Joint Board Meeting
April 8, 2019

Briefing: Draft ORCA Data Privacy Policy

Working with the ORCA agencies, IBI Group has drafted the attached ORCA Data Privacy Policy.

The draft policy has been reviewed by agency attorneys and other agency stakeholders.

This briefing is to go over the following topics related to development and implementation of the policy:

1. Coverage of Policy and Procedures
2. Data Release Guidelines
3. General Guidelines of Releasing ORCA Data
4. ORCA Data Aggregation
5. Location
6. Time Period
7. Amount of Data
8. ORCA Data Anonymization
9. Examples of Data Release

Next steps: The agencies and IBI Group will incorporate feedback then finalize the policy for Joint Board action. Business procedures will concurrently be developed for staff to implement the policy specific to each user type.

ORCA Data Privacy Policy - Final Draft

This policy is adopted by the Joint Board pursuant to Section 4.1.1.7 of the 2009 Amended and Restated Interlocal Cooperation Agreement ("Interlocal Agreement") for implementation by the Agencies who are participants in the ORCA Regional Fare Coordination Program.

1.0 PURPOSE

1.1. To establish an ORCA Data Privacy Policy that creates standards for responding to requests for the release of ORCA data in a way that:

- Complies with applicable laws and regulations;
- Provides the user with useful information; and
- Protects the privacy of individual ORCA cardholders.

1.2. To guide the identification of what data and in what format can be provided in response to a given request.

2.0 REFERENCES

2.1. Chapter 42.56 of the Revised Code of Washington (RCW), Washington State Public Disclosure Act

2.2. Chapter 47.04 RCW, Public Highways and Transportation - General Provisions

2.3. ORCA Public Records Disclosure Policy

3.0 DEFINITIONS

3.1. "Agencies" mean those transportation agencies who are current signatories to the Amended and Restated Interlocal Cooperation Agreement including: Everett Transit, Community Transit, King County Metro, Kitsap Transit, Pierce Transit, Sound Transit and Washington State Ferries.

3.2. "Card Serial Number (CSN)" means the unique serial number on each ORCA card.

3.3. "Data aggregation" means the process of manipulating data into summary form, usually based on a variable or set of variables.

3.4. "Data lifecycle" means the cycle of data from creation to destruction, including the storage, use, and disclosure of data.

3.5. "Data privacy" means the policies and guidelines related to collecting, using, disclosing, and destroying that personal information.

3.6. "Data Release" refers to the granting of access to or provision of data from the ORCA system to a party, internal or external to ORCA Agencies.

3.7. "Data Request" refers to any attempt by a party, internal or external to ORCA Agencies, to access and/or extract data from the ORCA system.

3.8. "Institutional Review Board" refers to a type of administrative body that reviews research involving human participants in order to protect the welfare, rights, and privacy of these subjects; institutional review is required for all research that receives indirect or direct support from the United States federal government.

3.9. "Personally Identifiable Information (PII)" means the personal information that could be used to identify or intends to identify an individual either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

3.10. "Public Disclosure Request" means, as required by the Washington State Public Disclosure Act (Chapter 42.56 RCW), that upon request, identifiable public records be made available for public inspection and copying.

3.11. "User Type" means any party, internal or external to the ORCA Agencies, who requests access to data from the ORCA system.

4.0 SCOPE

4.1. While there are privacy considerations throughout the lifecycle of data managed within the ORCA system, this Policy applies only to instances of Data Release.

4.2. The types of ORCA system data covered under this Policy include, but are not limited to, cardholder information, transaction records, business account information, and customer service records

4.3. ORCA data may be provided to a variety of users via a variety of sources, all of which are covered under this Policy.

4.3.1. ORCA data may be accessed both through an information request fulfilled by a Transit Agency employee or representative, as well through a self-service interaction with the ORCA system, for example through an ORCA website or a ticket vending machine (TVM).

4.4. Seven User Types have been created to cover the spectrum of potential ORCA Data Requests into a hierarchical structure.

4.4.1. Defined obligations and guiding principles inform the ORCA data that is appropriate to release to each User Type.

4.4.2. This Policy focuses on providing User Types with data they may need while also handling privacy considerations relative to the User Type.

4.5. Requests for ORCA data that fall outside this framework and the User Types defined in Sections 5 and 6 shall be handled on a case by case basis and may be subject to legal review by the ORCA Agencies if necessary.

