ONTARIO ENERGY BOARD

IN THE MATTER OF subsections 78(2.1), (3), (3.0.1), (3.0.2) and (3.0.3) of the *Ontario Energy Board Act, 1998*;

AND IN THE MATTER OF subsections 53.8 of the *Electricity Act, 1998*;

AND IN THE MATTER OF Ontario Regulation 453/06 made under the *Ontario Energy Board Act, 1998*;

AND IN THE MATTER OF an Application by the Independent Electricity System Operator ("**IESO**"), designated as the Smart Metering Entity("**SME**"), responding to the Ontario Energy Board's direction to file a new application, with certain elements, for a framework for third party access;

AND IN THE MATTER OF an Application by the Independent Electricity System Operator, designated as the Smart Metering Entity, for an Order regarding access to data by third parties and associated recovery of costs through the Smart Meter Charge and fees; as well as approval of the basic terms of the Data Use Agreement

APPLICATION

1. The applicant, the Independent Electricity System Operator ("**IESO**"), is a corporation without share capital continued under Part II of the *Electricity Act, 1998* ("**Electricity Act**").

2. On March 28, 2007, the IESO was designated as the Smart Metering Entity ("**SME**") by Ontario Regulation 393/07 made under the Electricity Act. The regulation came into effect on July 26, 2007. The objects of the SME as outlined in the Electricity Act include, in addition to other objects and business activities, to facilitate the collection and management of information and data, to store the

information and data related to the metering of consumers' consumption or use of electricity in Ontario and to provide and promote non-discriminatory access by distributors, retailers, the IESO and other persons to this information and data.

3. On September 30, 2016 the SME filed an application with the Ontario Energy Board ("**OEB**") to renew its licence, EB-2016-0284. A Third Party Access Implementation Plan for third party access to the data in the Meter Data Management Repository ("**MDM/R**") was included in the application. In its November 24, 2016 decision the OEB renewed the SME's licence and required the SME to collect the following information associated with each smart meter (modified where necessary to sufficiently render it non-personal information): (a) The postal code; (b) The distributor rate class; (c) The commodity rate class; and (d) Occupant change data.

4. Any reference to "data" in this application means any of the information and data related to the metering of consumers' consumption or use of electricity in Ontario, including the information the OEB required the SME to collect in its decision in EB-2016-0284.

5. The SME had collected the additional data required by EB-2016-0284 by January 1, 2017 as required by the OEB.

6. The SME then filed an application, EB-2018-0316, with the OEB on December 4, 2018 under sections 74 and 78 of the *Ontario Energy Board Act, 1998* (the "**OEB Act**") seeking approval to amend its license to enable it to provide third party access at market prices to de-identified smart meter data to third parties (the "**prior application**").

7. In its October 24, 2019 Decision and Order on the prior application the OEB found that:

i. the SME was already authorized to provide public offerings of highly aggregated smart meter data, and any costs to the SME in preparing such products would be considered part of its normal business operations and recovered through the Smart Metering Charge paid by distributors and ultimately passed through to all consumers with a smart meter;

ii. the SME was already authorized to provide the enhanced MDM/R data to the OEB or to the IESO in order to assist them in fulfilling their statutory mandates;

iii. That the SME should submit a new Third Party Access ("**TPA**") application, where TPA means providing third party information to other entities besides the OEB and the IESO, to the OEB by the end of 2021 and this application should include certain elements. These elements are described and responded to in EX A-3-1.

8. Since the October 2019 decision, the SME has been consulting and working with stakeholders on the elements of a new application to enable third party access to the smart meter data. In preparing this application the SME has considered the input received from residential and small commercial consumers with smart meters through the consumer research conducted by Ipsos, an internationally recognized leader in market research, which is included in this application at EX B-6-1 Appendix 1. The SME has also consulted with and considered input from intervenors to the 2018 application and other stakeholders. The SME has proceeded with this application mindful of the statement in the OEB's October 2019 decision that "the SME should proceed cautiously".

9. In August 2021 the SME licence was renewed with revised wording to Section 9.1, as shown below with emphasis added. With this revision already made the SME is not seeking changes to the wording in its licence through this application.

> **Section 9. Restrictions on Provision of Information**
>
> 1. The Licensee shall not use confidential or personal information regarding a Distributor, consumer, Retailer, or any other person obtained for one purpose for any other purpose without the written consent of the consumer, Retailer, or other person.[1]

10. The SME is seeking the following OEB approvals:

i. To expand the access or sharing of the data beyond the OEB and the IESO to Canadian Governmental Entities, which is defined as:

> federal and provincial governments, including ministries, agencies, boards, commissions, tribunals and wholly-owned corporations, or in the case of non-share capital corporations, where such corporations are controlled by a federal or provincial governments, as well as municipalities (or regional governments), universities, school boards, hospitals and First Nations. First Nations means a "council of the band" as that term is defined in subsection 2(1) of the Indian Act (Canada).

ii. Access to the data on a cost recovery model for requests with more complex requirements that require additional IESO staff time and resources to prepare.

[1] S 9.1 Smart Metering Entity Licence ES-2021-0191

iii. The basic terms of the Data Use Agreement, with the ability for the SME to tailor the Data Use Agreement to match the specific circumstances surrounding any particular disclosure.

11. The SME has filed evidence in support of this application as identified in the Exhibit List, Ex A-2-1. The SME may amend its pre-filed evidence from time to time prior to, and during, the course of the OEB's proceeding. In particular, should the SME identify a material change to its application, the SME will advise the OEB and update its pre-filed evidence. The SME reserves the right to amend its application accordingly, including making any necessary adjustments to the orders sought in this application.

12. The SME requests that a copy of all documents filed with the OEB by each party to this proceeding be served on the SME and the SME's counsel in this proceeding, as follows:

(a) The SME:

Ms. Miriam Heinz
Advisor, Regulatory Affairs
Independent Electricity System Operator

Mailing address:
120 Adelaide Street West, Suite 1600
Toronto, Ontario
M5H 1T1

Tel: 416 969-6045
Fax: 416 969-6383
Email: regulatoryaffairs@ieso.ca

(b) The SME's counsel:

Mr. Patrick G. Duffy
Stikeman Elliott LLP

Mailing address:
5300 Commerce Court West
199 Bay Street
Toronto, Ontario
M5L 1B9

Tel: (416) 869-5257
Fax: (416) 947-0866
Email: pduffy@stikeman.com

DATED at Toronto, Ontario, this 29th day of October, 2021

INDEPENDENT ELECTRICITY SYSTEM OPERATOR

____

By its counsel in this proceeding
Patrick G. Duffy

Filed: October 29, 2021
Exhibit A
Tab 2
Schedule 1
Page 1 of 1

SMART METERING ENTITY
FEES FOR ACCESS TO DATA BY THIRD PARTIES
(EB-2018-0316)

EXHIBIT LIST

Exhibit	Tab	Schedule	<u>Description</u>
A – ADMINISTRATION			
A	**1**	**1**	Application
A	**2**	**1**	Exhibit List
A	**3**	**1**	Background to this Application and Responding to the Board's Directions in EB-2018-0234
B – SUPPORTING EVIDENCE			
B	**1**	**1**	The Proposed Third Party Access Plan
B	**2**	**1**	Consultations with Prior Intervenors & Other Stakeholders
B	**3**	**1**	Terms of Access Principles
B	**4**	**1**	The Data Use Agreement ("**DUA**")
B	**5**	**1**	Tariff Sheet
B	**6**		**Appendix:**
B	**6**	**1**	Ipsos IESO Smart Meter Data Research
B	**6**	**2**	Privacy Analytics: An Independent Assessment of the IESO's Planned Privacy Strategy for Third-Party Data Access
B	**6**	**3**	Summary of SME Data Requests June 2021
B	**6**	**4**	Representative materials of webpages to be used by LDCs
B	**6**	**5**	Defined Terms And Acronyms

RESPONDING TO THE BOARD'S DIRECTIONS IN EB-2018-0234

The SME, filed an application with the OEB on December 4, 2018 under sections 74 and 78 of the OEB Act seeking approval to amend its licence to enable it to provide access to certain data about electricity usage to third parties at market prices[1].

The OEB issued its decision on that application October 24, 2019 (the "**prior decision**") and found that:

i. The SME was already authorized to provide public offerings of highly aggregated MDM/R consumption data without charge;

ii. The SME was already authorized to provide the enhanced MDM/R data to the OEB or to the IESO in order to assist them in fulfilling their statutory mandates; and

iii. Any costs to the SME in preparing such products would be considered part of its normal business operations and recovered through the Smart Metering Charge ("**SMC**") paid by distributors and ultimately passed through to all consumers with a smart meter

The OEB also directed the SME to develop a revised proposal for TPA and submit a new application by the end of 2021. This application was to include at least the elements described below. The elements from that decision, and the SME's response to them, are included below including, where appropriate, references to evidence in this application:

i. The application should summarize the SME's consultation with consumers including what it heard from consumers about the notion of selling de-identified consumption data;

[1] File # EB-2018-0316

(i) Ipsos was hired to conduct market research with residential and small business consumers on data security and privacy of consumption data, use cases and cost models. Ipsos was asked to prepare a report based on this research to allow the SME, the OEB and other interested parties, to better understand the expectations of Ontario consumers with smart meters on privacy protection, data use, access and pricing of the data that would be shared with third parties. The Ipsos report is attached to this application in the Appendix, Ex B-6-1, and summarized below. The Ipsos report, and an overview of the findings of the report, were provided to each of the intervenors in the SMEs prior TPA application during consultations on this application.

Ipsos consulted with 1,501 residential consumers and 200 small commercial customers throughout Ontario in late 2020. Ipsos prepared a summary of their consultation, which among other things, noted that consumers are more comfortable with the Data being shared with the public sector as compared to private sector entities. We have termed these public sector groups "Canadian Governmental Entities" and have defined this term in Ex-B-5-1 <u>Defined Terms</u>. They see the benefits and the value for the electricity sector as a whole, such as improving decision-making and the efficiency of the electricity system. Their concerns were around sharing the data with those entities outside the public sector. Consumers did not have concerns with on a no-fee or low-fee basis, provided it would not have a negative impact on consumers.

ii. A marketing plan should be developed to ascertain the demand for this data, its potential use and what third parties are prepared to pay. The plan should address pricing to ensure reasonably priced access by commercial and non-commercial users. Such a plan might also inform both the likely success of the self-funding access model coupled with the size of the commercial and non-commercial demand;

(ii) As described earlier, the SME is not proposing to sell the data at a price above its costs. As preferred by smart meter consumers, access to the data will only be provided to the Canadian Governmental Entities. Access will be provided under a no-fee model for standard requests, these costs will be absorbed in the Smart Metering Charge, and cost recovery (at the rate of $145/hour x the number of hours to fulfill) for requests with more complex requirements which require additional IESO staff time and resources to prepare.

The marketing plan, as described in the Board's decision, was to:

- assist in determining what third parties are prepared to pay,
- address reasonable prices for commercial and non-commercial parties, and
- inform the likely success of the self-funding access model coupled with the size of the commercial user's demand.

Given that the SME is proposing to provide access to organizations working in the public interest and at no cost for standard requests, as preferred by smart meter consumers, the SME has not prepared a marketing plan in support of selling the data.

The demand for the data and its potential use by the eligible category has been previously established in the OEB's decision January 2016 decision requiring the SME to collect certain data, EB-2015-0297, in the use cases described in the SME's prior Third Party Access application and in the OEB's decision on that application, EB-2018-0316, which stated that "Although, as the OEB has noted in previous decisions, there are benefits to making the data available to third parties, there are also risks[2]." Data access requests received by the SME up to June 2021 are attached to this application at Ex B-6-3 <u>Summary of SME Data Requests June 2021</u>.

iii. The SME should propose a protocol for receiving and dealing with consumer complaints regarding the release of the data. The OEB notes that the SME has proposed an Ethics Committee which could address any issues associated with the potential use of the data by a purchaser;

(i) When consumers do make enquiries about the data held by the SME, the SME has developed the communication approach described below in consultation with local distribution companies ("**LDCs**"), the Smart Metering Entity Steering Committee ("**SSC**"), the Electricity Distributors Association ("**EDA**") Communicator's Council and intervenors to the prior application. It is anticipated that the majority of consumer enquiries will be made to the LDCs, and likely a consumer's LDC, as they are the consumers' primary contact for electricity related information. Additionally, LDCs have call centre's equipped to deal with enquiries from their customers and an ongoing relationship with their customers. The SME does not have a relationship or a

[2] EB-2018-0316, pg 2

communication channel with smart meter consumers, it has a relationship with LDCs, and is not able to see an individual consumers' data – absent them providing personal information. While the IESO has a call center, it handles calls primarily from participants in the IESO administered markets, not from residential and small commercial consumers. Draft communication materials have been developed for use by LDCs. However, the SME recognizes that some consumers may contact the IESO and/or the OEB about the data held by the SME, such that the materials provided to LDCs will be provided to the OEB and used by the IESO to respond to these enquiries. The SME has also consulted with OEB staff to inform and assist them in preparing for any consumer enquiries. The SME will continue to work with the OEB staff to assist them in dealing with any consumer enquiries to the OEB on access to the data held by the SME. The draft communication materials have been designed to provide support in addressing potential customer questions or concerns, including those related to the privacy protections of the data. These materials will include scripts, FAQs, visuals as documents or as an online site that organizations can link to or refer customers to. The communication materials will continue to be developed and refined in collaboration with the organizations that are contacted by consumers: LDCs, the OEB and the IESO after the decision on this application is issued and experience is gained in dealing with these customer enquiries. The Information and Privacy Commissioner of Ontario ("**IPC**") recommended that where complaints or concerns cannot be resolved by the LDCs, the SME or the OEB that any of this organizations can make individuals aware of their ability to file complaints to the IPC's office. The SME is not seeking the Board's approval for either the protocol or associated materials as these will be living documents that will be revised and updated as the SME, LDCs and the OEB hear from consumers and learn more. Representative examples of the materials are attached as Appendix B-6-4 <u>Representative Materials To Be Used By LDC's</u>.

iv. The application should consider how to inform consumers of the fact that de-identified information will be released to third parties;

(i) As the SME is proposing to provide access only to those organizations which the Ipsos report shows consumers support having access (i.e. Canadian Government Entities), and as the Ipsos report shows consumer confidence in the IESO's ability to provide safe and secure data access, the SME does not propose to contact consumers with smart meters to inform them that access to the de-identified data held by the SME will be provided to the eligible category. LDCs who wish to inform their consumers of this initiative will be enabled and supported by the IESO through the communication materials described above.

Additionally, the proposed TPA plan is in accordance with privacy laws and has been reviewed with the IPC and, as no personal information will be provided by the SME under TPA, such access to the data is in compliance with section 9.1 of its licence (emphasis added):

> The Licensee <u>shall not use confidential or personal information</u> regarding a Distributor, consumer, Retailer, or any other person obtained for one purpose for any other purpose without the written consent of the consumer, Retailer, or other person[3].

The SME will make educational materials available in written format and on its website explaining the purpose of TPA, the benefits to Ontarians, the organizations that will have access and the process to enable such access, the privacy, ethical and security practices to protect the data. The SME will work with the LDCs to leverage these materials for use on call center scripts or on their websites.

v. The SME should seek approval of the basic terms of any Data Use Agreement ("**DUA**") with third parties. While recognizing that DUA's may need to be tailored to match the specific circumstances surrounding any particular release of data, the OEB's view is that there should be certain generic protections built into such agreements.

(i) Through this application the SME is seeking approval of the basic terms of the DUA, with the ability for the SME to tailor the DUA to match the specific circumstances surrounding any particular disclosure. The SME consulted on a draft DUA with intervenors who intervened in the SME's application that gave rise to the Prior Decision and has considered their comments in the version included with this application. Further evidence on this is provided at EX B-4-1 <u>The Data Use Agreement</u>.

[3] Smart Metering Entity Licence ES-2021-0191, S 9.1

Since the October 2019 Decision and Order the SME has:

i. Provided the OEB and the IESO access to the data.

ii. Provided highly aggregated data at no charge.

(i) The SME has not received any complaints about this data disclosure.

iii. Conducted research (utilizing Ipsos, an internationally recognized leader in market research) with 1,701, residential and small commercial smart meters customer across Ontario to discuss, hear and understand their issues and concerns around the provision of smart meter data to third parties.

iv. Consulted and worked with each of the parties that were intervenors in the SME's 2018 TPA application, which included Vulnerable Energy Consumers Coalition ("**VECC**"), Consumer Council of Canada ("**CCC**"), Building Owners and Managers Association ("**BOMA**") and the EDA and various of its committees in the development of this application and the DUA.

v. Consulted with each of Hydro One Networks Inc. and Toronto Hydro on the proposed mechanisms to deal with consumer enquiries and complaints to LDC's with respect to third party access to data.

vi. Consulted and worked with the SSC on managing consumer enquiries and complaints with respect to third party access to data.

vii. Shared information on this application and associated materials and consulted as appropriate with the following:

(i) The IESO's Stakeholder Advisory Committee

(ii) Information and Privacy Commissioner of Ontario

(iii) The Association of Municipalities of Ontario ("**AMO**"), and

(iv) The Association of Major Power Consumers of Ontario ("**AMPCO**").

viii. Shared information and provided updates on the application with Ontario Energy Board Staff.

THE PROPOSED THIRD PARTY ACCESS PLAN

Access to highly aggregated data is currently publicly available without charge, as set out on the SME's website. Access is also being provided to the OEB and the IESO without charge.

In preparing this TPA plan the SME has considered the results of consumer research conducted by IPSOS in late 2020 with 1,701 smart meter residential and small commercial consumers who provided their opinions on sharing de-identified consumption data with third parties. It also considers the comments and feedback provided by intervenors and other stakeholders in consultations on this application and the spirit of the OEBs decision on the SMEs prior TPA application, EB-2018-0316, (the "prior decision"). In its prior decision the final paragraph prior to the Order stated:

> "In summary, the OEB would like the SME to proceed cautiously given the concerns expressed. As the SME noted, this application raised novel issues. Although the OEB recognizes all the work the SME has done since the January 26, 2016 order; it agrees with the intervenors that there is still more work to do".[1]

Who will be able to access the data

Through this application the SME proposes to provide access to the data to organizations working in the public interest, ("**Canadian Government Entities**"), which are defined below and in Ex B-6-5 Defined Terms:

> Federal and provincial Canadian governments, including ministries, agencies, boards, commissions, tribunals and wholly-owned corporations, or in the case of non-share capital corporations, where such corporations are controlled by a federal or provincial government, as well as municipalities (or regional

[1]" EB-2018-0316, October 24, 2019 Decision and Order. Pg 15

governments), universities, school boards, hospitals and First Nations. First Nations means a "council of the band" as that term is defined in subsection 2(1) of the *Indian Act* (Canada).

Canadian Government Entities do not include following entities:

Private sector entities, publicly traded companies, individual doctors, professors, or government officials and all those entities that do not fall in one of the categories outlined above.

Through this application the SME is proposing that TPA be provided to Canadian government entities. The IESO is only providing access to public sector entities, this does not include the private sector, nor individuals in their personal capacity (they would have to seek access though their public sector institution).

What is the pricing model for access to the data

Access to standard data sets would be provided without charge and associated costs will be recovered through the SMC.

The SME is proposing that providing access to certain standard products, comprised of de-identified smart meter data in pre-defined time units (e.g. hourly, weekly, monthly, seasonally), in standard formats (e.g. csv, xlsx) be considered part of the SME's normal business operations and is proposed to be recovered through the SMC paid by distributors and ultimately passed through to all consumers with a smart meter, as the OEB allowed for in EB-2018-0316 for the public offerings and for data provided to the OEB and the IESO.

Standard products will be designed as easily repeatable data extracts that once set up will require a minimum level of effort from the SME in undertaking and managing them. Standard aggregations in standard formats would be derived from the data elements available for third party access to create privacy compliant data extracts: Total and/or Average Consumption Data aggregated by a pre-defined time unit (e.g. hourly, weekly, monthly), Distributor Rate Class (Residential, SGS<50kW), Commodity Rate Class (Time-of-Use, Tiered), Geographical Level (with highest granularity at 6 digit postal code). As the SME gains more operational experience and technology advances, the formats and the most commonly requested and useful aggregation levels are expected to evolve to maintain a minimal level of effort while serving the needs of requestors.

Access to more complex data sets, (visualizations, e.g. heat maps or complex analytics, e.g. trend analysis) which require additional staff time and resources to prepare, will be charged at a cost of $145/hour, thereby reducing any ratepayer burden that would be created. The cost will be the staff time and other resources required to prepare the data prior to access being provided. Requestors would be provided with an estimate of the cost to complete their request prior to signing the DUA which includes a clause to enforce payment of any fees, disbursements and other charges invoiced by the IESO minimizing any potential rate payer burden. Any monies generated though requests for more complex data sets will be tracked in the SME's previously approved Balancing Variance Account ("**BVA**[2]").

The SME is proposing to provide access only to Canadian Government Entities as defined in EX B-6-5 Defined Terms. This approach is supported by the preference indicated by consumers in the research conducted by Ipsos:

i. The results of the consumer research conducted with 1,501 residential and 200 small commercial consumers with smart meters indicated sharing smart meter data with the public section is most strongly supported due to the potential for 'greater good';

[2] SME Balancing Variance Account ("BVA")– provides the total of the SME's annual revenues, expenses, outstanding debt and the SLC balances.

ii. The consumer research indicated that providing data to Canadian Government Entities should be at no charge or at cost;

iii. Providing the data at no charge is in the spirit of the OEB decision on the SME's prior TPA application where it determined that the data should be provided to the OEB and IESO at no charge (emphasis added):

> As noted above, the OEB's January 26, 2016 order stressed that the enhanced data would help with the "design of conservation and demand management programs, the assessment of the effectiveness of time of use pricing, the design of distribution rates and time of use prices, and the regional planning of transmission and distribution systems." The OEB leads initiatives for the design of rates and prices, and the IESO coordinates regional planning and is responsible for the development of CDM programs funded through the global adjustment. It is therefore critical that both the IESO and OEB have access to de-identified customer consumption data for these functions. In view of the non-commercial, public interest in such access, it should continue to be provided at no charge.[3]

What are the privacy protections

In compliance with Section 9 of its licence, ES-2021-0191, the SME does not receive, have or retain any personal or confidential information of smart meter consumers hence it is not informing or seeking the permission of smart meter consumers to provide access to the data to Canadian Government Entities. The data sent to the MDM/R by LDCs does not contain street names or numbers, customer names or other personal information.
As required by the OEB[4] the SME collects the following information associated with

[3] October 24, 2019 Decision and Order, EB-2018-0316, pg 13
[4] [1] EB-2015-0297, January 26, 2016 Decision and Order, Pg 4

each smart meter (modified where necessary to sufficiently render it non-personal information):

- The postal code;
- The distributor rate class;
- The commodity rate class; and
- Occupant change data.

