Automatic license plate readers for parking enforcement

Initial Privacy Assessment

Delivered

Smart City PDX

01-27-2021

INITIAL PRIVACY ASSESSMENT REPORT

City of Portland Privacy Toolkit

WHAT IS THE INITIAL PRIVACY ASSESSMENT?

The Initial Privacy Assessment (“IPA”) is a method to quickly evaluate what are the general privacy risks of a technological solution or a specific use, transfer or collection of data to City bureaus or offices. This initial assessment is a way to identify factors that contribute to privacy risks and lead to proper strategies for risk mitigation or alternatives that may even remove those identified risks.

The Initial Privacy Assessment may lead to a more comprehensive Privacy Impact Assessment (PIA) and a 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 Assessments on an outward facing website for public access. IPAs do not include specific uses of technology or data other than those initially evaluated.

WHEN IS AN INITIAL PRIVACY ASSESSMENT RECOMMENDED?

An IPA 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?

City staff complete two documents:

- *The Initial Privacy Assessment form.* This document 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.
- *The Privacy Risk Assessment.* This document breaks the privacy risk into six different areas of evaluation: (1) Individual Privacy Harms; (2) Equity, Disparate Community Impact; (3) Political, Reputation & Image; (4) City Business, Quality & Infrastructure; (5) Legal & Regulatory; and (6) Financial Impact. Then compares risks to the likelihood of happening to create a single risk measure based on the worst-case scenario.

Executive summary

The pilot of the automatic license plate readers for parking enforcement consists of a solution that integrates automatic license plate readers hardware, with parking enforcement software. Data about parking rules are provided to the parking enforcement software. Real-time information is collected by a car with cameras mounted at different angles.

The worst-case scenario of the privacy impact assessment returns a high risk triggered by the *political, reputation and public image* risk issue due to the use of surveillance technologies and the public perception of such technologies based on history of lack of transparency and harm from surveillance.

It has not been possible to fully assess the privacy risk properly, as the privacy impact assessment team needs more documentation connected to the company's, and its subcontractors, privacy and data policies and additional information about the specific technological solution. Several assumptions have been made and further confirmation of the privacy safeguards in the contract and privacy policies are required. The conclusion of medium risk for individual privacy harms is based on the assumption that it will be minimal personal data collected and the company follows modern information protection and cybersecurity standards.

However, if there is no proper privacy risk assessment, the City may increase the likelihood of negative impacts and unknown risks.

The following table summarizes the outcome of privacy risks to the city.

Risk area	Risk level determined
Individual Privacy Harms	**Medium**
Equity, Disparate Community Impact	**Medium**
Political, Reputation & Image	**High**
City Business, Quality & Infrastructure	**Medium**
Legal & Regulatory	**Low**
Financial Impact	**Low**

The recommendation is to perform a comprehensive privacy impact assessment that includes clear data governance roles and responsibilities, the privacy risk mitigation strategy, and a communications plan to the public to provide a transparent process to this pilot.

Initial Privacy Assessment

	Portland initial privacy assessment for a technology, project, data sharing agreement or app solution
Version 0.2	**This information is considered restricted and for internal use only until the client clears to the public. This notice must be removed when authorized for publication**
Information	**Request information**
Bureau	BTS-PBOT
Assessment done by (name/email)	Hector Dominguez/hector.dominguez@portlandoregon.gov
Date of Assessment	January 27, 2021
Document status	**Delivered**
Name of the assessment	**Pilot of the automatic license plate readers for parking enforcement**
General description	This is a pilot for ONE vehicle with an automatic license plate reader (ALPR) for area parking permit enforcement.
Evaluation topic	**Assessment**
Purpose of the technology, project, data sharing or application	This pilot consists of a solution that integrates automatic license plate readers hardware, with parking enforcement software. Data about parking rules are provided to the parking enforcement software. Real-time information is collected by a car with cameras mounted at different angles. The information about a parking violation is uploaded to the cloud and made available to the parking tickets solution. The information can be accessed by officers in the field able to confirm read accuracy or add corrections and notes using handheld devices. Automation in parking enforcement allows efficient use of staff time and provides documented process in parking violations. It is not clear if information received by PBOT is only about vehicles in parking violation and will not be used to track any other purpose. It is not clear from the contract how PBOT will use this pilot to assess the effectiveness of the technology and future applications.

