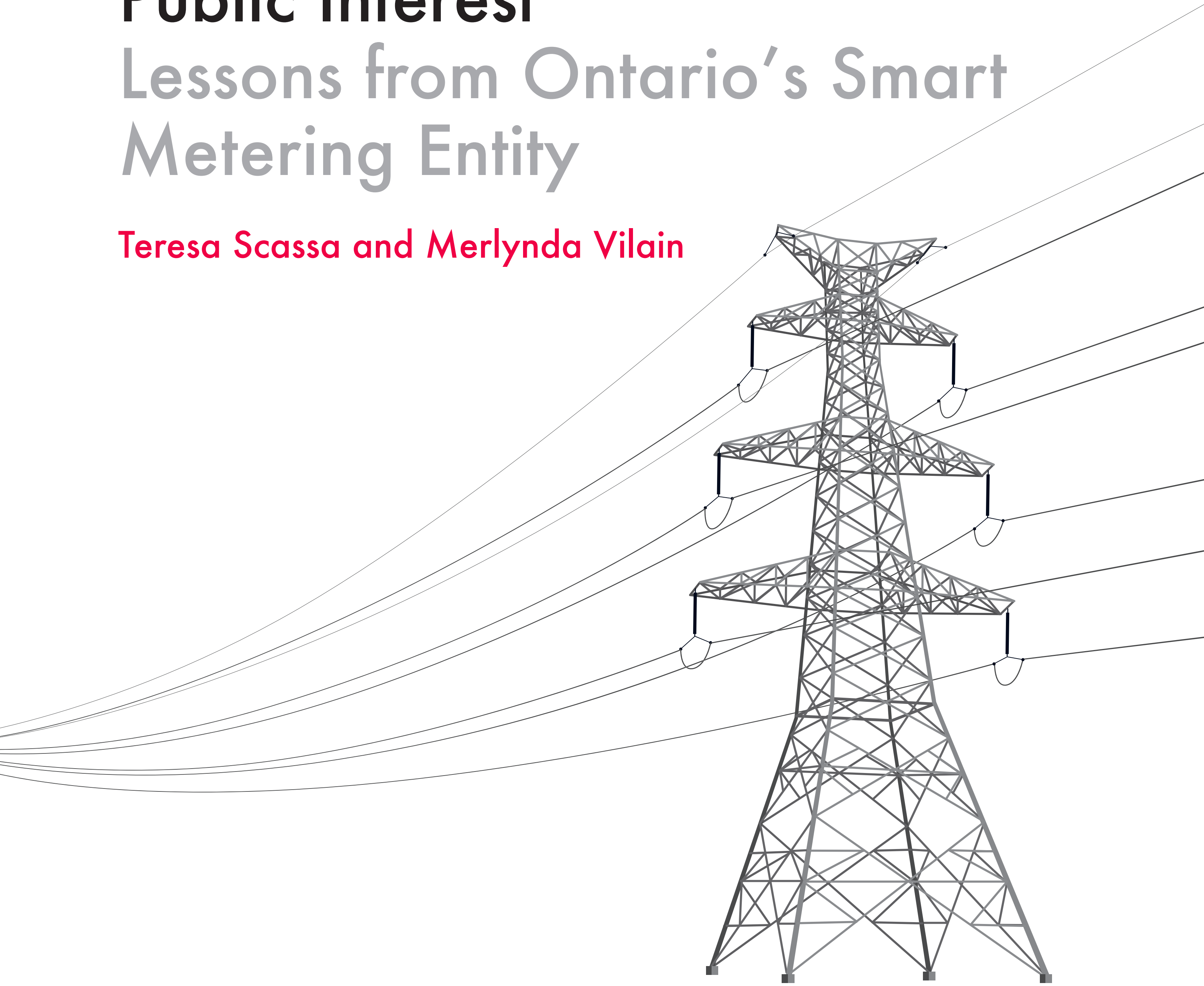
Centre for International Governance Innovation

CIGI Papers No. 221 — July 2019

Governing Smart Data in the Public Interest

Lessons from Ontario's Smart Metering Entity

Teresa Scassa and Merlynda Vilain



Centre for International
Governance Innovation

CIGI Papers No. 221 — July 2019

Governing Smart Data in the Public Interest

Lessons from Ontario's Smart Metering Entity

Teresa Scassa and Merlynda Vilain

CIGI Masthead

Executive

President Rohinton P. Medhora
Deputy Director, International Intellectual Property Law and Innovation Bassem Awad
Chief Financial Officer and Director of Operations Shelley Boettger
Director of the Global Economy Program Robert Fay
Director of the International Law Research Program Oonagh Fitzgerald
Director of Human Resources Laura Kacur
Deputy Director, International Environmental Law Silvia Maciunas
Deputy Director, International Economic Law Hugo Perezcano Díaz
Managing Director and General Counsel Aaron Shull
Director of Communications and Digital Media Spencer Tripp

Publications

Publisher Carol Bonnett
Senior Publications Editor Jennifer Goyder
Senior Publications Editor Nicole Langlois
Publications Editor Susan Bubak
Publications Editor Patricia Holmes
Publications Editor Lynn Schellenberg
Graphic Designer Brooklynn Schwartz
Graphic Designer Melodie Wakefield

For publications enquiries, please contact publications@cigionline.org.

Communications

For media enquiries, please contact communications@cigionline.org.

@cigionline

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fiber.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Authors

Teresa Scassa is a senior fellow with CIGI's International Law Research Program. She is also the Canada Research Chair in Information Law and Policy and a full professor at the University of Ottawa's Faculty of Law, where her groundbreaking research explores issues of data ownership and control. Teresa is an award-winning scholar and is the author and editor of five books and more than 65 peer-reviewed articles and book chapters. She has a track record of interdisciplinary collaboration to solve complex problems of law and data and was part of the Geothink research partnership. Teresa is a founding member of the University of Ottawa's Centre for Law, Technology and Society, is cross-appointed to the School of Information Studies at the University of Ottawa, and is a member of the Geomatics and Cartographic Research Centre at Carleton University.

At CIGI, Teresa's research focuses on the legal challenges associated with data ownership and the need for a national data strategy in a data-driven economy. Her research also covers the governance of smart cities' data and its implications for innovation, transparency, accountability, sovereignty and privacy.

Teresa has worked as a consultant for government and the private sector and has also worked with non-governmental organizations on issues within her areas of legal expertise. She is chair of the Canadian Statistics Advisory Council, a member of the Canadian government's Advisory Council on Artificial Intelligence and a member of the Digital Strategy Advisory Panel for Waterfront Toronto. Teresa holds degrees in civil and common law from McGill University, as well as an LL.M. and a doctorate from the University of Michigan. She clerked for Mme Justice Claire L'Heureux-Dubé at the Supreme Court of Canada from 1988 to 1989.

Merlynda Vilain is entering her final year of the six-year juris doctor (French common law) and bachelor of commerce combined program at the University of Ottawa.

About the Program

The International Law Research Program (ILRP) at CIGI is an integrated multidisciplinary research program that provides leading academics, government and private sector legal experts, as well as students from Canada and abroad, with the opportunity to contribute to advancements in international law.