Prior to sharing smart meter data the SME applies the protocols recommended by a privacy expert firm, which follow the IPC de-identification guidelines for structured data. For details see Ex B–6-2 Privacy Analytics: An Independent Assessment of the IESO's Planned Privacy Strategy For Third-Party Data Access.

CONSULTATIONS WITH PRIOR INTERVENORS AND OTHER STAKEHOLDERS

In preparing this application, the SME has consulted with multiple parties to gather feedback and input on the SME's plan to address the items raised by the OEB in its Decision and Order on the prior TPA application, EB 2018 0316. Consultations focused on the status and results of the actions taken, including the results of the IPSOS Consumer Research and seeking input on a proposed approach for this application.

Consulted Parties

In developing this application, the SME consulted with the following parties:

Organization
Electricity Distributors Association ("**EDA**")*
Consumer Council of Canada ("**CCC**")*
Vulnerable Energy Consumers Coalition ("**VECC**")*
Building Owners Managers Association ("**BOMA**")
EDA staff and the following EDA Committees: • Communicators Council • Finance & Corporate Issues Council • Regulatory Council and • Operations & Engineering Council
Hydro One Networks Inc.
Toronto Hydro
The SME's Steering Committee ("**SSC**")
The IESO's Stakeholder Advisory Committee ("**SAC**")
Association of Major Power Consumers of Ontario ("**AMPCO**")
Association of Municipalities of Ontario ("**AMO**") - Energy Task Force

* Intervenors from the most recent TPA application

** Hydro One Networks has not registered as an intervenor in the most recent TPA application, but has filed a letter during the adjudication process

OEB staff, the Ministry of Energy and the Information and Privacy Commissioner of Ontario ("**IPC**") were also kept up to date on the timing and nature of the application through several meetings and briefing materials.

Issues and comments provided by parties during these consultations and meetings have been considered and the application addresses all of these including a recommendation from select intervenors that an opt-out option should be considered. All recommendations were incorporated in the application, except for the opt-out option which after thorough consideration and extensive discussions with other stakeholders the SME has determined that an opt-out option is not appropriate or required for the reasons outlined below:

- As stated in Ex A-1-1 the SME does not collect or have in its possession any personal or confidential information on individual smart meter consumers.
- The SME is not seeking to share or provide access to any confidential or personal information regarding consumers, in compliance with Section 9 of its licence, as quoted below:

  > **Section 9. Restrictions on Provision of Information**
  >
  > The Licensee shall not use <u>confidential or personal</u> information regarding a Distributor, consumer, Retailer, or any other person obtained for one purpose for any other purpose without the written consent of the consumer, Retailer, or other person

- Not all LDCs have the capacity to implement an opt-out option. The LDCs would be the point of contact for customers to choose an opt-out option and would have to process that option, but not all LDCs could implement an opt-out option, therefore the opt-out option could not be uniformly implemented.
- The LDCs have quoted technical issues, logistical issues around prioritization with other initiatives, potential confusion with other data projects or cost implications of an opt-out option that was seen rather unnecessary given the

relatively low risk of customer complaints associated with access of non-personal, de-identified smart meter data by Canadian Government Entities.

The SME's Steering Committee

The SSC acts as an advisory panel to the IESO in its role as the SME for Ontario. It is a stakeholder committee that represents the interests of MDM/R service recipients. The SSC is made up of representatives from local distribution companies and the IESO in its role as SME and currently consists of eight members. Except for the members-at-large and the member representing the SME, members are appointed from among nominations made by MDM/R service recipients or entities eligible to become MDM/R service recipients. Distributor representatives may also be appointed from nominations submitted by the Board of Directors of the EDA or any successor organization. Current members are:

Andy Armitage LDC Chair Synergy North	John Dunne LDC Vice-Chair Hydro One Networks Inc.	Kevin Myers Elexicon Energy
Shelley Parker Alectra Utilities	James Wei Toronto Hydro	Luke Seewald London Hydro
Judy Lidster Hydro Ottawa Limited	Rob Koekkoek Orangeville Hydro	Marianne Blasman Burlington Hydro
James Murphy IESO Lead		

The IESO's Stakeholder Advisory Committee

The Stakeholder Advisory Committee provides appointed stakeholder representatives with the opportunity to present advice and recommendations on market development, conservation and planning decisions directly to the IESO's Board of Directors and

Leadership Team. Members represent consumers, generators, distributors/transmitters, related businesses/services and Ontario communities.

TERMS OF ACCESS PRINCIPLES

The terms of access are largely similar to those in the SME's prior TPA application, EB-2018-0234, but modified to take into account the fact that the SME will not be charging any amounts above cost for access to the data.

The SME will provide third party access to the data, on appropriate terms. This will take two forms:

1. the principled assessment of each request for access to the data; and
2. the contractual terms upon which access to the data shall be granted.

These are described in more detail below:

Principled Assessment of Requests for Access

Each request for access to the data will be assessed by the SME based on the principles set out below. The SME shall modify or decline a request not in keeping with the principles set out below:

1. ***Privacy*** – The SME respects privacy and is committed to protecting personal information. The SME is collecting data that does not contain personal identifiers[1] and will take steps to prevent any re-identification of data. The SME may modify a request or decline to provide access to the data where it believes that acceding to such a request would impede the SME's ability to meet its privacy obligations or would compromise the de-identification of a premise as per guidelines established by the Information and Privacy Commissioner of Ontario[2].
2. ***Security*** – The SME is entrusted with the electricity consumption data of Ontarians and works to ensure that the data remains secure through appropriate administrative, technical and physical safeguards to protect against

[1] The SME puts in place additional privacy filters to mitigate the risk of re-identification of an individual.

[2] De-identification Guidelines for Structured Data, June 2016, Information and Privacy Commissioner of Ontario.

unauthorized disclosure, use, alteration and destruction of the data. The SME will modify or deny any request for access to the data that may compromise the safeguards or the security of any of the data.

The SME seeks to ensure that those requesting access to the data have appropriate technological capabilities to receive, handle, safeguard and securely destroy the data, as applicable. The SME will modify or deny a request where the requester cannot demonstrate appropriate technical safeguards in place.

3. ***Ethical Works*** – the SME has high ethical standards and promotes the ethical use of the data. The SME reserves the right to deny or modify a request that is not in keeping with SME's ethical standards as determined by the SME, including, as applicable, with input from its Ethics Review Committee as discussed below.
4. ***Compliance*** – The SME is a creature of statute and is a regulated entity. The SME acts in accordance with its legal and regulatory obligations, and will assess each request to ensure fullfilling such a request would not interfere with its ability to adhere to its legislative and regulatory requirements.
5. ***Ratepayer value*** – The SME will undertake third party access in a manner that recovers costs for non-standard requests and provides value to SME ratepayers. The SME will provide a public benefit through providing access to the eligible category and continuing to provide public offerings available at no cost online.
6. ***Accessibility*** – The SME is committed to treating all people in a way that respects their dignity and independence, and meets the needs of stakeholders with disabilities in a timely manner. In considering a data request, the SME will take reasonable measures to prevent and remove barriers to accessibility and to meet the requirements under the *Accessibility for Ontarians with Disabilities Act, 2005*.
7. ***Quality*** – The SME wants to be a source for clear, reliable data. Where a request seeks data that is not of a sufficiently high quality, the SME reserves the right to deny or modify such a request.

Contractual Terms Upon Which Access Will be Granted

The SME will enter into a DUA with each person that will be granted access to the data as further described in Ex B-5-1, The Data Use Agreement.

Ethics Review Committee

As noted in the above item (3), Ethical Works, enabling access to the data by third parties entails the responsibility of ensuring that the data provided by the SME is used for ethical purposes. Therefore, the SME will evaluate each request to determine whether the request would promote the ethical use of the data. Where the SME has concerns about the ethical use of the data, it will engage an Ethics Review Committee. The Ethics Review Committee will have at least three members, one of which will be a reputable industry expert, external to the IESO.

THE DATA USE AGREEMENT

In its prior decision, the OEB stated that the SME should seek approval of the basic terms of any DUA with third parties (other than the OEB in its capacity as the SME's regulator). While recognizing that each DUA may need to be tailored to match the specific circumstances surrounding any particular release of data, the OEB was looking to approve certain generic protections built into such agreements.

A draft DUA was provided to all intervenors in the prior TPA application for their review and comment.

Comments were received from VECC's representative and counsel. No other party provided comments. These comments have been taken into consideration in the final form of the DUA.

We attach the terms of the DUA for the OEB's review and approval, including the basic terms as required in the prior decision. This is very similar to the form of data use agreement used in the IESO pilots and the recent disclosures of highly aggregated data, so in addition to comments from the intervenors, we have had the benefit of input from various pilot participants and highly aggregated data users. A summary of the pilots is provided at EX B-7-1-3 Summary of SME Data Requests.

The SME has included, *inter alia,* the following basic terms:

- License provisions setting out the scope of the data user's entitlements to use the data and making clear that it will not acquire any rights or title in the data not set out in the agreement.
- Restrictions on use of the data, including ensuring it is only used for the purpose outlined in the use case and will not be used to contact individuals to whom the data relates.
- Requirements to safeguard the data, including administrative, physical, organizational and technological safeguards.

- Requirements relating to appropriate policies and procedures about the security of the data, including as related to retention, transfer and destruction of information.
- Requirements to notify the SME in the event of demands for the data, unauthorized access to the data and any actual or suspected "data incident".
- Confidentiality requirements.
- Provisions that allow for the SME's assessment of compliance with the terms of the DUA.

Nevertheless, we agree with the OEB's observation although there are basic terms that remain common, such as those listed above, there will be the need to tailor the agreement for specific circumstances. Accordingly, the SME is requesting that any approval of the basic terms of the DUA allow for the SME to tailor the DUA to adapt to the needs of the requestor and/or the use case, while ensuring the protections outlined in the above paragraph 5 remain in place.

In addition, the SME developed Schedule 3 to capture terms that could change for each application. These include:

- A description of a use case to be assessed by the SME to determine it meets the principles described in EX B-4-1 <u>Terms of Access Principles</u>.
- A section allowing the SME the opportunity to be aware and approve any third parties listed who may have access to the data, for example if two municipalities were partnering to do a joint study. However, the SME would not provide the information to third parties that would not otherwise be eligible to receive the data.
- A section allowing the SME to undertake a risk assessment where data may be processed outside of Canada, and the country has been determined to have a

sufficiently robust legal and information security regime to permit processing outside of Canada. In practice, given the limits on eligible data users (i.e. the Canadian Governmental Entities) this is likely to be used infrequently but may come up in the context of a contractor that has data storage or processing outside of Canada.

- The SME will also allow the linkage of the data with other data sets only where they have been disclosed. This is to prevent attempts to reverse-engineer the data through layering on additional data sets; however, it does allow for meaningful use of the data where the linkage is appropriate. For example, electricity consumption per census district was usefully combined with COVID-19 social distancing mandates to inform research in understanding impacts to electricity usage in Ontario. The SME would assess the appropriateness of any proposed links in light of the proposed use case.
- Case-specific provisions such as length of use and any applicable fees.

There may be other instances where changes to the agreement is appropriate. Accordingly, the SME seeks the ability to tailor the DUA where appropriate, for example to accommodate requests from Ontario Ministries that must adhere to the requirements of the *Financial Administration Act* (Ontario) and are not able to provide indemnities without meeting the provisions of that legislation. These will be assessed on a case-by-case basis, but in any event would not change the basic protections outlined in paragraph 5, above.

COSTS AND THE SUGGESTED TARIFF SHEET FOR FULFILLING STANDARD AND NON-STANDARD DATA REQUESTS

Cost of fulfilling standard data requests

The SME has estimated that providing TPA standard requests and the public offerings of highly aggregated smart meter data to be approximately $350,000 per year, approximately $0.07/smart meter per year, based on the SME receiving up to 40 requests per year. Actual costs will vary based on the number of requests.

Charge for fulfilling non-standard requests

Costs for non-standard requests will be recovered from the requesting party at a charge of $145/hour. This hourly charge is a reasonable representation of the costs the SME will incur to fulfill these requests, the SME is not proposing to subsidize or profit from fulfilling these requests. The SME will track any funds generated resulting from non-standard requests in its BVA.

An estimate of the cost to fulfil a non-standard will be provided in advance of the SME performing the work.

Proposed costing sheet

Canadian Government Entities will be able to access the data at the cost schedule shown in Table 1:

Table 1

	Charge	Costs are recovered	Funds generated are
Public offerings of highly aggregated smart meter data	$0	Through the Smart Meter Charge	N/A
Standard request	$0	Through the Smart Meter Charge	N/A
Non-standard request	$145/hour	From the requestor	Tracked in the BVA

IESO SMART METER DATA RESEARCH

Summary of Research Results

FINAL REPORT

FOR DISCUSSION ONLY

ieso
Connecting Today.
Powering Tomorrow.

Ipsos

Contents

METHODOLOGY AND OBJECTIVES

Background

In 2016 the OEB directed the IESO to uncover the value of data residing in the MDMR by collecting additional data fields and presenting a plan to implement third-party access to the data. Late 2016 the OEB was satisfied with the collection of the data and the preliminary plan presented by the IESO.

Following extensive consultations in 2017 and 2018 with several organizations (public, private, the IPC, a privacy expert) the SME submitted a more detailed plan to the OEB, including a proposal to develop a monetization model to maximize ratepayer benefit.

In 2019 the OEB allowed sharing of highly aggregated data but asked the IESO to do further work in light of interveners' concerns, in particular to consult consumers to better understand their expectations on privacy protection, data use and pricing of the data that would be shared with third parties.

To inform this next submission due in 2021, the IESO commissioned IPSOS to conduct market research with residential and small business consumers.

Research Objectives

Objectives for each phase of the research are as outlined below.

Phase 1: Qualitative Online Focus Groups

- Testing comprehension of, and the language used to illustrate, data security and privacy protection, end use cases and cost models;
- Testing reactions to end use cases and cost models;
- How the use cases and cost models can be modified for optimal comprehension;
- Any differences between the two audiences – residential, and small business customers of LDCs

Note that findings for the qualitative phase are directional and not representative.

Phase 2: Quantitative Survey

- Attitudes towards the privacy of electricity data and government agencies making it available;
- Strength of concerns, expectations and perceived risks of sharing smart meter data including data privacy in general;
- Effectiveness (level of understanding) of educational material;
- Strength of benefit (value proposition) of sharing smart meter data (overall and for selected use cases);
- Level of support for concept of sharing smart meter data, final selection of specific use cases and monetization models;
- Determine the factors most important to driving importance of sharing smart meter data (key drivers' analysis) and segment consumers based on their attitudes towards data and privacy to quantify those with a high, moderate or low-degree of concern

Methodology

Phase 1: Qualitative Online Focus Groups

- A preliminary qualitative phase of research was used to inform the design of the quantitative survey. Four (4) focus groups were executed using an online platform and teleconference with small business and residential electricity customers in Ontario.

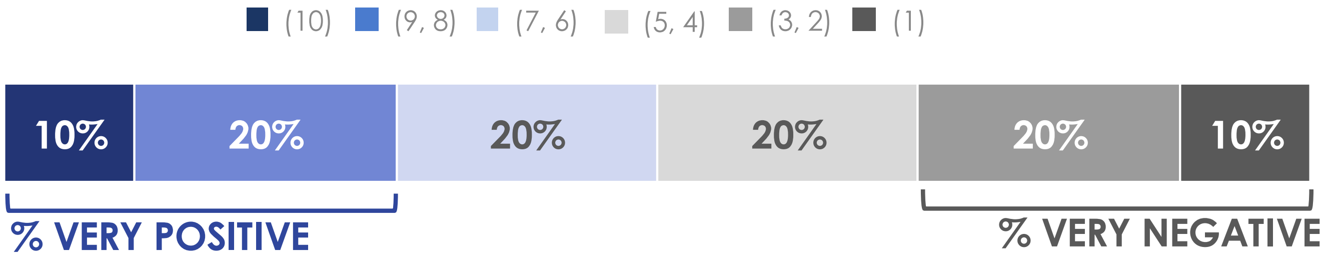
Phase 2: Quantitative Survey

- The survey was executed online among a representative sample of n=1,501 Adult Ontarians (Residential consumers) and n=200 Small Business consumers. Fieldwork was conducted between Oct. 28 – Nov. 11 2020.
- Sample was sourced from a mix of pre-recruited iSay panel sample and non-panel random Ipsos Ampario sample. For the Residential consumer survey, the sample was stratified and weighted to ensure the final sample is representative of the Ontario adult population by age, gender, and region. For the Small business survey, consumers were defined as decision-makers in organizations with 2-50 employees and included a mix of industry sectors.
- Results among Residential consumers are accurate to within +/- 2.9 percentage points and among Small business consumers to within +/- 7.9 percentage points. The credibility interval will be larger for sub-groups of the data. For more information on the use of credibility intervals, please consult the following document.
- Results for the quantitative survey formed the basis for the key findings of this report. Findings from the qualitative phase were consistent with the quantitative survey. Where necessary additional details from the qualitative research have been noted in the key findings to supplement the quantitative results.

Methodological Note: Reporting Conventions

Method of reporting 10-pt scales

- In this report, several questions are rated on a 10-point scale and responses grouped to express the range of sentiment. For the purposes of this study, respondents who answered 6 or higher are considered 'positive' and 5 or lower 'negative': 8-10 is considered 'very positive', 6-7 'somewhat positive', 5-4 'somewhat negative' and 1-3 as 'very negative'. Data is also presented for the most positive and negative sentiment (scale ends, 10 and 1).



- Reporting conventions are driven by the objectives of the research. The goal of the groupings used in this report was to ensure we appropriately captured the proportion of consumers who are broadly accepting or comfortable while demonstrating the strength of sentiment.

Mentions of Public Sector

- Throughout the report, references made to organizations in the 'public sector' refer to those in the business of public good such as educational institutions, municipalities, utilities or government entities.

KEY FINDINGS

Key Findings (1/3)

Consumers are generally supportive with the sharing and use of smart meter data and they see value in how the data could be used to improve decision-making in the electricity sector.

More than seven in ten Residential (71%) and Small Business (79%) consumers feel it is at least somewhat important for data produced by smart meters to be shared. Similar proportions feel it is very important (39% of Residential and 40% of Small Business) or somewhat important (32%, 39% respectively), while few feel it is not important (10%, 8%).

Sharing smart meter data with the public-sector is most strongly supported due to the potential for 'greater good'.

Reaction is positive for use by organizations in the public-sector and consumers are generally comfortable with their electricity data being used for analysis by educational institutions, municipalities, utilities or government entities. There is also some degree of expectation that IESO already actively uses the data it to help inform decisions.

Anticipated benefits for the initiative relate primary to public sector use and broad electricity system efficiencies such as cost savings/ lower rates through better planning and more accurate analysis.

When sharing smart meter data outside the IESO, consumers are most sensitive to the issue of ensuring privacy and security of data and to a lesser extent of potential users and uses.

The primary factor influencing perceived importance of the initiative is the degree to which consumers feel their data is secure and their privacy protected when aggregated in a non-identifiable way. For Residential consumers, it is also about who is using the data- as long as they are comfortable with the user they feel the uses will be acceptable. For Small Business, importance is driven by both who is using the data and whether the purpose has a direct impact on their business.

Key Findings (2/3)

Consumers feel generally confident in the IESO to protect their privacy and express less concern about internal use of the data. However, there is greater uncertainty about what happens with the data once with the requestors and their data security measures in place.

Nearly seven in ten Residential (66%) and Small Business (69%) consumers feel their smart meter data is generally secure and protected, while few feel it is not (15%, 11%). The visual detailing privacy protocols was well-received and helped to improve consumers' understanding and confidence in the process.

Consumers are generally skeptical that privacy or security measures could protect against unintended purposes once the data has left the IESO since this depends to a large extent on the requestor's data security measures. More detailed information on the process in place to audit and protect against improper use once the data has left the IESO and the data security measures for requestors would help manage this perception.

Support is weaker for sharing smart meter data with for-profit companies as consumers feel there is greater potential for misuse by these organizations.

Comfort is considerably lower for sharing data with private industry and the benefits of doing so not clearly understood. Consumers express broader concerns about the motives of these organizations and the potential for the data to be misused.

The qualitative research highlighted that concerns about for-profit use relate to uncertainty about how sharing the data would help consumers and the potential for their data to be used against them, such as being targeting for marketing or to increase the cost of services and products based on electricity consumption.

More clarity on how the data would be used by for-profit organizations, the value to consumers and additional details on protocols in place to protect against improper use would help to allay those who have concerns.

Key Findings (3/3)

Consumers want smart meter data shared with non-profits at limited price to ensure the anticipated benefits to the electricity sector are realized and want a profit for ratepayers generated from for-profit organizations.

Support is strongest for pricing models that would charge no fees or only recover costs from non-profits, to ensure their activities could contribute to the greater good, and that a profit should be generated from for-profit organizations.

The no fees pricing model *for all requestors* had the least support from both residential and small businesses among all options presented.

In summary, consumers are more comfortable with smart meter data being shared with the public sector compared to the for-profit sector, and feel it is reasonably important to do so. They clearly see the potential value to the electricity sector and want data shared with non-profits at limited price to ensure these benefits are realized.

Consumers are broadly comfortable with use of smart meter data in the public-sector and have the expectation that more widespread use would help to improve decision-making and the efficiency of the electricity system over time. Ensuring non-profit organizations have access to this data at limited price, so long as it doesn't have negative impacts on consumers, is a priority.

Concern regarding the initiative relates predominantly to use by for-profit organizations and how data could be misused by these organizations.

IMPORTANCE OF EXTRACTING VALUE FROM SMART METER DATA

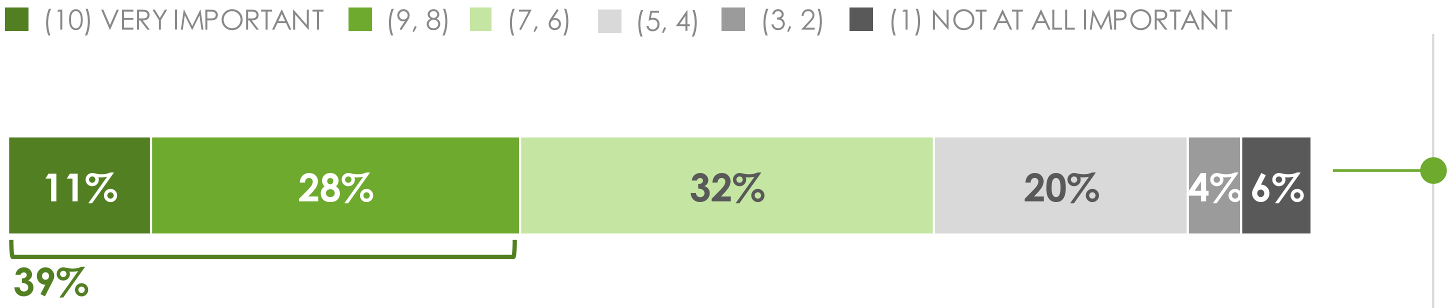
Overall impressions and drivers of importance

Perceived benefits and concerns with sharing smart meter data

Importance of extracting value from smart meter data

- More than seven in ten Residential (71%) and Small Business (79%) consumers feel it is at least somewhat important (rating of 6-10 out of 10) for data produced by smart meters to be shared. Similar proportions feel it is very important (39% of Residential and 40% of Small Business) or somewhat important (32%, 39% respectively), while few feel it is not important (10%, 8%).

