PBOT: Streetlight Data

Privacy Impact and Risk Analysis

Released version

Smart City PDX

January 17, 2025

PRIVACY ANALYSIS REPORT

City of Portland Privacy Toolkit

WHAT IS A PRIVACY IMPACT ASSESSMENT?

A Privacy Impact Assessment ("PIA") is a method to quickly evaluate the general privacy risks of a technological solution or a specific use, transfer, or collection of data to City bureaus or offices. The PIA is a way to identify factors that contribute to privacy impacts and risks and lead to proper strategies for risk mitigation or alternatives that may even remove those identified risks.

The Privacy Impact Assessment may lead to a more comprehensive Surveillance Assessment depending on the level or risks identified and the impacts on civil liberties or potential harm in communities.

In the interests of transparency about data collection and management, the City of Portland has committed to publishing all Privacy Impact Assessments on an outward facing website for public access. PIAs do not include specific uses of technology or data other than those initially evaluated.

WHEN IS A THRESHOLD PRIVACY IMPACT ASSESSMENT RECOMMENDED?

A PIA is recommended when:

- A project, technology, data sharing agreement, or other review has been flagged as having some privacy risk due to the collection of private or sensitive data.
- A technology has high financial impact and includes the collection, use or transfer of data by city bureaus or third parties working for or on behalf of the city.

HOW TO COMPLETE THIS DOCUMENT

A PIA consists of two sections:

- *The Privacy Analysis.* This portion identifies all important information related to the project description, data collection, use, safekeeping, and management; as well as a verification of existing privacy policies and measures to protect private information. This report is a summary of the analysis.
- *The Comprehensive Privacy Risk Assessment.* This portion breaks the privacy risk into six different Risk Types of evaluation: (I) Individual Privacy Harms; (II) Equity, Disparate Community Impact; (III) Political, Reputation & Image; (IV) City Business, Quality & Infrastructure; (V) Legal & Regulatory; and (VI) Financial Impact. It then compares those risks to their likelihood of occurring to create a single risk measure based on the worst-case scenario.

Executive Summary

This document presents the results of the privacy impact assessment of Streetlight Data for the Portland Bureau of Transportation (PBOT) and users from the Bureau of Planning and Sustainability.

The purpose of this project is to gather mobility analytics to make data-driven transportation decisions that reduce congestion, improve safety, and maximize the investment in infrastructure.

Streetlight Data is a SaaS Big Data analytics platform that sheds light on how vehicles, trucks, pedestrians, trains, and bikes move by applying proprietary machine learning algorithms and statistical techniques to a vast amount of contextual and location data obtained from government and industry partners.

The main identified risks are individual re-identification, potential targeting locations where vulnerable groups connect, and risk of using this geolocation services for other purposes. If the datasets are released there is a chance that individuals can be reidentified by their indirect identifiers despite being deidentified (e.g., home, work, other commonly visited places).

A vendor data leak would make this reidentification likely. If the vendor has a data leak, millions or more of these data points could be exposed.

The identified safeguards are purpose limitation, data minimization, deidentification, access limitation, and security controls. The vendor provides some privacy safeguards by limiting information queries, the minimum area of request, and aggregating mobility trips.

We also recommend the limiting of further sharing, limiting access to the datasets, logging queries to the system to provide better transparency and oversight, and creating tools for the project to limit public exposure of data.

For reducing the number of public records requests, we recommend creating a public dashboard with aggregated information describing how it is used and informing how information gets protected.

Highest risk is ‘Risk of inference and reidentification’ which is high impact but unlikely and based on the risk matrix, it represents medium to high risk. This risk is limited by the existing built-in restrictions to access queries of information in a 100 by 100 meters area and aggregating anonymized results.

Risk area	Risk level determined	Highlighted risks
Individual Privacy Harms	Medium	Risk of inference and reidentification
Equity, Disparate Community Impact	Medium	Risk of inaccurate demographic representation (e.g., race, ethnicity, income, etc.) Risk of targeting location and times where vulnerable groups or communities gather periodically.
Political, Reputation & Image	Medium	Risk of using this service for other use cases that are not initially considered.
City Business, Quality & Infrastructure	Medium	Risk that data delivered to the City will not match ground truth.
Legal & Regulatory	Medium	Risk of privacy breaches due to unclear privacy policies
Financial Impact	Low	Risks of hidden services costs

Privacy Analysis

Purpose of the technology, project, data, data-sharing, or application

The purpose of the project and technology is to gather mobility analytics to make data-driven transportation decisions that reduce congestion, improve safety, and maximize the investment in infrastructure. Streetlight's product is designed to give data-driven analytics of transportation patterns so local and state agencies can make informed decisions about budgets and development priorities, transportation equity, and the environmental impact of transportation.[1]

Data Lifecycle

The list consists of location-based services on smartphones, connected vehicles data, GPS data, commercial truck data, thousands of sensors, land use data, parcel data, census characteristics (e.g., demographics, vehicle ownership, housing density), and OpenStreetMap (OSM). These data are deidentified before being given to Streetlight Data for cleaning, quality assurance, privacy checks, and for other processing. It's then available for its users as mobility statistics only (output), not individual data points (input).

