PBOT: NovoaGlobal

Privacy Impact and Risk Analysis

Final draft

Smart City PDX

6/11/2025

PRIVACY ANALYSIS REPORT

City of Portland Privacy Toolkit

WHAT IS PRIVACY RISK AND IMPACT ANALYSIS?

The Privacy Impact Analysis ("PIA") 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. The PIA 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 Privacy Impact Analysis may lead to a more comprehensive Impact Assessment 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 in data collection and management, the City of Portland has committed to publishing all Privacy 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 PRIVACY IMPACT ANALYSIS RECOMMENDED?

A PIA is recommended when:

- A project includes surveillance technologies.
- 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.

WHAT IS IT INCLUDED IN A PRIVACY IMPACT ASSESSMENT?

City staff completes two sections included in a privacy impact assessment report:

- *The Privacy Analysis 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: (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. Then compares risks to the likelihood of creating a single risk measure based on the worst-case scenario.

Executive summary

The main purpose of this technology is to do speed limit traffic and red-light enforcement in high crash corridors in Portland. Portland Bureau of Transportation's (PBOT) Vision Zero program's goal is to eliminate traffic deaths and serious injuries on our streets. PBOT has installed speed and intersection safety cameras at and along the highest crash streets and intersections across the city and it is looking for a new vendor.

The privacy impact assessment is focused on NovoaGlobal's Speed-safe solution for speed limits enforcement. NovoaGlobal's solution offers a Dual Doppler Positional Radar that tracks the speed and position of multiple vehicles across several lanes simultaneously. NovoaGlobal collects the information from a speed camera and identifies the vehicle and owner, issuing a traffic violation citation with this information. PBOT and Portland Police receive a notification and validate the information if necessary.

The highest risk identified is Medium with no major issues. The whole process for collecting and identifying a speeding vehicle is mature and well understood by all participating parties. Information is protected and only the necessary information is shared using secure channels.

Two main issues connected to how the technology is applied were identified. First, the lack of transparency and communications can lead to misunderstanding and misinformation about the purpose of the cameras. Certain groups may be more concerned that information can be used for different purposes, like immigration enforcement or to pursue other criminal investigations. Oregon law constrains the use of speed cameras only for the purpose of traffic laws enforcement.

Second is the potential oversurveillance of low income or neighborhoods lacking public infrastructure. This could result in higher number of traffic violations on residents in these areas, creating economic burden on specific groups. PBOT's analysis of speed violators by county of vehicle registration from 2019-2023 found that 77% of violators were from outside of Multnomah County and 61% were from vehicles registered outside the region[1].

The following table shows a summary of the main privacy risks in this assessment.

Risk area	Risk level determined	Highlighted risks
Individual Privacy Harms	Medium	**Risk of intrusive private information requests to complete violation information.** Obtaining more than necessary information for a specific traffic incident may feel intrusive and having more information increases privacy risks and impacts. This non-required information can include demographics, and the City is not collecting this information. Demographics data

[1] https://www.portland.gov/transportation/vision-zero/high-crash-network-streets-and-intersections

Risk area	Risk level determined	Highlighted risks
		may be needed to comply with crime data standards and reporting incidents.
Equity, Disparate Community Impact	Medium-Low	**Risk of oversurveillance of neighborhoods where speed cameras are deployed**. This risk refers to the sense of being constantly watched due to the systemic presence of cameras in specific neighborhoods, usually low income and with little infrastructure. Citation data shows 77% of violators between 2019-2023 were from outside of Multnomah County. PBOT can improve information about these cameras and the benefits and impacts from using this technology.
Political, Reputation & Image	Medium-Low	**Risk of public mistrust due to the lack of transparency or available information.** Lack of transparency around the use of speed cameras can trigger misinformation and public mistrust. PBOT has a website describing the use of speed cameras for reduction of traffic incidents. However, further efforts to reach public awareness need to be done to reduce impacts due to lack of information on speed cameras. Misinformation about what cameras collect, how information is shared, and whether these devices live stream video and other parties can access them are common narratives in communities. Given that most people are not going to request information via public records, the main recommendation to reduce this risk and impacts is to proactively inform the community about the purpose of these cameras and add easy access to information about the effectiveness of this technology and build-in information safeguards.
City Business, Quality & Infrastructure	Medium	**Risk of vandalism or physical damage to equipment.** Speed cameras have been subjected to vandalism and shooting in the past. This risk can arise from public mistrust and disgruntled residents. Destruction of City property can lead to a criminal investigation.
Legal & Regulatory	--	No major privacy risk identified
Financial Impact	--	No major privacy risk identified.

