TRUST Ordinance Compliance

Cesar Mares

Contents

What Departments face

- Obtaining Board Approval
  - Drafting surveillance use policies and surveillance impact reports
  - Community Meetings
- Obtaining City Council Approval
  - Cybersecurity Risks Meetings
- Continual Compliance
  - Drafting Annual Surveillance Impact Reports

What the Board faces

- Documenting and assisting with Department's Progress
  - Surveillance Impact Report & Surveillance Use Policy
  - Annual Surveillance Report
  - Stay connected with departments while they're drafting them
  - Field any inquires related to the TRUST ordinance from City departments, escalate if necessary
- Reviewing and decide on surveillance technology procurement
- Other
  - Updates inventory of surveillance technology across city
  - Stay abreast with other local, state, and national government privacy and surveillance news, and emerging technologies

General Privacy Program

- People, Processes, and Tools
  - Privacy Leader, Privacy Analysts, Privacy Lawyers, Privacy Champions
  - PIAs, Consultation, Contracts, Privacy rights, privacy related Inquiries
  - Software for data governance, PIAs, Data Mapping, Risk MGMT
- Build the program with respect to relevant laws and risk appetite
  - “Minimum Viable Product” to “Above and Beyond”
  - Local governments find themselves not covered by state privacy law but may be under others like HIPAA, local public record request laws, or contractual obligations.
  - Because of this gap, it's almost necessary for local government to develop privacy/surveillance law

Portland’s Program (Overview)

- Privacy Team
- Privacy Resolutions
- Community Presence
- Privacy Impact Assessments
- Surveillance Technology Inventory

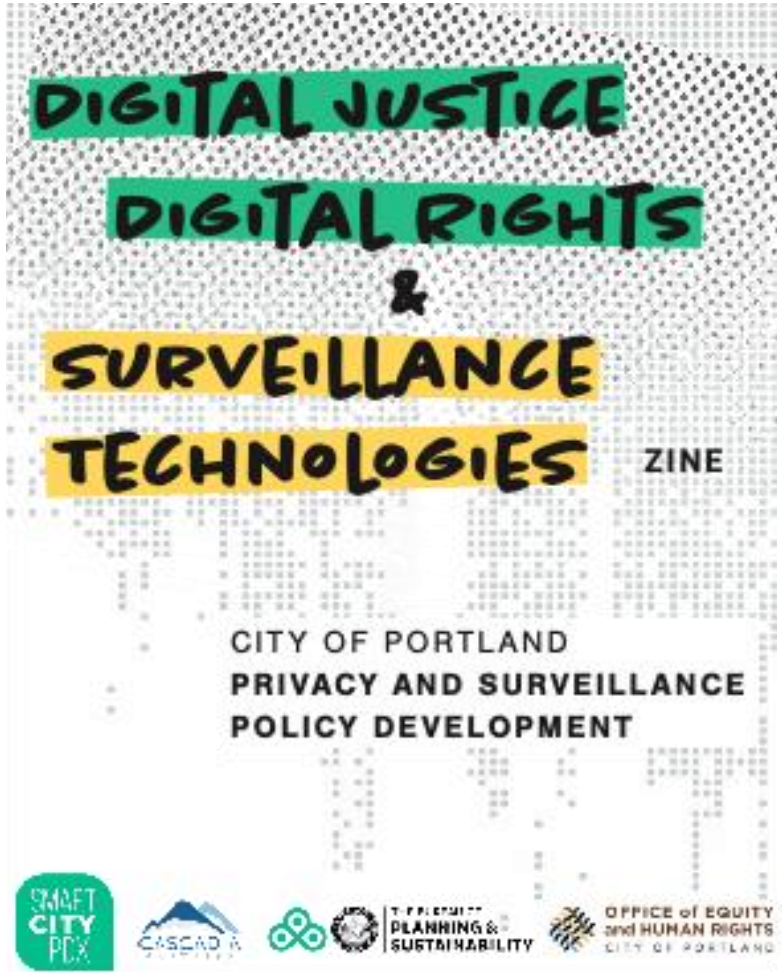
Portland’s Program (Privacy Team)

