2024 Privacy Impact Assessment

BLTN

[SPD]

1/29/2025

Contents

Privacy Impact Assessment Overview

What is a Privacy Impact Assessment?

A Privacy Impact Assessment (“PIA”) is an analysis of how personal data is gathered, processed, and used for a particular program, project, data initiative, or technology implementation (the terms may collectively be referred to hereafter as “effort”). The PIA asks questions about the collection, use, sharing, security and access of data involved in a City department effort. It also requests information about policies, training and documentation that govern use of the data and any associated technology. The PIA responses are used to determine privacy risks and mitigation measures to reduce those risks. To ensure transparency about personal data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a PIA required?

A PIA may be required when a project, program, or other data processing activity has been flagged through the privacy review process as having a high privacy risk.

How to complete this document?

As department staff complete the document, they should keep the following in mind.

- Department Subject Matter Experts (SME) are responsible for providing responses to the questions. *Please do not edit the questions or question descriptions that are part of the template.*
- All content in this report will eventually be published to the public. Therefore, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written principally using non-technical language to ensure they are understood by audiences unfamiliar with the topic.

1.0 Overview

1.1 Description: Please describe the effort.

Include high level descriptions of any technology and its intended use, the data collected or processed, and all third parties involved in the effort.

BLTN will replace Seattle Police Department's (SPD) existing Patrol Portal and our email distribution lists, allowing better sharing of criminal information bulletins both within Seattle PD and among the surrounding agencies. As criminals cross jurisdictional boundaries, so too must the information about their criminal activity cross between the affected agencies to better enable detectives to resolve incidents in coordination with surrounding jurisdictions. Seattle PD will limit sharing of bulletins within the platform as needed to meet operational/policy requirements.

1.2 Business Need: What business need/problem does this effort address?

Please describe why the department is undertaking this effort.

BLTN will replace Seattle PD's existing Patrol Portal and email distribution lists, allowing better sharing of criminal information bulletins both within Seattle PD and among the surrounding agencies.

1.3 Benefits: What are the anticipated benefits of this effort and how does it relate to departmental and/or City mission?

What is the intended outcome, goal, or benefit? Please provide any data or research demonstrating the anticipated benefits of the effort (e.g. academic studies, etc.).

BLTN will aid detectives in resolving criminal investigations more quickly and safely. By more effectively sharing criminal information bulletins within the Department, detectives will be able to benefit from the collective knowledge of the officers and detectives in SPD. Additionally, by digitizing already shared criminal information bulletins with surrounding police agencies, detectives will more quickly be able to connect the dots between cases that involve the same suspects, helping resolve more cases collectively.

1.4 Technology Details: Describe all technologies that support or will be used as part of the effort.

What systems interact with the data involved in this effort? This includes hardware and software throughout the data lifecycle (e.g. creation, collection, use, storage, disclosure, and destruction). Describe, by name and functionality, all technologies associated with the effort. For example: high-level Microsoft Forms to collect the data, Microsoft Excel to extract the data.

BLTN is a cloud based, CJIS secure environment that provides a platform for dissemination of criminal information bulletins. Rather than relying on the current practice of creating PDF bulletins that are sent out in a less secure way, BLTN allows detectives to create online bulletins, which can include photos and videos of crimes/suspects/missing persons, that will better assist detectives in incident resolution. Additionally, BLTN creates a curated feed for the end user, ensuring they see the bulletins most important to them and their work. BLTN also facilitates more efficient communication between detectives handling related cases by alerting them to the possibility of a connection between their cases, for detectives to further investigate through standard investigative measures. BLTN modernizes the practice of criminal information sharing and bulletin dissemination, replacing SPD's end-of-life technology, all in a CJIS secure environment.

1.5 Scope of Involvement & Use: Who is involved in the implementation or use of the technology, project, and associated data?

For example, what other departments, if any, are involved? Are external partners (e.g. community-based organizations) or vendors/consultants involved?

BLTN will be used by SPD personnel involved in the response to and investigation of crimes. BLTN will also be used by other police departments (subject to their own purchase). BLTN is a cloud-based solution managed by Multitude Insights, LLC.