The ILRP strives to be the world's leading international law research program, with recognized impact on how international law is brought to bear on significant global issues. The program's mission is to connect knowledge, policy and practice to build the international law framework — the globalized rule of law — to support international governance of the future. Its founding belief is that better international governance, including a strengthened international law framework, can improve the lives of people everywhere, increase prosperity, ensure global sustainability, address inequality, safeguard human rights and promote a more secure world.

The ILRP focuses on the areas of international law that are most important to global innovation, prosperity and sustainability: international economic law, international intellectual property law and international environmental law. In its research, the ILRP is attentive to the emerging interactions among international and transnational law, Indigenous law and constitutional law.

Acronyms and Abbreviations

APIs	Application Program Interfaces
DSAC	Data Strategy Advisory Council
FIPPA	Freedom of Information and Protection of Privacy Act
IESO	Independent Electricity System Operator
LDCs	local distribution companies
MDM/R	Meter Data Management/Repository
MFIPPA	Municipal Freedom of Information and Protection of Privacy Act
OEB	Ontario Energy Board
OIPC	Ontario Information and Privacy Commissioner
PbD	Privacy by Design
PIPEDA	Personal Information Protection and Electronic Documents Act
SME	Smart Metering Entity
SMI	Smart Metering Initiative
TOU	time of use

Executive Summary

The collection of vast quantities of personal data from embedded sensors is increasingly an aspect of urban life. This type of data collection is a feature of so-called smart cities, and it raises important questions about data governance. This is particularly the case where the data may be made available for reuse by others and for a variety of purposes.

This paper focuses on the governance of data captured through "smart" technologies and uses Ontario's smart metering program as a case study. Ontario rolled out mandatory smart metering for electrical consumption in the early 2000s largely to meet energy conservation goals. In doing so, it designed a centralized data governance system overseen by the Smart Metering Entity (SME) to manage smart meter data and to protect consumer privacy. As interest in access to the data grew among third parties, and as new potential applications for the data emerged, the regulator sought to develop a model for data sharing that would protect privacy in relation to these new uses and that would avoid uses that might harm the public interest.

The SME is a particularly interesting case study in that it involves public sector data, public and private sector stakeholders, and a considerable body of relatively sensitive personal information. It is a good example of a model that was required to adapt to changes in the value of the data collected and to new demands for access to that data by both public and private sector actors. The SME was pushed to collect additional data attributes to enrich the value of the data for potential users. This paper examines the SME model and the challenges it has faced over time and draws lessons for data governance that may be more broadly applicable for data stewardship.

The model of the SME may be particularly useful in the smart cities context. Smart cities feature both public and private sector actors and collect large volumes of human behavioural data. Consequently, there is strong public interest in appropriate data governance. In the smart metering and smart cities contexts alike, individuals have little choice but to have their data collected. The data collector operates from the premise that the reuse and repurposing of this data across different contexts has the potential to benefit the public. With a greatly diminished focus on consent, individuals and communities require frameworks that can assist in achieving the identified public interests while at the same time protecting individual and community privacy and ensuring that data is not used in ways that are harmful or exploitative.

Introduction

Smart technologies involve the collection of vast quantities of personal and/or non-personal data from embedded sensors. Increasingly, they are used by governments and the private sector in a range of contexts, including in smart cities. Examples of personal data collected by smart technologies include service consumption data (such as transit, utilities, parking or recreation) while examples of non-personal data can include data about infrastructure, environmental conditions and traffic patterns. Some data might also be aggregate depersonalized data regarding the movements of individuals or their vehicles. Such data can be used by municipalities to improve planning and services through a combination of smart analytics, artificial intelligence and machine learning. However, this data holds great potential and interest for private sector corporations, researchers and civil society actors. Determining what data should be collected, by whom, with whom it should be shared and under what conditions are increasingly important data governance issues for those who deploy smart technologies, including governments.

Data governance has been defined as "a framework which formalizes the roles, functions, and procedures within which an organization's data is well-managed and enabled as a strategic asset."[1] While much of the literature around data governance focuses on private sector companies, data governance is important to any organization that collects and uses data, and is commonplace within the public sector as well. As Barbara Cohn notes, data governance "sets forth an organization's vision, as well as its policies, protocols, and standards in support

[1] Barbara L Cohn, "Data Governance: A Quality Imperative in the Era of Big Data, Open Data, and Beyond" (2015) 10:3 ISJLP 811 at 813.

of attaining maximum value from data."[2] Depending on the nature of the organization and the nature of the data, data governance may require attention to issues of data quality, standards, data storage, protection of privacy and confidentiality, data security, data retention and disposal. In a growing number of contexts, data governance practices must address when and how data is to be shared and with whom.

This paper explores the data governance model designed for Ontario's smart metering system for electricity consumption. In Ontario, plans to introduce smart meters, designed to generate granular data about electrical consumption, led to concerns about how to balance the interests of public and private sector actors that are accessing and using this data with public concerns over privacy rights. To address these issues, the province created an SME that would be charged with the management of smart meter data.

This paper examines the SME and considers what lessons this model might provide for the creation of other data governance frameworks. The authors consider the context that gave rise to the creation of the SME, the type of data it collects and manages, and how data demands have evolved. They look at the legal instruments that established the SME, its terms of reference as they relate to the stewardship of data, the data governance policies and practices put in place, and the role of the public and consultation in developing this model.

The authors' work takes place in the shadow of debates over an appropriate data-sharing governance model for the proposed Sidewalk Labs-Waterfront Toronto Quayside "smart city" development. The Ontario government has launched a data strategy consultation that includes measures to support data governance for data sharing. In the last section of this paper, the authors identify a number of these measures to extract lessons that can be learned from the SME experience and that may be relevant to building future data governance frameworks for data sharing in the public interest.

The SME

Smart metering is a fundamental aspect of what is known as the "smart grid." Roy Raghavan defines the smart grid as "an electrical system that enables two-way flows of electricity and information in an attempt to reduce costs, increase reliability, and save energy."[3] As with other forms of smart technology, there is a degree of interactivity and consumer engagement. One of the features of the smart grid is that it enables consumers to play a more active role in energy conservation. In Ontario, while consumers are provided with more data about their consumption practices and presented with different options for conserving energy, they do not get to opt in or opt out of smart metering.[4] Smart meter data is therefore similar to smart cities data collection that is hard-wired into urban infrastructure.

Electricity pricing has been, and still is, a political problem for many governments, including Ontario's. To confront the challenging pricing scheme in the province, the Ontario government sought to reduce energy consumption by implementing a "culture of conservation."[5] This strategy, introduced in April 2004, included the Smart Metering Initiative (SMI), which rolled out smart electricity meters to measure the electricity amount and the usage time per household. The first target was to install 800,000 smart meters by 2007, with the installation for all residential and small-business ratepayers completed by 2010.[6] In spring 2009, Ontario's minister of energy and infrastructure announced time of use (TOU) billing as the new plan for energy

[2] *Ibid* at 814.

[3] Roy Raghavan, "An Examination of Smart Grid Privacy in Ontario" (2010) at 6, online: <www.eng.mcmaster.ca/sites/default/files/uploads/roy_raghavan_smartgrid.pdf>.

[4] Avner Levin, "Applying PIPEDA to the Smart Grid" (2011) at 8, online: <www.ryerson.ca/content/dam/tedrogersschool/privacy/documents/Applying_PIPEDA_to_the_Smart_Grid.pdf.>

[5] Auditor General of Ontario, *2014 Annual Report of the Office of the Auditor General of Ontario* (2014), c 3, s 3.11 ("Smart Metering Initiative") at 362, online: <www.auditor.on.ca/en/content/annualreports/arreports/en14/311en14.pdf>.

