City of Seattle Privacy Program

2019 Annual Report: Transforming Privacy

Abstract

The Privacy Office was created in 2015 to build public trust in how we collect and manage the public's personal information. In 2019 we continued our work to mature the services and operations that actualize this commitment. This report reflects on our activities and shares the program's direction.

Report prepared by the Privacy Team

- Ginger Armbruster, Chief Privacy Officer
- Sarah Carrier, Privacy Program Manager
- Nathan Merrells, Senior Privacy Specialist
- Omari Stringer, Privacy Specialist

Contents

Letter from the Privacy Office

It has been a busy and productive year here at the Privacy Office. We spent this year improving our service delivery, enabling the use of innovative technologies and evangelizing data privacy within the City and with our colleagues in other municipalities.

Privacy Team members Ginger, Nathan, Sarah and Omari at our Annual Training Kickoff event

Enabling Technologies

A vital part of our job is to help our departmental customers to improve their interaction with Seattle residents and visitors while upholding our commitments to the City's Privacy Principles. This year, we worked with departments to pilot the use of artificial intelligence to aid emergency response, improve resident outreach to deliver needed services through marketing automation tools and explore intelligent city technologies to improve traffic and building safety. Recent work on recommendations about using contracted unmanned aerial systems (UAS) will improve watershed asset management and emergency response to catastrophic events in the coming year.

Improving Service

We have improved our online review tool, OneTrust, adding an automated Risk Analysis component to our reviews. This will allow our team to apply more consistent standards to our evaluation of privacy risk for each new project or product we review and calculate how that risk is mitigated with the recommendations we provide through the review process. Additional work to add incident management is a new component of our online tool, providing a framework for managing and documenting privacy incidents for communications, workflow and legal and regulatory compliance. Finally, the addition of a service offering in our Citywide Service Hub tool allows us to provide a formal venue for customer consultation and training requests. These changes will allow us to provide both improved service and increased performance reporting on our activities.

Providing Leadership

Finally, our team has worked to increase municipal privacy awareness through a Citywide reintroduction of the Privacy Program. We have also participated in over 20 industry panels and consultations with other municipalities across the country as more and more entities seek to stand up similar programs. We foresee an increase in the importance of municipal privacy in 2020 in tandem with federal and state legislative activities and we want our program to continue to be positioned as a leader in this emerging arena.

Here's to a productive 2019 and more innovation and progress to come in 2020!

Ginger Armbruster

Ginger Armbruster
Chief Privacy Officer, City of Seattle

About the Privacy Office

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 on technologies we use to deliver needed services, ensuring that new and existing City programs across all departments appropriately manage and protect the information we collect.

The Privacy Office's continued mission is to increase public trust in the management of data collection through a principles-based privacy program. As part of Seattle Information Technology's goal to be a Best-in-Class Service Delivery organization, the Privacy Office supports the department by improving and streamlining the privacy review process, meeting or exceeding customer service expectations, providing a variety of training opportunities for all City staff, and finding innovative solutions to aid in creating internal efficiencies to improve our customer experiences.

2019 Program at a Glance

Below is a snapshot view of some of our achievements this year:

Key Accomplishments

A breakdown of some of our key program accomplishments for 2019 include:

- **Privacy Toolkit Modernization.** With the help of the Digital Workplace team, the Privacy Office became one of the first ITD divisions to migrate our content and resources to the new SharePoint Online Modern template. This project revitalized the Privacy Toolkit, allowing our Citywide customers to access important information, policies, and resources in a vastly improved experience.
- **Privacy Services Request Offering.** In order to expand our service offerings to our clients Citywide, the Privacy Office worked with the ITSM team to develop and launch a new Request Offering in the Service Hub to allow customers to schedule a consultation with the team regarding a specific project or technology, or to request a specific training related to facilitating their work in a privacy-protecting manner.
- **Approval of Surveillance Technologies.** On September 23rd, 2019, the Seattle City Council unanimously approved Ordinance 125936, which retroactively approved the use of the Seattle Department of Transportation's Closed-Circuit Television Traffic Cameras and License Plate Readers. This Council vote represents the first approval of a surveillance technology under the Surveillance Ordinance, and the culmination of two years of work by SDOT, Seattle IT, and other stakeholders.
- **Performance Visualization Improvement.** To streamline reporting and consolidate Privacy's performance goals, the Privacy Office performed a data gap analysis. This work resulted in more robust reporting capabilities allowing us to leverage data to drive outreach efforts, increase transparency, and improve overall service delivery. The culmination of this work is available to all City employees through a dashboard on the new Privacy Toolkit SharePoint site.
- **Surveillance Website Improvement.** Working with our Web Services Team, we recently conducted a Usability Evaluation of our Surveillance Technologies webpages, and subsequently re-designed and launched it with great improvements. The initial assessment of the webpages was a 58 / 100**.** The acceptable passing score and average is a 75 / 100. Following work with the Public Engagement Services' Usability team to identify specific areas of improvement and mockups of a potential re-design, the Privacy Office was able to successfully improve the website's design and functionality, bringing it to a new score of 79 / 100. We look forward to continuing this work in 2020.