City employees will be able to view aggregated statistics that sketch the movement of groups. For example, a quote taken from Streetlight Data website about their work in Portland, Maine, discusses their aggregation method: "of all the trips that crossed the Casco Bay Bridge in all 2018, X% were going to destinations in Meeting House Hill."[2]

StreetLight's Metrics are primarily derived from the following list[3]:

- Connected Vehicle Data (CVD)
- GPS data
- Commercial truck data for a range of weight classes
- Location-based services (LBS) mobility data
- Thousands of vehicular, bicycle and pedestrian sensors
- Land use data, parcel data
- Census characteristics (e.g., demographics, vehicle ownership, housing density)
- Road network and characteristics from OpenStreetMap (OSM)

---

[1] https://www.streetlightdata.com/big-data-privacy-in-maine/
[2] idem
[3] StreetLightData Sources and Methodology White Paper, December 2022 (consulted October 2024) https://learn.streetlightdata.com/hubfs/White%20Papers/Methodology%20and%20Data%20Sources/StreetLight%20Data_Methodology%20and%20Data%20Sources.pdf

Name of the entity owner of the application and website

Streetlight Data, inc.

Type of Organization

Private Entity

Scope of personal data collected. List all sources of data and information.

Sources
There are hundreds of data sources or suppliers that contribute to Streetlight Data's Service. They transfer data in bulk in secure cloud environments.

Scope Of Personal Data
Personal data is not collected by Streetlight Data or the City of Portland ("the City"). All data the vendor processes (e.g., obtains, analyzes, create statistics from) has been deidentified. Mobility Information is obtained by Streetlight Data and made available for the City as statistics. Any personal information will be aggregated and obfuscated to limit the possibility of identifying any single individual.

If location data can be reasonably linked to a consumer or consumer's device, then it's considered personal data. If location data is deidentified, then it is no longer considered personal data under the Oregon Consumer Privacy Act (OCPA).[4]

Suppliers give data to Streetlight Data after removing identifiers, then Streetlight Data gives its users aggregated statistics— another level of deidentification. It not entirely clear whether the data Streetlight holds can be used to reidentify someone. Either way, the City will not attempt to deidentify an individual under contract with the vendor.

Travel modes include: All Vehicles, trucks, bicycles, pedestrians, bussed and rail. See https://developer.streetlightdata.com/docs/available-metrics-1

This project details a subscription for PBOT to StreetLight insight. The Safety Data Essentials and Transportation modeling subscription allows to run an unlimited number of StreetLight Data's InSight analyses during the year within the limited geographic region around Multnomah County. Use will be subject to standard StreetLight End User License Agreement.

[4] https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/privacy/

Analysis includes the table below.

Planning solutions	Features included	Modes included
Safety data essentials	Traffic volume by day part and day type Segment and area level VMT Speed Travel time Vehicle hours of delay	All vehicles and trucks
Transportation modeling	Areal level VMT Origin-destination Origin-destination through a middle filter Trips to or from preset geographies	All vehicles and trucks

"Traveler attributes" are provided in bins for travelers in a zone, so not reported as individual data. The zones[5] request body property is a GeoJSON feature collection where the features are either MultiPolygons or LineStrings.

For U.S. 2020 Census:

- Equity Demographics:
  - The self-identified race and ethnicity of individuals in a household
  - The self-identified birthplace of individuals in a household
  - The self-identified English proficiency of individuals in a household
  - The self-identified disability status of individuals in a household
- Education/Income
  - The combined gross income in USD of all members of a household who are 15 years or older.
  - The highest level of education completed by individuals in a household
- Household Characteristics
  - The structure of the family in a household
  - The housing type for a household
  - The housing tenure for a household
  - The vehicle ownership for a household
- Employment Characteristics
  - The employment industry or occupation of individuals in a household
  - The employment class of individuals in a household, such as private or military

Traveler Attributes are not available for all query types and/or time periods. It's primarily available for zone related queries such as Origin-Destination (OD) analysis, Zone Analysis, etc. This is because of the area-based census data (tracts, etc.) which does

[5] https://developer.streetlightdata.com/docs/creating-zones

not apply to roadway segments easily. Within the OD analysis queries certain time periods do not have traveler attributes available. They are currently available in 2024 Connected Vehicle Data+ (CVD+) and 2019-2022 using the old location-based services (LBS) data.