2.0 Data Details & Collection Practices

2.1 Data Subjects: Whose data will be collected or processed as part of this effort?

Please provide all categories of data subjects (e.g., members of the public, City employees, contractors, etc.) as well as any sub-populations that might be involved (e.g., children, older adults/elderly, incarcerated or formerly incarcerated persons, unhoused persons, etc.)

BLTN will utilize information related to SPD employees involved in investigating criminal incidents as well as members of the public associated with those incidents. Those members of the public can be from any demographic. The data involved will come primarily from RMS, as well as some from CAD, all of which will be documented in the RMS investigation file.

2.2 Data Fields: What are the data fields and data types that are involved in this effort?

Please describe all data collected, stored, generated, analyzed, used, and/or shared, etc.

For SPD employees, the data fields used will include Unit of Assignment, Department, Job Title, Name.

For members of the public, the data fields used will include first and last name, date of birth or age, gender, race or ethnic origin (as it relates to physical description), height, and weight.

2.3 Data Collection: How is the data collected for this effort? What are the data sources for the data used or processed as part of this effort?

Please describe the methods of data collection (e.g., first-party collection which is collection directly from an individual; third-party collection which is collection through another entity, etc.). Also include the mechanism by which the data is collected (e.g., online form/survey, data purchase, data shared/provided by another department, etc.).

The current practice is that as information is gathered pursuant to a criminal investigation, which may include name, DOB or age, physical descriptors including height and weight, information about their vehicles or places of residence, it is necessary to include this information on criminal information bulletins used to correctly identify and/or locate suspects. These bulletins are shared between law enforcement agencies, not only as a means of assisting in identification and apprehension, but for officer safety purposes as well. BLTN is a CJIS secure environment specifically to facilitate this purpose.

BLTN will utilize information related to SPD employees involved in investigating criminal incidents as well as members of the public associated with those incidents. Those members of the public can be from any demographic. The data involved will come primarily from RMS, as well as some from CAD, all of which will be documented in the RMS investigation file.

2.4 Data Flow: Describe how data collected flows through the data lifecycle including the assets used to store and process the data. ("Assets" are things that support the information-related activities, such as software systems, appliances, databases, etc.)

In other words, after data is obtained, where will it go? Where will it spend most of its time? Will it stay put, or will it go somewhere else?

By looking at the information included on each bulletin posted, BLTN notifies users to other bulletins that, based on various information, may be connected to their bulletin. This can include crime type, date and time, suspect and/or vehicle descriptions, and information included in photos and videos within the bulletins. BLTN does NOT use facial recognition or any other biometric analysis. BLTN will only engage with Mark43 Records Management System (RMS) based upon direct input from the user. All access is role based. BLTN does not actively search, index, or pull in any information, other than what it is instructed to do.

2.5 Notice: At the point of data collection, how are individuals notified about the City's use, sharing, and disclosure of their personal data?

Please include all methods, processes, or mechanisms for notification. This may include the City's standard disclosure, use, and sharing notice.

As the information shared is related to open and active criminal investigations, and only shared with CJIS secure police departments, no notification is required or provided.

3.0 Data Use & Processing

3.1 Authorized Data Uses: What are the authorized uses of the data associated with this effort?

In addition to describing all authorized uses of the data, list any data use limitations and unauthorized data uses.

The data used by BLTN may only be used for legitimate law enforcement purposes, including criminal investigations and missing persons investigations.

3.2 Authorized Technology Uses: What are the authorized use cases for the technology associated with this effort? How may the technology be used?

In addition to describing all authorized use cases for the technology, list any technology use limitations and unauthorized technology uses.

Other law enforcement agencies, primarily those within King County. This will include local and state law enforcement agencies. Federal law enforcement agencies may join the platform in the future, as well as agencies from other states. Seattle PD is acutely aware of the concerns around SHIELD laws and Sanctuary City status. Seattle PD will not share information, nor will we participate in investigations related to immigration status or reproductive/gender affirming care. BLTN will support Seattle PD's stance in these cases and ensure Seattle PD bulletins are not shared beyond the scope authorized by Seattle PD.

3.3 Use & Management Policies: What policies (City or department-specific) apply to the use and management of the data *and* technology (if different than the data) associated with this effort?

Please name and describe all applicable policies.