Privacy Analysis

Purpose of the technology, project, data sharing or application

The City of Portland's Vision zero program has the goal of eliminating traffic deaths and serious injuries on our streets. The Portland Bureau of Transportation (PBOT) installs speed and intersection safety cameras at and along the highest crash streets and intersections across the city[2].

The City's current vendor is incapable of competently managing and expanding the automated enforcement cameras program. To increase speed and traffic signal compliance on the High Injury Network, PBOT needs one or more of the following:

- New and higher performing camera vendor.
- Pricing based on maintenance fee as opposed to per-citation case.
- Establish enforcement cameras as traffic control devices.
- Potentially resolve franchisee limitations that prevent placement of privately owned cameras on joint use poles.

This privacy assessment looks at NovoaGlobal's Speed-safe[3] solution for speed limits enforcement. NovoaGlobal's solution offers a Dual Doppler Positional Radar that tracks the speed and position of multiple vehicles across several lanes simultaneously.

This radar system is complemented with high speed 24MP still camera and high-definition video camera with the ability to store video and still images in the device, upload them to the vendor's cloud, or livestream video to an IP address accessible to law enforcement or transportation personnel.

Their Digital Video Recording (DVR) features automatically capture and stores a single image every 60 seconds at each location.

NovoaGlobal staff use these images and footage to gather information about the vehicle and the offender from national law enforcement databases that includes Nlets[4] and, in some cases, LexisNexis[5].

Once this information is integrated and ready, it is sent to an officer who validates the violation and starts the court process to decide fees according to business rules. If the defendant challenges the citation and requests a court hearing, a Circuit Court judge makes a ruling and

[2] https://www.portland.gov/transportation/vision-zero/safety-cameras
[3] https://novoaglobal.com/speed-safe/
[4] https://nlets.org/
[5] https://risk.lexisnexis.com/law-enforcement-and-public-safety

decides the appropriate fine amount[6]. A final statement is issued with all the information describing the violation and fees. A printed version is sent to the violator via mail.
ORS 810.435[7] regulates the use of photographs for speeding violations. Pictures "may be submitted into evidence in a criminal trial, grand jury proceeding or other criminal proceeding for the purpose of proving or disproving a felony or a Class A misdemeanor."

Photographs "may not be used in any criminal proceedings relating to the prosecution of a violation . . ., other than for the purpose of proving or disproving a violation [of traffic laws]."

Name of the entity owner of the application and website

NovoaGlobal, Inc.
https://novoaglobal.com/

Type of Organization

Private

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

Speed cameras collect information about vehicles in violation of traffic laws. These images and footage are used to identify two categories of information: vehicle and offender's information. In some cases, the owner of the vehicle differs from the offender's information, but the personal information collected from both are the same fields as described below.

Vehicle identification: Plate number, plate state, plate type, DMV Status, Registration expires, class, color, make, model, model year, status, VIN number.

Offender information: First name, middle name, last name, address, city, ZIP, State, Date of birth, Driver License. The field describing the offender's gender is not collected and left blank by default.

Owner information: First name, Middle name, Last name, Address, City, ZIP, State, Date of Birth, Driver license. The field describing the owner's gender is not collected and left blank by default.