How personal data is collected

Anonymized personal data is collected from Streetlight Data's industry partners by several avenues including connected vehicles and location-based services on smartphones. The city does not obtain or have access to personal data.

Frequency of Collection

Collection is made daily, weekly, and monthly.

Who can access the data?

The City has allowed 10 city employees to access the mobility statistics. This service will be only accessible to the Portland Bureau of Transportation (PBOT) and the Bureau of Planning and Sustainability (BPS)'s climate change and Portland Clean Energy Fund (PCEF) staff.

Where is the data stored?

Data is stored on Streetlight Data's cloud.

How data is shared

Data is accessed by the City via the web through an API.

How long is the data stored?

Data queried from the application is not stored on City servers and has limited applications by the user agreement with the vendor.

Effectiveness

The vendor offers several whitepapers and third-party validations attesting to the accuracy of their product.[6]

Privacy safeguards

1. Purpose limitation

[6] https://www.streetlightdata.com/whitepapers/

- Under contract, data products and subscription are used only for governmental transportation planning and operational analyses, and it should not be used for reidentification. [7]

2. Data minimization
    - PBOT and StreetLight Data Limit agreed that the sharing of statistics from Streetlight Data to PBOT and BPS is limited to only safety data and transportation modeling.
    - If zones or polygons on maps are too small, the zone will be flagged for review.
3. Deidentification
    - Vendor makes data suppliers deidentify the raw data, then vendor creates statistics that obscures individuals.
    - Streetlight Data employs a series of multi-step multi-layered technical safeguards including automated privacy and coverage checks that ensure sufficient aggregation based on dimensions such as time, space, and land use. [8]
4. Access Limitation
    - Only a small number of individuals at PBOT and BPS can access the statistics.
5. Security
    - Suppliers of data transfer in bulk in secure cloud environments.

AI/ML claims
Machine learning is used to filter erroneous data among other statistical purposes.

Privacy Policy link
StreetLight data does not offer a privacy policy; instead, the company offers data privacy principles. The company also offers a contact email for privacy issues
privacy@streetlightdata.com
https://www.streetlightdata.com/streetlight-data-privacy-principles/

Surveillance Technology
Yes.

Open source
No.

Proportionality and Necessity

---

[7] "Streetlight grants to Customer, for the subscription term specified in the applicable Order, a non-exclusive license to access and use the Data Products and Subscribed Output solely for governmental transportation planning and operational analyses" (MDAA)
Users (i.e., the City or PBOT) shall not use this tool for reidentification or attempt to use the platform to identify any specific person (MDAA)

[8] https://www.streetlightdata.com/big-data-privacy-in-maine/

“Proportionality and Necessity” refers to the balance of whether the means of collection and the data collected are proportional to complete a specified aim, that is, not collecting, retaining, or sharing more information than necessary to obtain statistics for transportation decisions. It is also important consider if there are less intrusive but equally effective ways to complete a specified aim. A technology could be said to be “proportional”, and the data processed “necessary”, if the data used does not process more information than necessary to complete its aim.

There may be a less intrusive avenue for collecting transportation data, however, manually collecting data for transportation analytics in Multnomah County may take months and may not be as accurate. The manual route, if pursued, could give a sketch of transportation but only for as long as the project is active. Retroactively collecting data could prove difficult. This tool has evidence of its accuracy, and it will take less time to obtain the necessary statistics for mobility decisions. Given that Streetlight Data has robust deidentification controls, the value of the vendor’s product will give PBOT the confidence to make data-driven transportation decisions.

Portland Privacy Principles (P3)

Data Utility*: All Information and Data processes must bring value to the City of Portland and the communities the City serves. The City will collect only the minimum amount of Personal Information to fulfill a well-defined purpose and in a manner that is consistent with the context in which it will be used.*

The City will not collect personal information, but in the spirit of the principle we are using only a portion of the data statistics available. We will not have available demographic information or traveler attributes such trip purpose, income, education, race, ethnicity, or household. Instead, we will have available speed, volume, travel time, origin destination, and trip to or from preset geographies limited to just vehicles and trucks not cyclists or pedestrians.