RESIDENTIAL (n=1501)



Very important (8-10) higher among:

- Consumers aware of how smart meters work
- Higher income households, University educated, Men

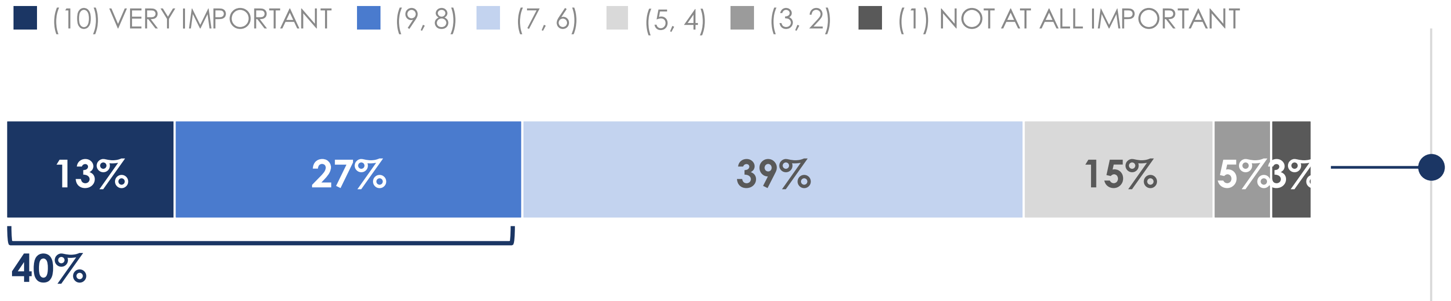
Somewhat important (6-7) higher among:

- Women, Under 55 years old

Low importance (1-3) higher among:

- Over 55 years old, Less formal education, Lower income households

SMALL BUSINESS (n=200)



Very important (8-10) higher among:

- University educated or higher, Organizations with 5-9 employees

Somewhat important (6-7) higher among:

- Organizations with 10-19 employees

Low importance (1-3) higher among:

- Over 55 years old, Organizations with 2-4 employees

Drivers of importance of extracting value from smart meter data

- The primary driver of importance for both Residential and Small Business consumers is the degree to which they feel their data is fully secure and privacy protected. Comfort with data aggregated in a non-identifiable way (such as by neighbourhood defined as 6-digit postal code) is also a prominent driver for both audiences. For Residential consumers, importance is also driven by comfort with potential public sector data users. For Small business consumers, importance is also driven by both potential users (specifically educational institutions) and use cases that directly benefit business.

RESIDENTIAL (n=1501)

1 Smart meter data is both **fully secure and privacy is protected**

2 Comfort with data **aggregated in a non-identifiable way** being used for analysis

3 Comfort with potential public sector **data users**

SMALL BUSINESS (n=200)

1 Smart meter data is **fully secure and your privacy protected**

2 Comfort with data **aggregated by all businesses in a non-identifiable way** being used for analysis

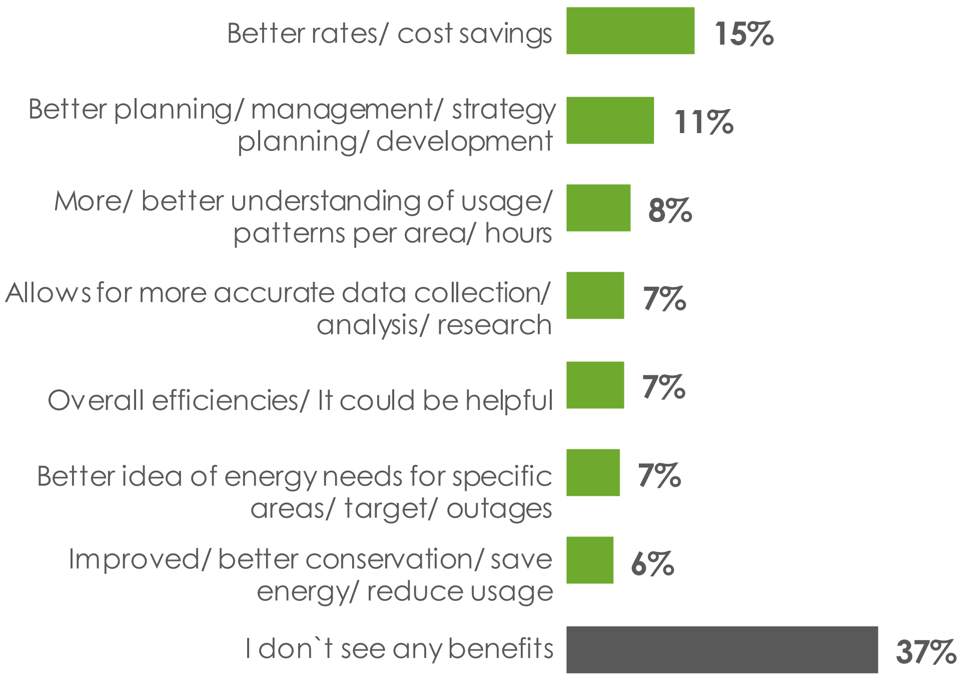
3 Comfort with potential **data users specifically education institutions**

4 Comfort with uses cases that directly benefit business

Benefits of Sharing Smart Meter Data- Unprompted

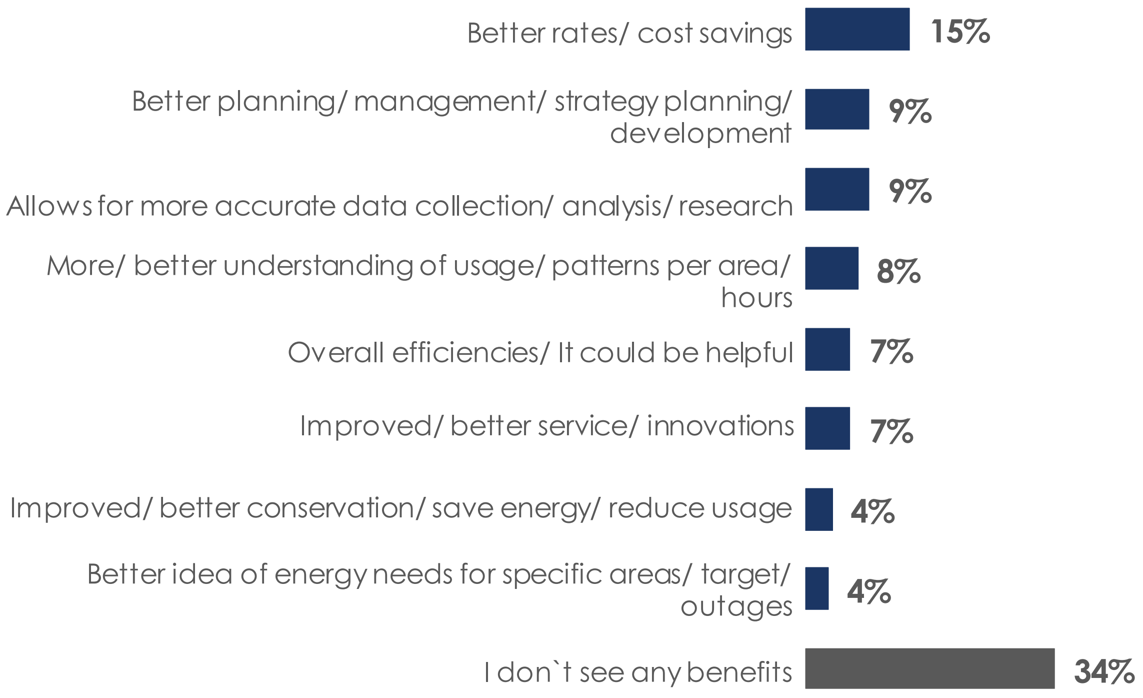
- When asked about the perceived benefits of sharing smart meter data, the most common themes relate to broad holistic benefits and efficiencies for the electricity system and the potential for cost savings. Results are consistent across Residential and Small Business consumers.
- Approximately one-third of both audiences could not imagine any benefits.

RESIDENTIAL (n=1501)



* Mentions less than 5% not shown

SMALL BUSINESS (n=200)

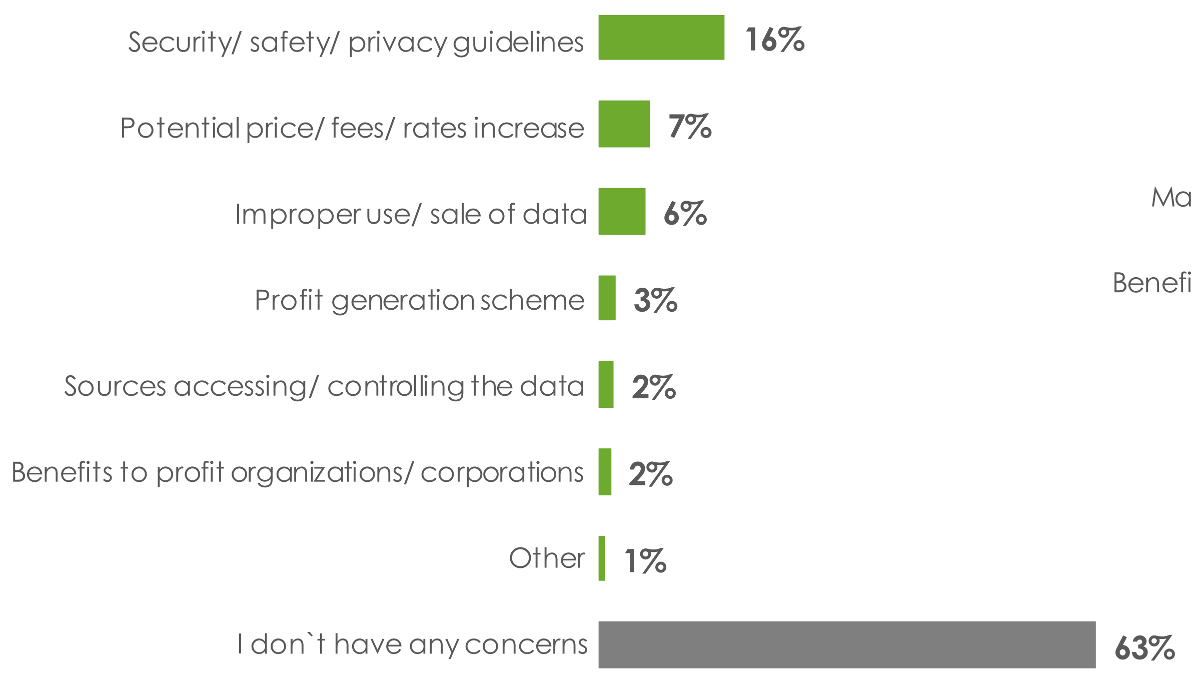


* Mentions less than 4% not shown

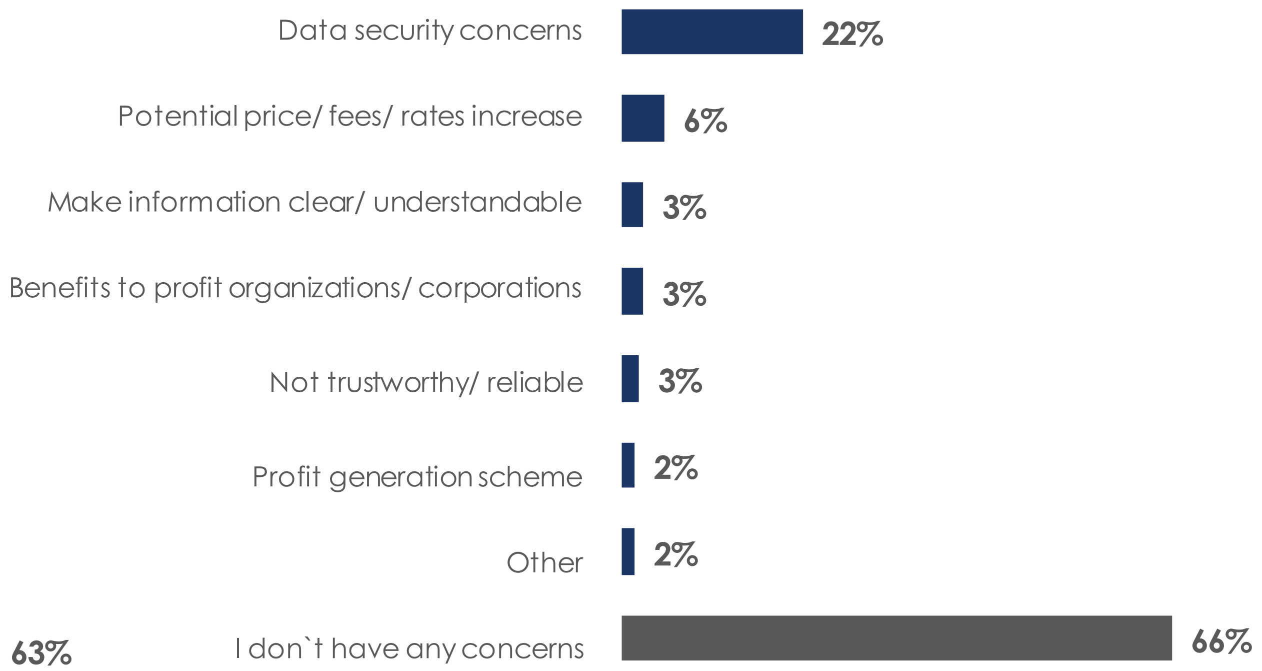
Concerns Not Yet Addressed- Unprompted

- The majority of Residential (63%) and Small Business consumers (66%) do not have any concerns with sharing smart meter data.
- Of those who do, the most common relate to data security and privacy. Other common concerns include the potential for rate increases or improper use or sale of the data.

RESIDENTIAL (n=1501)



SMALL BUSINESS (n=200)



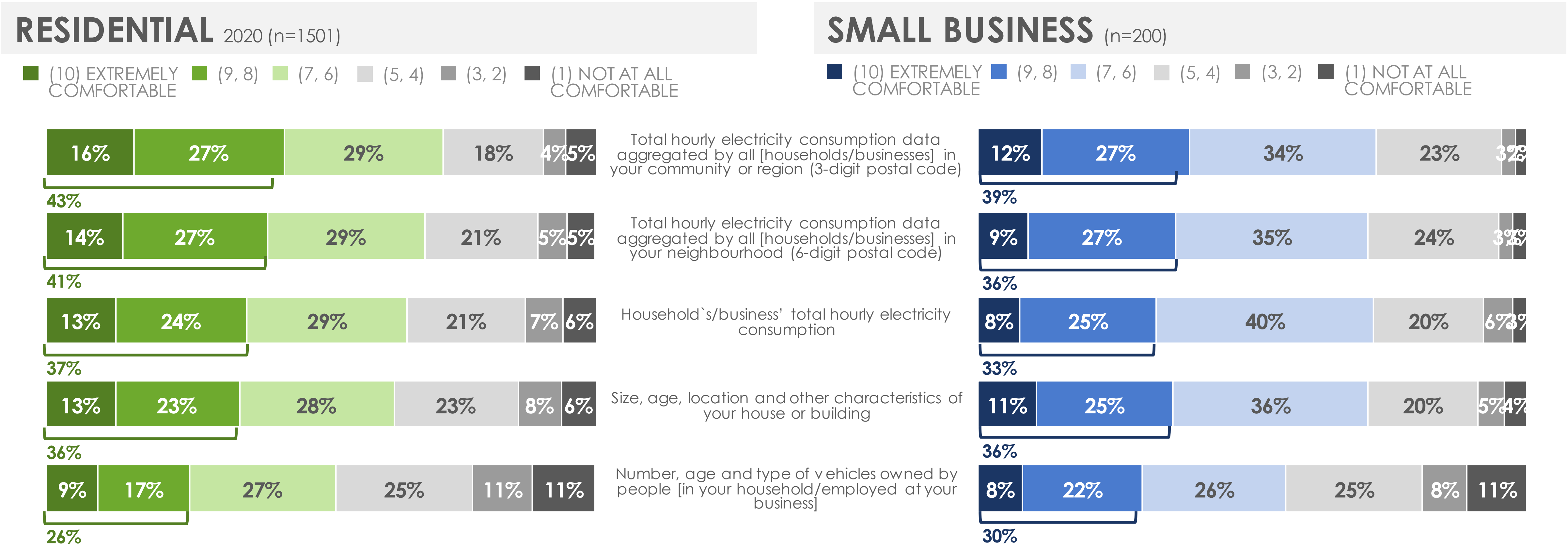
** Mentions less than 2% not shown*

COMFORT WITH SMART METER DATA BEING USED

Types of data use, potential users and support for specific uses

Comfort with Types of Data Use

- Residential and Small Business consumers are most comfortable with their electricity data being used for analysis, in a non-identifiable way, at a highly aggregated level. Few are not comfortable (rated 1-3) with electricity data being used for analysis regardless of the level of granularity.
- Notably comfort with electricity consumption data being used for analysis is consistent or higher than with other types of data already available in market such as characteristics of your house/ building or detail on vehicles owned by the household.

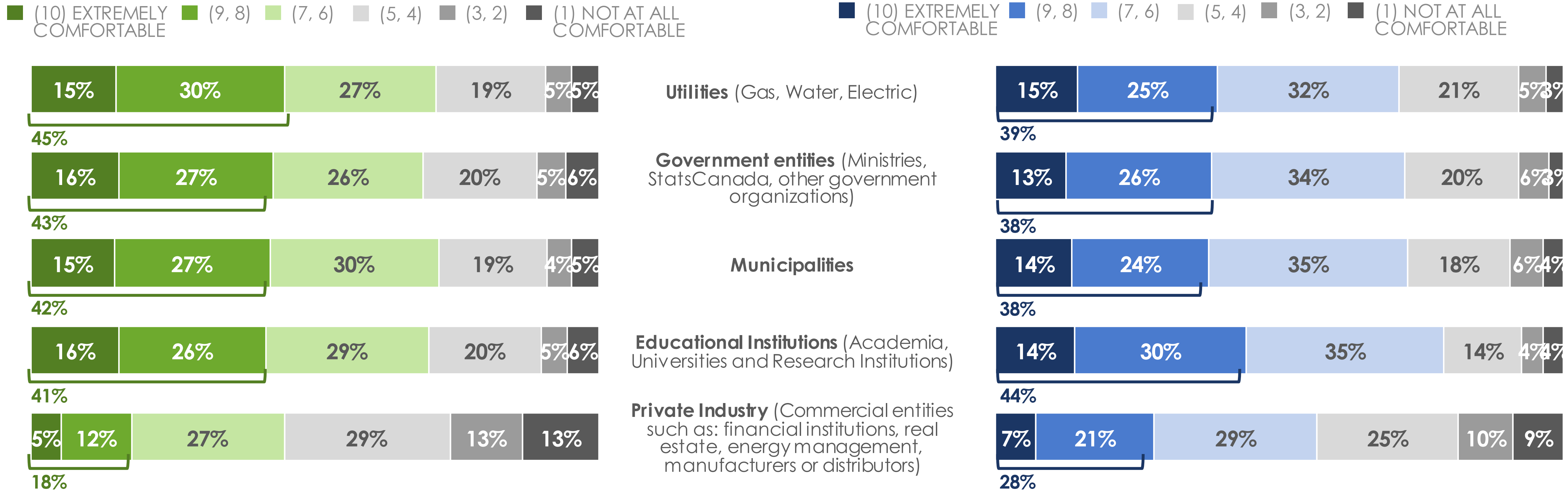


Comfort with Data Users

- The vast majority of Residential and Small business consumers are at least moderately comfortable (rating of 6 or higher) with non-profit organizations using smart meter data for analysis. Approximately four in ten are very comfortable (rated 8-10) sharing data with non-profit organizations, around three in ten somewhat comfortable (6-7), while few are not comfortable (rated 1-3).
- Comfort is considerably lower for sharing smart meter data with private industry.

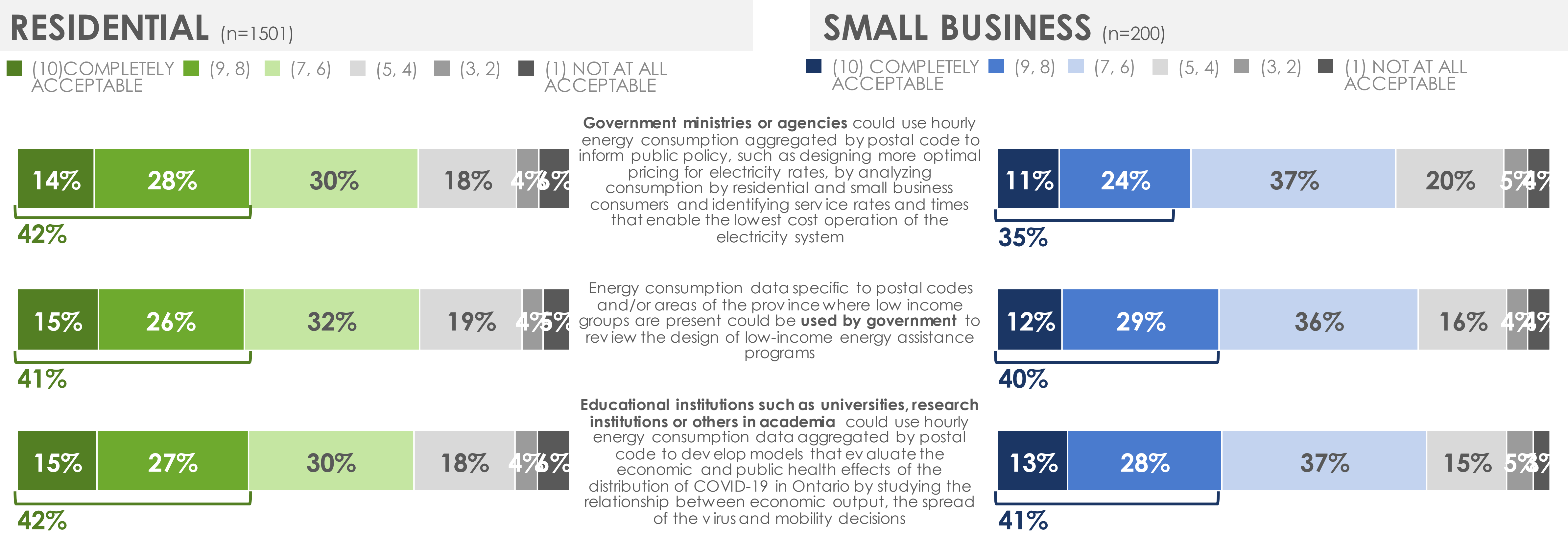
RESIDENTIAL 2020 (n=1501)

SMALL BUSINESS (n=200)



Acceptability of Select Uses for Smart Meter Data

- Consistent with comfort by potential users, a strong majority of Residential and Small Business consumers feel use cases for a non-profit organization is at least moderately acceptable (rating of 6 or higher). Four in ten feel each potential use by non-profits is very acceptable (rated 8-10), around three in ten somewhat acceptable (6-7), while few feel any use case is not acceptable (rated 1-3).