Offenders will be requested to fill in a form to pay violation fees to Multnomah County Circuit Court. This process includes sharing payment forms like bank accounts or credit card information. A third-party processes payment and the City of Portland does not collect this information.

[6] https://oregon.public.law/statutes/ors_810.180
[7] https://oregon.public.law/statutes/ors_810.435

In this case, the violation fines are paid directly to the Circuit Court and not to the City of Portland. Therefore, the City of Portland does not collect bank account or credit card information.

Portland Police officers and courts can see driving history. However, judges do not look at a person's driving history until the case has been adjudicated to provide an unbiased ruling. Police do not present driving history unless the history is pertinent to the case at hand, such as cell phone violations, where each violation can change the outcome based on the law.

In 2025, PBOT staff will begin reviewing, issuing and adjudicating violations from automated enforcement cameras. This authority for City "Duly authorized traffic enforcement agents" is granted by ORS 810.436 and 810.437. PBOT Agents will have much less access to sensitive info than PPB officers. These Agents will not have access to defendant's driving history.

After the judge has made a ruling, the judge will look at driving history to ensure the appropriate fine amount is instituted. On rare occasions, the judge will not allow police to lower the fine amount or may increase the fine over the statutory amount because the person's history is egregious.

How personal data is collected.

Information is first collected through devices installed on roads on Portland's High Crash Corridors. This information includes pictures and video footage from high definition and high-speed cameras. Once a vehicle is found in violation of traffic speed limits, cameras collect images of the vehicle, license plate, and the driver. This process is done by NovoaGlobal.

Required information to issue a violation citation and fees assigned to it are determined by searching using the license plate and the type of vehicle.

The identification of the offender's vehicle is done after the image collection using an Automated License Plate Reader that relies on the use of artificial intelligence technology for character and number recognition. The license plate identification is not done in real time. Data must be validated with an existing Department of Motor Vehicles (DMV) record, which NovoaGlobal access mainly through its Nlets account. Information can be also validated using LexisNexis as a last resort to get addresses and information about the vehicle.

NovoaGlobal has certifications and does background checks of employees to manage sensitive information. NovoaGlobal also fulfills FBI requirements and check data yearly.

DMV Access

To secure the identity of the registered owner of the vehicle involved in an alleged violation, NovoaGlobal's operators review the event images; obtain the license plate number, assisted by an automatic character recognition system, and the State of issuance.

NovoaGlobal staff access the Oregon DMV through a strategic partnership with the National Law Enforcement Telecommunications System (Nlets), as well as the expansive Lexis/Nexis database and various other state motor vehicle departments. The most recent vehicle owner information is obtained using these methods.

Once NovoaGlobal operators receive the registered owner information, they check the provided information against the photographic images to confirm the vehicle images match the provided information. Once confirmation is made, NovoaGlobal staff import the registered owner's information into the citation for further review and confirmation by a Portland Police Officer.

There is no transfer of information between NovoaGlobal and Portland Police other than citation and any relevant information for the citation (for instance, camera operation reports and mailed letters).

Portland Police or PBOT do not have access to NovoaGlobal servers or information openly. If the investigation requires any specific information, this is specifically requested. NovoaGlobal allows access to their system for citation approvals, camera system reports or some other basic data. This is the only time that PPB or PBOT would be accessing their system.

NLETS Access

Nlets, or the National Law Enforcement Telecommunications System, is an International Justice and Public Safety Network, a private not-for-profit organization offering a computer-based message switching system that links together and supports every state, local, and federal law enforcement, justice, and public safety agency for the purposes of sharing and exchanging critical information.

License plate and state is retrieved by NovoaGlobal over Nlets[8]. Portland Police may use their own access to Nlets to verify information sent by NovoaGlobal or through the state of Oregon's Law Enforcement Data Systems (LEDS)[9]. Most Police use LEDS for photo enforcement around returned mail (undeliverable citations) and find the correct address for the citation. This is only to ensure the citation can be delivered correctly or to verify the citation was mailed to the correct address.