5.0 DATA USER TYPES

5.1. The ORCA Data User Types are grouped based on:

5.1.1. The entity making the Data Request;

5.1.2. The purpose of the Data Request, and related, the permissible uses of ORCA data by the entity requesting it;

5.1.3. Any privacy concerns related to a User Type and the appropriate level of aggregation and anonymity for providing ORCA data;

5.1.4. Obligations a User Type must complete in order to access ORCA data;

5.1.5. Existing ORCA policies; and

5.1.6. The ORCA data that is currently available to the User Type.

5.2. Described in detail in the following sections, there are seven primary User Types:

5.2.1. ORCA Cardholders

5.2.2. Business Accounts

5.2.3. ORCA Agencies

5.2.4. Research Entities

5.2.5. Third-Parties

5.2.6. General Public

5.2.7. Law Enforcement

6.0 DATA RELEASE REQUIREMENTS

6.1. Section 6 describes the primary User Types.

6.1.1. For each User Type, a list of common reasons for requesting ORCA data is provided. These request purposes, while inclusive of a wide variety of use cases applicable to the User Type, do not necessarily represent the full spectrum of valid Data Requests.

6.1.2. Additionally, a set of guiding principles is defined. These principles are used to support Agency efforts to establish the ORCA data that is appropriate and permissible to provide to the User Type, and at what level of anonymity and aggregation.

6.1.3. Any obligations the User Type must fulfill in order to receive the ORCA data are, when applicable, also described in this section.

6.2. The guiding principles defined in Section 6 are intended to help establish the appropriate levels of aggregation and anonymity necessary to protect the personally identifying information (PII) of individuals. If an Agency determines that these thresholds put the privacy of an individual or individuals at risk, the Agency may exercise their discretion to define additional privacy rules on a case by case basis.

6.3. Requests for ORCA data that fall outside the defined User Types shall be handled on a case by case basis and may be subject to legal review by the ORCA Agencies if necessary.

6.4. USER TYPE 1 - ORCA CARDHOLDERS

6.4.1. User Type 1 includes all individuals that own an ORCA card.

6.4.2. PURPOSES FOR REQUESTS

6.4.2.1. Manage details of the ORCA cardholder’s account;

6.4.2.2. Review transaction history attached to the User Type’s ORCA card; or

6.4.2.3. Access information about the current status of the ORCA card.

6.4.3. GUIDING PRINCIPLES

6.4.3.1. Provide ORCA cardholders with the relevant data associated with their ORCA card and account; and

6.4.3.2. Prevent the disclosure of ORCA card data to customers who cannot establish ownership of the card.

6.4.4. OBLIGATIONS OF THE USER TYPE

6.4.4.1. ORCA cardholders must establish ownership of their card prior to receiving ORCA data.

6.5. USER TYPE 2 - BUSINESS ACCOUNTS

6.5.1. User Type 2 includes all entities that have an established Business Account agreement for Business Choice or Business Passport, both of which are regional ORCA programs that allow the business to provide ORCA cards to program participants and manage these cards.

6.5.2. PURPOSES FOR REQUESTS

6.5.2.1. Analyze program utilization and effectiveness;

6.5.2.2. Analyze the utilization and effectiveness of business-funded agency service hours;

6.5.2.3. Analyze travel patterns of ORCA customers associated with the business; or

6.5.2.4. Support investigations of fraud.

6.5.3. GUIDING PRINCIPLES

6.5.3.1. Provide enough data in an appropriate format for business accounts to make meaningful insights;

6.5.3.2. Provide data for a time range and aggregation level to prevent misinterpretations or overgeneralizations; and

6.5.3.3. Except in cases of fraud investigation, ensure that a single ORCA cardholder cannot be identified or tracked through the data provided.

6.5.4. OBLIGATIONS OF THE USER TYPE

6.5.4.1. Business Accounts must provide participating ORCA cardholders with terms of use, per established Business Account agreements.

6.6. USER TYPE 3 - ORCA AGENCIES

6.6.1. User Type 3 includes all Agency employees or Agency contractors.

6.6.2. PURPOSES FOR REQUESTS

6.6.2.1. Support Agency research, analysis, and planning;

6.6.2.2. Support efforts of Agency contractors;

6.6.2.3. Support program management and analysis;

6.6.2.4. Supplement public-facing reports or other publications; or

6.6.2.5. Support Agency investigations in defense of claims filed against it by a third party.

6.6.3. GUIDING PRINCIPLES

6.6.3.1. Provide data in an appropriate format for ORCA Agencies to make meaningful insights and plan service effectively;

6.6.3.2. Ensure that a single ORCA cardholder cannot be identified and tracked through the data provided when not required for the purpose of the request; and

6.6.3.3. Provide, for cases in which it may be publicly released in its original format, ORCA data in an appropriate format to:

- ○ Prevent misinterpretations or overgeneralizations; and
- ○ Ensure that a single ORCA cardholder cannot be identified or tracked.