Government ministries or agencies could use hourly energy consumption aggregated by postal code to inform public policy, such as designing more optimal pricing for electricity rates, by analyzing consumption by residential and small business consumers and identifying service rates and times that enable the lowest cost operation of the electricity system

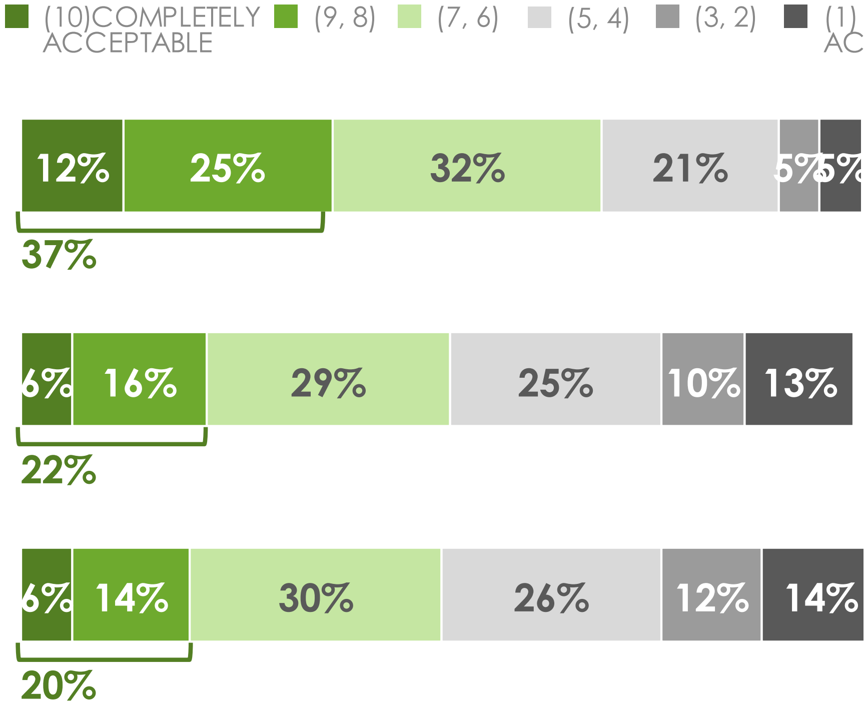
Energy consumption data specific to postal codes and/or areas of the province where low income groups are present could be **used by government** to review the design of low-income energy assistance programs

Educational institutions such as universities, research institutions or others in academia could use hourly energy consumption data aggregated by postal code to develop models that evaluate the economic and public health effects of the distribution of COVID-19 in Ontario by studying the relationship between economic output, the spread of the virus and mobility decisions

Acceptability of Select Uses for Smart Meter Data (cont.)

- A majority of Residential and Small Business consumers feel it is at least moderately acceptable (rating of 6 or higher) for smart meter data to be used by energy service companies to enable better targeting of conservation programs.
- Both audiences feel use cases by Insurance companies to add energy consumption data into their rate models or market research and advertising agencies to enrich existing data sets would be much less acceptable. Acceptability of use by either is particularly low among Residential consumers.

RESIDENTIAL (n=1501)

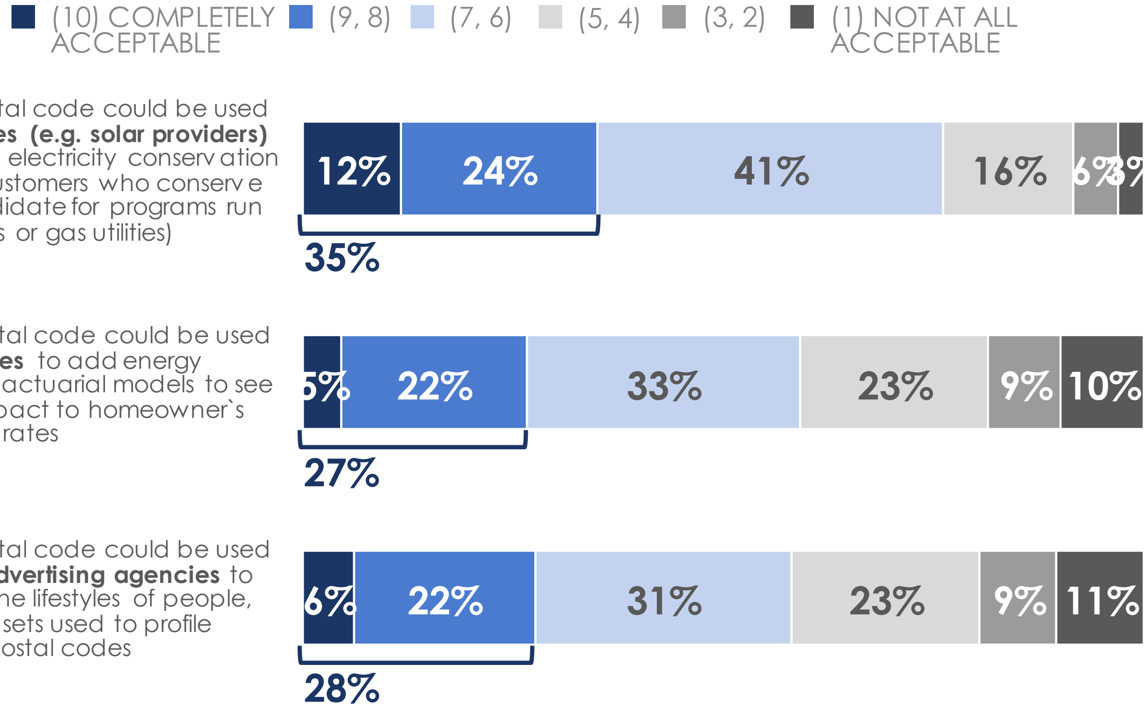


Energy consumption by postal code could be used **by energy service companies (e.g. solar providers)** to enable better targeting of electricity conservation programs by focusing on customers who conserve electricity (i.e. a good candidate for programs run by hydro companies or gas utilities)

Energy consumption by postal code could be used **by Insurance companies** to add energy consumption data into their actuarial models to see if there is a meaningful impact to homeowner`s insurance rates

Energy consumption by postal code could be used **by market research and advertising agencies** to make assumptions about the lifestyles of people, enriching existing data sets used to profile behaviours by postal codes

SMALL BUSINESS (n=200)



PRIVACY AND SECURITY

Impressions of security and privacy of smart meter data

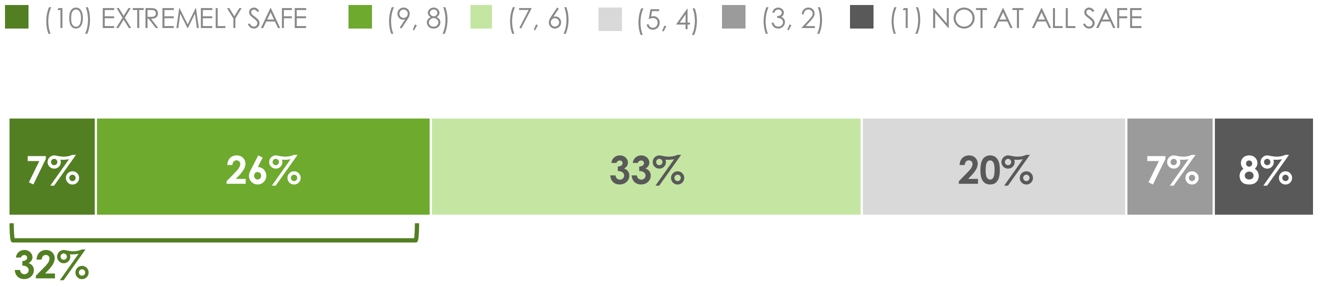
Assessment of privacy visual and depth of information shared

Attitudes towards sharing smart meter data

Privacy and Security of Smart Meter Data

- After being provided a description of privacy and security policies, approximately one-third of both audiences feel their smart meter data is very secure and protected (rated 8-10) or somewhat secure and protected (6-7), while few feel it is not secure and protected (rated 1-3).

RESIDENTIAL (n=1501)



Very secure/ privacy protected (8-10) higher among:

- Higher income households, University educated, Men

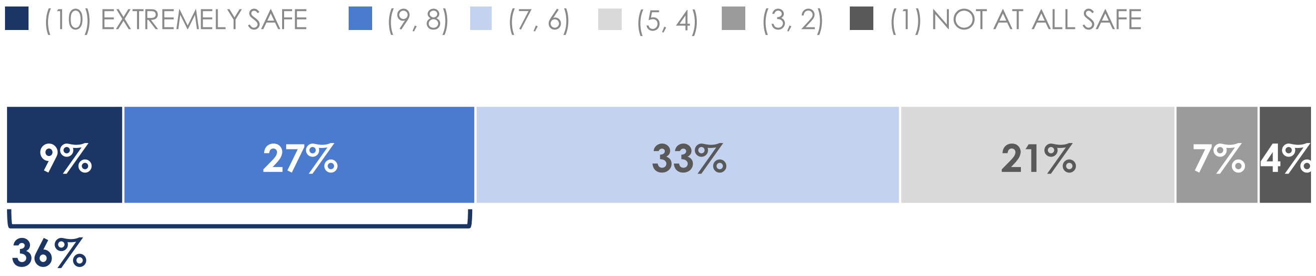
Somewhat secure/ privacy protected (6-7) higher among:

- Under 55 years old

Not secure/ privacy protected (1-3) higher among:

- Over 55 years old, Less formal education, Lower income households

SMALL BUSINESS (n=200)



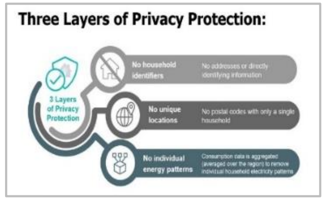
Not secure/ privacy protected (1-3) higher among:

- Over 55 years old, Organizations with 2-4 employees

Filed: October 29, 2021
EB-2021-xxxx
Exhibit B
Tab 6
Schedule 1
Page 24 of 42

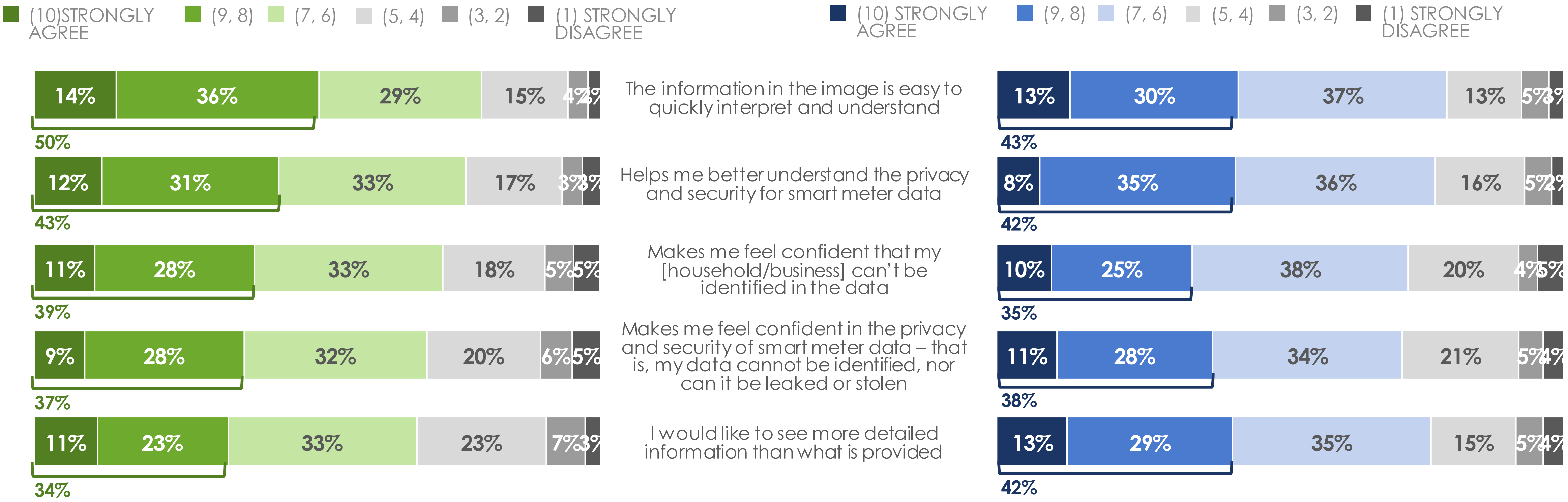
Assessment of Privacy Visuals: Three Layers of Privacy Protection

- The 'Three Layers of Privacy Protection' visual was positively received (rating of 6 or higher) by the vast majority of both Residential and Small Business consumers. It was rated highest for being easy to interpret, helping in understanding privacy and security of smart meter data and improving confidence in the process.
- A sizeable proportion of consumers would also like to see the visual complimented with more detailed information, particularly small business consumers.


Three Layers of Privacy Protection:
3 Layers of Privacy Protection
No household identifiers
No addresses or directly identifying information
No unique locations
No postal codes with only a single household
No individual energy patterns
Consumption data is aggregated (averaged over the region) to remove individual household electricity patterns

RESIDENTIAL (n=1501)

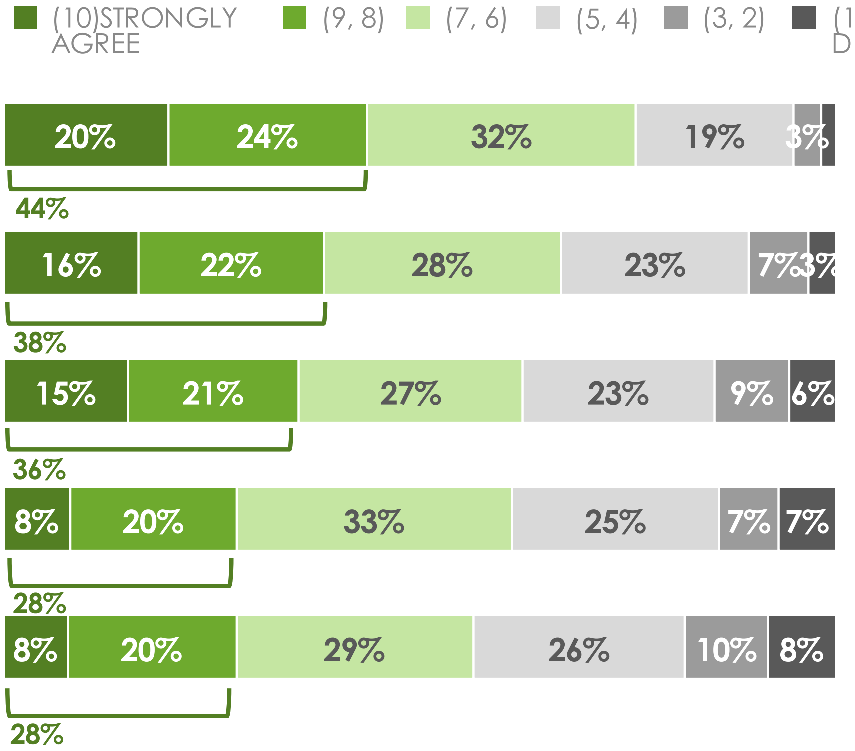
SMALL BUSINESS (n=200)



Attitudes Toward Sharing Smart Meter Data

- Agreement among Residential and Small Business consumers (rating of 6 or higher) is high that regardless of source or controls, no privacy or security measures can ensure against improper use. Concern is also reasonably high about the data being breached / stolen once it has been shared with a third party and that their data will be used against them.
- Consumers are more mixed in their opinions whether they consider aggregated electricity usage data to be sensitive personal information and trust that the IESO will have a robust process to audit and verify that data is used only for intended purposes once shared with a third-party.

RESIDENTIAL 2020 (n=1501)



These days no privacy or security measures can ensure that data from any government or other sources are protected from improper use.

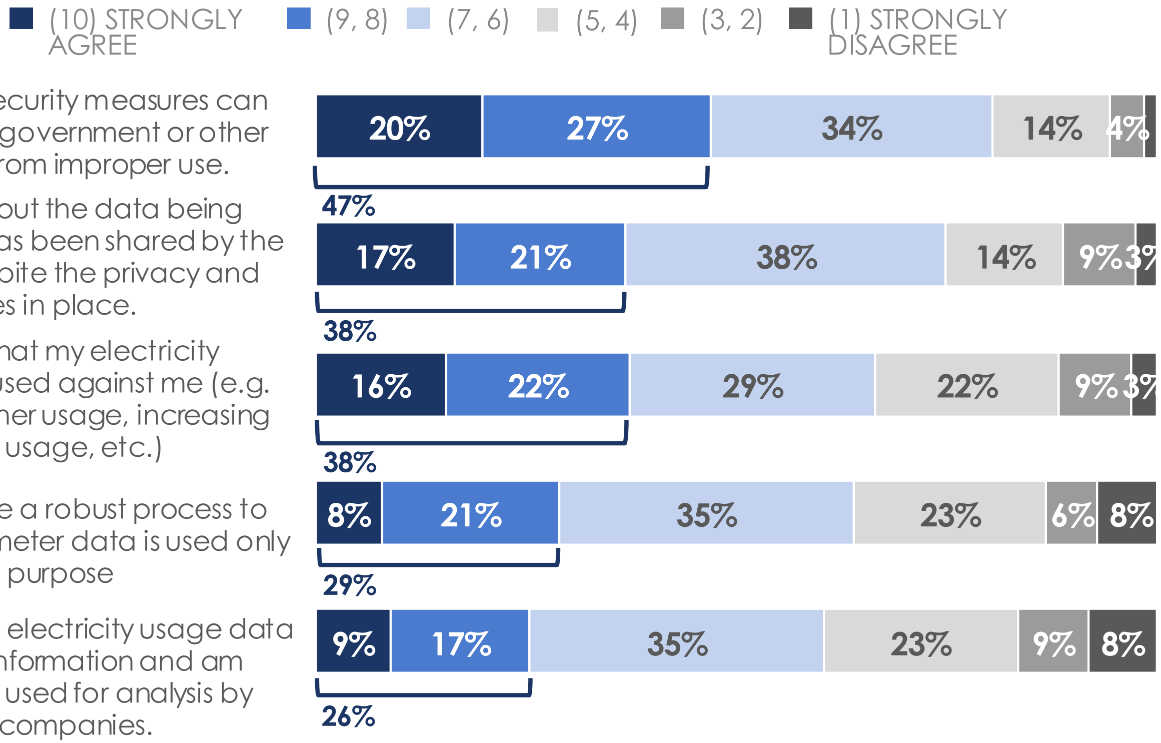
I am very concerned about the data being breached / stolen once it has been shared by the IESO with a third party despite the privacy and security measures in place.

I am very concerned that my electricity consumption data will be used against me (e.g. shaming consumers for higher usage, increasing rates based on my usage, etc.)

I trust that the IESO will have a robust process to audit and verify that smart meter data is used only for its intended purpose

I don`t consider aggregated electricity usage data to be sensitive personal information and am comfortable with it being used for analysis by government and companies.

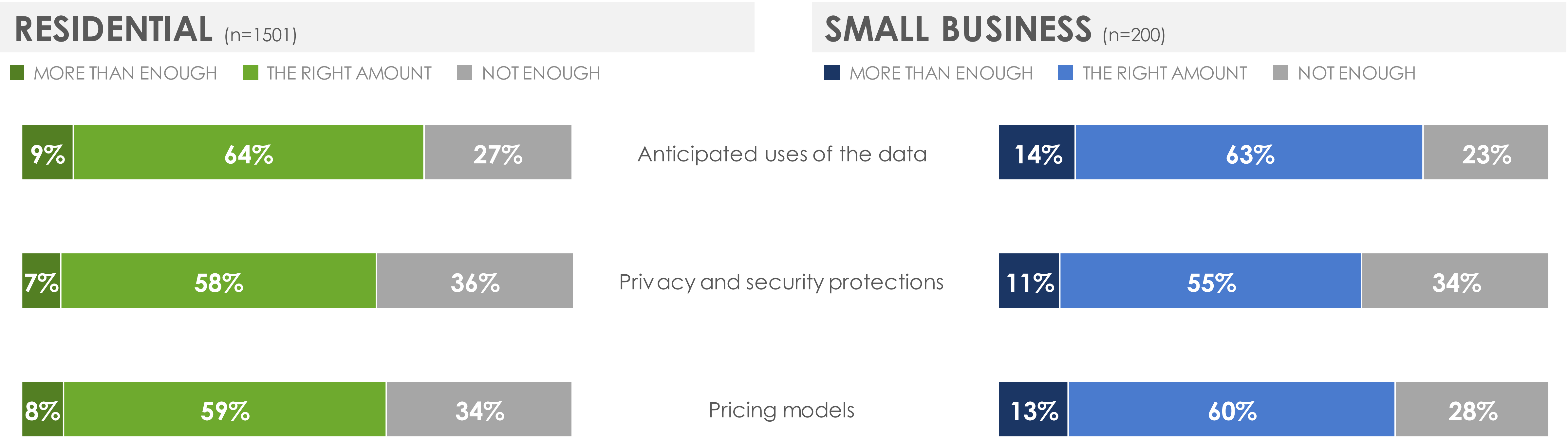
SMALL BUSINESS (n=200)



*data >2% not labelled

Depth of Information Shared

- The vast majority of Residential and Small business consumers feel that enough information (the right amount/ more than enough) was provided on all aspects of the smart meter data initiative. Around one-third of both audiences would like more information on privacy and security protections. A similar proportion of Residential consumers would like more information on pricing models.
- Those that felt that the right amount of information was provided are considerably more likely to feel the initiative is important and to support sharing with all potential users. Those that felt that not enough information was provided are much less likely to feel the initiative is important and to feel comfortable having their smart meter data shared.