Nlets is a national DMV data broker and aggregator between US and Canada. NovoaGlobal needs a letter of authorization from the Portland Police Chief and use the Originating Agency Identifier (ORI) number from the City to retrieve information from DMV Oregon. This authorization is done on a yearly basis. Police officers do not use LEDS for criminal purposes but only for traffic violations. Also, Offices do not use NLETS to access DMV records.

[8] https://www.nlets.org/about/who-we-are
[9] https://www.oregon.gov/osp/programs/cjis/pages/law-enforcement-data-systems.aspx

NovoaGlobal is a National Law Enforcement Telecommunications System (Nlets) Strategic Partner since November 2013.

Who can access the data?

Information collected from speed cameras is accessed and processed by NovoaGlobal staff. Portland Police Bureau receives violation information and confirms the information as required. Courts and judges have access to the incident description, vehicle and offender's information, violation, driving history, and other information pertinent to this case.

Once this information is transferred to Portland Police for processing from NovoaGlobal information system, a Police Officer will validate that a violation has occurred. A Police officer can make a recommendation of fines according to State of Oregon's guidelines[10]. A Police officer and authorized agents can request the statutory minimum, and Judges can only reduce to the statutory minimum. Judges can look at driving records after the verdict of guilty has been assessed to adjust the fine amount due to the driving history and the statutory requirements.

Multnomah County (the court Portland uses) will receive ticket information in a secure channel through the state system. NovoaGlobal will share this information directly after Portland Police validation but without having PPB as intermediary.

Courts and judges receive this information and can also access driving history and other information pertinent to this case.

PBOT's traffic & safety team has access to aggregated data from violations.

This data is a public record and subjected to public release if requested. Certain fields might be exempt from public disclosure according to Oregon's laws.

Purposes the data is used for.

Information collected from the speed cameras is used to start the process of identification of the vehicle and offending driver.

Verification of violation, clarity of image to determine identity, ownership, and vehicle type.

Case adjudication and ruling of violation fines and other legal outcomes. This information can be used in subsequent legal procedures including but not limited to payments, access to discounts, waivers, court procedures, and written statements.

[10] State of Oregon's schedule of fines effective as the date of drafting this assessment: https://www.oregon.gov/osmb/boater-info/Documents/Schedule_of_Fines_on_Violations_2021.pdf

Final verification and validation by a Police Officer before NovoaGlobal send the violation notification by mail.

Payment collection of violation.

Anonymized data can be used for improving the City of Portland's customer service, transportation planning, reporting of incidents, and the Vision Zero and other City programs[11].

Where the data is stored

Source footage is stored at NovoaGlobal's secure servers.

Portland Police do not store any data related to the validation. The Records Division stores data for the City's eCite program[12]. This data only includes citations submitted for adjudication, when allowed.

How data is shared

NovoaGlobal shares citation information about the violation via the Oregon Judicial Department's eCitation program[13]. File transfers are done securely via an FTPS[14] server.

Information that NovoaGlobal transmits regarding the citations goes directly to the courts. There is not a middle system, and it will not go through PPB or PBOT. An XML file transfer is a one-on-one communication and that is to keep the data between the producer and the receiver, with no interference. PPB will receive only a notification of this transfer.

How long is the data stored?

NovoaGlobal will retain the information according to the State of Oregon's retention periods[15].

Traffic and Other Citation Logs — Minimum retention: 1 year.
Traffic and Other Citations — Minimum retention: 3 years.
Traffic Violation Warning Records — Minimum retention: 1 year.

NovoaGlobal requires the City of Portland to sign a retention policy form.

[11] https://www.portland.gov/transportation/vision-zero/safety-cameras
[12] https://www.portland.gov/police/open-data/stops-data
[13] https://www.courts.oregon.gov/about/pages/integrations.aspx
[14] FTPS means Secure File Transfer Protocol.
[15] https://oregon.public.law/rules/oar_166-200-0350

Effectiveness

The effectiveness of the speed cameras is impacted by technical and environmental factors.