This is an overview of just a few of the major the projects we completed this year. Details about our operational progress and performance dashboard follow later in this report.

Legislative Activities 2019-2020

The active 2019 legislative agenda regarding data privacy continues into 2020 with consumer data protection a focus at both the state and federal level. Some of the items that have implications for our state and City of Seattle residents are listed below:

State

- The **California Consumer Protection Act (CCPA)** is a precedent setting consumer data protection law that establishes a broad range of requirements for online businesses. The law was passed early in 2019 but then underwent numerous amendments before going into effect January 1, 2020. While amendments provided clarification to important definitions, added a data brokerage registry, outlined breach notification changes and provided other updates, the GDPR-like set of consumer rights governing data collected by businesses that fit the eligibility criteria remains intact. Many thought leaders believe that this effort will follow the usual pattern of ground-breaking state level legislation being picked up by other states and eventually lead to legislation at the federal level. Microsoft has already stated that they will apply CCPA regulation to their U.S. business activities. This is an important one to watch to see what other states will do next year and how industry leaders will comply.
- Closer to home, **The Washington Privacy Act (WaPA** - **SB 6281)** seeks to offer similar consumer data protections to the California Consumer Protection Act (CCPA) that went into effect on January 1, 2020. These include requirements for companies to provide information about how data is collected and use, enable the ability to correct inaccurate information and delete data upon request under specific circumstances. While there is no private right of action the State Attorney General would be empowered to address violations on behalf of the public. The law would apply to companies with at least 100,000 customers that collect more than 50% of their revenues from sales, control or processing of personal data for 25,000 or more consumers.

  The WPA failed a House vote in the final 2019 session but was reintroduced at the start of the 2020 legislative session in Olympia, which started Monday, January 13th. This bill is a priority for the Governor as well as key state legislators, including the bill's sponsor Sen. Reuven Carlyle. In 2019, much debate revolved around the role of industry in shaping this legislation. Among the concerns expressed by the ACLU is that industry's involvement would result in a lighter regulatory burden for companies such as Microsoft and Amazon. It must also be noted that several legislators have already expressed their concerns about additional work that needs to be done on the bill to gain broader support and whether any differences may be resolved in this 60-day session.
- **The Use of Facial Recognition Services Bill (SB 6280)** acknowledges that there are some beneficial uses but seeks to put stringent limitations and require extensive reporting for any government agency seeking to use facial technology. It further requires public comment and engagement about new technologies before they are acquired; an external task force to be in place to provide guidance and

recommendations to the Governor by 2021; and annual technology accountability audits to ensure adherence to the law. It would also require annual testing to ensure that the technology works as represented. The bill did not pass out of committee in 2019, but Sen. Joe Nguyen has reintroduced it in the new 2020 session.

This law would have implications for use beyond police investigation and enforcement as this technology is in use in the private sector, from gaming and recreational design applications to mobile device authentication to a variety of Smart City sensor technologies. Despite limitations to protect civil rights, the ACLU has stated their continued opposition to the use of facial recognition and are likely to continue to seek an outright moratorium on all government uses.

- **The Remedies for Misuse of Biometric Data Bill (HB 2363)** establishes as a fundamental human right, the personal ownership of biometric identifying data such as fingerprints and other markers. It further requires the Attorney General and Chief Privacy Officer to stand up a task force made up of primarily civil libertarians and privacy advocates to present findings and recommendations to relevant legislative committees about legal remedies for data misuse violations.