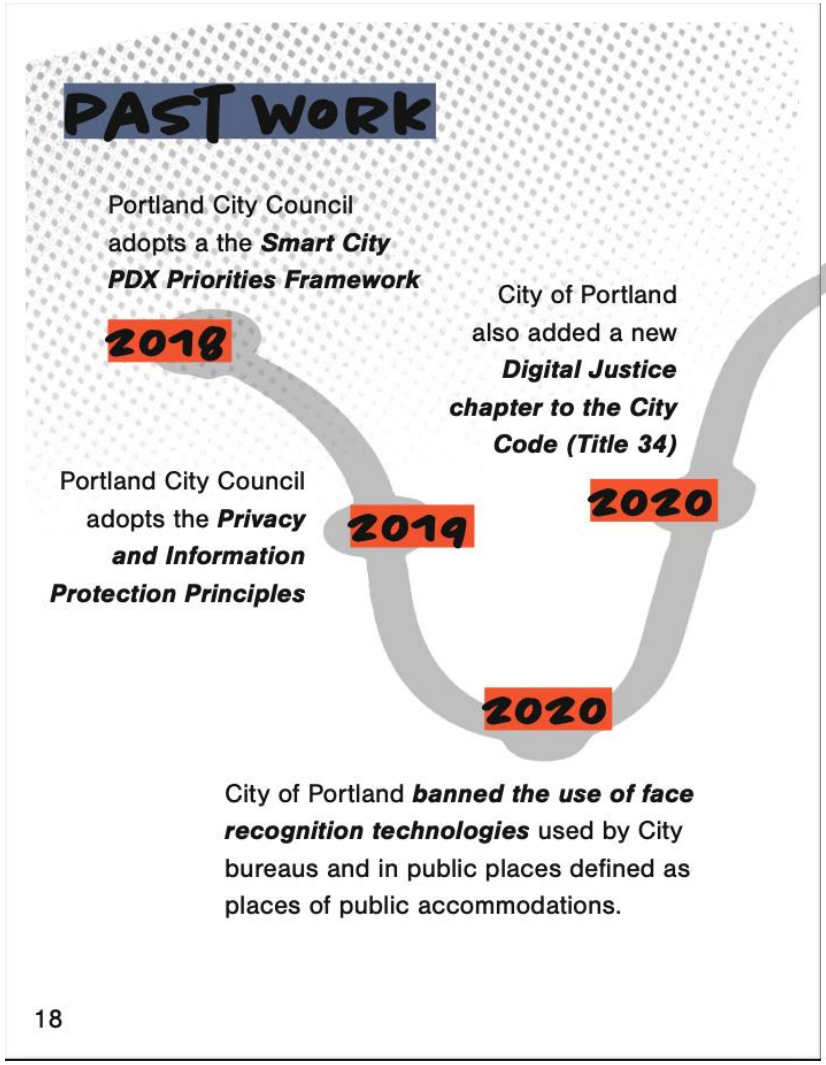
- Core
  - 2 privacy professionals
  - 2 equity professionals
  - 1 attorney
- Privacy Champions
  - Cybersecurity, IT
  - Department Heads and team members