These metrics will be used for transportation decisions that will contribute to safer, more efficient streets and greater utility on infrastructure investment. These statistics could help with altering roads to create a more bicycle friendly city, inform road construction and repairs, create safer intersections and cross walks, reduce traffic, or a slew of other benefits.

Full Lifecycle Stewardship*: Data, Metadata and Information will be secured and protected throughout its life cycle. That includes collection, storage, use, control, processing, publication, transfer, retention and disposition*

Data is processed according to Streetlight security and privacy standards while under Streetlight’s domain. The API that allows for data sharing should be reviewed to ensure

security and privacy. Processing under PBOT's domain must be reviewed to ensure that no unauthorized aggregated statistics are released. Statistics should not be held for longer than required by the City's records retention policies without a specified purpose, and such purpose should be shared with stakeholders.

Transparency and accountability*: How the City uses, manages and collects information is described clearly, accurately, and shared in an accessible way. Who creates, contributes to, and has access to that information is also clearly documented and communicated to all people who entrust city government with their data and information.*

The users of the tool will be limited, but the names of the users could be shared via a website or external facing avenue to increase accountability. Policies about the tool's management could also be shared.

Ethical and Non-Discriminatory Use of Data: *The City of Portland has an ethical responsibility to provide good and fair stewardship of data and information, following existing non-discriminatory protections, and commits due diligence to understand the impacts of unintended consequences.*

The data should be used for equitable benefits, not preferring specific groups or excluding specific groups. Our agreement with Streetlight largely uses vehicle and truck data so it could be assumed that most projects will be used to benefit those with vehicles and the logistics of trucks, however, these data certainly do not bar the benefit of the tool for cyclists and pedestrians. Decisions based on mobility analytics should be limited to only mobility decisions and further these mobility decisions ought to be ethical and non-discriminatory. Ethical and non-discriminatory decisions could be explored further as it relates to transportation decisions. Examples of unethical transportation decisions include the building of Dodger Stadium in Los Angles, or railroads and highways cutting through lower-income and BIPOC communities.

Data Openness: *Data, metadata and information managed by the City of Portland -- and by third parties working on behalf of the City -- that are made accessible to the public must comply with all applicable legal requirements and not expose any confidential, restricted, private, Personal Information or aggregated data that may put communities, individuals, or sensitive assets at risk.*

Data the City receives and has access to will be aggregated so the risk of reidentification of a single individual will be lower, however, without aggregation there is still a risk that auxiliary data sets or other information could be used to identify Individuals or predict future movements based on the previous movements of individuals.

Setting formats and contracts aside, If the data the City has access to was released, despite being aggregated, it may be a risk to privacy because of the sensitivity of location data. The privacy of individuals, in this case, competes with the communal benefits of the project. However, this is not to say that the City should not release transportation statistics in controlled, deliberate and privacy-focused manner. The API output could be aggregated (if open data is a dashboard), or polygons could be limited to a larger area preventing reidentification by community members along with other measures.

On a separate level, an open data model could share data regarding this project—metainformation, such as how long we have had the contract, how much this project costs annually or totally, what projects have come about because of this vendor's product, or what other projects this product has aided with by providing decision-makers mobility statistics.

Equitable Data Management: *The City of Portland will prioritize the needs of marginalized communities regarding data and Information management, which must be considered when designing or implementing programs, services, and policies.*

Current policy includes the city's contractual obligation to not reidentify individuals and a cap to the number of users of Streetlight's product. Because this product is exploratory in nature with little to no contact with community members (e.g., gathering survey information directly from community members), preemptive outreach could be done surrounding comfort levels, suggestions for transportation improvement, and raise awareness of data sharing agreements between phone applications, vehicle companies, and data brokers. With some outreach and transparency actions the City could increase the likelihood that our use of Streetlight's product will be used in a way that is equitable and consistent with the needs and interest of our community. Additional actions and policies that promote equity could be done following its procurement as well, however, these actions will need to be ideated, written and approved.

Automated Decision Systems*: The City will create procedures for reviewing, sharing, assessing, and evaluating City Automated Decision System tools -- including technologies referred to as artificial intelligence -- through the lens of equity, fairness, transparency, and accountability.*

There are no automated decision systems in this project or technology.

Privacy Impact Risk Severity Assessment

WORST CASE SCENARIO	Medium

Baseline (B): (T) – Technology level, (U) – use and application level.