Technical factors that impact effectiveness of the cameras include inherited limitations in each technology involved in the violation detection. The system uses multitracking radar, which is heavily impacted by the presence of fog. Other conditions like heavy rain may also impact the effectiveness of measuring a moving vehicle speed. This radar also has a 300 ft reach.

Once the vehicle is confirmed to move at the predetermined maximum speed, a high-speed camera collects the image of the vehicle, license plate, and driver. The information is filtered out and it is possible to request a report on the type of error that fails in image collection.

There are different types of failure modes including: controllable (blurry picture), not controllable (Fog) and other types of issues that reject an event. The reason likely issue is reported and aggregated to improve the system's effectiveness. These failures will trigger an 'unknown violation' status in the collection of information.

Identifying the offender is a process that involves information research, filtering, and validation. The process is not perfect, and this is one reason for collecting driver's picture to generate proof of the offense.

If the offender is different than the vehicle owner, the information retrieved from DMV or Nlets is different.

Owners have different tools to fix mistakes, and this include:

COI = Certificate of Innocence: This is included in the alleged violator's citation packet that is mailed or emailed to them. They can use this to attest that:

- They no longer own the vehicle
- Another registered owner was driving the vehicle
- Another person was driving the vehicle
- The vehicle was reported stolen before the date and time indicated on the citation

AFNL = Affidavit of Non-Liability. This is like the COI but relates to a vehicle that is owned by a business or employer. They can attest that:

- The vehicle was sold prior to the violations date
- The vehicle is owned, leased, or rented by a business or public agency and was driven by an employee, lessee, renter or other authorized driver at the time of allegation.

Proportionality, fundamental rights, frequency of the collection, and data protection and privacy issues like unintended data collection or processing.

Necessity and proportionality

The information collected to identify and then issue a traffic violation is reduced to vehicle, license plate, and photo proof of the driver, which is not used for any identity verification.

License plate number and type are used to validate the offender's vehicle. In the NovoaGlobal system, data from DMV is collected about the vehicle's owner's information. This is also duplicated into Offender information.

When a COI/AFNL is performed then that data will differ. The Owner will still be the owner, but the Offender will be changed.

Once the offense is processed and accepted, the offender enters their personal information to validate identity. A form will collect this based on pre-identified data.

Some fields in this form are not necessary for the violation but used for other purposes. Issues around identity verification and the need of using date of birth. Gender is not necessary for citation issuance or the paying the fees of the violation.

Information is intended to reduce duplicates and the list of offences, and their cases are kept by NovoaGlobal.

Individuals can access existing or previous cases using the license plate and a personal PIN provided on the citation that was mailed with the violation.

Privacy safeguards

The access and processing of information from a speeding violation is clearly separated and only the necessary information is shared among entities. Data sharing is also done using secure channels and according to existing laws.
Sensitive information from individuals, like history of violations or bank account or credit card numbers for payments, is only accessible to the stakeholders that need the information for processing or legal procedures.

Information is also protected according to existing information privacy laws.

Open source

No.

AI/ML claims

Yes. Only for license plate number identification from an image. The number is later validated by a person. There is no face recognition involved in identifying the driver.

Privacy Policy (link)

NovoaGlobal's privacy policy is applicable to the information collected on their website to review and pay for a traffic violation.
https://payment.zerofatality.com/vps/cgi/VP/citation_review

Privacy risk

Choose an item.

Surveillance Tech?

Yes

Portland Privacy Principles (P3)

Data Utility

The information collected for specific purposes, identification of vehicle and offender information, violation determination, processing of violation, and resolution, mostly collect the necessary information for that specific process. Some additional information is collected for demographic information.

Full lifecycle stewardship

Information is secure during the full life cycle and existing legal requirements are also enforced. Retention times are specified when the service agreement with the vendor is set. The parties participating in each step of processing information are responsible for the final destruction of information at the end of their respective retention time.