Name of the entity owner of the application and website	Schweers Technologies https://www.schweers.com Schweers Technologies is the US subsidiary of Schweers Informationstechnologie, an international company, that develops, designs and manufactures professional parking and code enforcement tools. https://www.linkedin.com/company/schweers-technologies https://www.schweers.com/index.php/us/products/license-plate-recognition/lpr-scan-car
Type of Organization	Private entity
Scope of personal data collected. List all sources of data and information.	ALPR has three scopes of work: (1) One scan car for APP (Area Parking Permit) enforcement, (2) Conversion of Politess Office which resides on the City server to Politess Web Office which is Hosted, (3) Scan Car integration with Hosted Politess Solution. https://www.portland.gov/transportation/parking/appp-info
How personal data is collected	The Politess solution access parking rules, including geolocated information of available parking spots, which get integrated with the Scan car solution captures the license plate number from a vehicle that is in a parking violation. This information contains the photo(s) from the scan car to provide a data trail from the scan car to the final valid ticket. The violation processing involves personal data and could potentially reveal sensitive personal data. Terms of service should be agreed in the contract. Based on assessment of the information provided, the data lifecycle goes as follows: The data is collected by the camera mounted on the car that automatically recognizes the license plates and checks them in the payment database. Data from this source includes picture, license plate, timestamp and location. More information is need to understand what the picture collects (i.e. just license plate, full view of the car, etc.). The data processed does not include special categories of personal data. However, individuals may be identified if this data is combined with other sources of information. The assumption is that data shared for enforcement does not include information about other criminal offences associated with the plate or vehicle owner. The data collected is minimized to fulfill the contract for parking enforcement under current system design. The frequency of data is not described.

	Company data retention policy is not described. This is important in case of infringements and following a settlement in open cases. Records should not be overridden. Personal data collection needs to be minimized to fulfil the contract. This is a recommendation from the City’s privacy principles. To learn more about it please visit: https://www.smartcitypdx.com/privacy-principles
Who can access the data	Not specified. Company's privacy policy is needed. Other privacy risks can exists due to PBOT data management.
Purposes the data is used for	Obtain license plate number and link it to a car owner's personal information in order to issue the parking violations.
Where the data is stored	Cloud services managed by a third party, Genetec.Cloud services provided by Microsoft Azure.
How data is shared	Automatic export of the ticket data to an FTP (File Transfer Protocol) location provided by PBOT and by using an export format provided by PBOT. Using FTP represents a vulnerability as anyone with the file location can have unauthorized access and make copies of those files. It is standard to use secure methods to access data, like accessing webpages using SSL certificates, SFTP or RESTful APIs.
How long is the data stored?	Not specified.
Effectiveness	The collection of personal information is effective when minimized to the collection of the minimum data required for the parking enforcement, fulfill the contract, and limit data transferred to the city for parking enforcement. Also, It is not clear what the company collects and stores in their servers in the context of

	this contract. The contract should also limit the time in which this information can be retained by the company.

Proportionality, fundamental rights, frequency of the collection, and data protection and privacy issues line unintended data collection or processing.	There is no conclusion on what privacy rights individuals may have based on the information provided. The expectation is that only applicable laws in Oregon can be enforced and no other privacy services like the possibility to remediate mistakes, provide or remove consent in data processing, or the option for an individual to know what the service provider keeps about them. There is also no information about the frequency of transferring or updating information from the service provider to the city. The initial privacy assessment has identified the following risks to this application of automatic license plate readers: Problematic data events The problematic data events are: leak of fines, leak of locations, leak of raw footage, leak of data about individual such as unique personal identifiers, like drivers license number, and home address Unauthorized collection of personal data The unauthorized collection of personal and sensitive data (i.e. driver license number, address, criminal history, or even biometrics) by the service provider working on behalf of the city may increase risks and impacts to individuals. Unauthorized uses of personal data This event happens when the organization or the service provider uses the collected data in other applications or processes that are not authorized or clearly defined in the contract or agreement. An example of this is when the service provider uses some information for marketing or for social research and production. This processing could include predictive analysis, fines or parking rules enforcement algorithms. The potential problems for the individual are: Leak of fines 1. Discrimination 2. Embarrassment 3. Financial damage Leak of locations 1. Spouse / ex checking somebody's whereabouts. 2. Stalker 3. Employer controlling you during work hours. 4. Employer controlling you outside work hours: visiting religious institutions, gay bars, doctor. 5. Police using location in discriminatory manner, for example investigating all Black people that were parked one block around the crime scene at the time of