Risk type (RT): (I) Individual Privacy Harms; (II) Equity, Disparate Community Impact; (III) Political, Reputation & Image; (IV) City Business, Quality & Infrastructure; (V) Legal & Regulatory; and (VI) Financial Impact.

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
U	I	1.1 Risks due to unauthorized data sharing of PII.	Low	Unlikely	On the vendor side, there are two sets of data: 1) unaggregated but deidentified data not shared with PBOT and 2) aggregated deidentified data shared with PBOT In all cases where personally identifiable information is not provided by the data service directly.	Low
T	I	1.2 Risk of inference and reidentification	High	unlikely	This case is interesting because no PII is collected but it can link location data with individuals. There exists some risk to reidentify information or patterns of mobility, then inferring the identity of individuals. The City receives aggregate data from more granular information about the locations of individuals. The vendor provides data with a minimum area of 100 by 100 square mts; which it is about a small block. Given the relatively small area, some blocks may only include few households or facilities of importance to specific community groups, like public health buildings, religious spaces, schools, critical infrastructure like substations or hazardous materials facilities. The vendor data service restricts queries and access to data and models. Limiting the information that can be accessed by the bureau.	Medium

T	I	1.3 Transparency Risk from not giving sufficient notice	Low	Likely	The City has the responsibility to be transparent on how this data is used and procured. The City gets this geolocated data from a vendor that aggregates and anonymized data from different sources. It could be the case that many of the individuals whose data points are inputs into this product do not know that their information is being used in this way. Because suppliers deidentified and sold the information that represented the locations of individuals, community members of Portland and other locations do not have the right to know or other rights regarding their data. To mitigate this risk, recommendations include: properly informing the public about the use and benefits from this product. Create publicly accessible open data dashboards with open data from how the platform is used and from analysis perform by the bureau. For reducing the number of public records requests, we recommend creating a public dashboard with aggregated information describing how it is used and informing how information gets protected.	Low
T	I	1.4 Risk of using data for other purposes.	Moderate	Possible	Potentially, other agencies may have access to this data and services. Mitigation of this risk must include proper oversight and supervision of information access activity and appropriate training on privacy and information protection of operators. Keep access logs up to date and within regular supervising schedules. This allows audits that can identify further risks or any potential breach.	Medium
U	I	1.5 Risk of under protecting private and sensitive information	Moderate	Possible	Privacy protections are loosely defined by the vendor's data privacy principles and do not describe how data is used and shared internally and with third parties. Information about consent or integrity and quality of data collected via 'opt-in' apps are not available as well. https://www.streetlightdata.com/streetlight-data-privacy-principles/	Medium

					Extensive revisions in the contract with the vendor should include all the privacy and information protection measures required by the City.	
T	II	2.1 Unethical or discriminatory mobility decisions	Moderate	Possible	Unintentionally, this service could be surveilling specific group on behalf of good intentions. A case could be monitoring mobility patterns of low-income neighborhoods with no consent or proper information, which can be perceived as surveillance and oppression. Mitigation strategies should include meaning engagement process with communities that are subject of analysis and programs impacts. Correlate proper demographic and socio-economic metrics that represent the residents that are intended to be represented. Also, include these equity metrics as part of the mobility analysis.	Medium
T	II	2.2 Risk of inaccurate demographic representation (e.g., race, ethnicity, income, etc.)	Moderate	Possible	This risk and impacts depend on the equity assessment and the type of equity data collected to validate representation. This risk is more impactful when used for major decisions like social capital investments. Intrinsic bias or inaccurate data may create more harm. Information is from the US Census and other publicly available information may not provide enough resolution to specific mobility patterns. Ground truth validation might be required for matching socio-economic and other demographics information.	Medium
T	II	2.3 Risk of identifying location and times where vulnerable groups or communities gather periodically.	High	unlikely	Collecting this information may identify specific groups, including their patterns and activities. This could include areas, community spaces, health centers, locations for worship, entertainment, and regular gatherings. The Bureau needs to be aware that creating queries around these areas should be identifies and, when possible, inform those groups and communities about the analysis done by the agency.	Medium
T	II	2.4 Risk of missing specific groups not being tracked by electronic devices.	Moderate	Possible	It is uncertain the amount of people who are not tracked by devices. These groups include children, people experiencing homelessness, elderly people, and others who have turned off geolocation features.	Medium