Other law enforcement agencies, primarily those within King County. This will include local and state law enforcement agencies. Federal law enforcement agencies may join the platform in the future, as well as agencies from other states. Seattle PD is acutely aware of the concerns around SHIELD laws and Sanctuary City status. Seattle PD will not share information, nor will we participate in investigations related to immigration status or reproductive/gender affirming care. BLTN will support Seattle PD's stance in these cases and ensure Seattle PD bulletins are not shared beyond the scope authorized by Seattle PD.

3.4 Data Processing & Analytics: Please describe how the data will be processed and analyzed in support of the intended business goal/outcome. Please include metrics.

Describe the scale of processing and analysis to the best of your ability, as well as whether analysis involves matching or combining datasets. Describe the fields required for joining, and the metrics the business will use for the analysis.

AI use: BLTN utilizes an algorithm (AI) to customize what bulletins are shown to each user based on what bulletins they have previously expressed interest in in alignment with their work. Additionally, BLTN uses AI to show users other bulletins that may be related to their own bulletin based upon various factors, including crime type, date and time of incident, suspect and/or vehicle descriptions, and information included in photos and videos within the bulletins. BLTN AI does not use any facial recognition or other biometric analysis to recommend connections between bulletins. Prior to connecting cases, detectives will have to independently validate the connection through standard investigative measures.

4.0 Legal Scope & Compliance

4.1 Governing Laws: What laws, regulations, rules, or contracts govern (a) the data, (b) the data processing activities, (c) the data sharing?

Washington State Criminal Records Privacy Act, Chapter 10.97 Revised Code of Washington (RCW)

Keeping and Release of Records by Juvenile Justice or Care Agencies, Chapter13.50 RCW

Public Records Act, Chapter 42.56 RCW

28 CFR Part 20

4.2 Compliance Measures: What are the compliance measures associated with the use of the technology or data? Who is involved with oversight of requirements defined in 4.1?

The service supports role-based permissions and is CJIS complaint for auditing. Records retention and role-based access (e.g., Public Disclosure Role) is configurable by the client (i.e., SPD). Subject Matter Experts (SMEs) such as the Records Manager and General Council will inform initial configuration and any configuration changes. A log of all requested changes, including decisions, will be maintained by the SPD Data Governance program in the form of a Data Governance Activity Log (DGAL).

4.3 Records Production Compliance: How is the data and/or associated records (e.g., reports, derivatives, etc.) retrievable in support of public disclosure requirements?

Records can be retrieved, within the 5-year retention period, in their native form (webpage) from the service. The Public Disclosure Unit will have broad access to the platform and be designated a role.

5.0 Data Security, Protection, & Storage

5.1 Data Access: Who will have access to the data? Who will have access to the technology (if different than who has data access)?

The data in BLTN will be accessible by SPD personnel with CJIS clearance and assigned to positions that support investigative efforts. This can include, but is not limited to, patrol personnel, investigations unit personnel, analysts, administrative assistants, sworn and non-sworn. The access to the technology is identical to the data access.

5.2 Access Authorization: What processes are prerequisites to a user's access of the data or technology (e.g., user authentication, business approvals/sign-off, documentation, etc.)?

Prior to being given access to BLTN, all users will have to have a verified SPD background, which includes compliance with CJIS access requirements, and a job assignment within SPD that necessitates access to criminal intelligence bulletins. A system administrator will verify all requirements are met before granting access.

5.3 Secure Storage: Where will the data be stored, and what security measures are in place for the storage of the data?

The data in BLTN is stored in the AWS gov cloud, which meets all CJIS security requirements.

5.4 Auditability of Data Access & Data Processing: How will the department ensure that data access and data processing activities are logged and auditable?

The BLTN system includes a usage log that tracks all activity within the system. This can be checked on a routine basis or as requested for the purposes of an investigation or query into a user's activity.

6.0 Data Sharing & Disclosure

6.1 Data Sharing Partners: Which entities (internal and external to the City) will be data sharing partners, if any?

Please describe all parties that will have access to both the data and data derivatives (including other City departments).