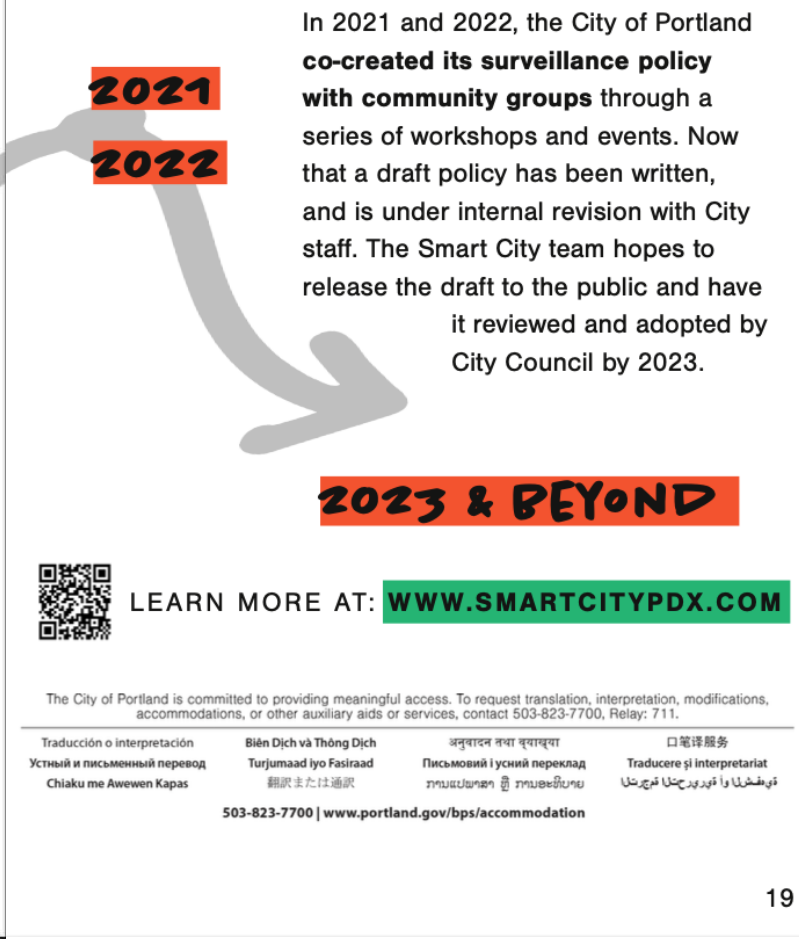
Portland's Program (Privacy Resolutions)

- Surveillance Technologies Resolution
  - Calls for a privacy threshold assessment and privacy impact assessment on all surveillance technology
  - Calls for the creation of a surveillance technology inventory
- Privacy Principles Resolution
  - Set privacy principles
  - Creates an internal workgroup on upholding these principles
- Face Recognition Ban
  - News: Ring cameras in Portland don't have this new function

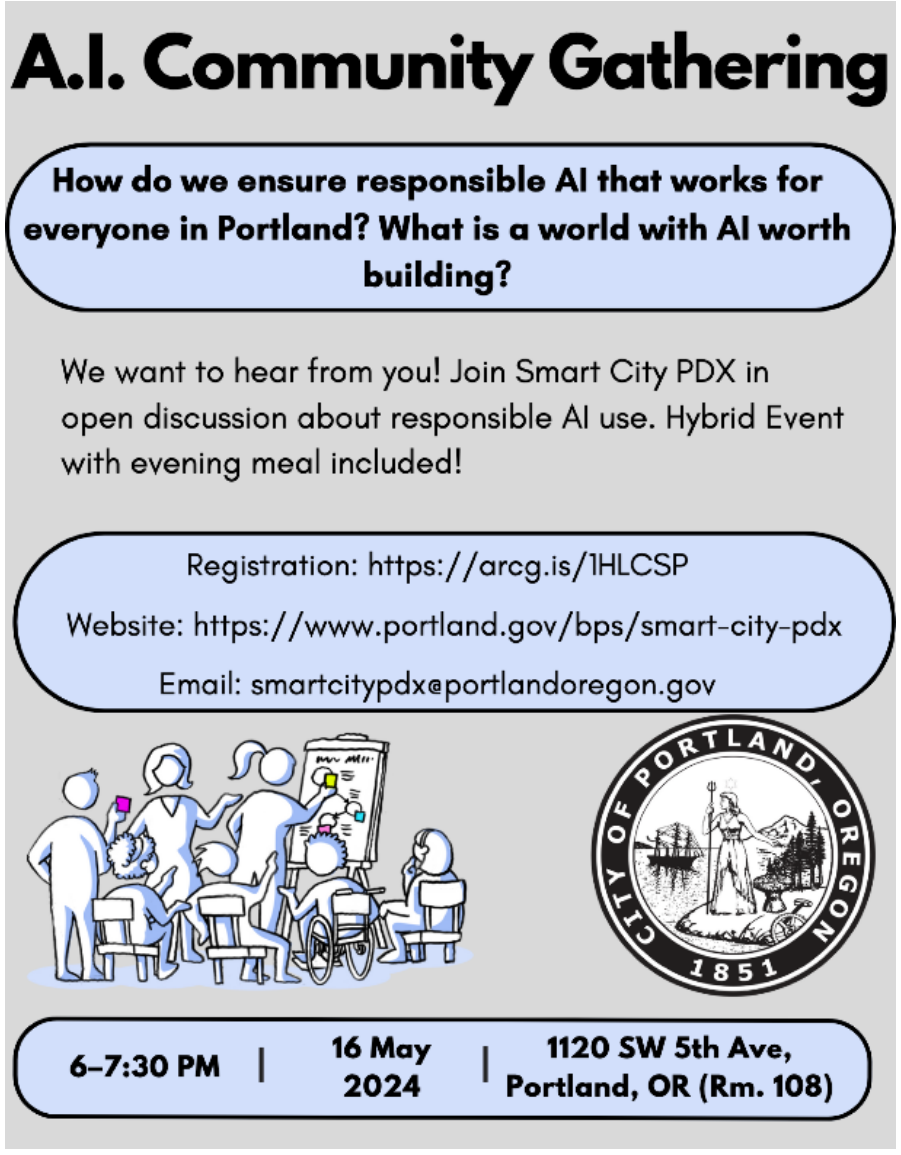
Portland's Program (Community Presence)