SUPPORT FOR PRICING MODELS

Support for Pricing Models - Information Provided

A detailed description of pricing models was provided before asking about support for each approach.

The IESO is also assessing potential pricing models that could be applied when sharing aggregated smart meter data with various other organizations.

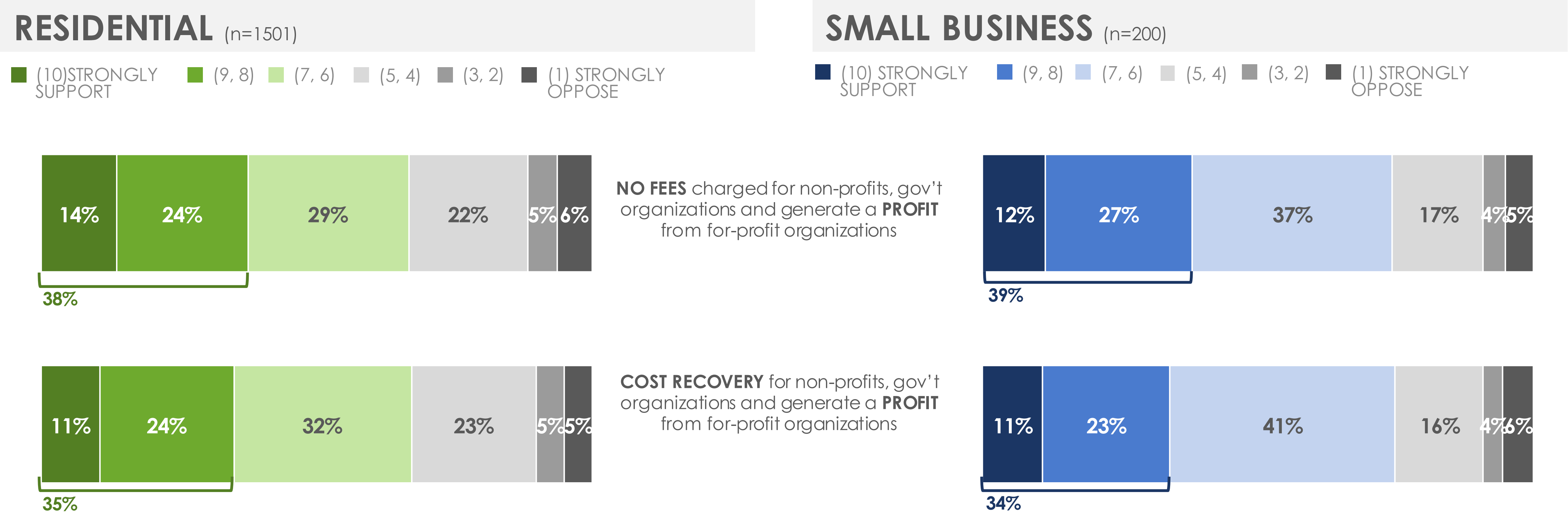
All pricing options would be subject to all applicable laws and regulations; privacy and security requirements other legal and ethical obligations of the IESO as an administrator of this project.

The IESO is a not-for-profit agency regulated by the Ontario Energy Board and has a mechanism to return all "excess" funds from any types of activities specific to their mandate back to consumers. While some of the pricing models described on the next screen would generate a "profit", all such references should be understood as overall gains for the electricity consumers. While such gains may not be material enough to actually reduce your electricity bills, they could help reduce some of the overall costs of the smart meter central data repository. Moreover, by enabling better data-driven decisions, the various requesting organizations could generate significant benefits to consumers.

Pricing Options	What does this mean for you as a consumer
1. **NO FEES CHARGED** for all data requestors, regardless of organization type	Consumers pay through the existing Smart Metering Charge that is already applied on each customer bill (currently at 57cents/meter/month).
2. **FULL COST RECOVERY**: all requestors get the data at COST	No impact for consumers as all costs will be recovered from the data requestors.
3. **NO FEES** charged to non-profits, government organizations and generate a **PROFIT** from For-Profit Organizations	Organizations that could be making a profit from using the data are paying for it at a higher rate than simply cost recovery, which in turn may benefit consumers in the long term.
4. **COST RECOVERY** charge to non-profits, government organizations and generate a **PROFIT** from For-Profit Organizations	All costs will be recovered plus, organizations that could be making a profit from using the data will be paying for it at a higher rate than simply cost recovery, which in turn t may benefit consumers in the long term.
5. Generate **PROFIT** from all data requestors, regardless of organization type	Ensures that all organizations , regardless of their non-profit / for-profit status are being charged at a higher rate than simply cost recovery, which may benefit consumers in the long term.

Support for Pricing Models

- Of all 5 pricing models tested, a strong majority of Residential and Small Business consumers are at least somewhat supportiv e (rating of 6 or higher) of pricing models that would charge *no fees (i.e. costs are covered by the existing SME charge of 57 cents/meter/month)* or *only recover costs* from non-profits and that would generate a *profit* from for-profit organizations (models 3 and 4 on previous slide).



RESIDENTIAL (n=1501)

SMALL BUSINESS (n=200)

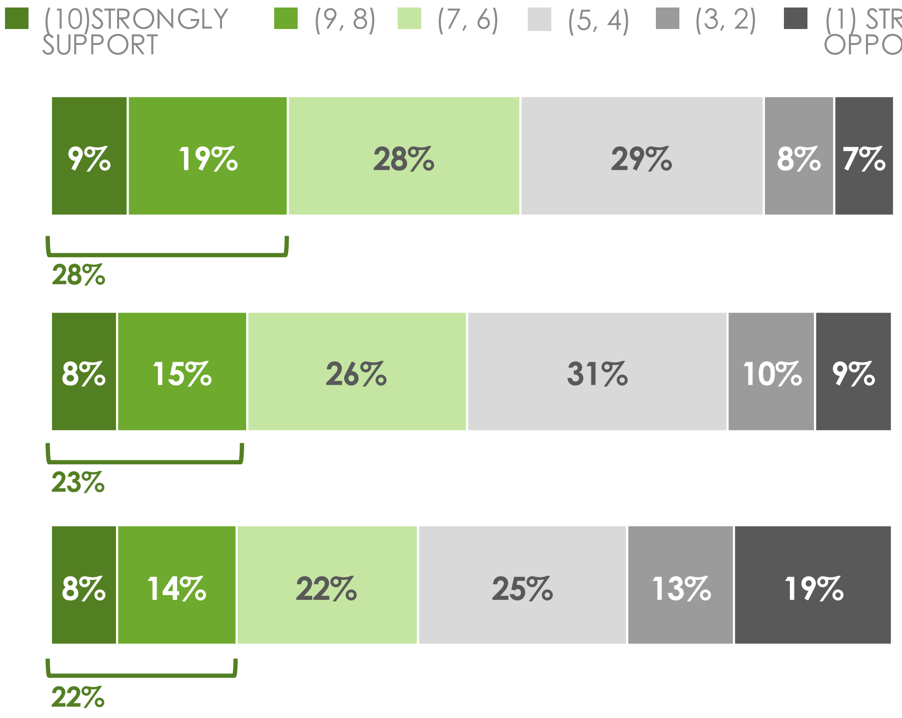
NO FEES charged for non-profits, gov't organizations and generate a **PROFIT** from for-profit organizations

COST RECOVERY for non-profits, gov't organizations and generate a **PROFIT** from for-profit organizations

Support for Pricing Models *(cont'd)*

- Support is lower for other pricing models presented including full cost recovery or profit generation for all requestors (models 1, 2 and 5 from slide 28).
- The no fees pricing model for **all requestors** had the least support from both residential and small businesses.
- The qualitative research highlighted that consumers felt that any pricing model that results in having ratepayers absorb costs would be the least acceptable. While support was highest for charging limited fees to non-profits this was contingent on the profit generated from for-profit requestors being enough to cover the costs that would otherwise be passed onto ratepayers.

RESIDENTIAL (n=1501)

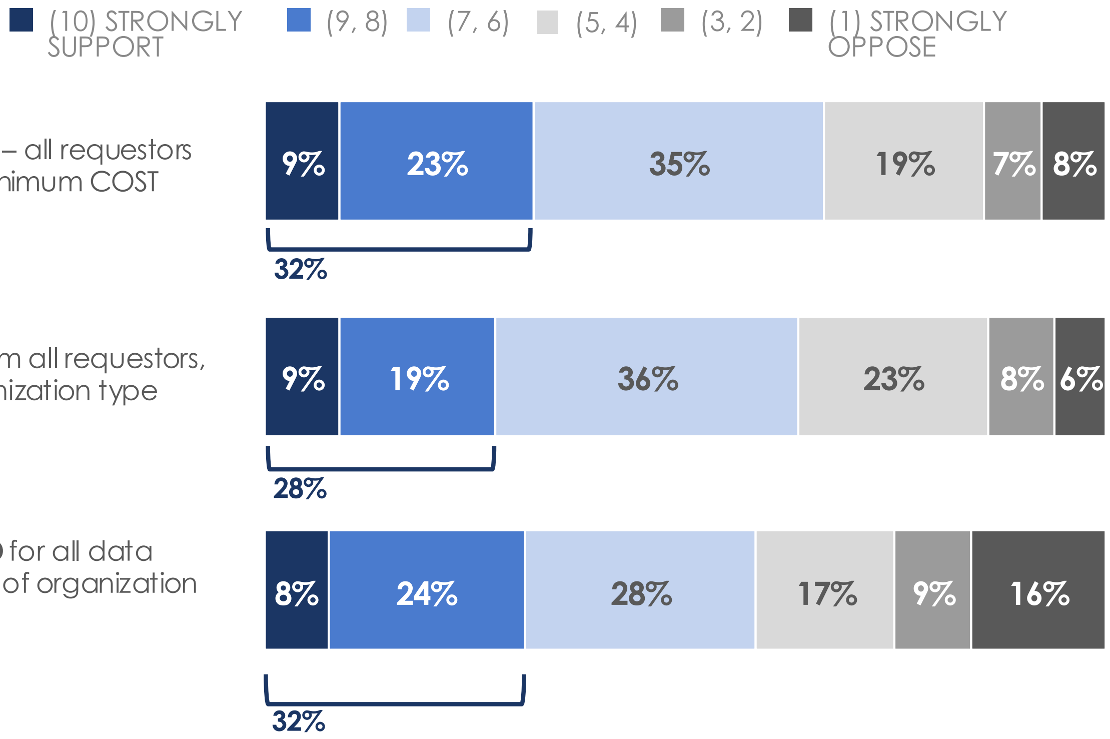


FULL COST RECOVERY – all requestors get the data at minimum COST

Generate a **PROFIT** from all requestors, regardless of organization type

NO FEES CHARGED for all data requestors, regardless of organization type

SMALL BUSINESS (n=200)



Qualitative Findings- Most were in favour of no fees or cost recovery for non-profits and making a profit from private companies. The no-fee model for all requestors was considered unacceptable by many.

Many were in favour of NO FEES *(i.e. costs are covered by the existing SME charge of 57 cents/meter/month)* option for non-profits and generating a PROFIT from for-profits. COST RECOVERY was also seen a favourable option for non-profits as many felt the cost of providing data to these organizations should not fall on them as the ratepayer. And, were heavily in favour of making a profit from those organizations who in turn would make money from the data.

Most participants think the “free for all” approach is unacceptable due to its negative impact on ratepayers. They were concerned that IESO will increase the electricity rates so that all organizations can access their data free of charge. In particular, there was general agreement that ratepayers should not be paying for private organizations using their data for creating more profit. A cost recovery only model for all requestors was more acceptable although few chose this as their preferred one.

I like that the for-profit organizations do have to pay for it. And then, I feel if someone is a not-for-profit, that there should not be a fee for them, for this information, if they’re working towards doing something better to help [everyone]. And then for me, as the final consumer, if it’s neutral to positive then that would be okay.

I know that coming from a university setting, that we often have a hard time getting funding for things, and accessing data is always a huge cost for any project. So if we can make that a little bit easier for universities and non-profits to access that data, then you get a little bit of profit margin from the for-profits, then that would be something that I’m for.

…..I don’t think the rate-payers should be paying anything for this data being used by other parties. So, option 4 with cost recovery for not-profits or government organizations, and this would be… there should be some profit margin for the profit organizations.

I just like, basically for the private sector, that the energy payers didn’t have to cover any costs, they were being fully reimbursed for that. And then for the for-profit, they are actually getting something back. Because if they’re going to agree to give all this energy usage, they should get something back. Otherwise, what’s the point for them to give it, their information, away?

APPENDIX

Key Differences By Subgroup

Information Provided to Respondents

KEY DIFFERENCES BY SUBGROUP

Key Differences By Type of Consumer

RESIDENTIAL

The most prominent differences in attitudes towards the smart meter initiative relate to education, income level and to a lesser extent age.

- Those in the high income and higher education level report stronger support for the initiative in comparison to those with middle to lower incomes and education levels.
- Those with lower incomes and education levels are more likely to rent (and have their utilities included) and have a weaker understanding of how smart meters work. The perceived benefits of sharing smart meter data are not as clearly understood and concerns related to data privacy and security heightened. Greater effort will be required explaining the value of the initiative, and addressing the main privacy and security concerns expressed in the research.
- Older Ontarians are more likely to have inherent concerns about the privacy and security of any type of data and have a harder time envisioning the potential benefits of sharing smart meter data. They are more likely to want more detailed information on the initiative to help satisfy their concerns, particularly related to the data security measures in place once shared with a third-party and provisions to protect against improper use.

Key Differences By Type of Business

SMALL BUSINESS

The most prominent differences in attitudes towards the smart meter initiative relate to the size of the organization.

- Organizations with 2-4 employees express weaker support for the initiative than those with 5 or more employees. They have an inherently higher degree of concern about the privacy and security of any type of data and seek reassurance about steps taken to protect smart meter data and the process to audit and verify use of the data once shared outside the IESO.

INFORMATION PROVIDED TO RESPONDENTS

Awareness of How Smart Meters Work- Information Provided

A detailed description of smart meters was provided before asking about awareness of how they work.

Smart meters are digital electricity meters that are able to measure how much electricity is used by each household and when it is used, every day.

Smart meters then send this hourly electricity consumption data over a wireless network to a secure central repository managed by the Independent Electricity System Operator – the IESO, to be verified before being used by your hydro company (such as Hydro One, or Alectra, etc.) to create your monthly electricity bill. The IESO is the provincial government's agency that ensures the reliability of the province's power system, balancing the demand and supply of electricity in our province ensuring there is enough power to keep the lights on for all consumer types, for the short and the long term. The IESO is regulated by the Ontario Energy Board – the OEB, an independent regulator who oversees Ontario's energy companies and the electricity and natural gas sectors.

There are currently over 60 hydro companies in Ontario, all using this centralized repository for smart meter data verification and billing, from over 5 million smart meters across the province.

Importance of extracting value from smart meter- Information Provided

A detailed description of smart meters was provided before asking about the importance of sharing aggregated electricity consumption data. Examples were also provided (see next slide).

With over 5 million smart meters in the province, the information accumulated in this central database over the past 10+ years can now be put to better use to support various organizations such as government, universities, municipalities or private industry with analysis and studies.

Sharing aggregated, electricity consumption data with a broad range of public and private organizations could help in the development of new policies, research, and other uses with benefits for the electricity system and ultimately the electricity consumer. Aggregated data refers to the total consumption of residences or businesses for a certain timeframe or geography.

All electricity consumption data provided would be irreversibly anonymized so that it is not traced to a household or an individual even when connected with other datasets. The most granular set would still be aggregated at the 6-digit postal code level (for example neighbourhood) and each group would have a minimum number of households as recommended by privacy experts working under the guidance of the Information and Privacy Commissioner of Ontario ("IPC"). A provincial office, independent of the government, that provides oversight of Ontario's access and privacy laws.

Importance of extracting value from smart meter- Information Provided

Some specific examples include:

Example 1: Electricity consumption data is one of the indicators of economic activity, the hourly data used for the graph shown below, is also used in combination with COVID 19 statistics, historic economic data and other public data to help University of Toronto, Carleton University and the University of Western Ontario understand the effect of the coronavirus infection on economic activity, and provide guidance on government policies to support Ontarians in greatest need.

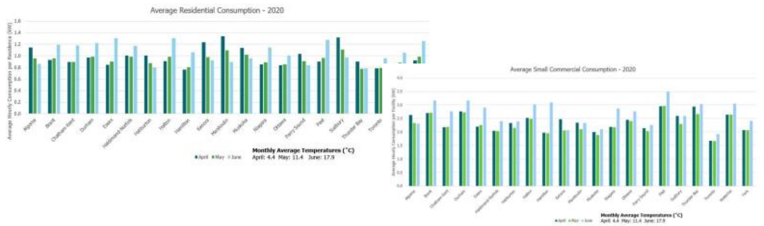
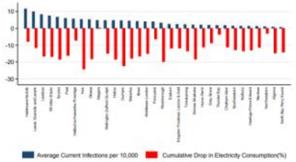
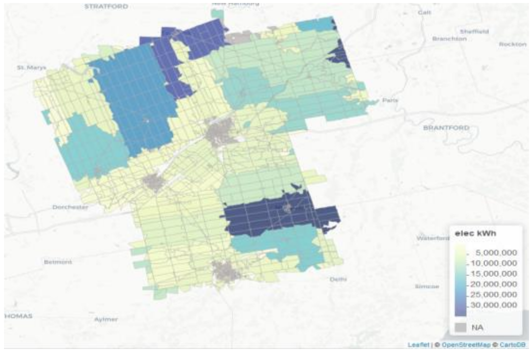


Figure 8: Average of Currently Infected Per 10,000 Population, April 07-15. Average Change in Electricity Consumption, Mar 15 - April 15



Example 2: Hourly Consumption Data aggregated by the 6-digit postal code is used to create this consumption map of Oxford County shown below. The colour of each shape represents the total consumption for all the houses and small businesses in that 6- digit postal code for a given period of time.

This data set is used by the County of Oxford to create a baseline, analyze change over time, and set objectives and actions to improve energy efficiency, and aid in the transition to 100% renewable energy. The same set of hourly data aggregated by traffic zone would allow a city planner to understand shifts in energy usage also aiding in community energy planning.



Comfort with Data Users- Information Provided

A detailed description of various potential users of electricity consumption data was provided before asking about comfort with different user groups.

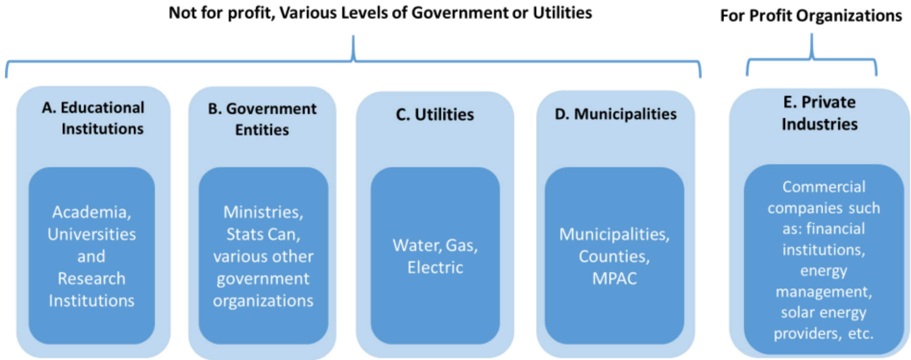
The Ontario Energy Board, has ordered the IESO to work on a plan to make the smart meter data available to a broad range of third party organizations, which could include public, not-for-profit (municipalities, universities, etc.) and commercial entities (banks, insurance companies, energy efficiency providers, retailers, etc.) for a broad range of purposes.

All data provided to third party organizations would be aggregated so that there is no tracing to a household or an individual even when connected with other datasets.

Each data request would be reviewed by an IESO committee before being approved to ensure the intended use is legal, fair and ethical.

All organizations wanting to have access to the data would be required to sign a contract, called a "Data Use Agreement" – this will ensure that they will have a legal obligation to protect the data on their side and only use it for the purpose that was originally requested for.

The IESO would also retain the right to audit these organizations and determine if there were any issues with how the data was stored, used and eventually destroyed.



Not for profit, Various Levels of Government or Utilities

For Profit Organizations

A. Educational Institutions: Academia, Universities and Research Institutions

B. Government Entities: Ministries, Stats Can, various other government organizations

C. Utilities: Water, Gas, Electric

D. Municipalities: Municipalities, Counties, MPAC

E. Private Industries: Commercial companies such as: financial institutions, energy management, solar energy providers, etc.

Privacy and Security- Information Provided

A detailed description of privacy and security policies was provided before asking about the perceived security and privacy of smart meter data.

Customer privacy and data security are foundational operating principles of the IESO's centralized smart meter data platform.

Measures are already in place to ensure that the electricity consumption data from smart meters that would be used for these various third-party applications is de-identified at the source: this means that any names, addresses or other personal identifiers are prevented from entering the database.

Areas where there may be only one home are not included in the data set. This makes all the data non-personal.

This smart meter central data repository is also subject to independent annual audits and special testing to ensure that the data remains protected at all time from external threats.

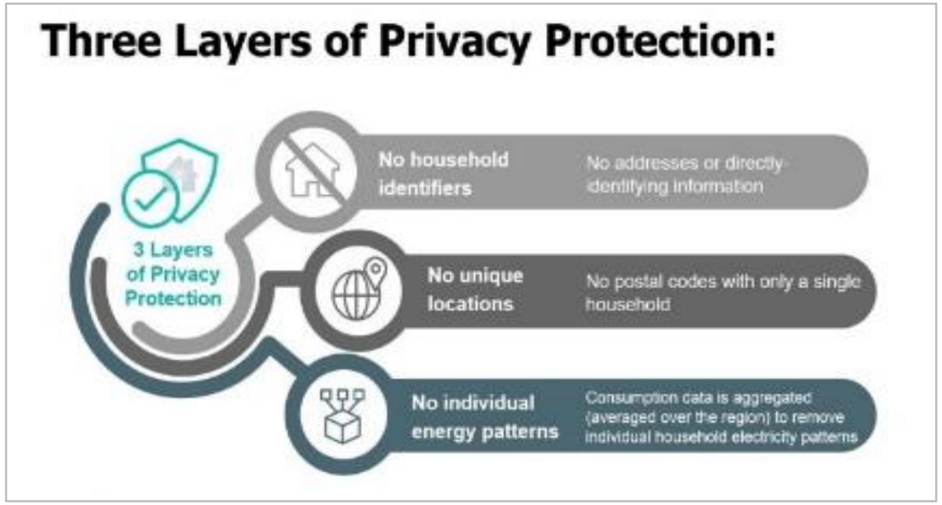
All organizations or individuals wanting to have access to the data would be required to sign a contract, called a "Data Use Agreement" which will impose upon the accessing party legal obligations to protect the data once in their custody or control and only use it for the purpose that was originally requested for.

