Foundation Working Group

Draft: Proposed Framework for Third Party Access

This document sets out a proposed high-level framework to provide third party access to both identifiable and de-identified data (the "Framework"). This Framework is designed to support future projects that would implement such access rights. This Framework assumes that all data will be handled in accordance with relevant privacy legislation and government directives; however, the potential impact of the draft government Open Data Directive has not been considered in this recommendation.

This document also assumes that a robust de-identification process would be part of any implementation. For the purpose of this document, the Data Custodian is the IESO/SME and the source system to be accessed containing the requested electricity consumption data is either the MDM/R or the MDM/R Data Mart. However, the general provisions of the framework would be applicable to different data custodians or different source systems containing other data.

Background

In 2004 the government of Ontario launched the Smart Metering Initiative. This initiative involved the installation of smart meters in homes and small businesses across Ontario and the establishment of the Meter Data Management and Repository (MDM/R), managed by the Smart Metering Entity (SME). The SME was created by the Electricity Act and the IESO is designated as the SME by O. Reg. 393/07. The Electricity Act, s. 53.7(3) sets out the objectives of the SME, one of which is:

> 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[.]

Categories of Access

This framework addresses four potential access scenarios:

1. Standard reports developed using de-identified electricity consumption data downloadable from a public website by any third party (de-identified);
2. Access requests for de-identified electricity consumption data, alone or matched with other data sets, that are fulfilled by the holder of the electricity data, the "Data Custodian", and available to authorized third parties (de-identified);

3. Access requests fulfilled by the requester through the Data Custodian's system access portal or interface, set up to permit access to de-identified electricity consumption data by authorized third parties (de-identified); and,
4. Access requests for personal electricity consumption data, alone or matched with other data sets, which are fulfilled by the Data Custodian and available to authorized third parties (personal information).

1. Downloadable Standard Reports from a Public Website (de-identified)

Standard reports derived from the MDM/R could be created and made available on the IESO's website for download by any third party. This would be similar in concept to the electricity system data currently available on the IESO website: http://reports.ieso.ca/public/RealtimeMktPrice/PUB_RealtimeMktPrice.xml

Funding the costs of developing and maintaining downloadable standard reports would be defined as part of the implementation of such a facility. Options could include these costs being part of regular SME operations or a separate cost recovery mechanism.

These reports would contain only de-identified data and would be in a format that could be used and analyzed. In developing standard reports, the IESO would consider reports based on a sample group to lower cost and with regional identifiers and sufficient temporal granularity to make them useful.

The terms and conditions of use governing third party access to this type of data may be similar to those already contained on the IESO website, and would comply with the IESO and SME licences and legislation. (See for example: http://www.ieso.ca/Pages/Terms-of-Use.aspx).

Use of the data would need to be limited to the purpose for which it was collected, and re-identification of the data would be prohibited.

2. Custom Data Requests Fulfilled by the Data Custodian (de-identified)

This category would be for custom requests for de-identified electricity consumption data, either on its own or paired with other data sets, and fulfilled by the Data Custodian. The results would be delivered to the requesting party via an agreed upon delivery channel. This service could include the requester providing the Data Custodian with additional data sets to be matched with the electricity data and then de-identified. The requestor would not have direct access to the source system of the data (e.g. the MDM/R) nor would they have access to personally identifiable information held in the MDM/R or MDM/R Data Mart.

The requestor would execute an agreement with the Data Custodian that includes terms and conditions of use governing third party access to this type of data could include provisions governing some of the same situations contemplated by the standard reports discussed above, as well as basic rules of access, including:

1) A registration process completed by the requestor, and upon successful completion it would be authorized to submit request(s).
2) Submitted requests would provide the following information:
    a) Specific data being requested,
    b) Intended use of the information (the requestor agreement would provide it could not be used for other purposes),
    c) Intended disclosure of the information (what other parties would have access to the data and at what level of granularity), and
    d) Other data sets to be matched with the requested data (if any), including the expiration date of the licence for these data source(s) (if applicable), information as to the level of granularity at which the data is to be matched and acknowledgment of compliance with any data access rules for the other data sets.
3) A request fulfillment assessment process would consider the following constraints and prioritization criteria:
    a) Current volume of requests to be serviced,
    b) Complexity and amount of requested information,
    c) Availability of resources (systems and personnel) and associated costs,
    d) Use of the information,
    e) Any laws, regulations or directives involved, particularly if deadlines have been imposed, and
    f) Organization requesting information.
    g) The expiration of any licence for additional data provided[1]
4) The requesting party would agree to certain terms and conditions, which may include the following:
    a) Cost structure for services,
    b) Payment terms for services,
    c) Requestor has in place effective controls to protect the security and privacy of data that meet or exceed the controls used by the Data Custodian (which they would require of any other recipient of the data),

[1] Any work or de-identified information that is the output of this process will not necessarily expire with the source data license expiration.

d) Ability for the Data Custodian to require the requestor (and any other recipient of the data) to be subjected to an independent audit and provide evidence to the Data Custodian to demonstrate the design and operating effectiveness of its security and privacy controls, and

5) Data would be de-identified following an appropriate de-identification process (see Proposed Recommendations on De-identifying Information for Disclosure to Third Parties) prior to being delivered to the requestor.

3. Data Access Requests fulfilled using a Portal or Interface (de-identified)

The broadest data access to third parties would be to allow them to retrieve or access de-identified data from the Data Custodian using a portal or interface into the source system. In addition to the terms and conditions of use contained in the above types of access (modified as needed), the IESO would also need to consider the following processes, rules and requirements:

1) The requestor would submit an application to be qualified to directly connect to the portal or interface, specifically accepting any terms and conditions relating to use of the portal/interface (in addition to the data itself). The application would be assessed by the IESO and only approved requestors would be allowed access.
2) The requestor would comply with the registration, connectivity and authentication processes and tests for direct access to the portal or interface by each qualified organization and would take responsibility for its individual users.
3) Access would be for a limited, agreed upon duration, and the requestor would agree to timely notification of the IESO of the removal of individual authorized user's access privileges to the portal or interfaces in accordance with the established processes and procedures of the Data Custodian.

4. Personal Information Requests that are Fulfilled by the Data Custodian

This category focuses on access to personally identifiable electricity information, on its own or paired with one or more other data sets.

Providing access to personal information to any third party, while protecting its privacy, involves many complicated issues and affects multiple organizations. Given the complexity of such access and that many use cases can be satisfied with de-identified data, the IESO is not recommending broad access to personal information at this time. The IESO's recommendation is that access to personal information be limited to federal, provincial and municipal governments for uses related to energy planning, policy development and other uses, as authorized by applicable legislation, licences, directives or notifications. Such access requests and resulting action would also be communicated to the LDCs whose customers' personal data is being accessed.

The access framework in this scenario may be similar to that noted for de-identified data; however, additional criteria would be required including:

1) Determinations about who can access the data and for what purpose
2) Control requirements over the security and privacy of data.
3) Compliance with privacy legislation

Conclusion

While this paper has outlined a Framework and considerations for access, the IESO notes that any future implementation would need to consider requisite legislative, policy and process requirements, including for the data matching service, that define in greater detail the governance framework, accountability and controls, including specifics relating to third party access to personally identifiable information.