[6] *Ibid*.

pricing.[7] Smart meters facilitated the new pricing structure because of their ability to monitor in real time the consumption of electricity.[8] The pricing structure was based on low prices overnight, higher prices during the mid-peak period and highest prices at peak weekday times.

The Ministry of Energy was the central planner for the SMI and collaborated with the Ontario Energy Board (OEB), which is the electricity sector regulator; the Independent Electricity System Operator (IESO), which is the designated SME since July 2007; and, finally, the local distribution companies (LDCs), which supply electricity to consumers and own the smart metering systems.[9] Although the SME is a division of the IESO, which has a separate licence from the OEB, the SME has its own steering committee. Its main responsibility is to develop, implement and operate a central meter data management system to be the repository of all energy consumption data collected from smart meters throughout the province.[10]

The central data hub, the SME's Meter Data Management/Repository (MDM/R), is operated by IBM.[11] This platform allows for secure "storing, processing, validating and managing hourly electricity consumption information to support LDCs' billing processes."[12] There are currently 65 LDCs integrated into the system, with around five million smart meters installed, which transfer data hourly.[13]

SME Legal Framework and Governance

Section 53.7 of the Electricity Act, 1998,[14] charges the SME with carrying out the government's SMI. The SME's mandate as it relates to data is set out in section 53.8:

> 2. To collect and manage and to facilitate the collection and management of information and data and to store the information and data related to the metering of consumers' consumption or use of electricity in Ontario, including data collected from distributors and, if so authorized, to have the exclusive authority to collect, manage and store the data....
>
> 4. To provide and promote non-discriminatory access, on appropriate terms and subject to any conditions in its licence relating to the protection of privacy, by distributors, retailers, the IESO and other persons,
>
> > i. to the information and data referred to in paragraph 2, and
> >
> > ii. to the telecommunication system that permits the Smart Metering Entity to transfer data about the consumption or use of electricity to and from its databases, including access to its telecommunication equipment, systems and technology and associated equipment, systems and technologies.

In 2007, the IESO (a Crown corporation) was designated by regulation as the SME.[15] The IESO is a not-for-profit Crown corporation without share capital.[16] Section 5(1) of Regulation 393/07 gives the SME exclusive authority over various functions such as receiving smart metering data and providing all services performed on smart metering data to create billing quantity data, including validation, estimating and editing

[7] Donald N Dewees, "The Price Isn't Right: The Need for Reform in Consumer Electricity Pricing" (2010) 124 CD Howe Institute Backgrounder 1 at 1, online: <www.cdhowe.org/sites/default/files/attachments/research_papers/mixed//backgrounder_124.pdf>. In 2010, the Ontario Energy Board (OEB) issued a final determination to mandate TOU pricing for regulated price plan customers: see OEB, "Determination to Mandate Time-of-use Pricing" (2010), online: <www.oeb.ca/industry/policy-initiatives-and-consultations/determination-mandate-time-use-pricing>.

[8] Dewees, *supra* note 7.

[9] *Ibid* at 363.

[10] *Ibid*.

[11] Barbara Vergetis Lundin, "MDM helps Ontario ISO keep up with utility transformation", *FierceEnergy* (11 February 2013).

[12] IESO, "SME Overview", online: <www.ieso.ca/en/Sector-Participants/Smart-Metering-Entity/SME-Overview>.

[13] *Ibid*.

[14] SO 1998, c 15, Schedule A, s 2 (as amended in 2006) [*Electricity Act*].

[15] O Reg 393/07, s 1.

[16] IESO, "Privacy Policy" (last modified 26 September 2018), online: <www.ieso.ca/privacy>.

services.[17] The mandate of the SME is established by law and regulation. This lays the groundwork for a data governance model with considerable government control. The mandate also makes it clear that the operations of the SME are subject to the public sector Freedom of Information and Protection of Privacy Act [FIPPA].[18]

Data Collected and the Purpose of Collection

The SME has the power to "directly or indirectly collect information and data relating to the consumption or use of electricity from consumers, distributors or any other person."[19] The SME was designed to provide a central point for collection, management and hosting of all of the province's smart meter data. Reciprocally, distributors, retailers and other persons must share any information required for the SME to conduct its business.[20] Data collected through the SMI is processed and stored in the SME's MDM/R.

Essentially, data travels from smart meters installed at a residence, a business or a sub-metering entity to neighbourhood collectors. These collectors transmit the data to control computers that transmit it to the MDM/R. It is the responsibility of the SME to accurately convert the data into TOU billing data and to send it to the LDCs,[21] which use this data to produce individual customer bills. The LDCs also provide customers with data dashboards that allow them to visualize their consumption patterns.[22] In this system, the LDCs (the local companies that provide electricity to customers) do not directly collect or process the raw smart metering data. Rather, this data is transmitted to the SME for processing, with each LDC receiving access to the subset of processed data it requires to deal with its customers.[23]

From a consumer perspective, the SME and its operations are invisible.[24] Consumers contact the LDC in their area and enter into a contract for the provision of electricity. The smart meter (which, once installed, remains on their property) collects consumption data, and the consumer receives a monthly bill from their LDC based upon this consumption. They also receive information about how to access their own personal data dashboard, which provides them with more fine-grained details about their electricity usage.

Shifting Purposes and New Data Collection

Although the original goals for collecting smart meter data related to greater energy efficiency, the data was also of interest to certain federal and municipal government departments and agencies, as well as to academic researchers. In 2013, a report issued by the Ontario Information and Privacy Commissioner (OIPC) explored the growing demand for access to SME data by the private sector.[25] This demand was linked to heightened interest on the part of consumers to access their own consumption data and on the part of companies seeking to develop new consumption management tools for business and residential customers. The growing interest in SME data came from "a new class of third parties wishing to gain access to granular and customer-specific usage data (e.g., app developers, software

[17] O Reg 393/07, *supra* note 15.

[18] RSO 1990, c F.31 [*FIPPA*].

[19] *Electricity Act*, *supra* note 14 at s 53.14(a).

[20] *Ibid*, s 53.15(1).

[21] Tracey P Lauriault, Rachel Bloom & Jean-Noé Landry, *Open Smart Cities in Canada: Assessment Report* (2018) at 74, online: <https://osf.io/preprints/socarxiv/qbyzj>.

[22] Information and Privacy Commissioner, *Building Privacy into Ontario's Smart Meter Data Management System: A Control Framework* (2012) at 10, online: <www.ontla.on.ca/library/repository/mon/26005/317398.pdf>.

[23] Note that the 2014 annual report by Ontario's Auditor General showed that in practice, not all LDCs supply data; not all rely on the central processing of the data to produce bills; and that there were problems and inefficiencies with the SME's ability to handle customer queries. The result is duplication of costs to some consumers. See Auditor General of Ontario, *supra* note 5.

[24] As discussed below, this complex arrangement may create confusion over which data privacy regime applies and who is responsible.