Other law enforcement agencies, primarily those within King County. This will include local and state law enforcement agencies. Federal law enforcement agencies may join the platform in the future, as well as agencies from other states. Seattle PD is acutely aware of the concerns around SHIELD laws and Sanctuary City status. Seattle PD will not share information, nor will we participate in investigations related to immigration status or reproductive/gender affirming care. BLTN will support Seattle PD's stance in these cases and ensure Seattle PD bulletins are not shared beyond the scope authorized by Seattle PD.

Law enforcement agencies share information as part of their standard operational requirements. No written agreement exists to memorialize this. However, agencies cleared to possess CJIS information are given an ORI number by the Washington State Patrol and this can be verified prior to engaging in data sharing. Additionally, an agency must be CJIS certified to gain access to the BLTN system. Data sharing terms included within the BLTN contract establish that Seattle PD owns the data.

6.2 Purpose for Data Sharing: What is the purpose of sharing data with the identified parties in the context of this effort?

Law enforcement agencies share information as part of their standard operational requirements. These bulletins are shared between law enforcement agencies, not only as a means of assisting in identification and apprehension, but for officer safety purposes as well. BLTN is a CJIS secure environment specifically to facilitate this purpose. The implementation of BLTN replaces a manual information sharing process; the information being shared is the same as in the current practice.

6.3 Sharing Restrictions: Describe any restrictions on data use and data access and identify the sources that impose those restrictions.

Data sharing agreements/contracts, department policies and procedures, department rules, laws, regulations, and other authorities may impose data restrictions.

Law enforcement agencies share information as part of their standard operational requirements. No written agreement exists to memorialize this. However, agencies cleared to possess CJIS information are given an ORI number by the Washington State Patrol and this can be verified prior to engaging in data sharing. Additionally, an agency must be CJIS certified to gain access to the BLTN system. Data sharing terms included within the BLTN contract establish that Seattle PD owns the data.

6.4 Agreement Updates: Please describe the process for reviewing and updating data sharing agreements.

Please describe the processes for initial development, agreement review, new uses of the data, and new access to the data (including internal and external to the City) as well as how often the agreement gets updated.

No written agreement exists to memorialize this. However, agencies cleared to possess CJIS information are given an ORI number by the Washington State Patrol and this can be verified prior to engaging in data sharing. Additionally, an agency must be CJIS certified to gain access to the BLTN system. Data sharing terms included within the BLTN contract establish that Seattle PD owns the data.

6.5 Records of Data Disclosure: How are records that document data disclosure/sharing maintained by the department?

Please describe how these records are documented either by technical functionality or business practices/processes.

Seattle PD's public disclosure unit will have full access as needed. Additionally, BLTN creates an audit log for every bulletin and every user action.

7.0 Data Retention & Destruction

7.1 Data Retention: What are the record retention schedules that govern both the raw data and any derived outputs (e.g., analyses, reports, transformed/cleaned datasets)?

Retention default is 5 years for the BLTN platform. The retention settings are configurable to the agency's preference.

7.2 Data Destruction: What mechanisms (technical or process-oriented) are in place to destroy improperly collected data?

Deletion from the BLTN platform can be done by the system administrator upon request from a detective. The act of deletion is captured in the usage audit log.

7.3 Responsible Staff: Who is responsible for ensuring compliance with data retention and data destruction requirements?

The admin configuring retention schedules would work in alignment with the City Clerk to ensure that retention and destruction requirements are met.

7.4 Purge Verification: What mechanisms (technical or process-oriented) are in place to ensure that data is properly destroyed after data retention periods have been met?

Automatic deletion within the system in accordance with set retention schedules in alignment with the city clerk.

8.0 Privacy Principles, Risks, & Controls

8.1 Privacy Risks, Harms, Mitigations, & Controls: What privacy risks exist for the effort, and what are the potential impacts on Seattle residents and/or other data subjects?

What are the controls or mitigations that are in place to address these risks, and reduce the likelihood that unintended harms are realized?

Privacy Risk: Data sharing from other jurisdictions with less strict privacy regulation might create concern about information that should not be available.

Mitigation: SPD will be using the technology as is outlined in permissible use. BLTN will respect the boundaried policies and configurations that are specific to SPD and partnering local departments. The implementation of BLTN replaces a manual information sharing process; the information being shared is the same as in the current practice. Seattle PD is acutely aware of the concerns around SHIELD laws and Sanctuary City status. Seattle PD will not share information, nor will we participate in investigations related to immigration status or reproductive/gender affirming care. BLTN will support Seattle PD's stance in these cases and ensure Seattle PD bulletins are not shared beyond the scope authorized by Seattle PD.

