Privacy Office
Seattle Information
Technology Department
December 2018

2018 Privacy Program Annual Report

City of Seattle Privacy Principles

We work to find a fair balance between gathering information to provide needed services and protecting the public's privacy.

We value your privacy…

Keeping your personal information private is very important. We consider potential risks to your privacy and the public's well-being before collecting, using and disclosing your personal information.

We collect and keep only what we need…

We only collect information that we need to deliver City services and keep it as long as we are legally required and to deliver those services. Whenever possible, we tell you when we are collecting this information.

How we use your information…

When possible, we make available information about the ways we use your personal information at the time we collect it. We commit to giving you a choice whenever possible about how we use your information.

We are accountable…

We are responsible for managing your personal information in a manner that is consistent with our commitments and as required by law. We protect your personal information by restricting unauthorized access and by securing our computing resources from threats.

How we share your information…

We follow federal and state laws about information disclosure whenever we work with outside governmental agencies and in answering Public Disclosure Requests (PDRs). Business partners and contracted vendors who receive or collect personal information from us or for us to deliver City services must agree to our privacy requirements.

Accuracy is important…

We work to maintain and use accurate personal information for City business. When practical, we will work to correct inaccurate personal information. We also direct our partners and contracted vendors to follow the same guidelines.

2018 Annual Report

The Privacy Office was created with the goal of building public trust in how we collect and manage the public's personal information. In 2018 we've worked hard to mature the services and operations that actualizes this commitment. This report reflects on our activities and shares the program's direction.

Letter from the Chief Privacy Officer

I was pleased to return to the City as Chief Privacy Officer in July 2017 and resume the work we started in 2015 to create the City of Seattle's Privacy Program. Information and technology transparency are critical to safeguard public trust in government. The City of Seattle's innovative program has led the way nationally for municipalities to ensure public privacy.

The intersection of municipal government and technology, in the use of big data analytics, the growth of the Internet of things, machine learning and artificial intelligence, facial recognition and social media analytics for example, increases public concern about how individuals' information is collected and used. Information collection and use practices that are acceptable in the private sector for convenience, comfort or entertainment often appears intrusive when used in the government setting.

This is further evidenced in the 2017 update to the Seattle Surveillance Ordinance, providing Council and public oversight in the review and approval of technologies for use in investigations. Primarily targeted at police technologies, the ordinance and subsequent amendments involve all City technology acquisitions that meet the definition of surveillance. This added component of the Privacy Program has created additional opportunities for public interaction, comment and education about City privacy practices.

We continue to grow the Privacy Program, with new tools, personnel and service offerings to assist the City in meeting the privacy and transparency commitments we have made to the public.

Ginger Armbruster,
Chief Privacy Officer

Content

Privacy Office Team

Ginger Armbruster, Chief Privacy Officer
Dylan Morris, Privacy Program Manger
Sarah Carrier, Senior Privacy Specialist
Nathan Merrells, Privacy Specialist
Omari Stringer, Graduate Fellow
Peggy Wang, Graduate Fellow

About the Privacy Program

The privacy program is designed to provide the structure and guidance required for City departments to incorporate the appropriate privacy practices into daily operations and to build public trust and confidence in how we collect and manage the public's personal information.

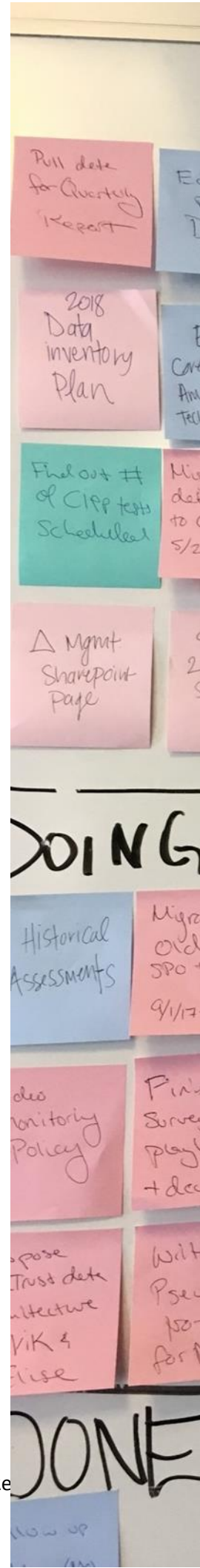
In 2015, we designed a citywide Privacy Program to provide guidance and tools to City employees when working with personal information. We convened a group of representatives from across 15 City departments to create policies and practices to define and implement a citywide program to address our privacy commitments. Since that start, the program has continued to grow. We now conduct hundreds of privacy reviews each year about the technologies we use to deliver needed services to ensure that new and existing City programs across all of our many departments use and protect information we collect.