[25] Ann Cavoukian & Jules Polonetsky, *Privacy by Design and Third Party Access to Customer Energy Usage Data* (Toronto: Information and Privacy Commissioner, 2013), online: <www.ipc.on.ca/wp-content/uploads/Resources/pbd-thirdparty-CEUD.pdf>.

vendors, device manufacturers, consumer service providers, and home security companies, etc.)."[26]

Two different initiatives are linked to this push for greater access to customer data. The first is the Green Button initiative, an industry-driven plan built on the 2012 call by the White House for new tools to assist consumers with accessing their energy consumption data so as to better manage their energy use[27] and to set industry-standard formats for utility consumption data. This initiative enables consumers to make their data portable, giving consent to third-party companies to access their data in order to provide products or services that meet their needs. The Green Button initiative also supports private sector development of these tools and services. The Ontario plan to have its LDCs participate in this initiative by adopting the Green Button data standards is set to take effect in July 2020.[28]

A second initiative relates to enhancing the data collected by the SME and increasing its availability to researchers, government and corporate actors. A first phase involved a decision to collect additional data in order to add value to the smart metering data.[29] This additional data was meant to include some form of location data. While this added value to the energy usage data, it also raised fresh privacy concerns.

In March 2015, the IESO set up the Foundation Project Working Group to explore enhancing smart metering data and making it more widely available.[30] The group was to examine the "potential for significant improvement in harnessing the value of the MDM/R data set for designing conservation and demand response programs, system planning, policy development, academic research and to support innovation in Ontario."[31] The working group issued its *Foundation Project Final Report* on November 4, 2015, which contained a "Framework for Third Party Access" and a "Framework for De-Identification of Information for Disclosure to Third Parties."[32] The report was careful to note that it contained only "high-level" recommendations, and that issues remained to be addressed prior to any implementation.[33] One of these issues was compliance with the province's FIPPA. It was noted that the additional location data elements, which were sought to be added to the smart meter data, would raise privacy compliance issues that would have to be addressed. The working group also recognized the value of data matching and analysis but acknowledged that this might raise privacy issues. The working group suggested that prior to any implementation, it would be important to identify an organization that could match data sets before issuing de-identified results.[34] The working group also flagged the cost issues associated with the processes necessary for implementing third-party access. Essentially, the report identified key issues to consider and resolve but stopped short of recommending specific actions for implementation.

According to the OEB, the SME was not taking full advantage of the collected data, stating "there are potentially much greater benefits to consumers from this consumption data, in particular by making non-personal information available to third parties to assist them in developing new innovative products and services that will enhance customer choice and control."[35] The OEB also wanted to see more information collected from consumers to enhance the usefulness of the data. In particular, the OEB imposed on the SME, effective January 1, 2017, to

> collect the following information associated with each meter (modified where necessary to sufficiently render it

[26] *Ibid* at 3.

[27] Green Button Data, "Green Button Data...secure, anonymous, digital", online: <www.greenbuttondata.org/>.

[28] Environmental Registry of Ontario, *Regulatory proposal for province-wide implementation of Green Button*, ERO 013-1874, online: <https://ero.ontario.ca/notice/013-1874>.

[29] OEB, *Report of the Board: Supplemental Report on Smart Grid* (2013), online: <www.oeb.ca/oeb/_Documents/EB-2011-0004/Supplemental_Report_on_Smart_Grid_20130211.pdf>.

[30] Lauriault, Bloom & Landry, *supra* note 21 at 75.

[31] IESO, *Foundation Project Final Report* (2015) at 1 [IESO, *Foundation Project*], online: <www.ieso.ca/-/media/Files/IESO/Document-Library/engage/foundation/Foundation-20151104-Foundation-Project-Final-Report.pdf?la=en>.

[32] *Ibid* at 8, 14.

[33] *Ibid* at 2.

[34] IESO, *Foundation Project*, *supra* note 31 at 3. The idea of having an independent body for data matching is discussed in detail in Lisa M Austin & David Lie, "Safe Sharing Sites" 94 NYU L Rev [forthcoming in 2019], online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329330>.

[35] *Ibid*.

non-personal information):

a. The postal code.
b. The distributor rate class.
c. The commodity rate class.
d. Occupant change data.

The directive required the depersonalization of any data. Other personal information, such as consumers' names, addresses or phone numbers are not available to the SME.[36]

In September 2016, the SME released its *Third Party Access Implementation Plan* following the *Foundation Project Final Report* recommendations. Under the plan, the new data elements required by the OEB order, including postal code, distributor rate class, commodity rate class and validation of occupant status, and the existing energy consumption data, were made available for third-party access in a "generalized and/or aggregated format."[37] Further, the *Third Party Access Implementation Plan* anticipated the use of Privacy Analytics Inc.'s specialized software to conduct a risk assessment with each request for data. Such assessments consider the context and intended use of the data in evaluating re-identification risk.[38] According to Privacy Analytics Inc. (the consultant retained to address privacy issues linked to de-identification and data aggregation), there is a small risk that, despite the recommended risk mitigation techniques, information contained in the MDM/R could be used by a recipient to identify the dwelling linked to the data. Therefore, the SME stated that rendering data as non-personal "has proven invaluable in setting the foundation and approach for any future requests to collect additional data."[39]

Although the IESO/SME is bound by the provincial FIPPA legislation, private sector actors requesting access to data in the MDM/R would be governed by the federal Personal Information Protection and Electronic Documents Act (PIPEDA),[40] at least as far as privacy is concerned. Of course, PIPEDA only applies to the collection, use or disclosure of *personal information* and may not be applicable to aggregate, de-identified data, unless it is determined that the data, when used in conjunction with other available data, can lead to the identification of specific individuals.[41] In any event, the SME's data governance plan includes the use of legal agreements with data recipients that will "govern duties, responsibilities, and obligations of each party, to ensure full compliance with data protection principles, and compliance with all applicable privacy laws."[42]

One way of delivering the data to third-party requesters is to evaluate and approve requests for direct access to the data via Application Program Interfaces (APIs). However, in its *Third Party Access Implementation Plan*, the SME indicated that direct access would only be considered "after the initial implementation has been operational for sufficient time to assess its effectiveness and success."[43] Without direct access, data delivery will be affected on a case-by-case basis, ensuring that the appropriate technical and security measures are in place to ensure privacy.[44]

Data Governance Structures and the SME

As noted earlier, the SME has its own steering committee (which has a subcommittee for technical aspects of the central hub called the MDM/R Technical Panel).[45] The steering committee is both an advisory panel and stakeholder committee, which represents the "interests of

[36] IESO, "Smart Metering Entity: Third Party Access Implementation Plan Frequently Asked Questions" (3 November 2017) at 2, online: <www.ieso.ca/-/media/files/ieso/document-library/smart-metering-entity/dsac/sme-faqs.pdf?la=en> [IESO, "Frequently Asked Questions"]. LDCs mask customer billing data when sharing smart metering data with the MDM/R. When the LDCs receive the processed smart meter consumption data from the MDM/R, they re-match it with the customer data for billing purposes. This process was recommended by Privacy Analytics Inc. (see Lauriault, Bloom & Landry, *supra* note 21 at 76).

[37] IESO, *Third Party Access Implementation Plan* (2016) at 4, online: <www.rds.oeb.ca/HPECMWebDrawer/Record/545198/File/document> [IESO, *Third Party Access*].

[38] *Ibid* at 18.

[39] *Ibid* at 20.

[40] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].