Transparency and accountability

Parties are responsible for reporting any information breach according to Oregon laws. However, as information is distributed and only accessible to the party doing a specific process, the risks of information breach are also minimized.

PBOT also maintains a list of locations with speeding cameras in Portland:
https://www.portland.gov/transportation/vision-zero/safety-cameras

Speeding traffic incidents are not reported as open data either PBOT or PPB.

Ethical and non-discriminatory use of data

Speeding cameras are installed in high crash corridors. Some neighborhoods where these cameras are installed are low income and it could create higher impacts for low-income households around those corridors, however PBOT's data analysis of violators demonstrates that 78% of violators are from outside of Multnomah County.

Anonymized information from speeding incidents is used to inform PBOT's Vision Zero program[16].

Data openness

Data from speeding cameras is not open and only images involved in the speeding incident are shared and only with the offender.

Automated Decision Systems

The license plate reader is the only automated decision system in this case. The outcome is always validated by human operators and verified with nationwide databases.

Consent.

No consent opportunities in this case.

[16] https://www.portland.gov/transportation/vision-zero

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	ID	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
U	I	1.1	Risk of unauthorize access to individual personal and sensitive information	Moderate	unlikely	The process of retrieving information to identify an offender vehicle and its owner enables different staff (in the vendor and Portland Police) access to databases with sensitive private information. This risk looks at the possibility that staff may do unauthorized search or queries for sensitive personal and private information using these databases. NovoaGlobal constraints access of Nlets or LexisNexis to the identification of a vehicle for their business offer. Staff are not allowed to perform other operations Performing periodic audits looking for unauthorized access or use of these databases can identify issues and loopholes. Training staff in information security and data loss prevention can be an ongoing strategy to reduce this risk.	Low
T	I	1.2	Risk of unauthorized sharing of Personal Identifiable Information	Moderate	unlikely	Unauthorized sharing of information can be unintentional or intentional with different purposes. Unintentional sharing of information is mostly due to lack of controls on data or training on information protection, roles and responsibilities. Intentional unauthorized data sharing is a more serious issue. In either case, this is considered a data breach and needs to be reported and treated as a security incident.	Low

						Preventive measures can be placed to reduce the possibility of this risk, like limiting the ways in which information is copied and stored or defining specific stations with no access to email and with only intranet access. Training staff in information responsibilities, limitations, and potential actions if unauthorized actions are done.	
T	I	1.3	Risk of intrusive private information requests to complete violation information	Moderate	Possible	Obtaining more than necessary information for a specific traffic incident may feel intrusive and having more information increases privacy risks and impacts. However, the program only collects information for required fields, including demographic information, on the citation and comply with crime incident reporting data standards. These fields need to be identified and kept optional. Portland's privacy and information protection principles recommend collecting only the necessary and minimum personal identifiable information for a specific and well-defined purpose. Staff from NovoaGlobal and City of Portland have limited access to personal information and the one collected is only required for issuing the violation notice and fees. Moving information from one entity to another is also limited and well established. These interfaces reduce risks from unnecessary information moving across organizations.	Medium
T	I	1.4	Risk of using face recognition to identify a specific individual	Moderate	rare	Images of the driver of the traffic violation get captured by the speed cameras. Using face recognition technologies to identify an individual is forbidden in the City of Portland. Neither the vendor nor the City are using face recognition technologies. The identify identification of the offender is only a copy of the vehicle's owner's information. No identification process relies on the image of the driver.	Low