The IESO will also retain the right to audit organizations that are using the data to ensure that the data is being properly used and well safeguarded once it leaves the IESO.

All these protections follow Ontario's Information and Privacy Commissioner ("IPC") guidelines and were developed by the IESO in collaboration with privacy experts.

Assessment of Privacy Visuals - Information Provided

Two visuals depicting the privacy and data security protocols for smart meter data were provided before assessing the effectiveness of the materials.



Three Layers of Privacy Protection:

3 Layers of Privacy Protection

No household identifiers

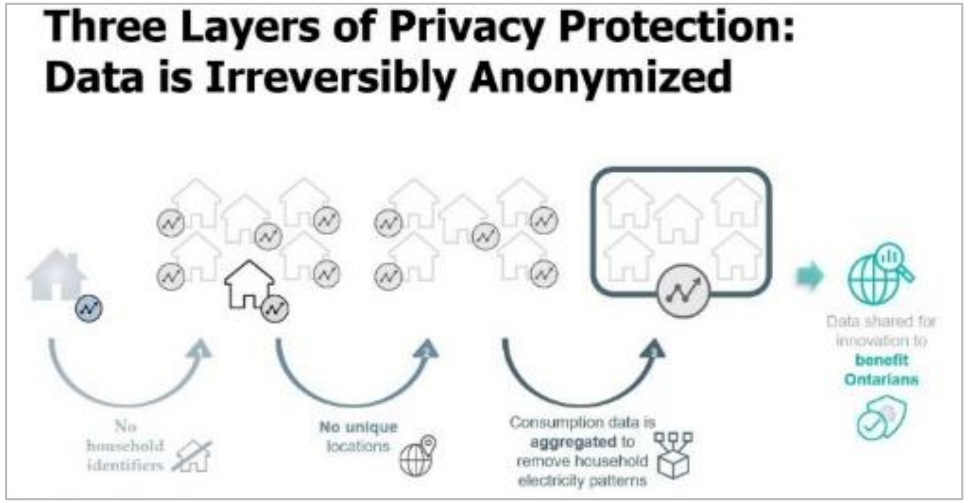
No addresses or directly-identifying information

No unique locations

No postal codes with only a single household

No individual energy patterns

Consumption data is aggregated (averaged over the region) to remove individual household electricity patterns



Three Layers of Privacy Protection: Data is Irreversibly Anonymized

No household identifiers

No unique locations

Consumption data is **aggregated** to remove household electricity patterns

Data shared for innovation to **benefit Ontarians**

PRIVACY ANALYTICS
an IQVIA company

An Independent Assessment of the IESO's Planned Privacy Strategy for Third-Party Data Access

30 August 2021

Document revision history

Date	Revision Notes
30 August 2021	V1: Initial report

TABLE OF CONTENTS

Executive summary

As Ontario's smart metering entity (SME), the IESO manages the Meter Data Management Repository (MDM/R), a central hub that contains hourly electricity consumption data used by electricity distributors to bill their customers. Part of the IESO's mandate as SME is to provide access to this data to distributors, retailers, the IESO and other persons, subject to the appropriate privacy protections.

In 2016, the Ontario Energy Board (OEB) directed the IESO to present a plan for third-party access to data in the MDM/R. After submissions to the OEB in 2016 and 2018, the IESO is submitting a new application in 2021. Under this plan, data will be made available to organizations that promote public good, including educational institutions, municipalities and government entities.

The IESO commissioned Privacy Analytics to conduct an independent privacy assessment and to ensure that recommendations previously made by Privacy Analytics are still valid for the IESO's third-party access plan. This document summarizes the results of this assessment and provides a succinct explanation of how the privacy of consumers will be protected under the IESO's new application. The assessment is based on information provided by the IESO verbally and in writing to Privacy Analytics. The report is intended for members of the IESO, the Ontario Energy Board (OEB), intervenors and interested members of the public.

Data plays an integral role in improving lives. The IESO's consumption data can yield societal, economic and environmental insights and innovation that provide value for Ontario residents in the form of better services, lower prices and reduced environmental impact of the electricity grid. According to an Ipsos study commissioned by the IESO and conducted in 2020, consumers generally support the sharing of smart meter data and recognize its benefits. They are particularly supportive when data is being shared with the public sector, since they believe that this can contribute to the greater good.

The IESO intends to offer consumption data from the MDM/R to public sector recipients in an aggregated form. Under the IESO's proposed plan, potential data recipients will be able to request aggregated electricity consumption data for a particular geographical area (measured as a set of postal codes) over a particular time frame in particular units of time (hourly, daily, weekly, monthly or seasonally).

When the IESO receives a specific request for aggregated data, it will assess whether the consumption data can be released as requested or needs to be further aggregated to adequately protect privacy. The aggregated data for each postal code area must contain a minimum number of premises. This minimum number is based on disclosure control best practices and is informed by the data release context, as covered in the body of the report. If there are some postal codes areas in the data that contain fewer than the recommended minimum number of premises, the data will be combined into larger postal code groups until this condition is met. To help protect the identity of single premises with high levels of electricity consumption, the IESO will also make sure that no one premise within any given postal code accounts for 75% or more of the total electricity consumption for that postal code area. Only the aggregated electricity consumption data across postal code areas will be shared. The IESO will also ensure that there is enough variability in electricity consumption data between consumers contributing to the average value in each postal code area. As an additional measure, the IESO may have data recipients sign a data use agreement that prohibits attempts to identify any premise in the data and that includes additional provisions for the security and control of the data.

Privacy Analytics' assessment has confirmed that if the IESO follows the process outlined in this report, any data shared with third-party recipients will be non-identifiable and the privacy of Ontario electricity consumers will be well protected. Data shared with third parties will be subject to three layers of privacy protection: household identifiers will be removed; no unique locations will be included; and no individual energy patterns will be provided. The IESO will also promote widespread benefits to be realized from the data while deterring misuses through enforceable data use agreements.

Section 1: Background

As Ontario's smart metering entity (SME), the IESO manages the Meter Data Management Repository (MDM/R), a central hub that contains hourly electricity consumption data used by electricity distributors to bill their customers. Part of the IESO's mandate as SME (hereafter simply IESO) is to provide access to this data to distributors, retailers, the IESO and other persons, subject to the appropriate privacy protections.[1]

In response to a request from the Ontario Energy Board (OEB), the IESO submitted a plan to the OEB in 2016 to provide third-party access to data in the MDM/R. Following extensive consultations, the IESO submitted a detailed data sharing monetization plan to the OEB in 2018. In 2019, the OEB approved public offerings of highly aggregated data and confirmed that the SME could share data with the OEB and IESO. The OEB, however, also asked the IESO to further develop their plan to respond to the concerns of intervenors.

In 2021, the IESO is submitting a new application to the OEB for third-party data access. Under this plan, data would be made available to organizations that promote public good, including educational institutions, municipalities and government entities. The IESO commissioned Privacy Analytics to conduct an assessment of privacy recommendations that Privacy Analytics had previously made. This document summarizes the results of this assessment and includes a succinct explanation of the privacy protections in place.

Section 2: Privacy protections in place

The IESO's consumption data can yield societal, economic and environmental insights and innovation that provide value for Ontario residents in the form of better services, lower prices and reduced environmental impact of the electricity grid. According to an Ipsos study commissioned by the IESO and conducted in 2020, consumers generally support the sharing of smart meter data and recognize its benefits.[2]

When the IESO shares electricity consumption data with third parties, the privacy of consumers must be protected. As part of this data sharing, the IESO plans to take measures to protect the privacy of Ontario consumers in accordance with existing standards and best practices. This section explains how the IESO intends to share consumption data with third party requestors in a way that is privacy protective. The privacy measures described below apply to all types of data product offerings to be included in the IESO's third-party access plan.

[1] Electricity Act, 1998, S.O. 1998, c. 15, Sched. A, section 53.8, https://www.ontario.ca/laws/statute/98e15#BK130

[2] Ipsos, IESO Smart Meter Data Research: Summary of Research Results (2021). For 7 in 10 residential (71%) and 8 in 10 small business (79%) consumers, it is at least somewhat important that smart meter data be shared. A sizable minority of 4 in 10 residential (39%) and 4 in 10 small business (40%) consumers believe that data sharing is "very important", while few (1 in 10) feel it is not important at all (10% residential and 9% small business).

Before the IESO receives a data request, the electricity consumption data of Ontario consumers is stored and protected in the MDM/R. This is meter-level data: it shows how much electricity individual residences and small businesses are consuming. At this point, several measures have already been taken to protect the privacy of consumers and to remove any personal identifiers in the data. Before sending data to the MDM/R, local distribution companies (LDCs) have removed the names and addresses of consumers. The LDCs have also removed any unique postal codes—those containing only one electricity consumer each—and have replaced them with a generic postal code. However, the data in this format is not yet ready to be provided to external recipients.

Before sharing with external participants, the IESO will apply further privacy protections. These protections include data aggregation: the IESO's plan is to offer the consumption data from the MDM/R to recipients in an aggregated form. Aggregated data is individual-level data that has been grouped together.

Under the IESO's proposed plan, potential data recipients will be able to request aggregated electricity consumption data for a particular geographical area (measured as a set of postal codes) over a particular time frame in particular units of time (hourly, daily, weekly, monthly or seasonally). The recipient will also request that the data be aggregated at a specific postal code level (3, 4, 5 or 6 characters). For example, a municipal government might request monthly consumption data for all postal codes within the municipality and that the total consumption data for each 5-character postal code be shown (e.g. MV5 3L).

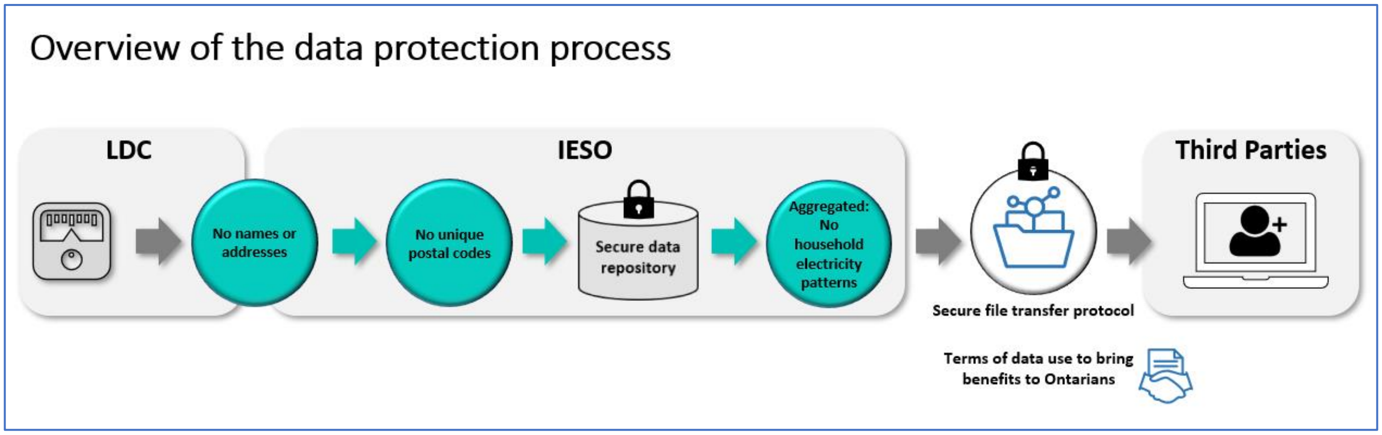

Overview of the data protection process
LDC
IESO
Third Parties
No names or addresses
No unique postal codes
Secure data repository
Aggregated: No household electricity patterns
Secure file transfer protocol
Terms of data use to bring benefits to Ontarians

Figure 1: The identifiability of electricity consumption data is gradually reduced on its path from local distribution company to third-party applicant.

When the IESO receives a specific request for aggregated data, it will assess the privacy implications of this request. More specifically, the IESO will determine whether consumption data can be released to the recipient in the form requested or whether the data needs to be further aggregated to adequately protect privacy.

To make this assessment, the IESO will aggregate the data to the postal code level requested by the recipient.

The IESO will then check how many consumers there are within each postal code area to ensure that each postal code area contains a minimum number of consumers. For example, if a municipality is requesting data aggregated by 5-character postal code, the IESO might check to ensure that the aggregated data for each postal code area in the data contains at least six consumers. The minimum number is based on informed recommendations and is influenced by the data release context. If the IESO has a strong contract in place with the data recipient, then the minimum number will be lower than if the data is being released publicly.

If some postal codes in the data contain fewer than the recommended minimum number of consumers, the data will need to be further generalized until this condition is met. This is done by combining the postal code data into fewer groups: if the recipient requested 5-character postal code data, for example, the IESO may be able to provide only data that is aggregated by 4-character postal code. The IESO then takes either the average or the total electricity consumption data across consumers within each postal code level. Only the average electricity consumption, the total electricity consumption and the number of premises within a postal code area may be shared. The IESO will also ensure that there is sufficient variability in electricity consumption data between consumers contributing to the average value in each postal code area. This additional protection ensures that the average value is not representative of all consumers within the group.

As recommended by Privacy Analytics, the IESO will also apply a dominance rule of 75% to the data. If a large majority of the electricity consumption within a postal code area is coming from a single premise, this consumer is more identifiable. The greater the percentage that can be attributed to a single premise, the closer that the electricity consumption for that premise is to the total electricity consumption of the whole postal code area and the more identifiable the energy consumption of that premise becomes. To avoid this situation, the IESO will make sure that no one premise within any given postal code accounts for 75% or more of the total electricity consumption for that postal code area. If there are premises that meet this condition, the aggregated data will be further generalized by postal code before it is released.

The data is now irreversibly transformed and can be shared with recipients. As an additional measure, the IESO may have data recipients sign a data use agreement before they receive the data. The data use agreement will:

- Specify and limit the ways in which recipients can use the data
- Limit the people within the recipient organization who can access the data
- Prohibit attempts to identify anyone in the data or link the data to any other data set
- Require the recipient to respond to IESO inquiries about how the data is being used and maintained

To transfer the aggregated data, the IESO will provide access to the data via a secure file transfer to an authorized technical contact from the recipient organization.

Section 3: Privacy Analytics assessment

In June 2021, the IESO engaged Privacy Analytics to assess the privacy protections planned for the new third-party data access application to be proposed to the OEB. This section contains a brief overview of the details of this assessment.

3.1 What we did

3.1.1 Objective

The objective of our assessment was to perform a complete and holistic examination of the privacy protections in place as part of the IESO's revised third-party data access plan submission.

3.1.2 Scope

Privacy Analytics has conducted a number of privacy risk assessments for the IESO since 2015 and has provided multiple privacy recommendations in these assessments. The IESO implemented the prior recommendations, embedding privacy into the end-to-end process. The assessment, conducted from June 2021 to August 2021, built on these prior assessments.

3.1.3 Method

As part of this assessment, we

- Reviewed our analysis from previous risk assessments to validate prior assumptions with the IESO
- Performed a scan of the industry landscape for any changes warranting consideration
- Reviewed the data offerings being contemplated by the IESO as part of its revised plan

Our findings are based on the information we gathered through verbal consultation with the IESO and IESO documents reviewed during our assessment. Our conclusions assume the accuracy and completeness of information provided to us by the IESO.

3.2 What we recommend

During the review of the IESO's revised third-party data access plan, the IESO confirmed that the following measures will be followed as part of the plan:

- Data shared with recipients will be aggregated and no individual-level data will be shared.

- Household-level indicators, even in pseudonymized form, will not be shared with recipients.
- To protect the identities of consumers, any data shared with recipients will be aggregated in groups of at least
  - 6 premises if there is a enforceable data use agreement in place with the data recipient
  - 9 premises if there is no contract in place but there are clear terms of use with a trusted recipient
  - 15 premises if the data is to be released publicly (further aggregation may be warranted to prevent geographically targeted advertising)
  - Alternative group sizes are possible with alternative privacy protections (e.g. highly controlled environments might warrant a group size of 3)
- Only the average or total energy consumption data across postal code areas may be shared, along with the number of premises in each postal code area.
- There is sufficient variability in electricity consumption data between consumers contributing to the average value in each postal code area.
- A dominance rule of 75% will be followed.
- The year that occupants move in and out of premises will never be shared (the day and month are not collected).

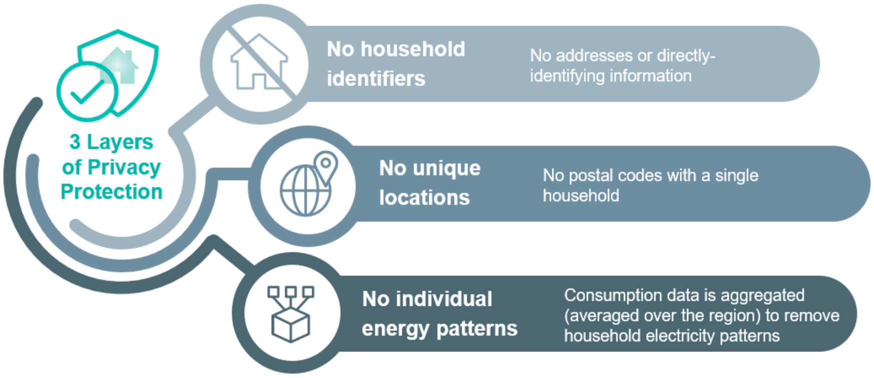
In addition to implementing the process as defined, we recommend that the IESO periodically review the privacy protections in place over time to ensure that shared data continues to yield the intended benefits and that any process changes remain privacy-preserving.

3.3 Conclusion

Our assessment has confirmed that if the IESO follows the process outlined in this report, any data shared with third-party recipients will be non-identifiable and the privacy of Ontario electricity consumers will be well protected.

As discussed above, data shared by the IESO will benefit from three levels of protection.

Three Layers of Privacy Protection.


3 Layers of Privacy Protection
No household identifiers
No addresses or directly-identifying information
No unique locations
No postal codes with a single household
No individual energy patterns
Consumption data is aggregated (averaged over the region) to remove household electricity patterns

Because (a) the aggregated data for each postal code area contains an appropriate number of premises and because (b) the aggregated electricity consumption data across postal code areas will be shared with sufficient variability to ensure the aggregated value is not representative of all consumers within the group and because (c) no one consumer in the group can contribute 75% or more of the consumption, the electricity consumption information cannot reasonably be used to identify a person or household. With all of these measures applied, the data is not identifiable and no personal information is shared.

Section 4: Results

The IESO's proposed third-party access data initiative was launched to benefit Ontarians. Sharing data with a range of public sector organizations could help in the development of new research and policies that improve Ontario's electricity system and yield other advantages for our society.

Our assessment of the IESO's plan to protect consumer privacy has concluded that the personal information of Ontario electricity consumers will be protected by a variety of measures: the data will be aggregated and will contain no household identifiers, no unique locations and no individual energy patterns. Taken in combination, such measures will ensure that the IESO shares no personal information.

Appendix A: Privacy protective measures

The purpose of this appendix is to provide more detailed explanation and justification of the privacy protective measures presented in the main report.

A.1 Reducing identifiability: An overview

Privacy protective measures must be applied to MDM/R data before releasing data to third-party applicants to ensure that no personal information about Ontario consumers is disclosed. In Ontario, personal information is defined as "recorded information about an identifiable individual."[3] Personal information includes items that are directly identifying, such a person's name or address. These direct identifiers are unique to an individual and can be used to identify an individual. If these identifiers are in the data, then one can learn something specific about the identified individual or household. For example, seeing someone's address in the data can reveal that household's electricity usage.

To protect the privacy of individuals in the data, direct identifiers can either be deleted or replaced. This protection does not negatively impact the usefulness of data for analytics since direct identifiers do not usually provide any useful information to researchers. All direct identifiers will be removed from the data before being stored in the MDM/R.

The removal of direct identifiers is not sufficient on its own to protect privacy. Personal information also includes indirect identifiers, which are instances of personal information that, used alone or in combination with other information, can uniquely identify an individual in the data. Indirect identifiers associated with premises in the MDM/R data include postal code, distributor rate class, commodity rate class and year of occupancy change. When combined with other information, an indirect identifier can potentially be used to reverse-engineer an individual's identity. For example, if a premise in the data set has a six-character postal code and there are only a few other premises within that postal code, it may be possible identify that premise by looking at its consumption patterns (e.g. identifying when an acquaintance is on vacation). The postal code information significantly narrows down the range of possibilities. Unlike direct identifiers, indirect identifiers can be a valuable source of insight for researchers and should be preserved as much as privacy considerations allow.

Multiple privacy protections are applied to the indirect identifiers and the consumption data in the MDM/R data prior to third-party access.

[3] Freedom of Information and Protection of Privacy Act, RSO 1990, c F.31, <https://canlii.ca/t/552kq> retrieved on 2021-08-12

A.2 Privacy protective measure #1: No uniqueness

In addition to names and addresses, LDCs remove any unique postal codes in the data and replace them with a generic postal code before sending data to the MDM/R. A unique postal code contains only one premise. To protect privacy, unique postal codes should be removed because any premise in a unique postal code is identifiable.

A.3 Privacy protective measure #2: Data aggregation

A.3.1 Protecting privacy in individual-level data with clusters

A database with individual-level data contains a separate record or row for every individual in the database, whereas aggregated data combines more than one individual in each record. As stated already, the IESO intends to share only aggregated data with third-party recipients and will not share individual-level data. However, to understand the principles of data aggregation, we first outline how individuals are typically protected in individual-level data sets.

To protect privacy in individual-level data sets, a measure of identifiability is generated for each individual in the set. This measure is generated by figuring out how much each individual looks like the other individuals in the data set across combinations of indirect identifiers. The more a participant is similar to other individuals, the lower the possibility that they can be identified since they belong to a group of similarly looking individuals (a “cluster”).

This is best illustrated with an example. To avoid confusing the IESO’s proposed aggregated data releases with individual-level data, let’s take an example that is not related to electricity consumption. A hospital keeps a database of hospital admittances. On September 9, 2020, Paul Smith was admitted to the hospital because of a broken leg. The database now contains a record for Paul Smith’s admittance. The record does not include Paul’s name, but it does include a unique id number, the date of admittance and the reason for the admittance (a broken leg). If Paul is the only person admitted to the hospital that day for a broken leg, the combination of the admittance date and the reason for admittance makes Paul’s record unique in the database. This increases the chance that Paul can be identified: if someone viewing the database knows that Paul was admitted to this hospital on September 9, 2020, for a broken leg, and if they see that Paul is the only person in the database admitted on that day for a broken leg, they can infer that this record is indeed that of Paul Smith.