[41] See discussion of this point in Teresa Scassa, "Geographical Information as 'Personal Information'" (2010) 10:2 OUCLJ 185 [Scassa, "Geographical Information"].

[42] IESO, *Third Party Access*, *supra* note 37 at 25.

[43] *Ibid* at 33.

[44] *Ibid* at 30–31.

[45] IESO, "Governance of SME", online: <www.ieso.ca/en/sector-participants/smart-metering-entity/governance-of-sme>.

MDM/R service recipients."[46] The MDM/R's primary service recipients — at least in the initial concept of the SME — are the LDCs, which receive data necessary for client billing from the MDM/R.

A Data Strategy Advisory Council (DSAC) was formed as a special expert committee to provide advice on the development of the implementation plan for third-party access to de-identified smart meter data.

In 2017, the IESO issued a call for nominations for the DSAC that included 12 to 15 members from five categories: electricity consumers (representing a mix of sectors); LDCs (representing different size utilities and different regions); consultants, academics and service providers/delivery agents; municipality representatives and the IESO chair (plus staff support and any appointed presenters).[47] However, the actual composition of the DSAC is currently heavily weighted toward commercial interests. The 14 members of the DSAC[48] are:

- seven LDCs/hydro network representatives;
- two municipalities;
- one municipal property assessment corporation;
- one smart grid integrator;
- one market analysis and management analytics company;
- one water agency; and
- one consumer-oriented company.[49]

There is no civil society or consumer advocacy group on the list, nor any group or body that might represent consumers' privacy concerns other than the LDCs who have advocated on behalf of their customers. Three observers are allowed to participate in the council's activities: the OEB, the Electricity Distributors Association and the Ministry of Energy. As for privacy or other public policy concerns, the SME sought advice from the OIPC and Privacy Analytics and maintained informal contacts with some academics.

Analysis

Technologies that facilitate the collection of certain types of data are often adopted with a specific goal in mind. In the case of smart metering in Ontario, the initial goal was to gather data to promote conservation and the management of the grid by providing the regulator and customers greater insight into consumption patterns. Smart meter data was then used to create and implement a TOU pricing scheme for the province. While TOU pricing may have some conservation benefits,[50] it was also intended to serve other goals, such as distributing demand for electricity more evenly.[51]

It is not surprising that other potential uses for smart meter data have arisen and that interest in accessing and using the data would come from different actors, including the private sector and researchers.[52] Raghavan suggests that the "full scientific, economic, and historical potential of smart grid data may not be fully understood, and its usefulness may indeed exceed beyond the original purpose for which it was stored."[53] While it is not unforeseeable that an interest might develop to collect additional data to use for new purposes, changes of this kind may expand the role of any data governance body, which in turn may raise issues about capacity and composition,

[46] IESO, "SME Steering Committee", online: <www.ieso.ca/en/sector-participants/smart-metering-entity/sme-steering-committee>.

[47] *Ibid*.

[48] IESO, "Data Strategy Advisory Council" at 2, online: <www.ieso.ca/-/media/files/ieso/document-library/smart-metering-entity/dsac/dsac-membership.pdf?la=en>.

[49] Interestingly, the consumer coalition is a US-based group called Powerconsumer Inc. This is actually a private sector corporation that describes itself as offering "a comprehensive suite of market analysis and customer-facing energy management analytics on a software-as-a-service platform." See Powerconsumer Inc., "About Us", online: <www.powerconsumer.com/about/>.

[50] These are questioned in the 2014 report by the Auditor General of Ontario, *supra* note 5.

[51] The success of this is also questioned in the 2014 report, *ibid*.

[52] See e.g. Teresa Scassa, "Public Transit Data Through an Intellectual Property Lens: Lessons About Open Data" (2014) 41 Fordham Urb LJ 1759 (the author notes that sensors to collect automatic vehicle location data in public transit systems were initially installed to aid in the better planning of bus routes and timetables. It became apparent that the data could also be used for real-time notification of transit vehicle arrival times. Further, there was demand for this data from developers outside public transit agencies.

[53] Raghavan, *supra* note 3 at 13. He notes: "In short, electric utilities are (or soon will be) collecting more information than they have in the past, and there is more reason to sell it to other parties" (*ibid* at 19). See also Jan Beyea, "The Smart Electricity Grid and Scientific Research" (2010) 328:5981 Science at 979–80.

as well as the suitability of the original governance framework. Governance regimes must have sufficient flexibility in order to respond to changing circumstances; they must also have mechanisms in place to ensure that there is proper transparency and accountability as the shifts take place.

In the case of the SME, one important question is whether there is sufficient public awareness of the collection of additional data attributes, new uses and new users of smart meter data. The public processes by which these changes have taken place are somewhat transparent due to the public mandates of the institutions involved and reporting obligations. However, because most consumers are not attuned to OEB activities, it will require some motivation on the part of consumers to follow and understand the changes. Many will lack the time, energy or expertise to do so. Data governance bodies therefore should have mechanisms in place to ensure continued public trust.

Smart Grid Data Governance and Privacy

Wherever massive quantities of personal data are collected, there are privacy issues, and the smart metering program in Ontario has raised its fair share of them. Smart metering has involved the roll out of a technology service that enables broad data collection across a sector — in this case an essential utility — with no opt-out. Consent is not a factor, since the public policy decision to introduce smart metering essentially dictates the basic terms for the consumption of electricity in Ontario. Under Ontario's public sector data protection law, consent is not a requirement for the collection of personal information.[54] This is similar to the smart cities context, where data collection may be hard-wired into urban infrastructure. However, in a context in which the data is shared directly with LDCs (some of which are private sector companies) and in which broader data sharing with the private sector is contemplated, the absence of a consent requirement may require much greater attention to privacy violations.

The smart metering context raises interesting challenges around how to identify and manage privacy issues. Ontario's approach was to address privacy in the design of the smart metering system. The SME and its data policies and governance are heavily influenced by Privacy by Design (PbD). In the case of third-party access to data, PbD approaches were used to ensure that no data would be released to third parties without first carrying out a risk assessment process to ensure that the data can be properly de-identified and that there is no re-identification risk if the data is combined with the third party's own data. Privacy Analytics developed a de-identification methodology for the SME that is "aligned with" de-identification guidelines produced by the OIPC.[55]

To some extent, the complex system was meant to create privacy buffers so that the MDM/R is the centralized point for the collection of all data, which can be aggregated and anonymized prior to being made available to third parties for different uses. At the same time, the MDM/R can provide customer data to the relevant LDCs for billing purposes. In theory, third-party developers interested in more detailed electricity consumption data would be able either to obtain and use the aggregate anonymous data supplied by the MDM/R, or to enter into separate agreements with individuals and LDCs to obtain access to their specific customer consumption data.

Interestingly, in the case of smart metering, the creation of a centralized data warehouse, combined with the ongoing relationships between LDCs and their customers, may have created some confusion as to what privacy rules apply, to whom and in what contexts. For example, in a study of smart metering in Ontario, Avner Levin found that industry participants interviewed for the study "did not distinguish between their electricity regulatory framework and their personal information protection framework."[56] In

[54] See *FIPPA*, *supra* note 18, s 39. Collection must take place directly from the individual, except in specified circumstances, and notice of the principal uses of the information must be provided.

