METRO BUSINESS PRACTICES FOR USE OF REPLICA DATA

January 2020

Table of Contents

INTRODUCTION 2

APPLICABLE TO 2

DEFINITIONS 3

GUIDELINES 4

BUSINESS PRACTICES 5

- Password Protection and User Access 5
- Data Storage 6
- Electronic and Physical Media 6
- Code of Conduct 6
- Validation Testing 6
- Publishing, Displaying, and Sharing Data 7
- Use in Combination with Other Data Sources 7
- Data Retention 8
- Requests for Replica Data 8
- Auditing 8
- Incident Reporting and Response 8
- Enforcement 9
- Responsibilities 9

REFERENCES 11

INTRODUCTION

Metro collects, shares, and uses data to support transportation and land use planning in the Portland region, and we work to get access to data that meets our needs and the needs of our partners while protecting people's privacy. Metro, in collaboration with several of our Public Agency Partners, is testing a new data tool called Replica that provides detailed data on travel patterns in a way that promises to maintain people's right to privacy. Replica is a new product, and Metro is working with it at a time when research is revealing that data on where people travel can reveal sensitive information. This document outlines business practices for handling Replica Data designed to protect people's privacy, allow Metro staff and Public Agency Partners access to information from Replica that supports their work, and uphold Metro's agreement with Replica.

Metro is testing Replica to ensure that it protects privacy and meets our standards for accuracy before proceeding to use the data, and taking a conservative approach to handling data during this initial validation testing period. Metro will update this document after we complete validation testing to address privacy risks or accuracy concerns revealed during the testing process. Metro will also continue to update these business practices to remain consistent with other Metro policies and procedures related to data privacy and with relevant updates to state and federal law.

APPLICABLE TO

All Metro and third-party users who have or manage access to Replica Data through Metro's agreement with The Replica Company.

DEFINITIONS

1. Replica: A high-fidelity, frequently updated simulation of regional travel patterns developed by a company also named Replica (see below). Replica uses location data from cellular providers and other data sources to build models of individual travel behavior, then applies these models to a synthetic population that closely, but not exactly, matches a metropolitan area's population. The resulting data provides detailed simulated estimates of current regional travel patterns, including mode, trip purpose, origin and destination, route, and demographic characteristics of travelers. These estimates are updated quarterly, and each update includes data for typical travel patterns during an average week within the relevant quarter.
2. The Replica Company: The company, also named Replica, responsible for developing, maintaining, and updating Replica. This document refers to this company as The Replica Company to distinguish it from the data product of the same name (see above).
3. Replica Dashboard: An online tool that displays Replica Data aggregated to a variety of scales, and allows users to map and filter the data using characteristics such as primary travel mode, trip purpose, race/ethnicity, and income. The dashboard allows users to query and download aggregate data for a limited number of trips. Most Replica Users will have access to Replica Data solely via the dashboard. The dashboard provides Replica Data in a format that is easy for non-technical users to interact with and that protects privacy by providing aggregate data on simulated trips, making it impossible to identify individuals or their trips.
4. Synthetic Travel Database: A data table describing each individual simulated trip included in a given quarterly Replica update, as well as all attributes associated with each trip. Selected Metro staff will have access to the Synthetic Travel Database, and will use it to inform Metro's travel model and conduct custom analyses to support Metro projects. Metro is limiting access to the database to a small number of expert users within Metro who are subject to stricter data handling guidelines because the detailed nature of the data increases the risk that it could be used to identify individuals and because Replica considers the database a trade secret.
5. Replica Data: Includes the Synthetic Travel Database as well as data viewed or downloaded through the Replica Dashboard.
6. Replica User: An employee of Metro or one of its Public Agency Partners who has access to the Replica Dashboard or the Synthetic Travel Database.
7. Expert User: A subset of Replica Users who are employees in Metro's Research Center and have access to the Synthetic Travel Database.
8. Public Agency Partner: A public-sector organization that participates in Metro's transportation planning activities, including transportation agencies and public universities located within Multnomah, Washington, Clackamas or Clark Counties. Selected staff at Public Agency Partners are eligible for access to Replica Data through Metro's agreement with The Replica Company, provided that they meet certain conditions and commit to uphold the business practices described in this document.