					Decisions involving this data should consider these groups that are not counted by the aggregation of information coming from mobile devices and other systems tracking people's mobility.	
T	III	3.1 Risk of image or reputation damage due to misuse of the technology.	High	Possible	To mitigate this risk, supervisors need to verify proper use of the technology, including any unauthorized access, data sharing, or use different from the original intended use. Lack of consent from collection of data impacts the relationship between the City and Portlanders. The City needs to be able to justify that harms are mitigated or avoided within the possibilities, and that the benefits fully justify the use of this data services.	Medium
U	III	3.2 Risk of reducing public trust due to overexposing significant locations for specific communities.	High	Possible	The risk of creating geofencing locations on places of interest that may seem questionable to some, and tracking mobility data may discover patterns that tag specific groups or other locations. Certain communities are more concerned about their cellphone data used to identify homeless camps that are "off grid" (for example in the woods, industrial or PBOT land, or places where most people would not expect to find frequent or sustained cellphone density). Similar fears of community tracking from people represented by groups covered by Title VI, and by the LGBTQ2IA+ communities, or to track protesters after a demonstration, users of a specific clinic, activists, refugees, undocumented immigrants, etc. To mitigate this risk, try to build safeguards on these sensitive locations or communities. Verify the use before doing any data query.	Medium
U	III	3.3 Risk of reducing public trust due to applications and use cases that are not initially considered.	Moderate	Possible	PBOT has specific initial uses for tracking mobility patterns that include vehicle mobility planning, transportation of people, goods, and transit, and identify people mobility patterns for reduction of carbon emissions and better planning in general. There is public concern when agencies use information, particularly when information is used without transparency or accountability. Certain geolocation and geofencing applications by law enforcement may create stress to communities under social stress or that have been historically targeted by government agencies.	Medium

					Limitation and logging of access either by the vendor or the agency can mitigate this risk and create more transparency to the public. Report methods and areas analysis to the public. Include the purpose and how privacy is safeguarded.	
T	IV	4.1 Privacy breach risk.	Moderate	rare	A meaningful privacy breach can happen when sensitive information gets released without proper authorization. In this case, sensitive locations can generate data and derivative products like mobility patterns, personal home addresses, health clinics, places of worship, schools, or community centers. Also, some sensitive data can also be generated from public demonstrations or mass events.	Low
T	IV	4.2 Risk that data delivered to the City will not match ground truth.	Moderate	possible	Geolocation systems may rely on aggregating data and building models from different sources. The City needs to validate information by matching results with other trusted service or by doing manual counts of mobility events, known as 'ground truth'.	Medium
U	V	5.1 Risk of privacy breaches due to unclear privacy policies	Moderate	Possible	The vendor does not have a privacy policy that clearly documents how information is collected, used, transform, and shared. The City needs to include all the required privacy legal clauses in the specific vendor contract or agreement. Work with the City Attorney's Office to determine the best alternatives.	Medium
U	V	5.2 Risk due to privacy or sensitive information breach.	Moderate	rare	Geolocation data has a big risk when directly linked to a specific individual or group, particularly if there are specific harms potentially created from this tracking. This includes people at risk of domestic or street violence, undocumented immigrants, gender non-conforming individuals, women seeking abortion support and professionals providing those services. The City needs to identify those locations of significance or potential sensitivity for a group.	Low
T	VI	6.1 Risks of hidden services costs	Low	Possible	Certain data services are designed in tiers, where basic levels only allow access to basic data; while more useful or required data or derive information might be available only in premium tiers of service.	Low

T	VI	6.2 Risk of vendor dependency or vendor-lock	Moderate	possible	There is an intrinsic risk where models and decision-making processes may depend on a specific vendor infrastructure or proprietary technology. In this case, geolocation and geofencing services can be built based on use cases and making sure to use general data and either own analytics models or require transparency from vendor.	low

Appendix A
Privacy risk assessment framework

Severity (Evaluate for the worst / highest possible impact)				
	A: Low	**B: Moderate**	**C: High**	**D: Extreme**
Individual Privacy Harms	Customer or "telephone book" information collected and could be disclosed (excluding utility customer data, protected by RCW)	Potential disclosure would be limited to non-financial, non-health related information; no personal identifiers (e.g., social security and driver's license #s)	Financial or other highly sensitive information would be collected and disclosable requiring action to remediate negative effects (example: non-HIPAA health data); i.e., credit report management required	Disclosure would result in extreme privacy impacts to highly regulated information; catastrophic public release of financial and personal information requiring credit report monitoring and other remediation
Equity, Disparate Community Impact	Little or no equity impact, technology delivered uniformly without reference to individuals or demographic groups	Accidental or perceived disparate impact to communities by nature of location of technology or service delivered	Intentional disparate equity impact resulting in community concern resulting in privacy harms, media coverage; loss of reputation, legitimacy and trust impacted	Extreme impacts to community, City experiences national media attention; widespread public concern and protest; significant breakdown in business processes associated with damage control
Political, Reputation & Image	Issues could be resolved internally by day-to-day processes; little or no outside stakeholder interest.	Issues could be raised by media and activist community resulting in protests and direct community complaints	Disclosure would likely result in heavy local media coverage; reputation, legitimacy and trust impacted	Likely national and international media coverage; serious public outcry; significant breakdown in business processes associated with mitigation and damage control
City Business, Quality & Infrastructure	Management of disclosure issues would represent negligible business interruption; resolved with no loss of productivity	Issue management would result in brief loss of services; loss of < 1 week service delivery; limited loss of productivity	Significant event; loss of > 1–3-week loss of services; critical service interruption to delivery of infrastructure services	Extreme event; business collapse for department services; loss of > = 3 months of data or productivity; critical business infrastructure loss > 1 month
Legal & Regulatory	Adverse regulatory or legal action not indicated or highly unlikely	Relatively minor incident, regulatory action unlikely; possible legal intervention or consultation for addressing data exposure or loss	Adverse regulatory action likely – i.e., fines and actions associated with CJIS, HIPAA, PCI, NERC, COPPA violations, etc.	Major legislative or regulatory breach; investigation, fines, and prosecution likely; class action or other legal action

Financial Impact	$0-$500 impact; internal costs covered, and no significant external costs incurred	>$500 - $5,000; internal and external costs associated with legal consultation, system rework, overtime	> $5,000 -$50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime	> $50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime

Likelihood Analysis

For assessing probability of risks

Likelihood	Probability
Almost certain	Likely to occur yearly
Likely	Likely to occur every 2 years
Possible	Likely to occur every 5 years
Unlikely	Likely to occur every 10-20 years
Rare	Has never occurred

Risk Matrix

	Low	**Moderate**	**High**	**Extreme**
Almost Certain				**High**
Likely				
Possible		**Medium**		
Unlikely				
Rare	**Low**			

Appendix B
Definitions

Automated Decision System	A process, set of rules, or tool based on automated processing of data to perform calculations, create new data, or to undertake complex reasoning tasks. This includes advanced methods like artificial intelligence and machine learning, visual perception, speech or facial recognition, and automated translation between languages.
Data	Statistical, factual, quantitative, or qualitative information, in digital or analog form, that is regularly maintained or created by or on behalf of a City bureau and is in a form that can be transmitted or processed.
Data Governance	Definition of policies, processes and framework of accountability to appropriately manage data as a strategic asset.
Digital Age	This current era whereby social, economic and political activities are dependent on information and communication technologies. It is also known as the Information Age or the Digital Era.
Information	Information is the result of Data being processed, organized, structured or presented, allowing it to be used and understood.
Information Protection	A system of Data processing practices related to personally identifiable or identifying Data for the protection of privacy. This includes the management of individual pieces of personal Information, securing Data against unauthorized access, corruption or loss.
Metadata	A set of Data that describes and gives information about other Data, including its description, origination, and accuracy.
Open Data	Data that can be freely accessed, used, reused and redistributed by anyone.
Personal Information	Information about a natural person that is readily identifiable to that specific individual. “personal information,” which include, but are not limited to: • identifiers such as a real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers; • payment card industry such as bank account numbers or access codes; • personal health data, such as health history, symptoms of a disease, current health care information, medical device identifiers and serial numbers; • commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies; • biometric information; • internet or other electronic network activity information, that includes browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement; • geolocation data, vehicle identifiers (including serial numbers and license plate numbers); • audio, electronic, visual, thermal, olfactory, or similar information; • professional or employment related information; • education information, provided that it is not publicly available; and • inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes
HRAR 11.04 Protection of Restricted and Confidential Information	