[55] IESO, "Frequently Asked Questions", *supra* note 36 at 2. See also IESO, *Third Party Access*, *supra* note 37 ("Considering that patient data is some of the most sensitive type of shared data, the SME believes that using the Health Care industry as the gold standard for data compliance and protection is a prudent approach to safeguard the data of Ontario's electricity consumers, and as such the SME made an early decision to adopt the most stringent rules applied in the health care industry to the smart meter data" at 18).

[56] Levin, *supra* note 4 at 11.

other words, LDCs assumed that privacy issues relating to the collection, use and disclosure of smart metering data were being addressed in the regulatory framework established to govern it, leaving no other privacy issues to be addressed in their relationships with their customers. However, this is not the case. A customer's relationship with a private sector LDC would entail obligations for the company under PIPEDA.[57] The situation is more complex in the case of LDCs that are owned solely or predominantly by municipalities. In those cases, the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)[58] may provide the applicable privacy regime.[59]

The layered relationships in this scheme create other privacy conflicts. For example, in the *Foundation Project Final Report*, it is noted that decisions about access to the MDM/R data are not in the hands of the LDCs that collect and transmit customer data, and that have an ongoing relationship with their customers.[60] The LDCs were particularly concerned about the possibility that the MDM/R might release personal information to government agencies or law enforcement, compromising the LDCs' customer relationships. The *Foundation Project Final Report* made recommendations to mitigate these concerns, but the tension is nonetheless interesting and challenging.

Both Levin[61] and Michael Geist[62] have noted the potential for confusion around privacy governance that arises, in particular in the Canadian context, where different laws apply depending on whether the party collecting, using or disclosing the personal information is part of the public or private sector. While PIPEDA applies to data collected, used and disclosed as part of the relationship between the customer and a private sector LDC, smart metering data in the hands of the SME may be subject to Freedom of Information and Protection of Privacy legislation. Uncertainty of this kind might best be addressed by clarity in the enabling legislation about which privacy laws are meant to apply to which actors and in which contexts. Smart cities data governance may raise similarly complex issues since public sector and private sector actors are likely to be deeply intertwined in the delivery of certain products or services, in the creation of platforms and/or in the supply of data.

Levin is also critical of the potential for PbD principles to replace a more robust approach to privacy in data governance. Although he does not dismiss the positive aspects of PbD, Levin notes that the challenges of rapid design and deployment of new technological systems can lead to reliance upon PbD as a panacea for privacy concerns. He writes:

> Faced with the monumental tasks of revamping their systems, and introducing components and structures that will facilitate the environmental and security goals of the Smart Grid that are key to its definition, such as generation facilities embedded within the distribution system, two-way transmission, load management and prediction, etc., utilities have little attention to spare to the privacy implications of the Smart Grid, and executives are by nature individuals with engineering backgrounds and focus. Even when attention is paid to privacy and personal information protection, the approach, perhaps due to Ontario's IPC Privacy by Design ideology, remains focused on the design of systems and components that will achieve some technological, privacy-supporting purpose.[63]

This is an important reminder that not all privacy issues can be resolved at the design stage. It remains necessary to consider policy issues and principles and to do so in a responsive and ongoing manner.

One example of a privacy issue not addressed by the PbD approach to smart metering relates to the surveillance and law enforcement potential

[57] For example, the privatized Hydro One company states in its privacy policy that its relationship with customers is governed by PIPEDA, *supra* note 40. See Hydro One Inc., *Privacy Code* (2017), online: <www.hydroone.com/privacy>.

[58] RSO 1990, c M.56.

[59] This is nonetheless murky. For example, HydroOttawa's privacy policy provides that its customers' privacy is governed by MFIPPA *and* PIPEDA. See HydroOttawa, "Privacy Policy" (October 2016), online: <https://hydroottawa.com/about/policies/privacy>.

[60] IESO, *Foundation Project, supra* note 31 at 3.

[61] Levin, *supra* note 4.

[62] Michael Geist, *Smart Grids and Canadian Privacy Law: An Examination of Current Laws and Future Work* (Ottawa: Standards Council of Canada, 2015).

[63] Levin, *supra* note 4 at 40.

of smart metering data. Fine-grained electrical consumption data can be matched to specific individuals (as the billing procedures make clear). This data can be used to detect abnormal usage patterns, and those patterns can be linked to specific illegal activities, such as operating an illegal grow-op. The Supreme Court of Canada has struggled with issues of privacy in relation to data held by third-party organizations.[64] Where the data-holding entities are part of the public sector, the ability to share data between different government agencies or departments may be enhanced.[65] The *Foundation Project Final Report* noted in its recommendations that its panel was unable to reach consensus on the extent to which government actors should be able to access personally identifiable information collected through smart metering.[66] The fact remains that the collection of ever-increasing, fine-grained data about the activities of individuals increases the potential for surveillance. The importance of this fact —amplified in the smart cities context — should not be lost in platitudes about not having anything to fear if one has done nothing wrong.

Although there were privacy challenges inherent in the original plan for the centralized collection of smart meter data, the expansion of data attributes collected and the plans for allowing third-party access to data raised additional privacy and governance issues. These were addressed in some detail in the *Third Party Access Implementation Plan*. First, as noted earlier, the SME adopted PbD principles. It sought expert advice from the consultant Privacy Analytics Inc. as well as the OIPC in the design of its privacy practices. The SME was careful about what identifiers could be used in the additional collected data. For example, when it was determined that a location element was required, the SME opted to use a postal code instead of a street address. In cases where LDCs provided street addresses in the data provided to the MDM/R, this data was masked, and it was later recommended that LDCs no longer provide such data. Privacy risk assessments were developed for use not just in determining whether de-identification was sufficient for the proposed third-party use of data but also in assessing the third parties and their trustworthiness in terms of data sharing.[67] The SME also carefully considered the method of data sharing — ruling out the use of direct third-party access via APIs until greater experience with third-party data sharing was acquired.[68] Data sharing with third parties would be subject to data-sharing agreements that would place limits on how third parties could use the data provided. Audit mechanisms were considered as well as follow-up measures and the traceability of where data sharing occurred. This would ensure, for example, that requirements in the data-sharing agreement for the third party to destroy data after use were met.[69] Attention was also paid to governance structures both external and internal to the IESO.[70]

While PbD in the smart metering system has focused on de-identification as a strategy for enhancing privacy, it is increasingly recognized that there may be broader concerns raised by the collection and use of aggregate, de-identified consumer behavioural data.[71] To some extent, these broader concerns are acknowledged in the *Foundation Project Final Report* where recommendations relating to the management of requests for de-identified data include developing criteria on appropriate uses of de-identified data, creating processes for privacy impact or privacy risk assessments and implementing data-sharing agreements to ensure compliance with any limits placed on the use of de-identified data.[72]

[64] *R v Spencer* [2014] 2 SCR 212, 2014 SCC 43 (CanLII); *R v Gomboc* [2010] 3 SCR 211, 2010 SCC 55 (CanLII).

[65] For example, under Ontario's FIPPA, *supra* note 18, s 42(g), a government body may disclose personal information "where disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result."

[66] IESO, *Foundation Project*, *supra* note 31 at 3.

[67] IESO, *Third Party Access*, *supra* note 37 at 28.

[68] *Ibid* at 33.

[69] *Ibid* at 31.

[70] *Ibid* at 27.