GUIDELINES

1. Metro and its Public Agency Partners should use Replica Data to inform transportation planning decisions and make the transportation system safer, more efficient, and more equitable.
2. Metro is responsible for establishing, monitoring, and enforcing business practices for use of Replica Data obtained through Metro's agreement with Replica.
3. Metro requires that the Replica Company ensure that Replica Data cannot be used in and of itself to identify individuals or their travel patterns. Metro acknowledges that research, law and public knowledge concerning data and privacy is evolving, and implements additional safeguards to ensure that Replica Data is used responsibly and that if the company does not meet this obligation risks can be quickly identified and addressed.
4. Each Replica User has a responsibility to protect privacy when using Replica Data, to protect the confidentiality and security of Replica Data, and to notify the Replica Project Manager if they have privacy concerns about the data or its use.
5. Prior to gaining access to Replica Data, each user must affirm their commitment to privacy and responsible use by reading these business practices and committing to follow and enforce them in writing.
6. Metro and its partners are testing the utility and privacy protection of Replica Data for a limited duration (one year) in order to inform future decisions about transportation data collection.
7. Metro's Research Center acts as the steward of Replica Data, and is responsible for implementing these business practices.

BUSINESS PRACTICES

Password Protection and User Access

1. Replica Data must be password-protected. Password and user management will adhere to password protection standards as defined by Metro's *Information Security policy*, and must follow current minimum standards for password complexity.
2. Replica Users may not allow others to use their login or password to access Replica data.
3. The Research Center Director will appoint a Replica Project Manager to manage access to Replica Data and implement these business practices.
4. For the Replica dashboard:
    a. Staff at Metro and Public Agency Partners are eligible for access to the Replica dashboard.
    b. Metro Public Agency Partners must execute an intergovernmental agreement with Metro committing to implement the business practices in this document and designating an Agency Lead before Metro will consider granting access to Public Agency Partner staff.
    c. Individual staff must submit requests for access to the Replica dashboard via email to the Replica Project Manager, and include:
        i. Name of the person accessing the data
        ii. Description of intended uses of the data
        iii. A signed form acknowledging and committing to uphold the business practices described in this document
    d. Access to the Replica Dashboard is subject to the Replica Project Manager's discretion. The Replica Project Manager will refer any questions about granting dashboard access to the Research Center Director.
    e. The Replica Project Manager will maintain a list of all approved Replica Users.
    f. Access to the Replica dashboard is managed by The Replica Company, which will provide each approved Replica User with a unique ID and require each user to create a password upon request from the Replica Project Manager.
    g. Metro Replica Users must notify the Replica Project Manager if they are terminating their employment with Metro or no longer require access to Replica Data.
    h. Agency Leads must notify the Replica Project Manager if Replica Users from their agencies are terminating their employment or no longer require access to Replica Data.
    i. The Metro Project Manager will promptly request that The Replica Company terminate access for any user that no longer requires it.
5. For the Synthetic Travel Database:
    a. Access to the Synthetic Travel Database is limited to selected Expert Users, who are Metro Research Center staff or other Metro staff designated by the Replica Project Manager who have well-defined use cases for the data and have the

skills and expertise necessary to conduct analysis of the database while adhering to these business practices and protecting privacy.

b. The Replica Project Manager will communicate the business practices described in this document to Expert Users and collect a signed form acknowledging and committing to uphold these business practices prior to granting staff access to the Synthetic Travel Database.
c. Access to the Synthetic Travel Database is subject to the Replica Project Manager's discretion. The Replica Project Manager will refer any questions about Expert User access to the Research Center Director.
d. The Replica Project Manager will maintain a list of all Expert Users.
e. Access to the Synthetic Travel Database is managed by Metro Information Services, which will grant Expert Users access to the Synthetic Travel Database through Metro's centralized authentication service, as described in Metro's *Information Security policy*.
f. The Metro Project Manager will monitor use of the Synthetic Travel Database by Expert Users and promptly request that Information Services terminate access for any Expert User that no longer requires it.

Data Storage

6. Metro Information Services will store the Synthetic Travel Database on a secure folder within the Metro internal file network accessible only to staff granted access by the Replica Project Manager via the "Expert User List" described above.