U	I	1.5	Risk of using information for other purposes	High	unlikely	This risk refers to the possibility of using the collection of images from the vehicle, driver, and license plate to other purposes than traffic violations. Many people in the Portland community are concerned that images collected by speed cameras will be shared with other agencies or used for other criminal cases. ORS 810.435[17] defines how the use of photographs for speeding violations. Pictures may be submitted into evidence in a criminal trial, grand jury proceeding or other criminal proceeding for the purpose of proving or disproving a felony or a Class A misdemeanor. Photographs taken under these laws may not be used in any criminal proceedings relating to the prosecution of a violation, other than for the purpose of proving or disproving a violation. Request for information are handled according to the law and existing regulations. In addition, the vendor has implemented information protection measures that keep information usage under the existing purpose only.	Medium
T	II	2.1	Risk of oversurveillance of neighborhoods where speed cameras are deployed	High	unlikely	This risk refers to the sense of being constantly watched due to the systemic presence of cameras in specific neighborhoods, usually low income and with little infrastructure. This risk can create higher number of violation citations on low-income households compared with neighborhood with no cameras and creates some economic burden, although data analysis by PBOT has demonstrated that a supermajority of violators come from outside of Multnomah County. The deployment of speed cameras responds to high crash and incidents in corridors. Having effective communications and public engagement strategies informing neighborhoods about the purpose of this technology and enabling public input about these deployments can help to reduce the feeling of being watched. Having physical and online information about the purpose and effectiveness of these cameras can also justify its deployment in the	Medium

[17] https://oregon.public.law/statutes/ors_810.435

						light of public interest by reporting effectiveness of these devices. These cameras cannot zoom or tilt to change their field of view. The only purpose of this system is to identify vehicles moving at higher speeds than allowed in a high crash corridor. Some Cities have developed strategies for limiting the number and authorizing deployment of these cameras. These strategies include advisory or oversight public bodies and participation of governance bodies to guide and define use of these cameras, particularly in low income or neighborhoods lacking public infrastructure.	
T	II	2.2	Risk of ineffective information collection from non-English speakers' and people unfamiliar with the citation system	Moderate	unlikely	Non-English speakers, new Portlanders, elderly people and people with disabilities may have problems interacting with the citation system, which may lead to incomplete information or delivering wrong personal information. These situations impact the effectiveness of the processes designed to educate and help individuals to cover or challenge violation fees accordingly. Simplifying the collection of information and describing these fields with simple terms. This facilitates automatic translation. Screen readers and features that make information accessible to people with physical or mental impairments will increase effectiveness of information collection and reduce the risk of people sharing unnecessary personal data. Consult the Office of Equity of Human Rights for further support on these issues.	Low
T	II	2.3	Risk of inaccurate demographic representation	Moderate	unlikely	The collection of demographic information about the offender must be well justified. Adding unnecessary personal information creates more privacy risks and they need to be balanced with overall benefits. Administrative rule ADM-18.03 describes the City of Portland demographic data standard. This policy guides the collection of demographic data from the public.	Low

						An inaccurate collection of demographic information can create bias and misrepresent a system issue. An overall recommendation is to keep the collection of demographic data optional and anonymized. This means creating a separate process to collect this information, if the information is not necessary for processing traffic violations reported by the speed cameras.	
T	III	3.1	Risk of unauthorized disclosure of fines or violation of a specific individual	Moderate	rare	Unauthorized public disclosure of information that has not been validated or should not be disclosed due to regulations or legal constraints can impact the public trust in the use of speed cameras and accuracy of the violations. The current procedure has clear check points and only specific information is shared between entities involved in issuing a traffic violation. The risk of unauthorized public disclosure is low; however, high interest cases may create public pressure to disclose specific information. Publicly available information about the procedures to request public records and what data can be disclosed in these cases, can guide public entities like media outlet or other interest parties on what are the options available to them.	Low
T	III	3.2	Risk of public mistrust due to the lack of transparency or available public information.	Moderate	Possible	The lack of transparency or ineffective public communications around the use of speed cameras can trigger misinformation and public mistrust. Misinformation about what cameras collect, how information is shared, and whether these devices live stream video and other parties can access to them are common narratives in communities. PBOT already has publicly available information about where speed cameras have been deployed[18]; however, having better metrics describing how effective these devices are in reducing crashes and traffic speed can improve public trust in this technology.	Medium