Advancing Program Maturity

Privacy is part of the department's common goal of customer service for both the public and departments we serve by ensuring privacy reviews occur quickly, prioritizing shorter, more frequent reviews along with self-service tools and training for City staff. We use Lean principles and Kanban work management tools to ensure work flows constantly and quickly, prioritizing small iterative reviews over long, ineffective engagements.

The City's privacy maturity model was developed from International Association of Privacy Professionals (IAPP) frameworks for privacy programs. In 2017 Seattle was operating an "Ad-Hoc" Privacy Program. By using the P-Ops approach to privacy program management, the team implemented a series of strategic improvement projects to reach a "Defined" state in 2018.

2017	2018		2019	
Ad Hoc	**Repeatable**	**Defined**	**Managed**	**Optimized**
Unstructured approach where privacy policies, processes, and practices are not sufficiently defined or documented. Privacy management is mostly dependent on initiatives by individuals rather than processes.	Privacy is viewed as a compliance exercise and the approach is largely reactive with some guidelines. There is limited central oversight of the privacy policies, processes, and practices, with siloed approaches between units.	Privacy policies, processes, and practices are defined, comprehensive to meet business needs, and are consistently implemented throughout. There is a holistic and proactive approach with widespread awareness.	Privacy is embedded into the design and functionality of business processes and systems and is consistent across the agency. Well-defined governance and oversight structures exist.	Privacy is viewed as a strategic initiative with a clear agency culture of continuous improvement. The agency is viewed by stakeholders and the public as a leader in privacy management, introducing innovative initiatives to meet their needs.



Key Performance Indicators

0.7

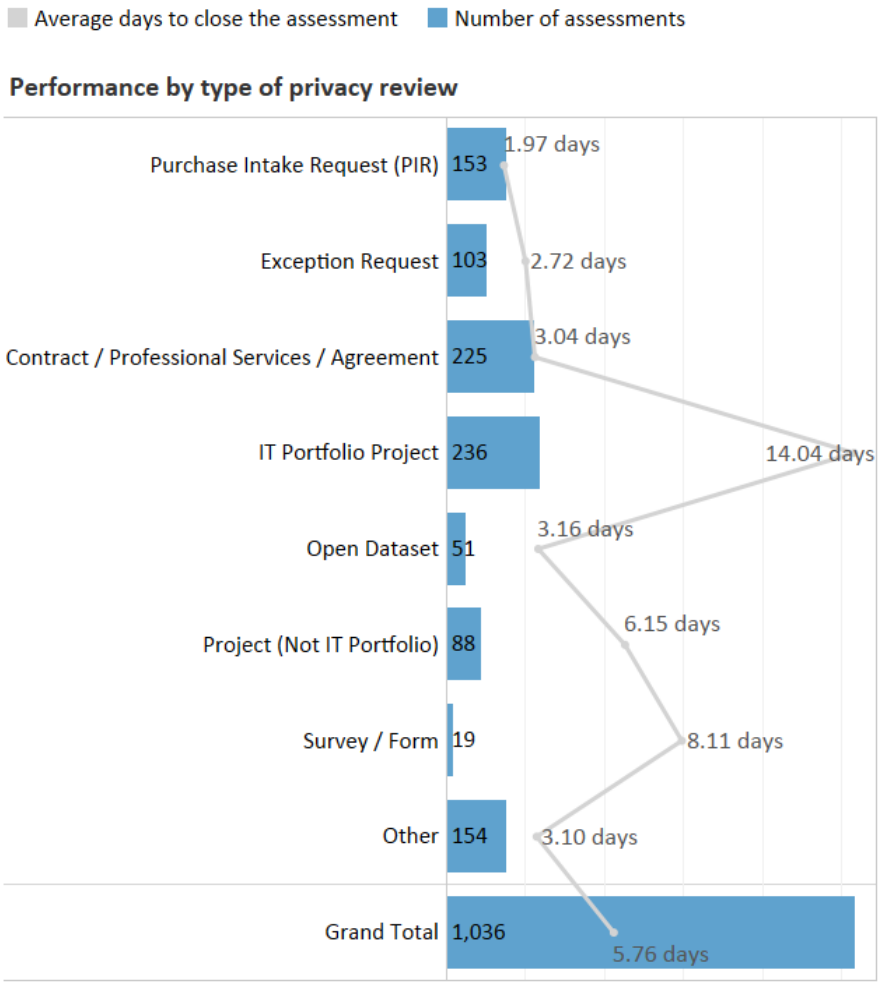
days on average to complete an initial privacy review

