FOUNDATION WORKING GROUP SESSION #1

Privacy, Security and Third Party Access

April 22, 2015

ieso
Independent Electricity System Operator

Objective

- Develop the rules for access to data by third parties that preserves the security and privacy of personal information.
- Requesting Working Group input on:
  - Conditions for access to data by third parties
  - Additional controls to support access to data by third parties

Authority to Collect and Use Data

- FIPPA sets controls on the collection of personal information, but permits it where authorized by law. The *Electricity Act, 1998* authorizes the SME to collect information and data related to the metering of consumers' consumption
- Pursuant to FIPPA, the IESO and its agents and contractors who are acting on its behalf may use the MDMR data for purposes including (as required by FIPPA)
  - (i) to comply with the law [eg. (including the *Electricity Act, 1998*);
  - (ii) where use has been consented to by the individual; or
  - (iii) for a purpose consistent with the purpose for which the information was obtained

MDM/R Security & Privacy Overview

- Security and privacy controls in place, governing all data in the MDM/R, including personally identifiable information.
- The IESO and IPC published paper “Building Privacy into Ontario’s Smart Meter Data Management System: A Control Framework”, that describes the internal control systems in place to protect smart meter and related in the MDM/R, including:
  - Control Environment, Organization Registration, Access to MDM/R Application, Interfaces and Data, Meter Data Collection, Master Data Management, Meter Data Validation and Estimation, MDM/R Operational Service Provider Controls, Change Management, Incident Management, Access Security
- Leveraging International Standards (ISO 27002) for security systems and data.
- Annual CSAE 3416 audit, that includes in its scope assessment of IESO’s controls over access to systems, interfaces, and data, as well as controls to prevent unauthorized access to system and data.
- The IESO has processes for fulfilling access requests from LDCs and their agents (eg. organization registration, service request processes, authentication, encryption)
- IESO’s sample controls are provided in the Appendix.

Note: for discussion purposes only

Questions for the Working Group

- Any feedback on the controls in place at the IESO/SME for protecting data in the MDM/R including personal information?
- What is the Definition of a Third Party in the context of access to MDM/R data?
  - **Consider**: An organization or user who is not the IESO, the LDC, a Customer Contracted Agent, Retailer, or one of their authorized agents.
- What additional measures should be in place to support access to data by Third Parties subject to the *SME License* (Article 9) and applicable Legislation?

IESO Disclosure of Data to Third Parties

- FIPPA permits disclosure of personal information on several grounds including: (i) consent of the individual; (ii) a purpose consistent with that for which it was obtained; (iii) to comply with the law.
  - Information that has been aggregated or depersonalized is not considered personal information and therefore limits on disclosure under FIPPA would not apply.
- The IESO as the Smart Metering Entity the has obligation (as defined in the *Electricity Act, 1998* and the *SME License)* to "To provide and promote non-discriminatory access, on appropriate terms and subject to any conditions in its licence relating to the protection of privacy, by distributors, retailers, the IESO and other persons",
- This authorization is subject to privacy restrictions in the IESO's SME's License (Article 9) "Restrictions on Provision of Information" which include similar permitted disclosures – such as in accordance with the law and where consent has been obtained).

Third Party Access

- *9.2 The Licensee shall not disclose information regarding a distributor, consumer, retailer, or any other person to any other party without the written consent of the distributor, consumer, retailer, or other person, except where such information is required to be disclosed:*

  (a) to comply with any legislative or regulatory requirements, including the conditions of this Licence;

  (b) for billing, settlement or market operations purposes; or

  (c) for law enforcement purposes.

  – What are the use cases for Third Party access to data?

Third Party Access

- *9.3 The Licensee may disclose information regarding distributors, consumers, retailers, or any other person where the information has been sufficiently aggregated such that the distributors', consumers', retailers', or other person's particular information cannot reasonably be identified.*
  - What techniques are acceptable such that “particular information cannot reasonably be identified”?
  - **Consider**:
    - Anonymization and aggregation techniques
    - Should License be clarified to explicitly consider anonymization techniques?