Electronic and Physical Media

7. The Synthetic Travel Database or any excerpt thereof may only be copied onto physical or removable electronic media or removed from secured Metro facilities with written authorization from the Replica Project Manager and the Information Services director.
8. Electronic or physical media containing Replica Data must be stored securely; labeled as confidential; and be physically retained, stored, or archived within secure Metro locations.

Code of Conduct

9. Replica Users may not attempt to use Replica Data, either alone or in combination with other data, to identify or personalize data subjects, obtain personally identifiable data or otherwise attempt to invade people's privacy, except for the purposes of ensuring that Services and Content adequately safeguard people's privacy during validation testing.

Validation Testing

10. Metro will validate Replica Data prior to applying Replica Data in transportation planning processes and projects.
11. Validation will involve reviewing documentation of the methodology and data sources used to create Replica and iteratively testing a sample of Replica Data to ensure that the

data are accurate and protect privacy, using a set of criteria that are defined in Metro's agreement with The Replica Company. Metro and its Public Agency Partners will only accept further updates to Replica Data if these criteria are met.

12. During the validation period, only Metro and two other agencies that are providing data to support the validation process – TriMet and the City of Portland – will have access to Replica Data. Access will be limited to staff from Metro, TriMet and the City of Portland who are participating in the validation process.
13. The Metro Replica Project Manager will designate Metro staff who have access to the data during the validation period, and the Agency Leads from TriMet and the City of Portland will designate staff from their respective agencies, subject to the approval of the Replica Project Manager. Consistent with the User Access practices defined above, designated staff from Metro, TriMet, and the City of Portland will have access to the Replica Dashboard and to documentation provided by the Replica Company. In addition, selected Expert Users from Metro will have access to the Synthetic Travel Database.
14. During the validation period, Metro, TriMet, and the City of Portland will not apply Replica Data in planning processes, nor publish, display, or share data except in the context of training sessions designed to prepare potential Replica Users to interact with the data.
15. The validation period will be over when the Replica Project Manager and Agency Leads from TriMet and the City of Portland agree in writing that Replica Data meets the validation criteria.

Publishing, Displaying, and Sharing Data

16. Replica Users and Expert Users may publish, share or display information derived from Replica Data for the purpose of informing public decision-making or supporting transportation and land use planning.
17. Replica Data can be published, displayed, or shared, either alone or in combination with data from other sources, under the following conditions:
    a. The data is aggregated such that each aggregation includes a minimum of three individual trip records.
    b. The data does not include the full set of attributes that are included in the Replica Data.
    c. Includes proper attribution and display of all applicable copyright, trade mark and trade secret notices.
    d. Does not otherwise compromise privacy or trade secret information.
18. Replica Users should direct any questions about publishing, displaying or sharing Replica Data to the Replica Project Manager.

Use in Combination with Other Data Sources

19. Replica Users must aggregate Replica Data such that each aggregation includes a minimum of three individual trip records before combining Replica Data with data from other sources.

Data Retention

20. Metro will retain Replica Data in accordance with Oregon Public Records Law.

Requests for Replica Data

21. The Replica Project Manager and supporting staff will help Metro Records and Information Management staff deal promptly with all Public Record Requests regarding Replica. The Replica Project Manager and supporting staff will comply with Metro's *Public Records Requests policy and procedures* and the Replica Project Manager will designate a Replica Public Records Request 'point person' under those policies to be the Replica contact for the Metro Records Officer.
22. Metro staff that receive public records requests for Replica Data or other records related to Replica will immediately notify the Replica Project Manager, the Replica Public Records Requests point person, and the Metro Records Officer.
23. Public Agency Partners that receive public records requests for Replica Data or other records related to Replica will immediately notify the Replica Project Manager and defer to Metro in responding to these requests. The Replica Project Manager will notify the Metro Records Officer immediately upon receipt of such requests.
24. In the event that Metro receives a public records request for Replica Data, the Office of the Metro attorney will document any legal restrictions that may exempt Replica Data from disclosure under Oregon law and ensure compliance with relevant third party legal agreements, working closely with the Metro Records Officer.
25. Metro will not share Replica Data with law enforcement agencies unless required by a court order.