6.6.4. OBLIGATIONS OF THE USER TYPE

6.6.4.1. ORCA Agency employees that request and receive ORCA data must follow applicable laws and Agency policies.

6.6.4.2. Agency contractors that request and receive ORCA data must follow non-disclosure rules set by individual ORCA agencies.

6.7. USER TYPE 4 - RESEARCH ENTITIES

6.7.1. User Type 4 includes all entities that request ORCA data for research purposes.

6.7.2. PURPOSES FOR REQUESTS

6.7.2.1. Support research efforts concerning the ORCA system or ORCA programs.

6.7.2.2. Support general transportation-related research efforts.

6.7.3. GUIDING PRINCIPLES

6.7.3.1. Provide data in an appropriate format to assist with effective research efforts;

6.7.3.2. Ensure that data provided complies with ORCA cardholder consent; and

6.7.3.3. Ensure that data provided complies with Institutional Review Board-approved research methods, when applicable.

6.7.4. OBLIGATIONS OF THE USER TYPE

6.7.4.1. Research entities that request and receive ORCA data must follow non-disclosure rules set by the ORCA Agencies, the research organization, or the Institutional Review Board.

6.8. USER TYPE 5 - THIRD-PARTIES

6.8.1 User Type 5 includes any external entity working but not in a contractual relationship with an ORCA agency on transportation programs.

6.8.2 PURPOSES FOR REQUESTS

6.8.2.1 Support program functionality; or

6.8.2.2 Analyze program utilization and effectiveness.

6.8.3 GUIDING PRINCIPLES

6.8.3.1 Provide enough data in an appropriate format for third-party partners to make meaningful insights on program effectiveness;

6.8.3.2 Provide appropriate data to support program functionality;

6.8.3.3 Ensure that a single ORCA cardholder cannot be identified or tracked; and

6.8.3.4 Ensure that data provided complies with ORCA cardholder consent.

6.8.4 OBLIGATIONS OF THE USER TYPE

6.8.4.1 Entities that request and receive ORCA data must follow non-disclosure rules set by individual agencies or the third-party.

6.9 USER TYPE 6 - GENERAL PUBLIC

6.9.1 User Type 6 includes public Data Requests through standard public record request processes.

6.9.2 PURPOSES FOR REQUESTS

6.9.2.1 Requests for ORCA data from User Type 6 may be made for any reason, so long as the request is not exempt under Chapter 42.56 RCW.

6.9.3 GUIDING PRINCIPLES

6.9.3.1 Provide data for a time range and aggregation level to prevent misinterpretations or overgeneralizations; and

6.9.3.2 Ensure that a single ORCA cardholder cannot be identified or tracked through data provided.

6.9.3.3 Ensure that ORCA data provided complies with the ORCA Public Records Disclosure Policy.

6.9.4 OBLIGATIONS OF THE USER TYPE

6.9.4.1 User Type 6 carries no obligations for receiving ORCA data; Agencies cannot request information about the purpose of the request or planned use of provided data.

6.10 USER TYPE 7 - LAW ENFORCEMENT

6.10.1 User Type 7 includes all Data Requests by law enforcement agencies.

6.10.2 PURPOSES FOR REQUESTS

6.10.2.1 Support law enforcement efforts, including but not limited to investigations, arrest, prosecution, or defense of the accused.

6.10.3 GUIDING PRINCIPLES

6.10.3.1 Support law enforcement investigations through disclosure of ORCA card data and associated PII when legal requirements for Data Release are met;

6.10.3.2 Only release PII to law enforcement with a court order (e.g. search warrant or subpoena) (see RCW 42.56.330(5)(b)).

6.10.4 OBLIGATIONS OF THE USER TYPE

6.10.4.1 Law enforcement requests may only be fulfilled if legal requirements for Data Release are met.

6.10.4.2 ORCA data may be released to law enforcement without a court order when the person or entity that owns the PII gives written consent.