[71] Such concerns may include whether aggregate de-identified data is used either to profile and target individuals or communities in ways that are unethical. Some of these issues are linked to the emerging concept of "group privacy," addressed in Linnet Taylor, Luciano Floridi & Bart van der Sloot, eds, *Group Privacy: New Challenges of Data Technology* (Cham, Switzerland: Springer, 2017).

[72] IESO, *Foundation Project*, *supra* note 31 at 14–18.

Data Governance for Sharing: Lessons from Ontario's SME

The data governance regime put in place for Ontario's SME, and adapted over time, offers some useful lessons as governance for data sharing becomes increasingly important in a data-driven economy. Ontario's SME is a public sector body with a mandate to share data with both public and private sector actors and, in doing so, facilitate a range of different objectives. At source, the data is personal information capable of revealing intimate details of individuals' private lives. Although de-identified in the hands of the SME, the data's sharing nonetheless raises privacy issues, as well as concerns about ethical reuse. The SME and its experience therefore provide an interesting context in which to explore some of the risks and challenges of smart data governance in the public interest. Below, the authors highlight a number of the lessons learned.

Data Governance for Sharing Is Complicated but Must Give Individuals and Communities a Voice

The experience of the SME reveals the complexity of data governance where one of the goals is to enable data sharing. Essentially, the SME had to deal with one category of data — electrical consumption data from smart meters — on a province-wide basis. Establishing the physical and technological infrastructure was a challenge in its own right; at the same time, privacy protection had to be built into the design. Considerable effort was invested in ensuring that privacy would be protected; for example, the SME itself does not hold customer identity information (this remains with the individual LDCs).

It is clear that choices made in the system design are important and can have long-term consequences. Data standards, for example, may have implications for the suitability of the data for reuse.[73] After-the-fact changes to the ways in which data are collected and stored may be costly and difficult to implement. Security is also a key consideration.

Data governance requires the creation of governance bodies and, in some cases, advisory panels. A governance body must be created on some legal basis and must have a mandate to govern according to specified criteria. In this case, a pre-existing public entity was designated as the SME. Its mandate was set by the energy sector regulator. It is interesting to note that although the SME is responsible for managing the smart metering data, it takes direction from the regulator, and its mandate may shift over time. With data governance structures, it is important to consider how their mandate is set and who may have the authority to change it. The public interest is never entirely self-evident and can be perceived differently depending on social circumstance or ideology.

As a public body, the SME was charged with administering the data in the public interest. At the outset, the public interest served by the data gathering was identified as energy conservation and better energy management. The move to share data more widely was driven by the additional goal of stimulating innovation through providing the private sector with useful data. Among other things, such data can be used to provide consumers with more hands-on tools to manage their electricity usage. Data sharing will also serve other interests that are not clearly defined, as it may enable unforeseen public and private sector applications for the data. Because the SME is a public body, it is the government, through the energy regulator, that ultimately identifies the public interest to be served. The fact that this may change with government priorities or even governments themselves — perhaps even dramatically — could lead to significant changes in the nature and character of data governance. Depending on the governance body and the reason for its creation, consideration should be given to whether some core features or principles should be more firmly entrenched (for example, through legislation). Clear no-go zones might be established that would

[73] For a discussion of data standards, see Michel Girard, "Canada Needs Standards to Support Big Data Analytics" CIGI, Policy Brief No 145, 4 December 2018, online: <www.cigionline.org/publications/canada-needs-standards-support-big-data-analytics>.

require much greater public engagement to change if it were even considered necessary to do so.

Ideally, a governance body will be representative of the interests at stake. In some cases, it may establish advisory bodies that should represent stakeholder perspectives. However, the identification of relevant stakeholders or interests is important. Although the SME was attentive to privacy issues once it perceived them as arising, its stakeholders were primarily industry actors. In the case of the IESO's DSAC, for example, the membership included only one "consumer" voice (a company that supported the use of energy consumption data to develop digital tools for consumers). If a body is intended to be representative of diverse interests, the process by which those interests are identified and how their representatives are chosen is significant.

Oversight and accountability are also important issues when establishing a governance body. The SME, as a public body, is subject to the same oversight as other public entities in Ontario, including periodic audits by the Auditor General.[74] Further, any collection, use or disclosure of personal data is subject to the oversight of the OIPC.

The Uses for Data May Change Over Time

Although a data governance scheme for data sharing may require planning, forethought and consultation, it is unlikely to remain static over time. This is in particular the case because the value, applications and potential of data continue to rapidly evolve. The SME case study demonstrates how data collected for one purpose (for example, energy conservation) became useful for achieving other purposes (for example, stimulating innovation). These purposes may not be confined to the same sector, as the SME explains that data collected by a public sector actor became useful to multiple public and private sector entities. The SME is also an example of how a plan to provide data to customers through dashboard applications expanded to include a goal of allowing customers to "port" their data to third-party providers of analytics services.

While the SME developed a thoughtful and detailed approach, and one that seems relatively robust, it is important to keep in mind the dynamics of the technological context. Any data governance scheme would have to be flexible enough to adapt to changing circumstances. In its *Third Party Access Implementation Plan*, the SME notes that its de-identification approach is scalable.[75] It also indicates that its extensive work sets "the foundation and approach for any future requirements to collect additional data."[76]

More Is Often Better — for Data Users

Although data limitation is an important principle of data protection and of PbD, the thirst for data in data analytics and machine learning means that both greater volume and variety are desirable. While, on the one hand, data protection principles may favour limiting the type and scope of data collected, users of the data may find that additional data points will make linking to other relevant data easier, increasing its value. Location data is particularly valuable but can lead to the re-identification of individuals.[77]

This is reflected in the experience of the SME. As the potential for third-party uptake and use of smart metering data grew, it was evident that the data would be much more useful if it contained a geographic component. Pressure to expand the data attributes that are collected should be anticipated, and mechanisms should be in place to consider and consult on such changes. It should also be kept in mind that some changes might significantly alter the privacy profile of the data-sharing exercise. Where the initial collection of the data is accompanied by assurances to the public about data limitation, subsequent changes may be seen as a breach of such an undertaking.

Privacy Is Important and Multifaceted

A large part of the governance work carried out by the SME was related to the imperative of protecting privacy. There is enormous value for both public and private sector actors to match different data sets in order to obtain richer insights. However, data matching increases privacy risks, in particular the risk that individuals can become identifiable in

[74] *Auditor General Act*, RSO 1990, c A.35, s 9.

[75] IESO, *Third Party Access*, *supra* note 37 at 18.

[76] *Ibid* at 20.

[77] Scassa, "Geographical Information", *supra* note 41.

de-identified data sets. The process recommended by Privacy Analytics and adopted by the SME was one where there would be a "very small" risk that the smart meter data "could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify a dwelling that is a subject of the information."[78] This does not, however, address the reality that not only do "reasonably available" data sets change over time, but that some private sector actors will have their own data sets — that are not publicly available — and that might be used to re-identify individuals. This is no doubt why the SME plan includes using data-sharing agreements to provide an additional barrier to re-identification. It is worth noting that the Foundation Project Working Group considered the benefits of data matching taking place "at the source level, prior to de-identification."[79] They noted that there "would be value in having an entity that could match electricity data with other data sets and release the de-identified results."[80] This idea does not seem to have been pursued.