But suppose that Paul Smith is not unique in the database and that there are five other patients who were admitted to that hospital that day for a broken leg. In this case, Paul Smith is one of 6 patients in the database who all have the same characteristics (i.e. set of indirectly identifying information) associated with them. If someone tries to guess which one of them is Paul, they will only have a 1 in 6 chance of guessing correctly (and even then, they probably will not be able to confirm whether their random guess was correct or not). Paul’s identity is protected because he is part of a cluster of 6 patients who appear to be similar based on what is known about them.

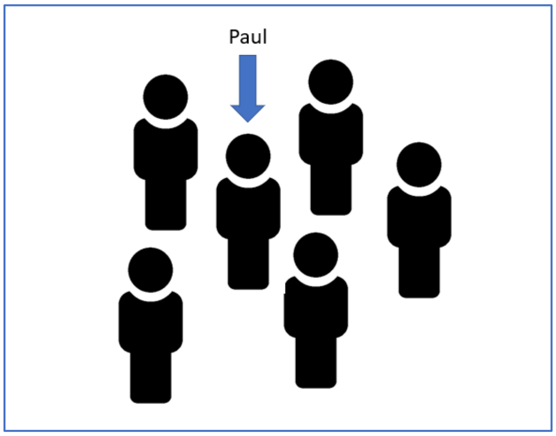


Figure 2: Paul's identity is protected because he "looks similar" to other patients in the data.

This is a fundamental concept in data privacy protection: the more each individual in the data set is similar to other individuals, the less identifiable each individual is. The level of privacy in a data set is determined primarily by the cluster size for each individual: the greater the cluster size, the stronger the privacy protection.

To increase the cluster size in a data set, information can be generalized. For example, if Paul's cluster size is not big enough, his reason for admittance and those of other patients could be generalized from "broken leg" to "broken bone". This could increase Paul's cluster size, since his record in the data set will be now similar to anyone else admitted to that hospital who broke a bone, and not just to those who broke a leg.

A.3.2 Aggregating data to protect privacy

When the IESO aggregates data in a privacy protective way, the process is similar to the one involved when reducing the identifiability of individual-level data. This process starts with the individual-level data before it is aggregated. The first step is to determine the cluster size of each premise in the data set and whether it meets the minimum cluster size. Then, wherever necessary, the data is generalized to ensure that the cluster for each premise in the data meets the minimum size. Once this is done, the data is ready to be aggregated by cluster. Each aggregated group of data is made up of a cluster of premises that have the same indirect identifiers. The difference between the individual level data and the aggregated data is that the latter has an extra element of privacy protection. When someone looks at the individual-level data, they can still see the exact electricity consumption for each premise, but with aggregated data one only sees either the total or average electricity consumption for the aggregated group.

When data is aggregated, the minimum group size of the aggregated data should be informed by disclosure control best practices and the context for data access (e.g. a controlled data release versus an uncontrolled data release). If data is released publicly, it can be viewed by anyone and the minimum group size needs to be higher than in other contexts. In contrast, if the data is released only to a trusted organization that has signed a data use agreement, the minimum size of each aggregated group can be lower. This in turn allows for greater insight and utility to be preserved in the shared data, supporting a wider number of benefits.

As part of its current plan, the IESO will share data with recipients that have signed a strong data use agreement. In this context, Privacy Analytics has recommended that each aggregated data group in the shared data contain at least 6 premises. Privacy Analytics has previously provided alternate recommendations for different release contexts, and any of these would be acceptable assuming the minimum cluster size is informed by the context.

Once the data is aggregated, no individual electricity patterns are visible in the data. These are averaged across all households in the applicable cluster.

A.4 Privacy protective measure #3: The dominance rule

Although aggregation by minimum group size is the primary privacy protective measure that the IESO will employ, Privacy Analytics has also recommended a couple of additional measures to reinforce privacy protection. The first of these is a dominance rule: no one premise within any aggregated group can account for 75% or more of the total electricity consumption for that group.

This rule is in place to protect the identity of any premise that consumes a disproportionate amount of electricity relative to the other premises in their group. Assume that a very large house exists in postal code area with five other much smaller residences and that these six premises form an aggregated group in the data. With six premises, the group may meet the minimum group size requirement for a particular data release. But if the large house consumes an inordinate amount of the electricity for that group and if one has reason to assume that most of the electricity consumption is coming from that house, it becomes easier to look at the total electricity consumption for the group and to estimate the amount of electricity that the house is using. To avoid situations like this one, Privacy Analytics has recommended that no one premise within any given postal code account for 75% or more of the total electricity consumption for that postal code area. If there are premises that violate the dominance rule, the aggregated data will be further aggregated before it is released.

A.5 Privacy Measure #4: The minimum variance rule

The minimum variance rule—the second of the two additional measures—addresses the situation in which there is very little variation in the electricity consumption of the premises within an aggregated group. If the electricity consumption amounts in the group are very similar to each other and if someone has reason to believe this to be true, it is easier for that person to estimate the electricity consumption of any one premise within the group, since the electricity consumption of most or all of the premises in the group will be close to the group average.

To address this, Privacy Analytics has recommended that the coefficient of variation of electricity consumption amounts within any aggregated group be at least 0.1. Variance is a measurement of the spread between numbers in a data set. To calculate the variance for an aggregated group, the mean electricity consumption for that group must first be calculated. Then the mean is subtracted from each value in the group. The resulting numbers are added together and divided by the number of premises to produce the variance. When the variance of an aggregated group in the shared data set is at least 0.1, the average electricity consumption value for the group is not representative of the electricity consumption of all the premises in the group.

A.6 Summary

When the measures discussed above are applied to the IESO data, it is fully de-identified. Since the data has been aggregated into groups of an appropriate minimum size, individual-level data is no longer accessible to the recipient. Moreover, measures have been taken to guarantee (a) that no premise in an aggregated group can be identified in the data because of its high electricity consumption, and (b) that levels of consumption within an aggregated group have sufficient variation. Taken together, these measures ensure that the privacy of consumers in the data is protected.

Appendix B: Further reading

These sources provide further details on disclosure control best practices and the methodology used by Privacy Analytics in its assessment.

Aggarwal, Gagan, Rina Panigrahy, Tomás Feder, Dilys Thomas, Krishnaram Kenthapadi, Samir Khuller, and An Zhu. 2010. “Achieving Anonymity via Clustering.” *ACM Transactions on Algorithms* 6 (3): 49:1-49:19. https://doi.org/10.1145/1798596.1798602.

Arbuckle, L., E. Moher, S. J. Bartlett, S. Ahmed, and K. El Emam. 2017. “Montreal Accord on Patient-Reported Outcomes Use Series – Paper 9: Anonymization and Ethics Considerations for Capturing and Sharing Patient Reported Outcomes (PRO).” *Journal of Clinical Epidemiology* 89 (April): 168–72. https://doi.org/10.1016/j.jclinepi.2017.04.016.

Arbuckle, Luk, Michelle Chibba, Khaled El Emam, and Ann Cavoukian. 2019. “Chapter 13 Privacy, Confidentiality, Security and Ethics.” In *Population Health Informatics: Driving Evidence Based Solutions into Practice*, edited by Ashish Joshi, Lorna Thorpe, and Levi Waldron, 335–60. Jones & Bartlett Learning.

Arbuckle, Luk, and Khaled El Emam. 2020. *Building an Anonymization Pipeline: Creating Safe Data*. Sebastopol, CA: O’Reilly Media.

Arbuckle, Luk, and Muhammad Oneeb Rehman Mian. 2020. “Engineering Risk-Based Anonymisation Solutions for Complex Data Environments.” *Journal of Data Protection & Privacy* 3 (3): 334–43.

Arbuckle, Luk, and Felix Ritchie. 2019. “The Five Safes of Risk-Based Anonymization.” *IEEE Security & Privacy* 17 (5): 84–89.

Article 29 Data Protection Working Party. 2014. “Opinion 05/2014 on Anonymisation Techniques.” Opinion WP216. Brussels, Belgium. https://bit.ly/3g7I30n.

Bohli, Jens-Matthias, Christoph Sorge, and Osman Ugus. 2010. “A Privacy Model for Smart Metering.” In *2010 IEEE International Conference on Communications Workshops*, 1–5. https://doi.org/10.1109/ICCW.2010.5503916.

Buchmann, Erik, Klemens Böhm, Thorben Burghardt, and Stephan Kessler. 2013. “Re-Identification of Smart Meter Data.” *Personal and Ubiquitous Computing* 17 (4): 653–62. https://doi.org/10.1007/s00779-012-0513-6.

Christine M O’Keefe, Stephanie Otorepec, Mark Elliot, Elaine Mackey, and Kieron O’Hara. 2017. “De-Identification Decision-Making Framework.” CSIRO Reports EP173122 and EP175702. Office of the Australian Information Commissioner. https://bit.ly/3smEo3I.

Efthymiou, Costas, and Georgios Kalogridis. 2010. “Smart Grid Privacy via Anonymization of Smart Metering Data.” In *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 238–43. IEEE. https://bit.ly/3CUWqia.

El Emam, Khaled. 2013a. *Guide to the De-Identification of Personal Health Information*. Boca Raton, FL: CRC Press (Auerbach).

———, ed. 2013b. *Risky Business: Sharing Health Data While Protecting Privacy*. Trafford.

El Emam, Khaled, and Luk Arbuckle. 2013. *Anonymizing Health Data: Case Studies and Methods to Get You Started*. Sebastopol, CA: O'Reilly Media.

El Emam, Khaled, Luk Arbuckle, Gunes Koru, Benjamin Eze, Lisa Gaudette, Emilio Neri, Sean Rose, Jeremy Howard, and Jonathan Gluck. 2012. "De-Identification Methods for Open Health Data: The Case of the Heritage Health Prize Claims Dataset." *Journal of Medical Internet Research* 14 (1): e33. https://doi.org/10.2196/jmir.2001.

El Emam, Khaled, Fida K. Dankar, Régis Vaillancourt, Tyson Roffey, and Mark Lysyk. 2009. "Evaluating the Risk of Re-Identification of Patients from Hospital Prescription Records." *Canadian Journal of Hospital Pharmacy* 62 (4): 307–19.

El Emam, Khaled, Fida Kamal Dankar, Romeo Issa, Elizabeth Jonker, Daniel Amyot, Elise Cogo, Jean-Pierre Corriveau, et al. 2009. "A Globally Optimal K-Anonymity Method for the De-Identification of Health Data." *Journal of the American Medical Informatics Association: JAMIA* 16 (5): 670–82. https://doi.org/10.1197/jamia.M3144.

El Emam, Khaled, Elizabeth Jonker, Luk Arbuckle, and Bradley Malin. 2011. "A Systematic Review of Re-Identification Attacks on Health Data." *PLoS ONE* 6 (12). http://bit.ly/2hYogS0.

El Emam, Khaled, David Paton, Fida Dankar, and Gunes Koru. 2011. "De-Identifying a Public Use Microdata File from the Canadian National Discharge Abstract Database." *BMC Medical Informatics and Decision Making* 11 (53).

Elliot, Mark, Elaine Mackey, and Kieron O'Hara. 2020. "The Anonymisation Decision-Making Framework 2nd Edition: European Practitioners' Guide." Manchester, UK: UKAN Publications. https://eprints.soton.ac.uk/445373/.

Future of Privacy Forum. 2017. "A Visual Guide to Practical Data De-Identification." https://bit.ly/3g5PCoe.

HITRUST Alliance. 2015. "HITRUST De-Identification Framework." Frisco, TX: HITRUST.

Information and Privacy Commissioner of Ontario. 2016. "De-Identification Guidelines for Structured Data." https://bit.ly/3xTIEsB.

Information Commissioner's Office. 2012. "Anonymisation: Managing Data Protection Risk Code of Practice." Information Commissioner's Office. https://ico.org.uk/media/1061/anonymisation-code.pdf.

Institute of Medicine. 2015. "Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk." Washington, D.C.

ISO/IEC. 2018. "Privacy Enhancing Data De-Identification Terminology and Classification of Techniques." International Standard 20889. International Organization for Standardization.

Iyengar, Vijay S. 2002. "Transforming Data to Satisfy Privacy Constraints." In *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 279–88. KDD '02. New York, NY, USA: ACM. https://doi.org/10.1145/775047.775089.

Jelasity, Márk, and Kenneth P. Birman. 2014. "Distributional Differential Privacy for Large-Scale Smart Metering." In *Proceedings of the 2nd ACM Workshop on Information Hiding and Multimedia Security*, 141–46. ACM Press. https://doi.org/10.1145/2600918.2600919.

Machanavajjhala, A., J. Gehrke, D. Kifer, and M. Venkitasubramaniam. 2006. "L-Diversity: Privacy beyond k-Anonymity." In *22nd International Conference on Data Engineering (ICDE'06)*, 24–24. https://doi.org/10.1109/ICDE.2006.1.

Martinez, Carson, and Elizabeth Jonker. 2020. “A Practical Path Toward Genetic Privacy in the United States.” https://bit.ly/2XwJr6l.

National Academies of Sciences, Engineering, Medicine. 2015. *Concepts and Methods for De-Identifying Clinical Trial Data. Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk*. National Academies Press (US). https://www.ncbi.nlm.nih.gov/books/NBK285994/.

National Institute of Standards and Technology. 2012. “Guide for Conducting Risk Assessments.” Special Publication SP-800-30 Rev 1. Gaithersburg, MD: NIST. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=912091.

Office for Civil Rights. 2020. “Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.” Washington, DC: Department of Health and Human Services. https://bit.ly/3yUAMIB.

PhUSE De-Identification Working Group. 2015. “De-Identification Standards for CDISC SDTM 3.2.”

PPC (Japan). 2017. “Report by the Personal Information Protection Commission Secretariat: Anonymously Processed Information. Towards Balanced Promotion of Personal Data Utilization and Consumer Trust.” https://bit.ly/3mc8zcL.

Samarati, Pierangela. 2001. “Protecting Respondents’ Identities in Microdata Release.” *IEEE Transactions on Knowledge and Data Engineering* 13 (6): 1010–27.

Simson Garfinkel. 2015. “De-Identification of Personal Information (NISTIR 8053).” Gaithersburg, MD: National Institute of Standards and Technology.

Singapore Personal Data Protection Commission. 2018. “Guide to Basic Data Anonymisation Techniques.” https://bit.ly/3g9upK5.

Skinner, C. J. 1992. “On Identification Disclosure and Prediction Disclosure for Microdata.” *Statistica Neerlandica* 46 (1): 21–32. https://doi.org/10.1111/j.1467-9574.1992.tb01324.x.

Sweeney, Latanya. 2002. “K-Anonymity: A Model for Protecting Privacy.” *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems* 10 (5): 557–70.

Willenborg, Leon, and Ton de Wall. 2001. *Elements of Statistical Disclosure Control*. 1st ed. Lecture Notes in Statistics 155. Springer-Verlag New York. DOI:10.1007/978-1-4613-0121-9.

SUMMARY OF DATA REQUESTS RECEIVED BY THE SME TO DATE (CURRENT AS OF OCTOBER 2021)

Below is the list of all the data requests that have been submitted to the SME to date, including from those organizations with an authorized use cases for data requests that have been fulfilled by the Smart Metering Entity to date. The information is divided into four tables below:

- **Table 1** includes requests that were part of the planning process for the application submitted in 2018. The objective of undertaking those pilot test cases via the Data Strategy Advisory Council ("**DSAC**") in 2018 was to learn and validate the broader model that would become operational: test the designed processes, policies and procedures, and to establish the value proposition of the data request based on real-life examples, handled in a controlled, public and transparent environment.
- **Table 2** includes the cases that have been fulfilled with public level aggregations; OEB in Order and Decision EB 2018-0316 enabled and mandated the IESO to create high level aggregations that could be shared publicly.
- **Table 3** includes those cases fulfilled to support OEB and IESO processes or projects.
- **Table 4** includes expressions of interest from different parties, these requests were not fulfilled due to various reasons: the absence of a mandate enabling us to move forward, projects on hold or cancelled.

In all cases, privacy and security rules have been applied, as provided by the privacy expert (Privacy Analytics Inc) in accordance with the IPC Guidelines. All the organizations listed in tables 1 and 2 have signed a Data Use Agreement "**DUA**") with the IESO.

Table 1. Pilot Test Cases (completed in 2018)

Requesting Organization	Authorized Use & Comments
Oxford County	To create an accurate electricity baseline for improving energy efficiency (EE), and aiding in the transition to renewable energy. Data set used to support the measurements related to the County's target to use 100% Renewable Energy by 2050.
IESO	To improve short- & long-term demand forecasting through better system modelling. As of 2019 given OEB Order EB 2018-0316 IESO is able to receive data updates from the SME. It is receiving data that have helped improved the forecasting models.
City of Guelph	To identify priority areas for energy efficiency (EE) / distributed generation (DG) programs via energy mapping; support GHG targets with an emissions inventory.
Enbridge Gas	To establish load profiles to help predict the GHG impact of the power system and support emission reduction.
OEB	To better understand small commercial energy use patterns and to make more informed pricing decisions.
Ministry of Economic Development, Job Creation and Trade	To assess net migration trends in regions, as well as overall economic activity. This is part of a broader initiative, leveraging non-traditional data sources as proxies for economic activity to support evidence-based decision making, strategy formulation, and performance evaluation.

*The data requests consisted of de-identified consumption data aggregated at the Postal Code level by Distributor Rate Class (i.e. Customer Type), Commodity Rate Class (i.e. Price Plan) for varying periods of time and geographies depending on the use case.

1 **Table 2. Public Level Data Use Cases**

Requesting Organization	Authorized Use & Comments
University of Toronto	Use Case 1: The data would be used to understand the correlation between the aggregated consumption data with the diffusion infection rate of COVID-19 and the social distancing measures. Use Case 2: To develop and estimate an econometric model to evaluate the economic and public health effects of the diffusion of COVID-19 in Ontario. The results will be published as public policy briefs and papers.
University of Western Ontario	The data would be used to examine the current pricing mechanisms in place in Ontario, for different classes of consumers and propose alternative pricing arrangements that promote the efficient and equitable recovery of electricity costs. The results will appear in the form of an Ivey blog or Policy Brief. More advanced research may appear in a refereed energy journal.
Carleton University	The data will be used to gain insights on additional effect of COVID-19 and look at heterogeneity across several dimensions. The researchers aim to produce an academic article and publish in a peer-reviewed journal.
Ministry of Energy, Northern Development and Mines	Use Case 1: Highly Aggregated statistics on electricity consumption by consumer classes (residential and small general service <50kW) and time of use buckets (on peak, mid peak and off peak) - to inform pricing changes under the COVID Emergency Orders and future pricing policy direction. Use Case 2: Public Data what impacts the COVID-19 pandemic has had on electricity consumption (residential and small

	business), controlling for seasonality, with regional and demographic analyses.
Queen’s University	The data would be used to understand the historical patterns of electricity consumption in Ontario to later investigate how electricity consumers would change their consumption patterns in response to electricity tariff designs. The results of the research may be published in academic journals in the field of economics.

*The public data set consists of consumption data aggregated at the Census Division level by Distributor Rate Class (i.e. Customer Type) and Commodity Rate Class (i.e. Price Plan) from 2018 to 2020.

Table 3. OEB and IESO Use Cases

Requesting Organization	Authorized Use & Comments
OEB	Monthly report for analysis of consumers by distribution rate class and commodity rate class (TOU and TIERED). The OEB is monitoring number of customers on TOU and TIERED and total consumption by TOU bucket or by TIERED as applicable. Report to monitor the number of RPP customers who switch price plans. The report measures the number of customers who switch from TOU to Tiered separately from those who switch from Tiered to TOU
IESO	IESO’s Demand Forecasting team uses the smart metering data to support internal analysis and projections or to inform the public on the most recent trends

1 **Table 4. Expressions of Interest (NOT FULFILLED)**

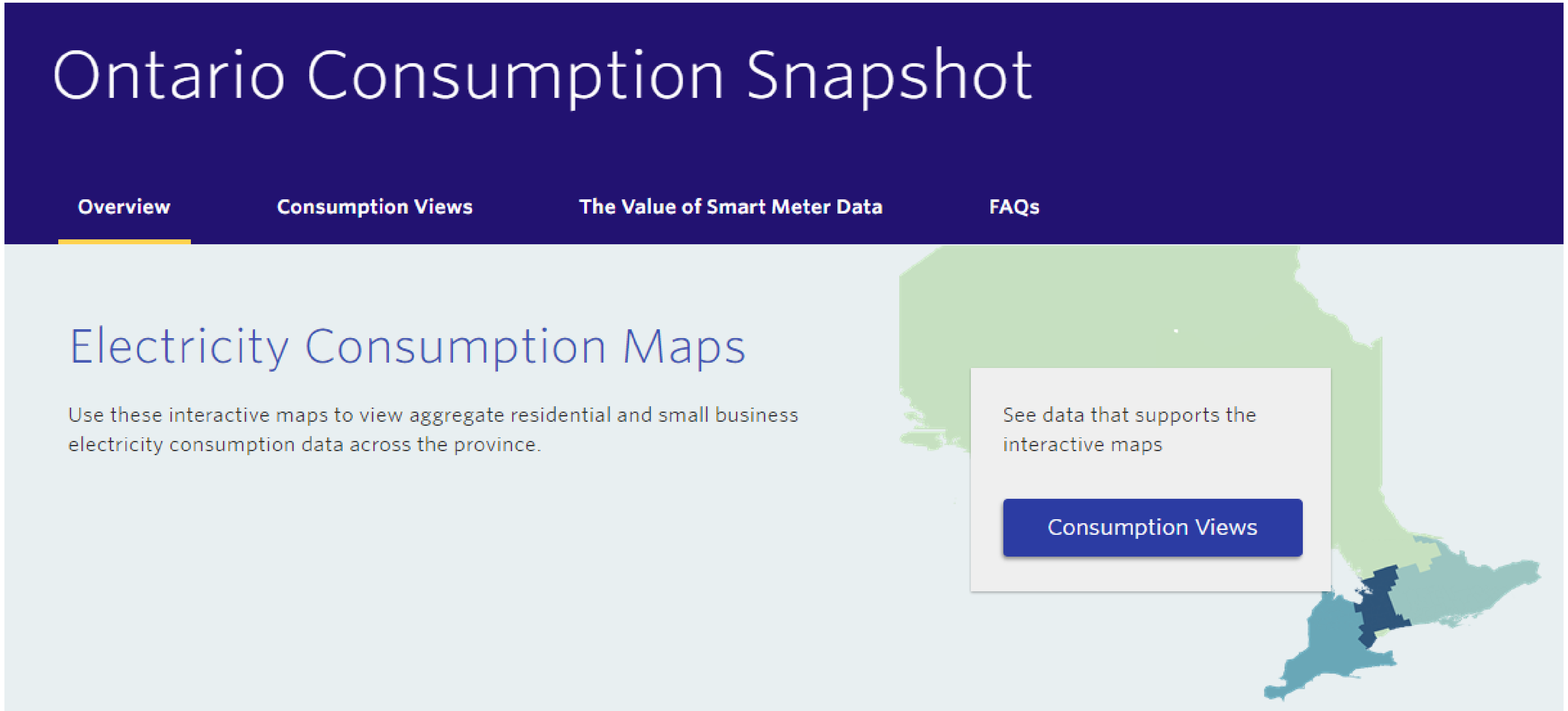
Requesting Organization	User Type	Brief Description Use Case
Ministry of Finance	Government	Different levels of analysis on business-level energy consumption data.
Ministry of Energy, Northern Development and Mines	Government	Continuity of data shared during the pilot process described on Table 1.
StatsCanada	Government	Different use cases, to include smart meter read data as part of existing public energy related tables.
Natural Resources of Canada	Government	Research on the impact of Renewals (Wind and Solar) on the Distribution Feeders.
Canadian Nuclear Laboratories	Government owned/Contractor operated	To support the research efforts on examining the impact of COVID-19 on power demand.
Rural Association of Ontario	Broader Public Sector	To perform statistical analysis using data segmented for rural/urban geographies, to support their role of publishing data on rural socio-economic trends.
Ivey Business School	Broader Public Sector	Research on household electricity prices, comparative research across various jurisdictions requiring energy consumption levels by RPP customers across the different TOU time periods.
University of Sydney (Australia) University of Ottawa University of Calgary	Broader Public Sector	Several use cases, one on estimating the effect of carbon rebates and electricity support payments in British Columbia and Ontario
Carleton University	Broader Public Sector	To understand how COVID-19 affected electricity consumption and how these effects vary with key socioeconomic variables at the Toronto FSA level, as captured by publicly available statistics. To evaluate if areas with more COVID-19 cases show larger changes in

		electricity consumption and how these vary with socioeconomics
University of Toronto	Broader Public Sector	Use Case described in Table 2, however with different lower levels of aggregation to better track business types.
Bord Gais Energy (Ireland)	Private	To help inform their forecasted load profiles for residential customers (looking at other jurisdictions due to lack of historical data being in the first phase of Smart Meter's rollout).
Lixar	Private	To support a study contracted by an Ontarian not-for-profit organization to understand the impacts of Covid-19.
Milestones Plus Consulting Group	Private	To support market research for a smart metering company.
Requests from individuals	PhD Student	To evaluate some of Ontario's electricity conservation policies.