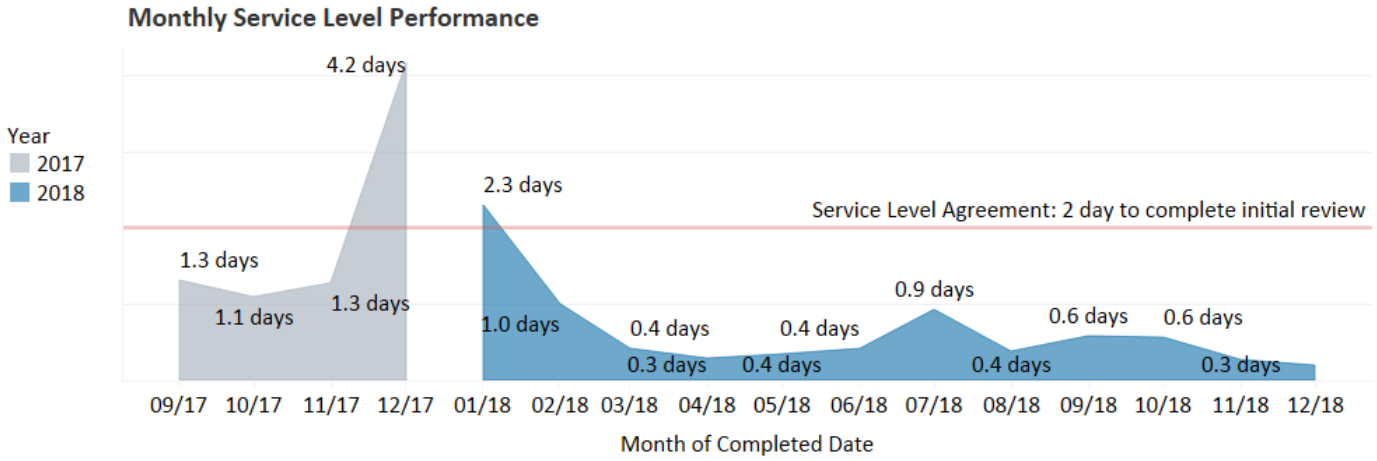
89%

assessments with an initial review completed in less than 2 days

1,004

reviews completed since the Surveillance Ordinance went into effect, September 2017 - December 2018





Key Accomplishments

- **Implemented Privacy Review and Risk Management Tool.** Privacy Team has recently acquired OneTrust, an assessment and risk management tool which will improve the efficiency of the privacy and surveillance assessment process and security intake process. This is the first step in their on-going efforts to streamline the review process make it easier to complete.
- **Privacy Review Process Gap Analysis and Revision.** The Privacy Program conducts reviews as part of numerous IT acquisition and change processes, such as purchasing and IT project stage gate review. To ensure compliance with the Surveillance Ordinance and operation effectiveness, the team completed a gap analysis of Privacy's integration into the five primary IT technology acquisition processes and recommendations for improvement.
- **Data and Survey Demographic Data Collection Playbook.** The City of Seattle collects personal information from the public so that we can provide important services, particularly to vulnerable populations. This Playbook introduces the privacy implications of municipal surveys and provides a guide for how to design a survey that collects demographic data in a manner consistent with the City's Privacy Principles.
- **If-Then Planning Tool for IT Project Reviews.** In cooperation with Orrick and the City Attorney's Office, the Privacy Office created a privacy recommendation tool for technology projects to identify action items and risks mitigations prior to completing their privacy review. The goal of this work is to automate project manger's ability to minimize privacy risk, prior to a review, thus decreasing the privacy review process time and increasing staff empowerment.
- **Pseudonymization Framework Proof of Concept.** Pseudonymizing data is a privacy risk mitigation technique that adds protection without compromising the integrity of the data for reporting and analysis by allowing staff to generate pseudonyms for personal and demographic data, much like anonymization, but which can be re-linked to the access-controlled source data table(s) by select individuals. This pilot determined that pseudonymization is most effective in environments with robust data access controls and analytic maturity.
- **Tailored Forms for Surveys, Open Datasets and Contract Reviews.** Using the OneTrust platform, the Privacy team created specific reviews for Open Datasets and Contract reviews to minimize the assessment form length and time to complete, while improving the quality of information received. This was a direct response to client feedback from City staff.

Surveillance Review

The City of Seattle Surveillance Ordinance 125376 took effect on September 1, 2017 and is designed to provide greater transparency to City Council and the public when the City acquires technology that meets the City's definition of surveillance. For each new technology that meets the criteria for surveillance, a City department must prepare a **Surveillance Impact Report** ("SIR"). These reports include an in-depth review of privacy implications, especially relating to equity and community impact, which are then submitted for public comment. **The first public comment period on Surveillance Technologies opened October 8, 2018**, and covered six technologies used for parking, traffic, and emergency response.

1. Closed Circuit, Traffic Cameras
2. License Plate Readers
3. Emergency Scene Cameras
4. Hazardous Material Cameras
5. Automated License Plate Readers
6. Parking Enforcement

The SIR process entails the following five steps.

What is Surveillance?

By ordinance, surveillance is defined as 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."** Certain technologies, such as police body cameras and technologies for everyday office use, are excluded from the law.

Additional Accomplishments

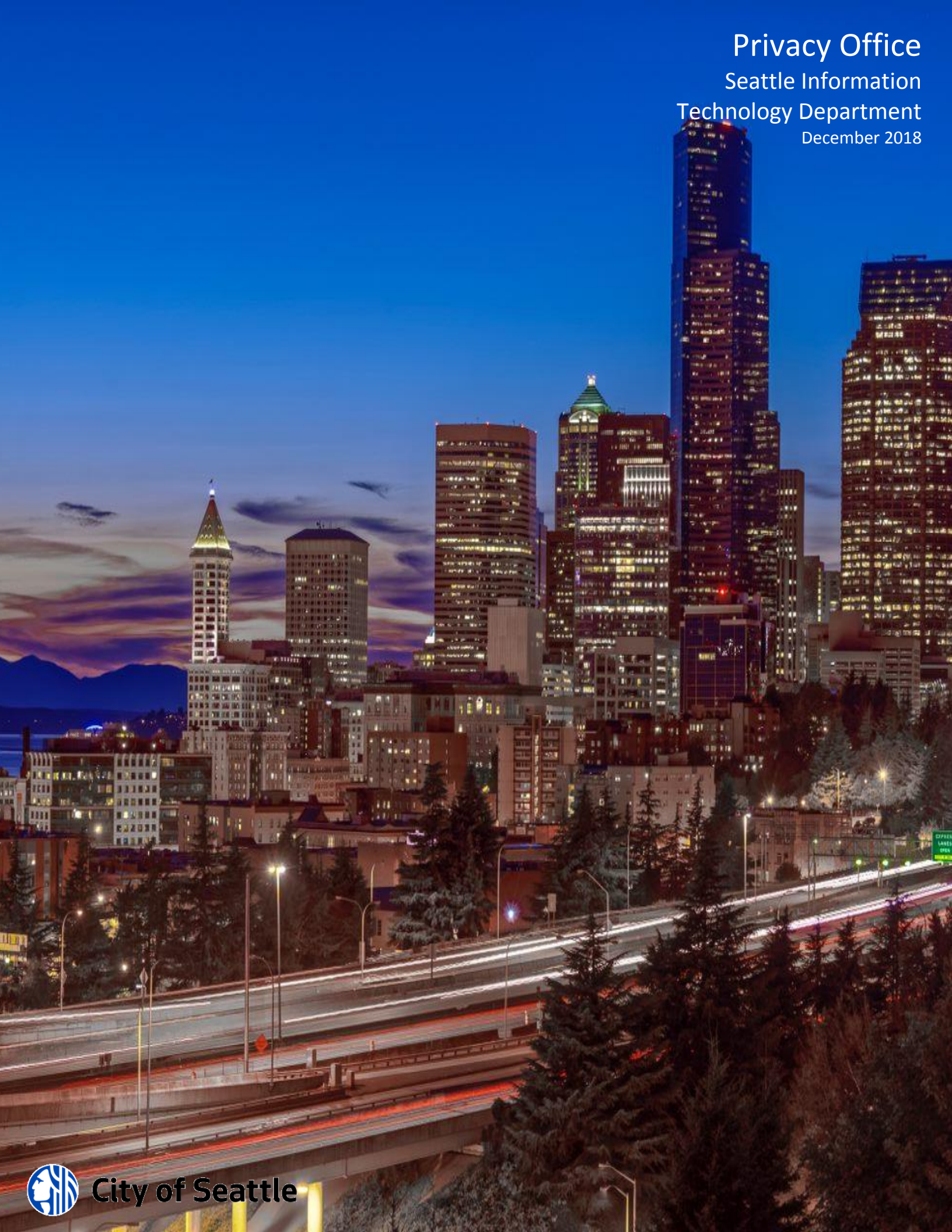
- **Q1-Q4 Technology Acquisition Reports**
- **Surveillance Impact Report Playbook**
- **Surveillance Master List Updates**
- **Website Re-Design**

1. An **initial draft** of the SIR is created, which includes a privacy impact assessment, financial information, and an equity assessment.
2. The draft SIR and supporting materials are released for **public comment**.
3. The **finalized SIR**, including collection of all public comments, is completed.
4. An advisory working group reviews the SIR and provides a **Civil Liberties and Privacy Assessment**.
5. **City Council reviews** the SIR and determines the use of the surveillance technology.

Privacy Office

Seattle Information Technology Department

December 2018



City of Seattle