Privacy	The ability of an individual to be left alone, out of public view, and in control of information about oneself.
Confidential	Information that is made confidential or privileged by law or the disclosure of information that is otherwise prohibited by law or City policy.
Restricted	Some restrictions or limitations on the use of or disclosure of the information.
Principle of proportionality	The principle of proportionality requires that the processing of personal information must be relevant to, and must not exceed, the declared purpose
Surveillance Technologies	technologies that observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.
Privacy terms	
Effectiveness	This refers to how a specific technology or solution fulfills the pursued objective.
Proportionality	Proportionality is a privacy principle that personal data collected and processed should be adequate, relevant, and limited to that necessary for purpose processed. Proportionality has multiple dimensions. Data collected and used should be adequate, because collecting too little information may lead to incorrect or incomplete information on a data subject. It should also be relevant and limited to what is necessary in relation to the purposes for which it is collected and processed ('data minimization'), both in terms of scope and time (data retention). The proportionality principles consideration of the amount of data to be collected. If excessive data is collected in relation to purposes, then it is disproportionate. Examples: Using biometric data like fingerprints to identify individuals when identity cards would suffice.
data protection	Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes. Data protection is also known as data privacy or information privacy. Data protection should always be applied to all forms of data, whether it be personal or enterprise. It deals with both the integrity of the data, protection from corruption or errors, and privacy of data, it being accessible to only those that have access privilege to it.
Frequency of the collection	Periodicity of the data collection.
Privacy safeguards	Measures designed to improve privacy and information protection. It can be represented as below, as, or greater than industry standard and best practices
privacy fundamental rights	Privacy fundamental rights are set to help individuals in being assured of the protection and privacy of their personal data. The General Data Protection Regulation contains a set of 8 privacy fundamental rights. These rights are not legally binding in the US.
Right to information	This right provides the individual with the ability to ask for information about what personal data is being processed and the rationale for such processing. For example, a customer may ask for the list of processors with whom personal data is shared.

Right to access	This right provides the individual with the ability to get access to personal data that is being processed. This request provides the right for individuals to see or view their own personal data, as well as to request copies of the personal data.
Right to rectification	This right provides the individual with the ability to ask for modifications to personal data in case the individual believes that it is not up to date or accurate.
Right to withdraw consent	This right provides the individual with the ability to withdraw a previously given consent for processing of personal data for a purpose. The request would then require stopping the processing of personal data that was based on the consent provided earlier.
Right to object	This right provides the individual with the ability to object to the processing of their personal data. Normally, this would be the same as the right to withdraw consent if consent was appropriately requested and no processing other than legitimate purposes is being conducted. However, a specific scenario would be when a customer asks that their personal data should not be processed for certain purposes while a legal dispute is ongoing in court.
Right to object to automated processing	This right provides the individual with the ability to object to a decision based on automated processing. Using this right, a customer may ask for this request (for instance, a loan request) to be reviewed manually, because of the believe that automated processing of the loan may not consider the unique situation of the customer.
Right to be forgotten	Also known as right to erasure, this right provides the individual with the ability to ask for the deletion of their data. This will generally apply to situations where a customer relationship has ended. It is important to note that this is not an absolute right and depends on your retention schedule and retention period in line with other applicable laws.
Right for data portability	This right provides the individual with the ability to ask for transfer of his or her personal data. As part of such request, the individual may ask for their personal data to be provided back or transferred to another controller. When doing so, the personal data must be provided or transferred in a machine-readable electronic format.

Privacy risk	The term “privacy risk” means potential adverse consequences to individuals and society arising from the processing of personal data, including, but not limited to: 1. Direct or indirect financial loss or economic harm; 2. Physical harm; 3. Psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma; 4. Significant inconvenience or expenditure of time; 5. Adverse outcomes or decisions with respect to an individual’s eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services; 6. Stigmatization or reputational harm; 7. Disruption and intrusion from unwanted commercial communications or contacts; 8. Price discrimination; 9. Effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity assessing privacy risk, that significantly: A. Alters that individual’s experiences; B. Limits that individual’s choices; C. Influences that individual’s responses; or D. Predetermines results; or 10. Other adverse consequences that affect an individual’s private life, including private family matters, actions and communications within an individual’s home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used. 11. Other potential adverse consequences, consistent with the provisions of this section, as determined by the Commission and promulgated through a rule.
Risk of individual privacy harms	The likelihood that individuals will experience harm or problems resulting from personal data collection and processing
Risk of equity, disparate community impact	The likelihood that specific groups will experience harm or problems resulting from the collection of multiple sources of personal data and their processing.
Risk of political, reputation & image issues	The likelihood that collection or processing of private data may result in harm on professional or personal relationships, harm in reputation or image.
Risk of city business, quality & infrastructure issues	The likelihood that the collection or processing of private data may impact or expose city relationships, agreements, or any other contract, or the quality of those businesses, or built infrastructure
Risk of legal & regulatory issues	The likelihood of any violation of existing laws or regulations by the collection or processing of private information
Risk of financial Impact	The likelihood that ongoing costs in management, collection or processing of private data may become financially inviable or present costs that may not be considered