*These data requests were not accepted due to the absence of a mandate to enable the SME to share lower levels of aggregation (compared to public data), also as some projects were placed on hold as requestors needed more time to assess their needs.

Sample Web Materials: Landing Page

Users would be able to link to this sitelet.

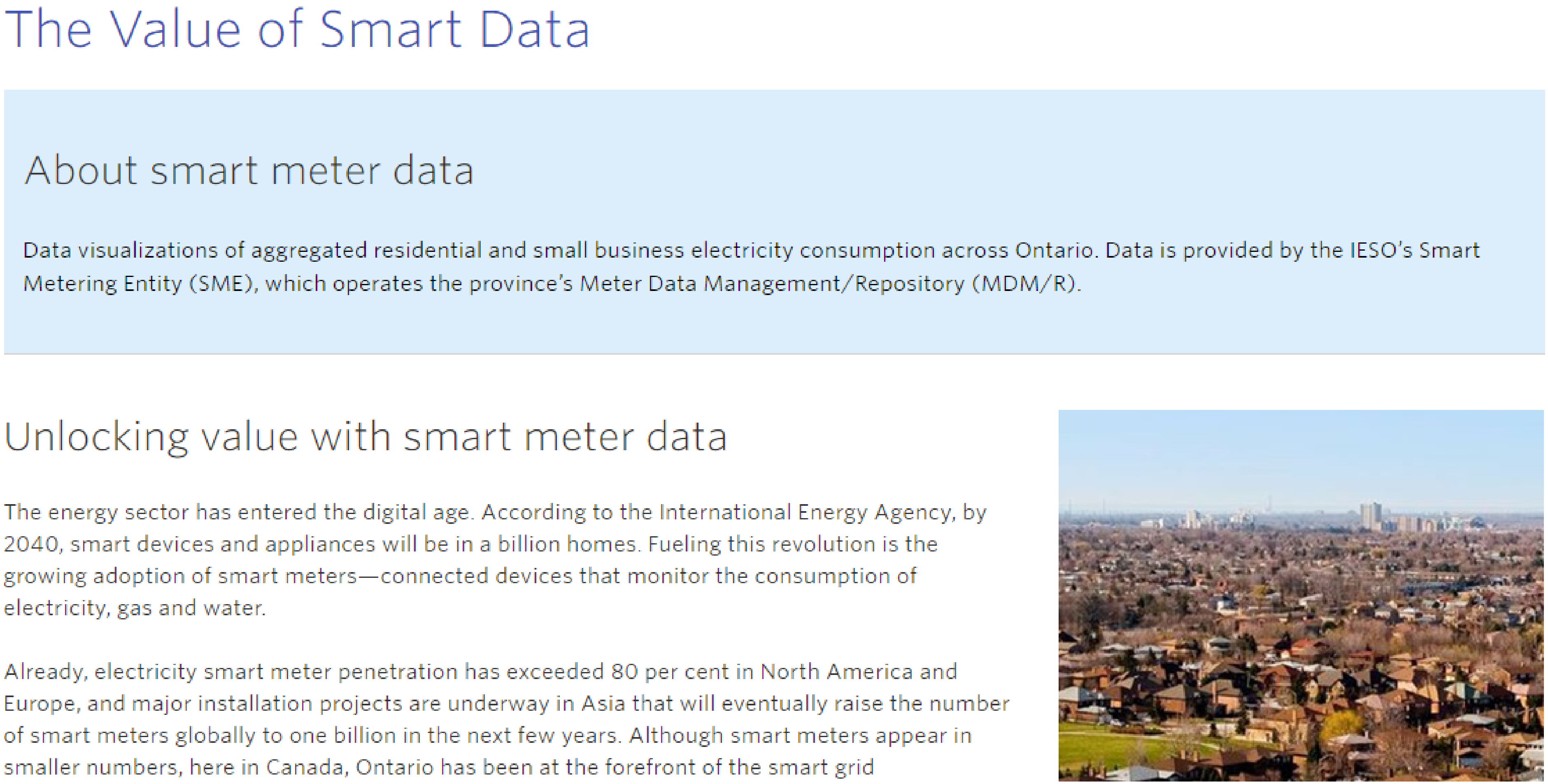


Electricity Consumption Maps

Use these interactive maps to view aggregate residential and small business electricity consumption data across the province.

See data that supports the interactive maps

Sample Communication Materials: Purpose of TPA



The Value of Smart Data

About smart meter data

Data visualizations of aggregated residential and small business electricity consumption across Ontario. Data is provided by the IESO's Smart Metering Entity (SME), which operates the province's Meter Data Management/Repository (MDM/R).

Unlocking value with smart meter data

The energy sector has entered the digital age. According to the International Energy Agency, by 2040, smart devices and appliances will be in a billion homes. Fueling this revolution is the growing adoption of smart meters—connected devices that monitor the consumption of electricity, gas and water.

Already, electricity smart meter penetration has exceeded 80 per cent in North America and Europe, and major installation projects are underway in Asia that will eventually raise the number of smart meters globally to one billion in the next few years. Although smart meters appear in smaller numbers, here in Canada, Ontario has been at the forefront of the smart grid

Sample Communication Material: Use Cases

The Value of Smart Meter Data – Case Study

What does it take to transition to a low-carbon, sustainable energy future? For Oxford County, this is not a hypothetical question. In 2015, the County set a goal to do just that through the adoption of local renewable generation, energy efficiency and make the switch to more electric vehicles.

Powering Tomorrow

Oxford County – Mapping electricity consumption data to plan for a community's future

Oxford County used the aggregated electricity consumption data from local smart meters to build an energy dashboard that can help the County move towards its goal of a low-carbon, sustainable energy future. Learn more

Enter smart meter data

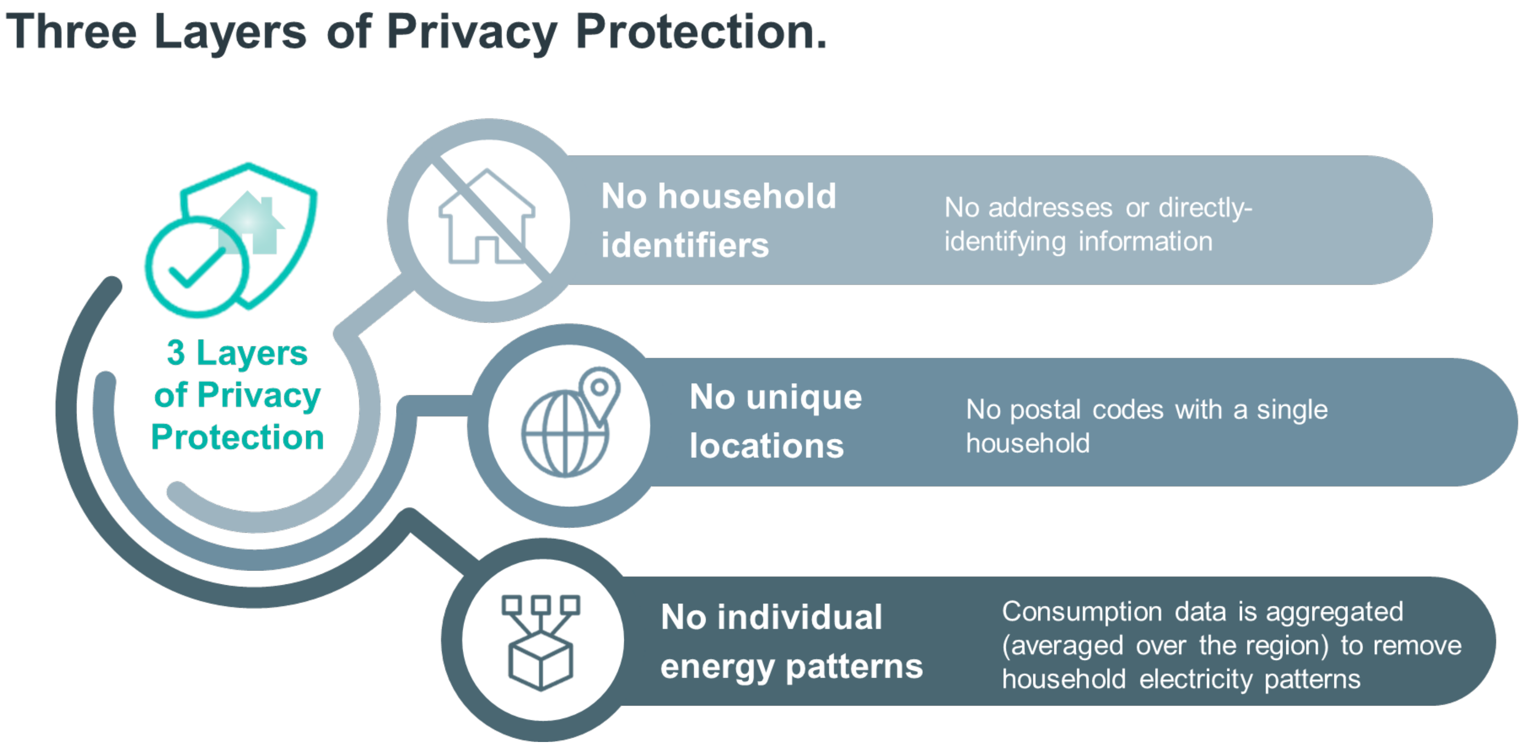
As part of a pilot project, the IESO's Smart Metering Entity provided Oxford County with four years of aggregated electricity consumption data from smart meters installed in residential locations and small businesses in the area. By correlating the smart meter data with other data sources—including municipal property assessments, spatial land use analysis and cumulative information on the use of different fuels—the County aims to create an energy dashboard that tracks how energy consumption is shifting across the County.

"Using the aggregated data from one postal code as a prototype, we mapped out different profiles of residential homes based on their size and age," explains Peter Crockett, Chief Administrative Officer of Oxford County. "We then used that data to generate typical load profiles for various residence type—creating a baseline scenario for homeowners. Ultimately, this will be incorporated into an online tool that allows people to either enter data from their electrical bills or use the baselines we've created to analyze how their energy bills and energy output would be affected if they adopt different measures—like switching to electric vehicles, adding solar panels or replacing their furnace."

> *Using the aggregated data from one postal code as a prototype, we mapped out different profiles of residential homes based on their size and age.*
>
> *— Peter Crockett, Chief Administrative Officer, Oxford County*

Sample Communication Materials: Privacy Protections

Sample of a visual tested in the IPSOS Research, this was positively received by the consumers and rated highest for being easy to interpret and helpful in explaining the privacy and security of smart meter data.



Three Layers of Privacy Protection.

3 Layers of Privacy Protection

No household identifiers

No addresses or directly-identifying information

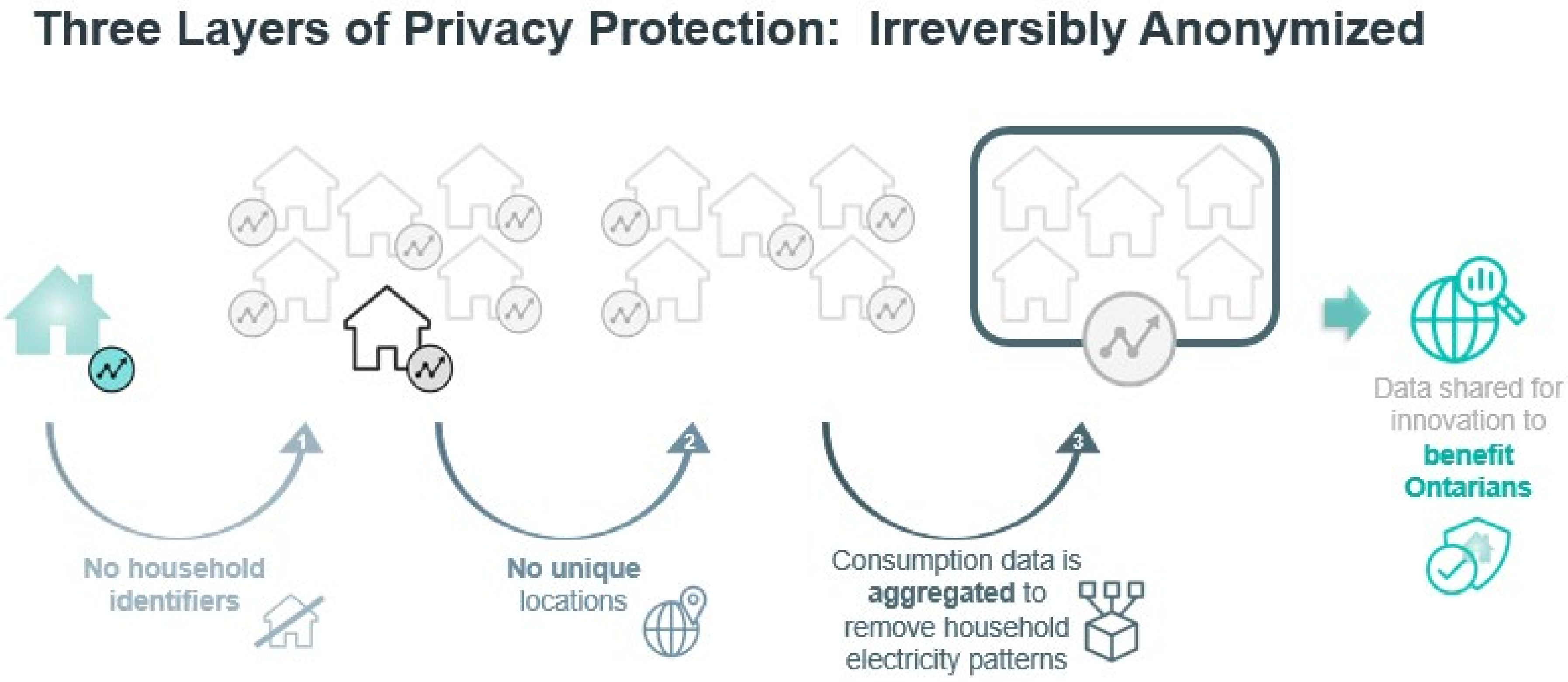
No unique locations

No postal codes with a single household

No individual energy patterns

Consumption data is aggregated (averaged over the region) to remove household electricity patterns

Sample Communication Materials: Privacy Protections



Three Layers of Privacy Protection: Irreversibly Anonymized

No household identifiers

No unique locations

Consumption data is **aggregated** to remove household electricity patterns

Data shared for innovation to **benefit Ontarians**

Sample Communication Materials: Privacy Protections

No Personal Data. No Household Energy Data. Privacy First.

DEFINED TERMS

Canadian Governmental Entities

Federal and provincial governments, including ministries, agencies, boards, commissions, tribunals and wholly-owned corporations, or in the case of non-share capital corporations, where such corporations are controlled by federal or provincial governments, as well as municipalities (or regional governments), universities, school boards, hospitals and First Nations. First Nations means a "council of the band" as that term is defined in subsection 2(1) of the Indian Act (Canada). "Canadian Governmental Entities" does not include private sector entities, publicly traded companies, individual doctors, professors, or government officials and all those entities that do not fall in one of the categories outlined above.

Highly aggregated data

Aggregations of Data at either the Census Division level or Customer Type (Residential and Small General Service <50kW consumers).

Prior Decision

The Ontario Energy Board's October 24, 2019 decision on the Smart Metering Entities prior Third Party Access application, EB-2018-0316.

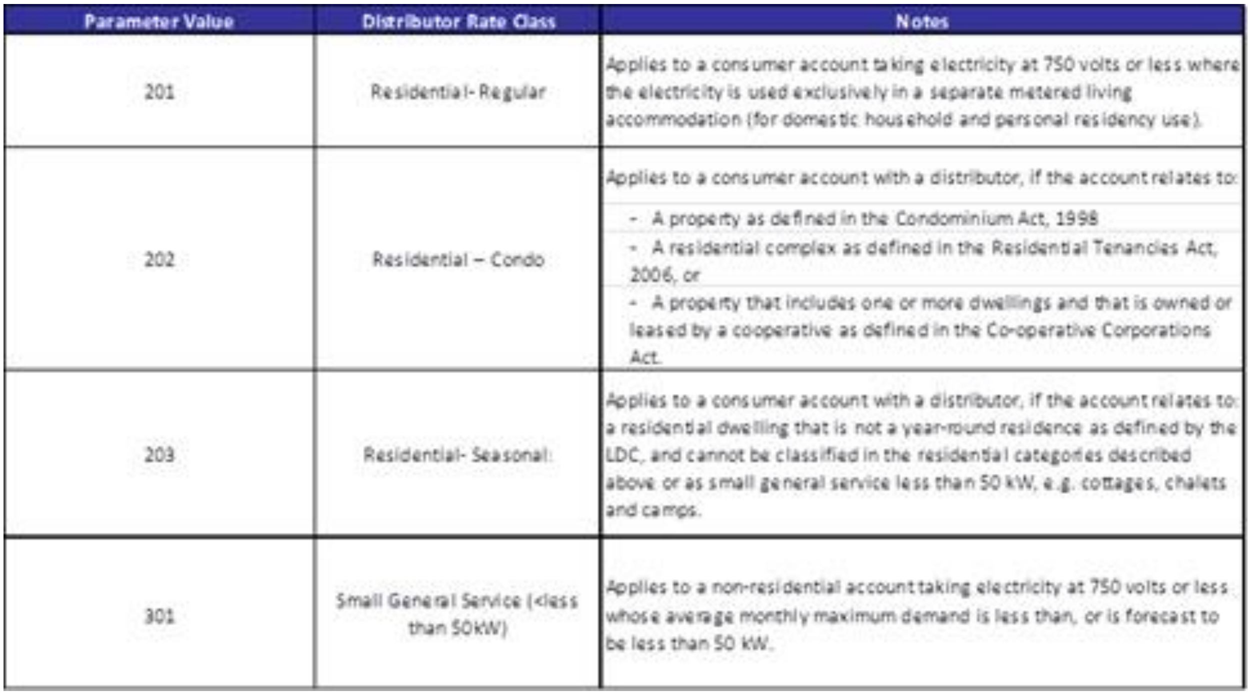
Prior intervenors

Means those intervenors in the proceedings leading to the Prior Decision.

Third Party Access ("TPA")

TPA means providing third party information to other entities besides the IESO.

Distributor Rate Classes



Parameter Value	Distributor Rate Class	Notes
201	Residential- Regular	Applies to a consumer account taking electricity at 750 volts or less where the electricity is used exclusively in a separate metered living accommodation (for domestic household and personal residency use).
202	Residential – Condo	Applies to a consumer account with a distributor, if the account relates to: - A property as defined in the Condominium Act, 1998 - A residential complex as defined in the Residential Tenancies Act, 2006, or - A property that includes one or more dwellings and that is owned or leased by a cooperative as defined in the Co-operative Corporations Act.
203	Residential- Seasonal:	Applies to a consumer account with a distributor, if the account relates to: a residential dwelling that is not a year-round residence as defined by the LDC, and cannot be classified in the residential categories described above or as small general service less than 50 kW, e.g. cottages, chalets and camps.
301	Small General Service (<less than 50kW)	Applies to a non-residential account taking electricity at 750 volts or less whose average monthly maximum demand is less than, or is forecast to be less than 50 kW.

ACRONYMS

AMO: the Association of Municipalities of Ontario

AMPCO: the Association of Major Power Consumers of Ontario

BOMA: Building Owners and Managers Association

BVA: Balancing Variance Account

CCC: Consumer Council of Canada

Data: Any of the information and data related to the metering of consumers’ consumption or use of electricity in Ontario, including the information the OEB required the SME to collect in its decision in EB-2016-0284

DUA: the Data Use Agreement

EDA: the Electricity Distributors Association

Electricity Act:	the *Electricity Act, 1998*, S.O. 1998, c. 15, Sched. A, as may be amended from time to time.
IESO:	Independent Electricity System Operator
IPC:	the Information and Privacy Commissioner of Ontario
LDC:	local distribution company
MDM/R:	the Meter Data Management Repository
OEB:	the Ontario Energy Board
OEB Act:	the *Ontario Energy Board Act, 1998,* S.O. 1998, c. 15, Sched. B, as may be amended from time to time
Prior Decision:	The OEB's October 24, 2019 decision and order on the SME's prior TPA application, EB-2018-0316
SMC:	the Smart Metering Charge
SME:	the Smart Metering Entity
SSC:	the Smart Metering Entity Steering Committee
TPA:	Third Party Access
VECC:	Vulnerable Energy Consumers Coalition