Portland's Program (Community Presence)



Project purpose

This work aims to support the City of Portland to develop policies, best practices, training materials, communications, and public involvement, on responsible use of Artificial Intelligence and Automated Decision Systems. This work also includes developing initial priorities and gathering City stakeholders that need to be part of these discussions.

Project background

The 2019 City resolution that established the City of Portland's privacy and information protection principles and 2023 surveillance technologies resolution define Automated Decision Systems (ADS) as the processes, set of rules, or tools 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, image generation, speech or facial recognition, and automated translation between languages.

City Council directed BPS's Smart City PDX program to develop initial policies for the City's use of Automated Decision Systems with the adoption of the Surveillance Policy via Resolution 37608 in February 2023, with the recognition that this work would be in partnership with BTS, OEHR and others.

An AI workgroup was created including city staff from the Bureau of Technology Services' enterprise services group and the information security group, the Office of Equity and Human Rights, Office of Management and Finance's risk management group, the Smart City PDX team, City Auditor's Office, and City Attorney's Office. City staff from the Bureau of Human Resources, and the City's Administration Office representatives are invited as well.

Portland's Model (Surveillance Tech Inventory)

City infrastructure and strategies to build this inventory.

The City of Portland owns thousands of devices and services that can be considered surveillance technologies. These devices include security cameras, drones, automatic license plate readers, Bluetooth sensors and other traffic monitoring systems, etc.

Many of these devices are managed by City's IT services provided by the Bureau of Technology Services (BTS); however, City bureaus can own their own devices or information services without those devices necessarily becoming part of the City's IT management portfolio. City bureaus can contract with third parties and contractors for specific services.

All these scenarios and the large number of devices make the design, implementation, and maintenance of the Citywide inventory complex and expensive. Therefore, our team has proposed an inventory framework that separates technologies from use cases and individual devices. In this way, we can focus resources and time to maintain only those devices and uses of technology that have the most public interest.

Surveillance technologies inventory framework.

The inventory of technologies and their use policies will be described in three different layers to provide the ability to procure technology or vendors that have been already vetted and make the procurement of technology more effective.

Layered approach.

The citywide inventory of surveillance technologies is a way to describe all the spectrum of technologies used by the City of Portland, OR. This proposal divides the description of surveillance technologies owned by the City in three layers: by technology type, by technology application, and by individual devices.

Layer 1: By technology

Building a higher-level catalog of technologies will allow agencies to identify what are the specific aspects of compliance, use restrictions, data management, and resources dedicated to it. Each technology type needs to have a unique feature that defines it, either by the type of information it generates, the manufacturing processes of devices, or the general purpose of it.