	the crime. Leak of raw footage 1. Who is in the vehicle 2. Who are you with 3. Pedestrians doing something embarrassing, funny, wrong. 4. Location of the moving cars Leak of data about individuals (driver’s license number, address, etc.) 1. Unauthorized access to state services 2. Identity theft 3. Stalking (home address) Unauthorized collection of personal information 1. Increased and unknown risks to the City and the individuals 2. Privacy violation 3. Unknown processing of information Unauthorized uses of personal data 1. additional risks due to third parties use 2. Errors and biases in prediction analysis 3. manipulation due to marketing or social research

Privacy safeguards	Access to the applicable provider's privacy policy was not accessible and privacy safeguards could not be determined. Privacy safeguards include: • restriction to access collected data within the organization and third parties • Limitations in personal data collection • Third party audits • Data protection measures like use of encryption and security credentials • Data collection is minimized, only necessary data is collected • Narrow, clearly defined uses of data collected
Open source	No
AI/ML claims	Undefined
Privacy Policy (link)	Not provided
Privacy risk	High
Surveillance Tech?	Yes
Portland Privacy Principles (P3)	
Data Utility	This principle recommends comparing the proposed solution with existing processes. In this case, having an agent going around streets and verifying manually what cars are in potential parking violations is lengthy and expensive. Automating this process may save staff time and resources and provide more transparency to the violation tickets cases.
Full lifecycle stewardship	Privacy protections need to be present through the collection, storage, processing, sharing, and discarding of information
Transparency and accountability	Information transformations need to be documented and with a clear point of contact responsible for it
Ethical and non-discriminatory use of data	Clear ethical and anti-discriminatory measures need to be in place. Special considerations to cases where privacy risks may impact people of color and vulnerable communities more.
Data openness	Design for data openness and transparent processes. Data openness needs to be accessible, timely and accurate.
Equitable data management	allow public participation in the decision-making process

Automated Decision Systems	Pay special attention to the use of formulas and algorithms that impact a resolution for parking infringement. This includes predictive algorithms, use of big data, artificial intelligence, and machine learning. The presence of errors, and biases in data through its lifecycle. Look for third party audits and, when possible, ask for information about whitepapers or any academic or research document that supports the application of automatic decision systems.
Optional	
Consent	Not applicable.

Privacy Impact Risk Severity Assessment form

WORST CASE SCENARIO	High

1. Individual Privacy Harms

Impact: High
Likelihood: Unlikely
Total Risk level: **MEDIUM**

Justification:
Individual risks can originate from leak of fines, leak of locations, leak of raw footage, leak of data about individuals such as unique personal identifiers. High risk is present when sensitive information is included in the transfer to the company. Sensitive information includes driver license number and criminal or fines history and location history.

The potential problems for the individual are:
Leak of fines
1. Discrimination
2. Embarrassment
3. Financial damage

Leak of locations
1. Spouse / ex checking somebody's whereabouts
2. Stalker
3. Employer controlling you during work hours
4. Employer controlling you outside work hours: visiting religious institutions, gay bars, doctor
5. Police using location in discriminatory manner, for example investigating all black people that were parked one block around the crime scene at the time of the crime

Leak of raw footage
1. Who are you with
2. Pedestrians doing something embarrassing, funny, wrong
3. Location of the moving cars

Leak of data about individuals (driver's license number, address, etc.)
1. Unauthorized access to state services
2. Identity theft
3. Stalking (home address)

Unauthorized collection of personal information
1. Increased and unknown risks to the city and the individuals
2. Privacy violation
3. Unknown processing of information

Unauthorized uses of personal data

1. Additional risks due to third parties use
2. Errors and biases in prediction analysis
3. manipulation due to marketing or social research

Comments: The likelihood of the risk is estimated

2. Equity, Disparate Community Impact

Impact: Moderate
Likelihood: Possible
Total Risk level: **MEDIUM**

Justification:
Bias in data due to history of infringements, income, or location in the city. Bias can also come from deployment of devices (oversampling and subsampling).

ALPR can also be perceived as a thread to civil liberties and privacy. A main concern from the public is the monitoring of activities and the use of mobility data for social behavior research.

People of color mistrust the fair application of law enforcement. The deployment of ALPR needs to include clear mechanisms for transparency and accountability and inform these communities properly.

Comments: The likelihood of the risk is estimated

3. Political, Reputation & Image

Impact: High
Likelihood: Likely
Total Risk level: **HIGH**

Justification:
Identity capture. The public may be concerned that ALPR will capture personal identifiable information (PII) without notice or consent. The public may perceive ALPR cameras as an invasion of their privacy and the collection of images may be stored and include vehicle occupants, license plate numbers of vehicles not in parking violations, etc. and link that information with geolocation, allowing third parties to do additional research and identify an individual.

Uses outside the scope of this application. Public trust is linked to the civic contract, transparency and accountability. When the city uses data for purposes other than those originally specified, the public is less likely to cooperate and trust technological deployments. This may include use of personal or protected information by another city bureaus

Lack of public access to information. Communities impacted by over surveillance mistrust how the government deploys technologies like ALPR. The lack of transparency on what the project is about, collection of data, oversight and reporting, will reinforce negative past experiences of lack of communication about data being collected in the right of way, how that data is used, who is allowed to see that data, and also tied to harmful experiences with surveillance and being targeted.

Comments: The likelihood of the risk is estimated

4. City Business, Quality & Infrastructure

Impact: Moderate
Likelihood: Possible
Total Risk level: **MEDIUM**

Justification:
Lack of data governance. Without a clear description of roles and responsibilities will increase the possibility of a privacy breach and reduce mitigation or resolution strategies.

Lack of the surveillance policies. Without policies in place that include proper safeguards, responsibilities, transparency, and accountability. A surveillance policy may include public participation, oversight and reporting procedures.

Lack of civil liberties assessments. Abuse of access to sensitive information and impact to civil liberties and rights of individuals may end up unaccountable.

Risks related to quality can be:
* data collection errors
* lack of data governance
* lack of proper mechanisms for data sharing
* technology dependency
* security attacks and breaches
* lack of staff training
* lack of auditing and oversight
* lack of equipment maintenance

Comments: The likelihood of the risk is estimated

5. Legal & Regulatory

Impact: Moderate
Likelihood: Unlikely
Total Risk level: **LOW**

Justification:

The service provider may need historical information for parking enforcement. The contract should specifically clearly be a method for secure data access and transference from and to the City. These procedures depend on enforcement rules.

Not following data retention regimes for collected data can lead to legal challenges and increase other risks like privacy breach.

Data breaches must be reported by law.

Law enforcement may request information about parked vehicles or vehicles in parking violations connected to a criminal investigation. If similar rules exist, they need to be clear to the public.

Comments: The likelihood of the risk is estimated

6. Financial Impact

Impact: Moderate
Likelihood: Unlikely
Total Risk level: **LOW**

Justification:
This is a pilot project and costs need to be contextualized and properly scaled to evaluate financial effectiveness.

Data breaches may have a high financial impact in insurance and loss compensations or settlements.

Return of investment of this technology is connected to effective parking enforcement and reduction of staff costs.

Any legal suit for civil liberties violation can be costly.

Comments: The likelihood of the risk is estimated