Auditing

26. The Replica Dashboard will require users to specify their name, email, and use case before downloading data. This data will be accessible to the Replica Project Manager.
27. Information Services will maintain logs of access to Synthetic Travel Data and share these with the Replica Project Manager.
28. The Replica Project Manager will periodically audit Metro Replica Users' use of Replica Data.
29. Agency Leads must maintain logs of Replica Data use within their agencies and arrange for the Replica Project Manager to audit use of Replica Data within their agencies at the Replica Project Manager's request.

Incident Reporting and Response

30. Replica Users suspecting improper use of Replica Data, failure to follow the business practices identified in this document, or a security incident or breach of Replica Data should immediately notify the Replica Project Manager via email, and if applicable, their Agency Lead.
31. The Replica Project Manager will recommend a plan to respond to the incident. The plan must be approved by the Research Center Director and, where applicable, the Information Security and Planning and Development Directors, before implementation.

Enforcement

32. If Replica Users violate the business practices identified in this document, the Replica Project Manager will take disciplinary actions potentially including suspension or termination of access to Replica Data for the Replica User in question or, in the case of non-Metro users, for the relevant Public Agency Partner.
33. If the Replica Project Manager determines that a violation of these business practices merits disciplinary actions other than those described above, the Replica Project Manager will recommend an approach for responding to the violation. The approach must be approved by the Research Center Director and, where applicable, the Information Services and Planning and Development Directors, before implementation.

Responsibilities

Replica Users must:

- Read the Replica Data Business Practices and sign an acknowledgement of having done so in order to access Replica Data.
- Notify the Replica Project Manager and/or their Agency Lead if they are terminating their employment or no longer require access to Replica Data.
- Ensure the confidentiality of the login or password they use to access Replica Data.
- Not attempt to use Replica Data, either alone or in combination with other data, to identify or personalize data subjects, obtain personally identifiable data or otherwise attempt to invade people's privacy. Exceptions to this practice may be made only for the purposes of ensuring that Replica Data adequately safeguards people's privacy during validation testing.
- Follow relevant business practices when publishing, displaying, or sharing Replica Data to combining Replica Data with data from other sources.
- Immediately notify the Replica Project Manager or their Agency Lead if they suspect improper use of Replica Data, failure to follow the business practices identified in this document, or a security incident or breach of Replica Data. Metro Replica Users may also notify their supervisor, the Human Resources Director, or the Office of the Metro Attorney.
- Direct questions about these business practices to the Replica Project Manager and/or their Agency Lead.

The Replica Project Manager must:

- Approve Replica Users' access to Replica Data and work with the Replica Company and/or Information Services to manage access.
- Maintain records of Replica Users.
- Communicate these business practices to Replica Users and maintain records of Users' commitment to uphold these business practices.
- Audit Replica Users' use of Replica Data to ensure observance of these business practices.

- Respond to Replica Users' questions about these business practices.
- Designate points of contact within Metro for responding to Requests for Replica Data.
- Oversee the validation testing process and make a determination about whether Replica Data meets the validation criteria.
- Recommend approaches for responding to incidents and taking disciplinary action in the event that Replica Users violate these business practices.
- Refer questions about access, incident response, or enforcement of business practices to the Research Center Director.

Public Agency Partners must:

- Execute an intergovernmental agreement with Metro committing to implement the business practices in this document and designating an Agency Lead in order to access Replica Data.
- Immediately notify the Replica Project Manager of requests for public records related to Replica and defer to Metro in responding to these requests.

Agency Leads must:

- Notify the Replica Project Manager if Replica Users from their agencies are terminating their employment or no longer require access to Replica Data.
- Notify the Replica Project Manager if they suspect improper use of Replica Data, failure to follow the business practices identified in this document, or a security incident or breach of Replica Data.
- Maintain logs of Replica Data use within their agencies.
- Arrange for the Replica Project Manager to audit use of Replica Data within their agencies at the Replica Project Manager's request.
- Refer questions or concerns to the Replica Project Manager.

The Research Director must:

- Designate a Replica Project Manager.
- Work with the Replica Project Manager to resolve questions about access to Replica Data.
- Approve responses to incidents and disciplinary actions (other than termination or suspension of access to Replica Data).
- Coordinate with other Department Directors as needed to implement these business practices.

REFERENCES

Information Services: Information Security Policy

Information Services: Acceptable Use Policy

Information Services: Public Records Requests Policy and Procedures