Third Party Access

- *9.4 The Licensee shall inform distributors, consumers, retailers, and any other person of the conditions under which their information may be released to a third party without their consent.*
  - Do LDCs or others already have a framework in place for giving notice to consumers?
  - How should notice be provided to consumers?

Third Party Access

- *9.5 If the Licensee discloses information under this section, the Licensee shall ensure that the information provided will not be used for any other purpose except the purpose for which it was disclosed.*
  - What should the allowed purposes be for disclosing information to Third Parties?
  - What methods can be used to ensure that the information will not be used for any other purpose except for the purpose for which it was disclosed?
    - **Consider**: Terms of Use and Non-Disclosure Agreement as conditions for providing information to a Third Party

Are there any other questions that should be asked and answered by the Working Group?

Appendix - References

- **Health-Care Requirement for Strong Encryption**, Ann Cavoukian, Ph.D., Information & Privacy Commissioner of Ontario - https://www.ipc.on.ca/images/WhatsNew/fact-16-e_1.pdf
- **Building Privacy into Ontario's Smart Meter Data Management System: A Control Framework**, IESO and IPC, May 2012 https://www.ipc.on.ca/images/Resources/pbd-ieso.pdf
- **Privacy by Design Principles**, Information & Privacy Commissioner of Ontario
- **ISO-IEC_27002-2013** - International Standard: Information technology – security techniques – code of practice for information security controls
- **Trust Services Principles and Criteria** for Security, Availability, Processing Integrity, Confidentiality and Privacy, American Institute of Certified Public Accountants and Charter Professional Accounts of Canada (2014)
  - Used by service providers and data custodians to implement and demonstrate that they have appropriate security and privacy controls in place.
- **MDM/R Operations CSAE 3416 Audit** - in accordance with the Canadian Standard on Assurance Engagements for Reporting Controls at a Service Organization, set out in CPA Canada Handbook – Assurance ("CSAE 3416").

Appendix – Sample Security & Privacy Controls

- Authorization – process for authorizing access to an organization and user, including specifying the level of access or privileges (both logical and physical)
- Access Administration - process for granting, removing, and reviewing access to organizations and users (logical and physical)
- Authentication - process of determining whether organization or user, in fact, who or what it is declared to be (eg. certificates/keys, user ID and password, and other techniques)
- Password policies and standards
- Physical security and protection from damage
- Network security and perimeter controls including firewalls, intrusion detection and prevention services
- Disclosure controls, including secure communication – eg. encryption of data in transit
- Technical vulnerability management (eg. patching)
- Awareness and training
- Change management to prevent unauthorized changes from being made to systems and data

Appendix - Privacy Legislation

- *Freedom of Information and Protection of Privacy Act* (FIPPA)
- *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)
- *Personal Information Protection and Electronic Documents Act* (PIPEDA)

FIPPA

- Pursuant to R.R.O. 1990, Reg. 460 the IESO is designated as an “institution” and is subject to FIPPA.
- FIPPA protects personal information held by certain Ontario public institutions by creating a regime that governs the collection, use and disclosure of personal information by those institutions.

FIPPA and MFIPPA

- Personal information is defined as information about an identifiable individual, including, among other things, family status, information related to financial transactions, any identifying number assigned to the individual, the address of the individual, and that individual's name where it appears with other personal information. It does not include certain business contact information.
- MFIPPA creates a similar privacy regime that applies to municipalities and other municipal entities, including LDCs incorporated pursuant to s. 142 of the *Electricity Act, 1998*.

PIPEDA

- PIPEDA is a federal law that applies to private-sector organizations that collect, use and disclose personal information in the course of undertaking commercial activities.
- Personal Information is broadly defined as information about an identifiable individual (but does not include certain business contact information).
- PIPEDA does not directly apply to the IESO, municipalities and other public-sector entities, but may apply to private sector third-parties.

Appendix - Other Relevant Documents

- *Electricity Act, 1998*
- Ontario Regulation 393/07
- Smart Metering Entity License ES-2007-0750