[18] https://www.portland.gov/transportation/vision-zero/safety-cameras

						Clarifying that the purpose of these cameras is only for reducing traffic incidents and identifying over speeding and offenders for law enforcement purposes. Additional transparency measures can be added with information describing purpose and ownership of the equipment on site. Online, this information can also identify locations where speed cameras are installed. Signs can describe the purpose of the device, to differentiate it from security cameras and other uses. Almost all the data and information related to the program can be found through public records requests.	
U	IV	4.1	Risk of privacy data breach.	High	rare	Privacy data breaches are the unauthorized extraction or disclosure of personal or confidential information. Privacy breaches are usually connected to cybersecurity issues in the data stewardship pipeline. Both, NovoaGlobal and the City of Portland are implementing modern information security practices, and the likelihood of this risk is low or rare; however, it is still possible, and organizations need to keep constant monitoring of IT infrastructure and training of staff on information security issues. Also, the impacts of this risk are reduced by minimizing personal information collection and data transfers between entities. This is something that NovoaGlobal and the City of Portland are already doing.	Medium
U	IV	4.2	Risk of misidentification of vehicle and ownership	Moderate	unlikely	The process depends on a mix of automated tools and human analysis and interventions. The risk of misidentification is small due to the different checkpoints to verify information retrieved from different data systems. In the case of identifying the wrong vehicle due to ill intention or a verification failure, the person who has done no wrongdoing can challenge this decision with two procedures: Certificate of Innocence. This is included in the alleged violator's citation packet that is mailed or emailed to them. They can use this to attest that: • They no longer own the vehicle	Low

						• Another registered owner was driving the vehicle • Another person was driving the vehicle • The vehicle was reported stolen before the date and time indicated on the citation Affidavit of Non-Liability. This relates to a vehicle that is owned by a business or employer. They can attest that: • The vehicle was sold prior to the violations date • The vehicle is owned, leased, or rented by a business or public agency and was driven by an employee, lessee, renter or other authorized driver at the time of allegation. This information and access to these forms are also available online[19]. Officers review citations before submission and approval to verify any discrepancy and clarity in the vehicle identification.	
T	IV	4.3	Risk of low camera performance due to low maintenance.	Moderate	unlikely	Camera lenses can get obstructed due to dirt, foliage growth, or other environmental factors. Regular maintenance of devices should be part of the operations plan. Devices can also declare when the expected end of life and potential replacement of the camera is. This can be assessed by the vendor.	Low
T	IV	4.4	Risk of vandalism or physical damage of equipment	Moderate	Possible	Speed cameras have been subjected to vandalism and shooting in the past. This risk can appear from public mistrust and grunted residents. Destruction of City property can lead to a criminal investigation. The most common strategy is to put these devices out of reach and clearly inform people about the purpose and report any incident or attack to the integrity of these devices to service lines.	Medium

[19] https://www.portland.gov/transportation/vision-zero/speed-safety-camera-citations

T	V	5.1	Risk of using the speeding data information to identify vehicles involved in criminal activities, including stolen vehicles.	Moderate	rare	There is a legal risk derived from using this information for purposes other than speeding traffic incidents. Oregon law prescribes how footage, if retained, can or cannot be used, this includes using it as evidence for anything else. There might be some risks of lawsuits against the City due to privacy overreach and violation of the 4th amendment. City staff involved in speed cameras information management need to be trained and aware that using information from speeding cameras cannot be used as evidence in court.	Low
U	VI	6.1	Risk of unplanned cost due to equipment upgrades or fixes to improve information protection or detection effectiveness.	Low	Possible	Speed cameras are a mature technology used by government for long time. However, new features like the addition of automatic object or context identification or other artificial intelligence tools could be added as part of the service. These new services may offer benefits and additional unplanned costs. Additional costs due to maintenance and operation may be unplanned due to foreseen causes. It is important to understand what it is under the vendor's warranty, plan maintenance to service devices, and understand upgrades and financial implications derived from these new features.	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 on 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 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 are 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 belief 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