While individual privacy is important (and is a key component of PbD), it is not the only consideration. Where the collected data provides, on its own or in combination with other data, insight into group behaviour, there may be additional concerns. Such data may be used to make decisions about the allocations of resources, surveillance or policing, or the distribution of certain benefits. Thus, the aggregate de-identified behavioural data may have negative consequences for specific groups or communities.[81] There should be some means to avoid these broad harms and failing that, to address and rectify them.

There may also be ethical issues around particular uses of the data collected, even if it is largely de-identified or aggregated. Some uses might be considered inappropriate, even if no specific individuals are identified. For example, using aggregate and de-identified data to identify certain audiences for manipulative messaging would be an unethical use of the data. Rather than simply make aggregate, de-identified data available to third parties, a governance decision might involve requiring those seeking access to data to submit documentation outlining the proposed use of the data. The purposes can be reviewed and any licence with the party seeking the data can place explicit limits on data reuse. The SME seems to contemplate some form of oversight based on proposed use of data as well as contractual terms to limit reuse.

Complex Partnerships Raise Complex Challenges

The SME operates within the provincially regulated electricity grid, and its operations are province-wide. The *Foundation Project Final Report* notes the structure of Ontario's electricity industry was different in significant ways from that of other North American jurisdictions, and it required the pooling and integration of data from more than 70 LDCs. This is in contrast with jurisdictions in which there is a sole provider, resulting in a single large data set.[82] Further, the SME may share data with different levels of government as well as with private sector companies. This multiplicity of relationships can make governance more complex. The situation is also made more challenging by the fact that Canada's data protection regimes are different for public and private sector actors. The SME is a public body governed by provincial public sector data protection law while some of the LDCs are private sector entities governed by PIPEDA.

Complexities of this kind are even more likely to be present in the smart cities context, where data collection and storage may involve both private and public sector actors. The number and degree of engagements with actors governed under different regimes may determine whether the complexity is manageable under existing frameworks or whether a new data governance framework is required with *sui generis* dispositions regarding issues such as privacy and data sharing.

Data Governance Requires Funding

Data sharing — in particular where there is a large volume or wide variety of data at issue — can be costly. Some of these costs will be linked to the basic infrastructure required, such as hardware and

[78] IESO, *Third Party Access*, *supra* note 37 at 20.

[79] IESO, *Foundation Project*, *supra* 31 at 3.

[80] *Ibid*. For a more detailed discussion of this idea, see Austin & Lie, *supra* note 34.

[81] See e.g. Alessandro Mantelero, "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection" (2016) 32:2 Computer L & Security Rev 238 at 246.

[82] IESO, *Foundation Project*, *supra* note 31 at 1.

software, networks and data security.[83] Other costs will be linked to needs for staff to oversee the data collection and sharing and, where necessary, to make decisions about when to share, with whom and on what terms. Where the data governance framework requires decisions about collecting new data, or enhancing data already collected, this too will require staffing and expertise. Funds may also be required to provide oversight of data use by licensees and to enforce licences or take remedial action in cases of non-compliance.

In addition to recognizing the costs involved in data governance, there should be a plan in place to fund the governance mechanism, in particular if it is important to ensure that the data-sharing framework is sustainable in the long term. This may require charging fees for access to and reuse of data. The *Foundation Project Final Report* identifies cost as an issue in the discussions about the sharing of electrical consumption data. It proposed a number of different options for third-party access to this data and noted the need to "develop cost estimates and consider user/implementer needs, to assess which options, if any, to carry forward."[84]

If fees are charged, the data provider would have to consider whether the goal is to recover the costs of data governance or to generate revenue that might be used to support other initiatives. Consumers may be interested in user fees for access to their data, which is used to reduce their energy costs. It may also be necessary to determine whether these will be flat fees, or if fees will vary depending on the identity of the user or the goals of the use (for example, no charge for public sector researchers or other government entities, and a graduated fee scale for private sector companies based on their size or volume of business).

Repeatable Frameworks Can Reduce Costs and Facilitate Sharing

The growth of artificial intelligence, the rise of smart cities and the importance of data within the economy mean that it will be increasingly necessary to design frameworks for data sharing. The process by which the data-sharing framework was developed for the SME was long and complex, and it has generated much reusable knowledge and experience, although it is perhaps not as well-known or as easily accessible as it should be. Knowledge sharing is important since, in order to match the pace of rapid technological advancement, it will be necessary to develop data governance frameworks with relative speed and flexibility. There is a clear need for repeatable frameworks, standards and template agreements that can be adapted to data sharing in a range of contexts. The SME notes that legislation might be necessary or useful to create frameworks for public sector data sharing; it might also be useful to have legislation that supports the creation of independent third-party data governance mechanisms, such as civic data trusts.[85] More research is required to provide detailed case studies of emerging and existing frameworks for data sharing in order to derive useful knowledge from these contexts.

Conclusion

This paper has provided a case study of Ontario's SME as a mechanism for managing data sharing in the public interest. The SME is an interesting case study for a number of reasons. It is an example of a data governance mechanism that involves public sector data, public and private sector stakeholders, and a considerable body of relatively sensitive personal information. It also provides an example of a model that had to adapt to changes in the value, demand and applications for the data collected, as well as take direction from the regulator for the collection of additional data attributes to enrich the usefulness of the data for new categories of data users. The SME provides a rich context in which to examine some of the challenges relating to data sharing in the public interest and with privacy protection at the forefront. The complexity in the development and unrolling of the model is daunting. However, it is to be hoped that the lessons learned will not be lost to others seeking models to follow or adapt.

Central among the lessons learned are the needs to establish a clear and transparent

[83] IESO, *Third Party Access*, *supra* note 37 at 41.

[84] IESO, *Foundation Project*, *supra* note 31 at 3.

[85] For a discussion of civic data trusts, see Sean McDonald & Keith Porcaro, "The Civic Trust", *Medium* (4 August 2015), online: <https://medium.com/@McDapper/the-civic-trust-e674f9aeab43>.

regulatory framework and to identify or establish a body responsible for data governance. In establishing this body, careful thought must be given to identifying stakeholders and ensuring their proper representation. While privacy regulators can provide important guidance, the participation of civil society actors, including privacy advocates, should not be overlooked.

The model of the SME may be particularly useful in the smart cities context. Smart cities feature both public and private sector actors, they may collect large volumes of human behavioural data and there is a strong public interest in appropriate data governance. Indeed, in the smart metering and smart cities contexts alike, individuals have little choice but to have their data collected. The data collector believes that the reuse and repurposing of this data across different contexts has the potential to benefit the public, as well as to produce other benefits broadly in the public interest. With a greatly diminished focus on consent, individuals and communities require frameworks that achieve the identified public interests. These frameworks must protect individual and community privacy and ensure that data is not used in ways that are harmful or exploitative.

Authors' Note

The authors gratefully acknowledge the feedback provided by Tracey Lauriault on an earlier draft of this paper. Thanks also to Michel Girard for sharing a document and thoughts on the issues raised in this paper, and to the reviewers for their helpful comments and feedback.

About CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and have received support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

À propos du CIGI

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan doté d'un point de vue objectif et unique de portée mondiale. Nos recherches, nos avis et nos interventions publiques ont des effets réels sur le monde d'aujourd'hui car ils apportent de la clarté et une réflexion novatrice pour l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques internationales, et le droit international. Nous comptons sur la collaboration de nombreux partenaires stratégiques et avons reçu le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline