Portland initial privacy assessment for a Technology, Project or app solution

Information	Request information
Bureau	Portland Bureau of Transportation
Assessment done by	Hector Dominguez
Date of Assessment	May 27, 2020
Name of the App or Service	**Replica**
General description	Replica is a computer simulation tool that helps customers – which include city planners, such as state and local governments – understand the movement of a population in and around a city or other location, how a population uses certain resources, and trends and other information concerning a prescribed location.
Evaluation topic	**Assessment**
Software purpose	Replica supplies customers with insights about their city that can help with transportation planning, city and neighborhood planning, parks, recreation and facility management, traffic planning, understanding real estate trends, health and human services, and other issues.
App creator name and website	Replica (https://replicahq.com)
Type of Organization	Private entity
Scope of personal data collected	Information collected about individuals from third parties includes: * Location data, including information concerning location of individuals' devices. * Purchase transation data, including information relates to transactions at certain stores, restaurants or establishments that accept payment cards.
How personal data is collected	Replica does not collect information directly from individuals in their service operation. Rather, it obtains information about individuals in connection with providing the service from data providers. Different data providers are including mobile apps, cellular vendors, WiFi and bluetooth hubs, credit card transactions. Replica also collects data from publicly available sources like the US Census and transportation and transit information. Replica does not collect minors, children and students data.
Who can access the data	Access restrictions to raw data to third party and Replica staff exists.
Purposes the data is used for	How information is used: * To create location simulations. * to operate the service. * To comply with the law. * For compliance, fraud prevention, and safety.
Where the data is stored	Replica uses industrial standards that include organizational, technical and physical safeguards designed to protect information.
How data is shared	No sharing information about individuals. To affiliates under their privacy policy To service providers on Replica's behalf under their privacy policy. To professional advisors as professional services. For compliance, fraud prevention and safety on business transfers.
How long is the data stored?	Data from individuals gets regularly deleted when it is not longer needed to provide the service, except as prohibited by law. It is not specified on what periodicity if any.
Effectiveness	As raw data is transformed into a synthetic environment, the service requires larger sample sizes to become more accurate. ML models may infer social patterns not collected originally. This feature may expose personal or collective social behavior. Replica requires multiple filtering features and proprietary algorithms to identify cases of abnormal individual trips or expose minors data. Losing data sources may reduce algorithms accuracy. data requires calibration that takes time and its performance impacts accuracy, requiring more raw personal data. Data accuracy may change by the season or anomalies like the current public health crisis. This may demand more collection of personal data. Complex mobility models may not be accurate when using synthetic data and more personal information may be needed.

Proportionality, fundamental rights, and data protection and privacy issues	Replica uses reasonable approach for collecting personal data for the service they provide. However, the right to provide consent is delegated to data brokers that collect raw data from different sources. It is argued that users 'opt-in' when using geolocation services. This is a broad statement, as different geolocation services may have different terms and conditions and privacy policies. Also, it is not specified what kind of 'opt-in' services users are agreeing to. Even though there might be an option for opting out of some mobile services. This might be difficult for users with low digital literacy or using devices constrained by the service providers or manufacturers. There is a claim that data vendors are audited by Replica for consent, personal metadata and minors data. It is not clear if those audits are available to third party auditors or the public. Once replica has access to individuals data, it implements reasonable privacy protection measures above to industrial standards.
Privacy safeguards	Using a proprietary synthetic population approach to de-identify individual data. Different industrial standard processes to de-identify personal information. Do not share individual information to customers Do not receive data about all of the individuals in a city or location. Location data about individuals with unique travel pattern is not included.
Open source	No
AI/ML claims	Yes
Privacy Policy (link)	(as accessed on 5/27/2020) https://drive.google.com/file/d/1QsRP1O8duLuf4qUdkUicNx5J4X4aJzeQ/view This privacy policy is missing the mandatory contact information.
Privacy risk	Yes
Portland Privacy Principles (P3)	
Data Utility	There is no enough transparency to determine the minimum amount of personal information for the purpose of Replica.
Full lifecycle stewardship	The privacy policy and provided documentation show implementation in each step in data lifecycle.
Transparency and accountability	The app is closed and under intellectual property protection. It is not clear if audits are public and available to customers. Privacy terms are transfer to data brokers that source raw data.
Ethical and non-discriminatory use of data	There is no mention of ethics or non-discriminatory use of data or privacy rules.
Data openness	Closed app.
Equitable data management	Not mention of any social equity value.
Automated Decision Systems	Closed app and there is general mention of algorithms used in the system. Details are not available to the public due to intellectual Property protection.
Optional	
Consent	There is a mention to having the ability from individual that get their data collected having the ability to opt-in. However, it is an independent process from the owner of the app and in general opting-out is a feature that depends on data providers.