- **The Consumer Protection Requirements for Data Brokers Bill (HB 1503)**, held over from 2019 and reintroduced in the 2020 session, empowers the state Chief Privacy Officer and Attorney General to require data brokers to pay an annual registration fee and to disclose certain information regarding their practices, including opt out opportunities and whether the data may be sold. Failure to register could result in a $10,000 annual fine. The bill further requires brokers to implement a comprehensive information security program to protect personally identifiable information and prohibits the acquisition of personal information through fraudulent means or its use for illegal purposes such as stalking, committing a fraud or engaging in unlawful discrimination. The Attorney General and Chief Privacy Officer are required to compile a report with legislative options for protecting consumer data privacy.

Federal

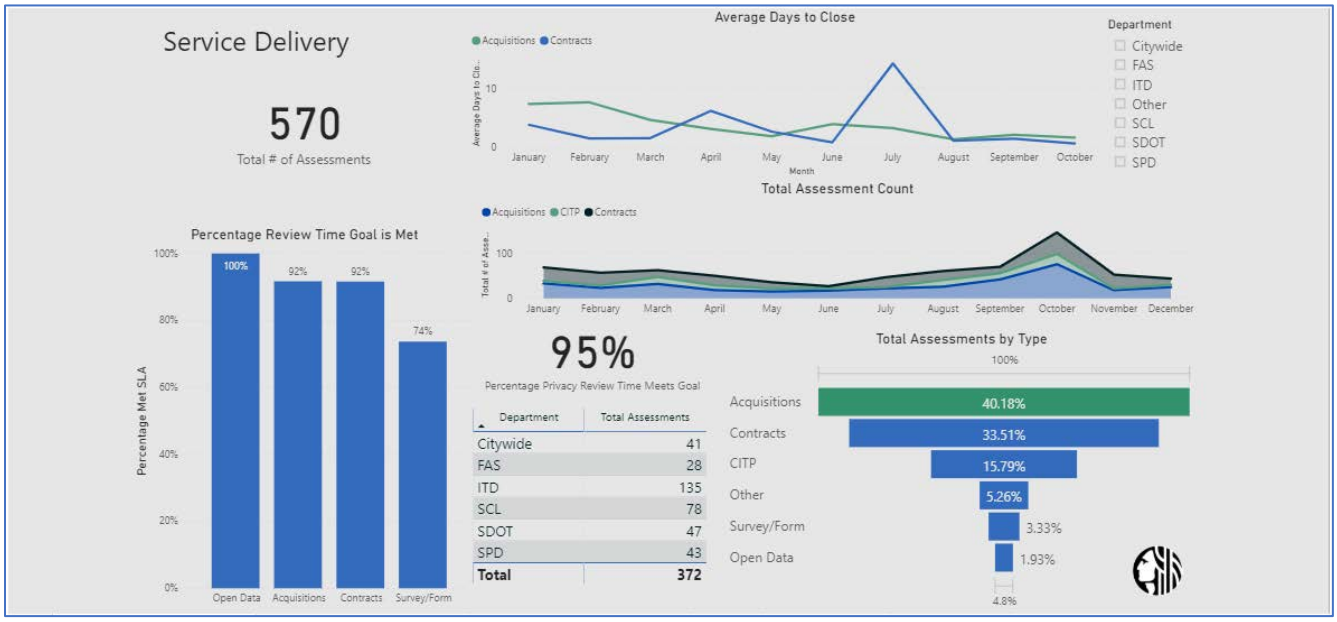
Both Senator Maria Cantwell (D-WA) and Representative Suzan Delbene (D-WA) have been instrumental in sponsoring federal legislative efforts. Until we have a federal law in place, the U.S. will continue to lag the European Union and the General Data Protection Act that provides broad consumer data protections for EU residents. In the absence of federal legislation, international companies will continue to build their privacy practices around the GDPR and CCPA laws and they become the de facto standards for consumer data handling practices.