Privacy Risk: Sharing data with third parties can increase risk associated with a lack of control over the data. Additionally, the source of the information may place restrictions on the information that can be disclosed or shared, increasing potential legal risk.

Mitigation: Before disclosing information to third parties, the City must confirm it has the authority to share the information with recipient agency or third party for recipient's intended purposes. For example, the City must confirm it has provided notice and choice to individuals to disclose such information, or that such sharing is conspicuously disclosed to the data subject, or that City is authorized to disclose such information under law or under provisions of City privacy policy. Additionally, the source of the information may place restrictions on the information which could limit or prohibit the City's ability to re-disclose such information to third parties. BLTN is contractually committed to ensuring compliance with the contractual terms around data protection and third party sharing restrictions.

Privacy Risk: Personal data elements collected on data subjects considered to be part of a vulnerable population present an increased and potentially disproportionate risk associated with individual privacy harms and confidentiality.

Mitigation: Data subjects who may be considered part of a vulnerable population, may require additional protections throughout the data lifecycle. This risk should be considered with an RSJ and equity lens when collecting or processing personal information for data subjects who may be part of a vulnerable population. Consultation with the Privacy Program, Subject Matter Experts, and the City Attorney's Office is advised. BLTN has partnered with SPD to ensure that all of the above risks have been mitigated by restriction and protections around vulnerable population information.

Privacy Risk: Concern around biometric information collection/sharing.

Mitigation: BLTN AI does not use any facial recognition or other biometric analysis to recommend connections between bulletins. This includes gait analysis.

AI Risk: Generative AI report writing functionality can lead to overreliance on technology, confabulations (hallucinations) and other concerns around LLM data quality and training.

Mitigation: Feature will not be used or enabled for SPD.

AI Risk: Automation bias: overreliance on technology to identify patterns and connect unrelated PDFS. BLTN utilizes AI to customize what bulletins are shown to each user based on what bulletins they have previously expressed interest in in alignment with their work. BLTN uses AI to show users other bulletins that may be related to their own bulletin based upon various factors, including crime type, date and time of incident, suspect and/or vehicle descriptions, and information included in photos and videos within the bulletins.

Mitigation: Prior to connecting cases, detectives will have to independently validate the connection through standard investigative measures. Feedback is provided to BLTN about usefulness of tool.

Multitude Insights has worked with experts at MIT and Harvard to develop the following framework:

Multitude's Evolving Ethical AI Framework:

Our Evolving Ethical Framework has six principles and is designed to be revisited and changed as the bias landscape changes. We revisit it regularly to make sure that it reflects our values and value proposition.

1. **First, do no harm**: The development and deployment of AI systems at Multitude should not cause harm to individuals or society as a whole. This includes avoiding discrimination, protecting privacy, and ensuring that AI systems are secure and reliable.

2. **Put the benefit of the community first**: AI systems should be developed and deployed with the goal of benefiting society as a whole. This includes ensuring that AI systems take into account all members of society, regardless of their background or socioeconomic status.

3. **Procedural fairness**: The development and deployment of AI systems should be guided by principles of procedural fairness. This includes ensuring that AI systems are transparent, explainable, and accountable.

4. **Distributive fairness**: The benefits and risks associated with AI systems should be distributed fairly across society. This includes ensuring that the benefits of AI systems are not concentrated in the hands of a few individuals or organizations.

5. **Never force a decision on a human**: AI systems should not be used to make decisions that override the autonomy or free will of human beings. This includes ensuring that humans have the ability to review and challenge decisions made by AI systems.

6. **Continual iteration and reevaluation**: The development and deployment of AI systems should be an ongoing process that involves continual iteration and reevaluation. This includes monitoring the performance of AI systems over time, identifying areas for improvement, and making changes as necessary.

The Multitude Evolving Ethical AI Framework is based on the principles of ethics, fairness, transparency, and accountability. By following these principles, we can ensure that AI systems are developed and deployed in a way that benefits society as a whole while minimizing potential harms.