Layer 2: By application

This level will describe technology by agency and use. It will include a bulk number of devices or users of a specific surveillance technology. A specific application is defined by the specific user or users of it and how specific surveillance technologies are being adapted to the specific purpose or utility use.

Layer 3: By devices

This level will identify specific devices. These devices will include a specific technology and define application. Devices could be physical or virtual. Cases of virtual devices may include apps or software products that surveil people. The program *currently lacks funding and resources to do an extensive inventory of individual devices.*

Appendix. Summary of minimum required fields

This list is the minimum and mandatory fields of the surveillance technologies inventory.

Title	Description	Type	Format	Required
surveillanceID	Unique identifier for this surveillance technology type (index)	String	default	Required
Surveillance_name	Surveillance short name	String	default	Required
purposeOfTechnology	Description of how the technology will be used (Max 1000 characters)	String	default	Required
Status	Status of the technology of project. From a list "[active, inactive, in maintenance, decommissioned, etc.]".	String	default	Required
Vendor.vendorID	Unique vendor ID from SAP (PO Listing Report/Vendor Name)	String	default	Required
Vendor.vendorName	Vendor's name from SAP. PO Listing Report/Vendor Name Contract Listing Report/Vendor Name	String	default	Required
IsGeolocated	Boolean that flags whether the technology or devices are deployed physically	boolean	binary	Required
Justification	Text describing why is this technology is used (1000 characters max).	String	default	Required
SurveillanceImpactAssessment.includeSIA	Boolean flag describing whether this technology has an impact assessment (Required only for new tech)	boolean	binary	Required
Privacy_policy	URL or text to the vendor's or City's privacy policy of this technology	String	default	Required
Data_collected	Schema or description of collected data. Use a data descriptor template.	String	default	Required
AccessToData	List of entities accessing data collected by this technology in array form as "[stakeholder1, purpose],... "	String	default	Required
processingDescription	General description of how data is processed	String	default	Required
Supervision.Monitoring	Description of how technology is monitored.	String	default	Required

Portland's Model (Privacy Impact Assessments)

- Structure of PIA: Fact Discovery, Risk ID, Risk Mitigation, Inform Policy
  - Important facts: Tech, Data, Use, Location, Problem, Contract Language
- Prospective View
  - Given important facts haven't been decided finally, the prospective view is an Iterative processes of proposing facts, identifying risks, and mitigating risks by changing facts.
  - Compare risks stemming from decisions; privacy professional acts as a guide.
  - Downside: Labor intensive, requires privacy expertise, requires connection throughout to mitigate emerging risks
  - Like the Surveillance Impact Report and the Surveillance Use Policy
- Retrospective View
  - Facts are mostly immovable (dead set)
  - PIAs are only able to ID risks, suggest certain mitigations, and create use policy; cannot easily change important facts
  - Downside: More risks due to the lack of ability to mitigate during the project
  - Like the Annual Surveillance Report

Takeaways for San Diego

- What City departments know
  - Technology procurement, vendor management, public records requests, data governance (data retention schedules, data classification)
- What City departments don’t know
  - Cybersecurity, Privacy, and Law
    - Privacy risks, mitigations, privacy by design, FIPs, PETs, NIST
    - E-discovery, legal analysis/interpretation, privacy torts, civil liberties, civil rights

Takeaways for San Diego

- Surveillance Use Policies, Surveillance Impact Reports, and Annual Reports
  - Prospective and Retrospective
    - In creating these documents, departments will be asked to make the decisions, and set facts, as they think about risks and mitigations; or do this with an eye toward the improvement
  - Quality
    - It will be the first time departments will be doing assessments; they will be novice at first
    - After the first time, annual assessments may become better with time, or stay at a novice level because of employee turnover, promotions, shifting job descriptions, etc.
  - Process
    - Stay connected with departments about their assessments before and between Board review (if possible)
    - Bring on City Staff, volunteers, or contractors to divide work appropriately

Thank you

Any questions?