Both bills are directed at private sector businesses and consumer data rights but will establish expectations around data collection and use transparency that we may see translate to the public sector in the future. In the current political climate, it will remain to be seen how these important efforts at enacting federal regulation will proceed:

- Rep. Suzan Delbene reintroduced her 2018 **Information Transparency and Personal Data Control Act** bill, aimed at providing the Federal Trade Commission and states attorneys general with increased jurisdiction and powers over consumer data rights.
- Sen. Maria Cantwell, with co-sponsors Sens. Schatz, Klobuchar and Markey, have introduced the **Consumer Online Privacy Rights Act (COPRA).** It emphasizes a variety of data rights, including opt out of data transfer, rights over sensitive data, access, portability as well as deletion and correction. It addresses security and staffing requirements, while establishing eligibility and exceptions. It further adds the right of private action and beefs up the powers and resources of the Federal Trade Commission in enforcing the law. Interestingly, COPRA would not preempt state law if it offered stronger protections, establishing the law as a data protection floor not a ceiling.

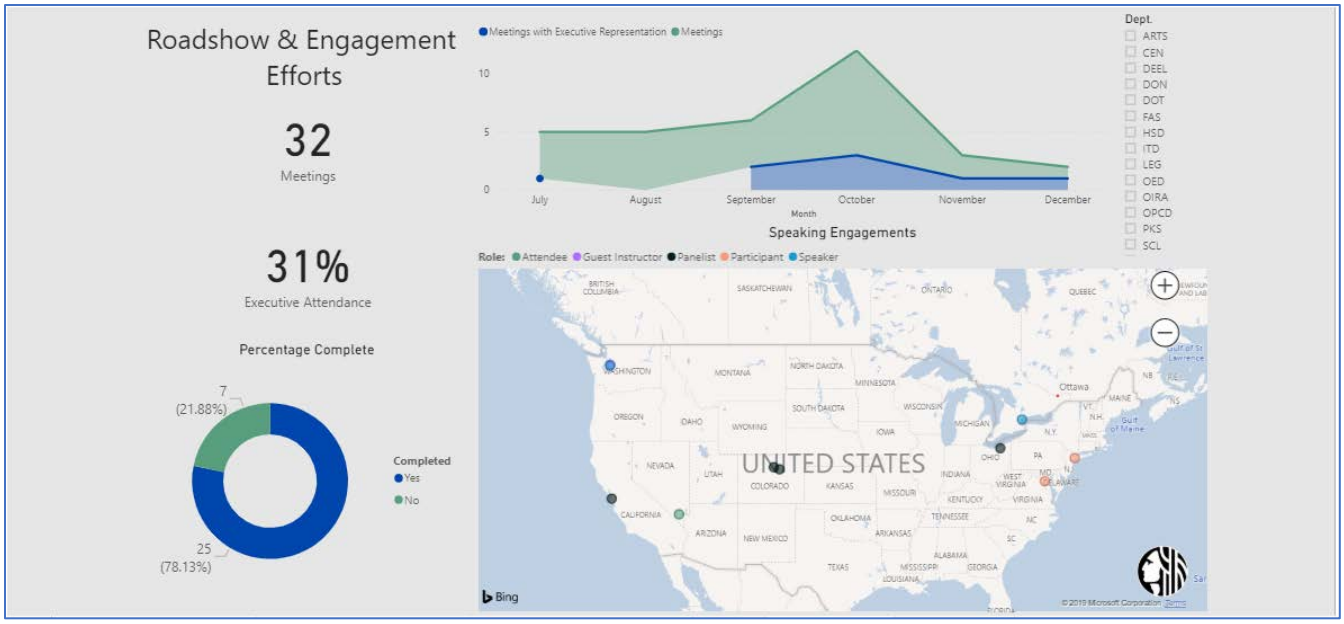
Performance & Outreach

This year, our department changed how we measure performance to an Objectives & Key Results (OKR) model used in many leading technology companies around the world. Working with Power BI and system data from our online assessment tool, OneTrust, and Service Hub, we can now represent our work performance in an accessible dashboard. Following are the key results we achieved this year:



A critical part of a successful program is understanding who our customers are and how we are meeting their service needs. Our online review tool, OneTrust, provides insights into the number and type of reviews we conduct, how we are performing against our service commitments and how the work is divided between departments. Observations from these performance numbers include:

- Of the over 600 reviews conducted this year, more than 40% were related to new technology acquisition, followed by service contracts at 33%.
- Despite a spike in July, we are consistently reducing the time to complete both purchase and contract reviews.
- While we are largely achieving our goal to conduct reviews according to our service delivery commitments, we have some work to do to meet our 5-day review goal for reviews of forms and surveys.
- Information Technology is our largest customer. Together with four of the City's major customers (City Light, Transportation, Police and Finance) they constitute the bulk of our work.

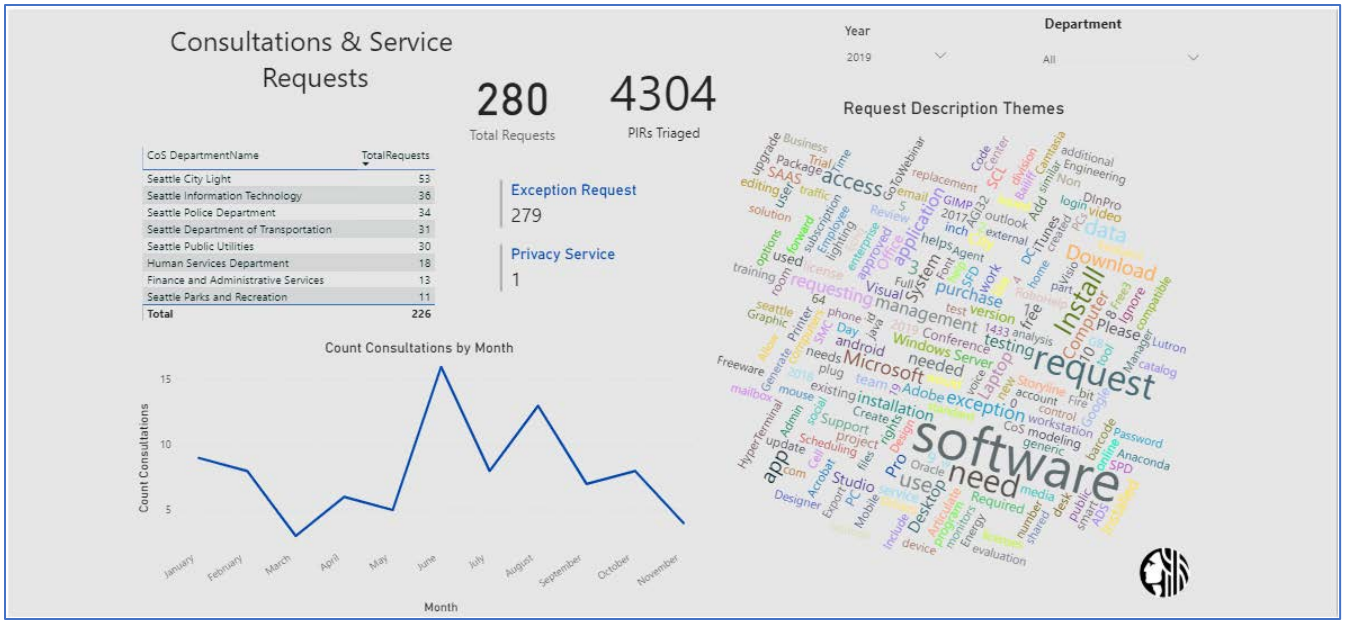


Scheduling meetings with executives, leadership and operational teams across all City departments, we conducted our Privacy Roadshow to reintroduce our program to new leadership and answer their departments' privacy related questions. In 2019 we accomplished the following:

- Scheduled meetings with more than 19 City departments.
- Presented our program details to over 250 City employees.

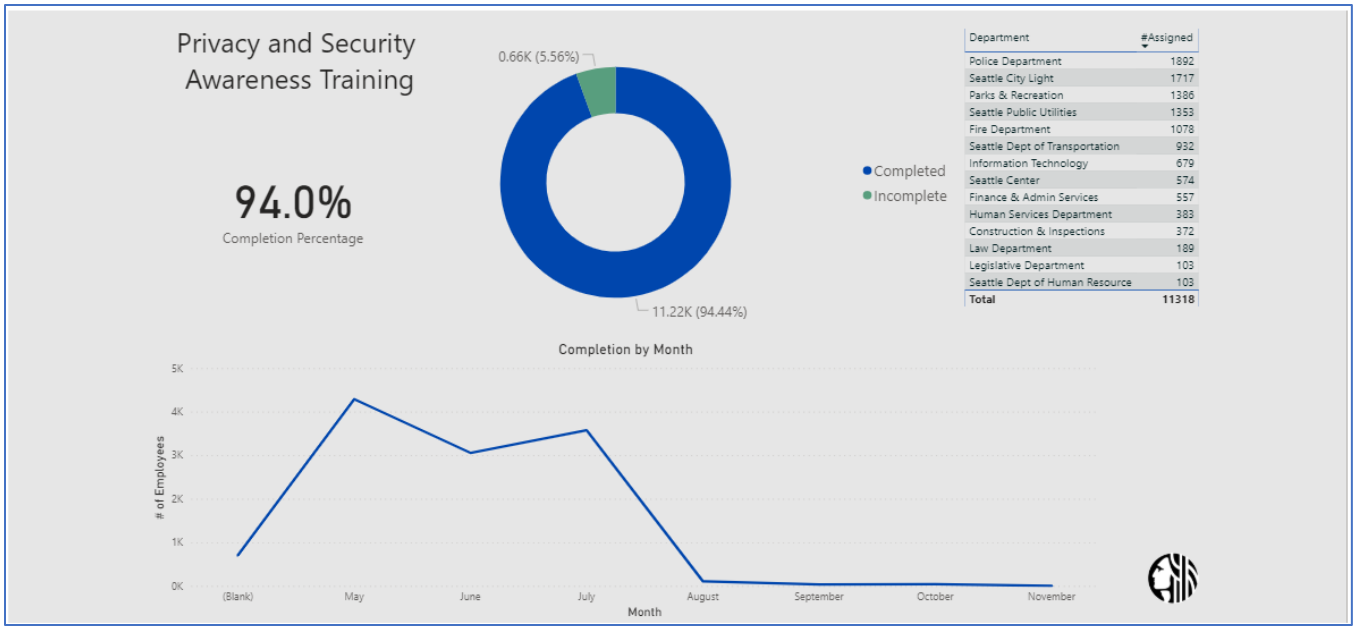
In addition to internal outreach, we spent time meeting counterparts in other cities and participated in academic meetings and informational panels across the country and Canada:

- Consulted with over 20 municipalities that are beginning to stand up their own privacy programs.
- Participated in 12 industry and academic meetings contributing information about our privacy program and surveillance ordinance.



In addition to completed reviews, we now report on the consultations we conduct with customers and Service Requests that are processed through the Service Hub. This amounts to:

- Completing over 270 hardware and software exception reviews, with City Light as our top customer.
- Executing on 92 consultations and training requests Citywide.
- Completing risk assessments for over 4,300 purchase requests.



Training and awareness about the requirements and risks associated with the public's data are integral to a successful privacy program. We are proud that the Citywide completion rate for the annual online Privacy & Security course was 94% - with the Information Technology department finishing at 99.9% completion! This a testament to the dedication and commitment of each of our employees to this important subject. Key take-aways are:

- 11, 318 employees completed the online course – equating to a 94% City-wide online course completion rate.
- The Department of IT showed leadership with a 99.9% completion.
- The top departments for taking the online course this year were Police, City Light, Parks, Public Utilities and Fire – thank you!

Surveillance Ordinance Compliance

The beginning of 2019 saw the successful completion of public engagement and finalization for the first SIR technologies for review, which included:

- Computer Aided Dispatch (Fire and Police)
- Acyclica (SDOT)
- Current Diversion Technologies (City Light)
- CopLogic (Police)
- 911 Logging Recorder (Police)

Per Council request, the Privacy Office also worked on developing a Condensed Surveillance Impact Report (CSIR), which is meant to provide a high-level overview of the applicable policies and procedures related to the use of the specified technology. The addition of the CSIR to the SIR process has extended the effort to approve retroactive technologies, and work on retroactive approvals is expected to continue into 2020. Accomplishments for 2019 include:

- The first two Surveillance Impact Reports for SDOT's CCTV Traffic Cameras and License Plate Readers (LPR) were approved unanimously by City Council on September 23, 2019.
- By the end of 2019, the 12 additional SIRs were completed and awaiting Council consideration in 2020.

Additional Accomplishments:

- Hosted one Public Engagement meeting
- Submitted four CTO Quarterly Reports
- Completed the Annual CTO Surveillance Equity Report
- Completed the Annual SIR Status Report
- Successful redesigned the Public Website providing surveillance program details
- Provided administrative support to 11 Surveillance Working Group meetings

Special Thanks

Saad Bashir, Chief Technology Officer
Sam Zimbabwe, Director SDOT
Kate Garman, Mayor's Office
Jason Cambridge, SDOT
Adiam Emory, SDOT
Greg Doss, Central Staff
Lise Kaye, Central Staff

Moving Forward: Privacy 2020

The Privacy Office strives to provide best-in-class customer service for our City departments and ultimately the public we all serve. We are working to accomplish this by building privacy into our City systems and processes and maturing our program. Below is the maturity model we are following, derived from the General Accounting Privacy Principles version:

Privacy Program Maturity Model

2017	2018-2019		2020-2022	
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.

In the coming year, the Privacy Office will continue to advance our program maturity, driving toward a "Managed" Privacy Program by focusing on growth in the following three objectives areas:

1. Privacy by Design

We continue to work with internal groups to identify ways to integrate privacy into City processes. In the coming year we will be working on the following:

Incident & Breach Workflow Automation. Following the successful implementation of assessment automation in the OneTrust platform, the Privacy Office acquired an Incident & Breach management system that will further prepare the City to respond effectively and efficiently to privacy incidents. This tool will also provide new tracking and reporting capabilities to determine the effectiveness of the Privacy Incident Response Plan.

Pilot of AI Privacy Tool. As part of Seattle IT's objective to continue creating a modern and innovative experience, the Privacy Office successfully launched a pilot of a next generation compliance tool, Privaci.ai. The solution leverages artificial intelligence, targeted data discovery, and assessment automation to build a comprehensive view of the City's privacy risk, as well as prepares us for future compliance efforts.

Systems Integration. Privacy and Security reviews are currently not conducted on credit card purchases. We will be working with the DSR team in the coming year to create improved oversight into this process. In addition, while we are part of the IT stage gate review process, in 2020 we will be implementing a review prior to go-live for new development projects, to ensure that privacy recommendations are appropriately incorporated into new projects before they are launched.

2. Internal Awareness

With 34 departments and over 13,000 employees at the City, we consider it vital to continue our efforts to drive awareness about data privacy. In the coming year, we will provide the following:

Data Privacy Day. As we have for the past three years, we will take advantage of the upcoming International Data Privacy Day on January 28, 2020 to provide our employees and the public with reminders and new insights into the importance of securing and protecting sensitive data in our personal and professional lives.

Privacy and Security Training. In March, we will conduct our 3rd annual awareness training to ensure that all new and current City employees understand our commitments to the public's data privacy. We are working with our partners in Training, Security, Law and the City Clerk's office to ensure that that the course information is up to date and reaches our employees.

Consultations. Now that we have a service offering in our ServiceHub online tool, we will be able to report the training and consultation requests we receive and complete over the next year. Our goal is to grow this part of our privacy service offering and tailor our delivery to meet the needs of our internal customers.

Roadshow Meetings. We started our Privacy Roadshow this year to reintroduce our program to all City departments and answer their privacy related questions. We plan to continue this activity tin 2020 to meet with all departments to ensure that the Privacy Principles and program are part of Citywide operations.

Champions Reboot. We will be revamping the current Privacy Champions Program, increasing the number and quality of external speakers, sharing important privacy updates. Our goal is to leverage this program for privacy outreach and awareness Citywide.

3. Public Outreach

As our mission is to increase public trust about how we manage sensitive public information, we recognize the importance of making the public aware about our activities, including the following:

Public Awareness. In 2020, we plan to increase our outreach to the public about privacy topics and how the City is tackling data privacy concerns. We have identified opportunities to partner with the Seattle Public Library to deliver public workshops. We will continue our outreach to residents in the City of Seattle through meetings and presentations. We have also committed to creating a publicly facing Privacy Blog to increase our online presence.

Updated Websites. We will continue our work to update and improve our public outreach through optimizing our external website. We have worked with our Web Services team to discover ways to streamline our web properties to ensure that members of the public can more easily find information about both our Privacy Program and Surveillance Ordinance compliance work.

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 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.

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.

We tell you 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.

We tell you 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 understand the importance of accuracy

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.

Privacy Office

Seattle IT

Best-in-Class Digital Service Delivery Team