City of Portland

Digital Justice and Surveillance Technologies Work Session

Smart City PDX and Office of Equity and Human Rights

January 11, 2022

THE BUREAU OF PLANNING & SUSTAINABILITY

OFFICE of EQUITY and HUMAN RIGHTS CITY OF PORTLAND

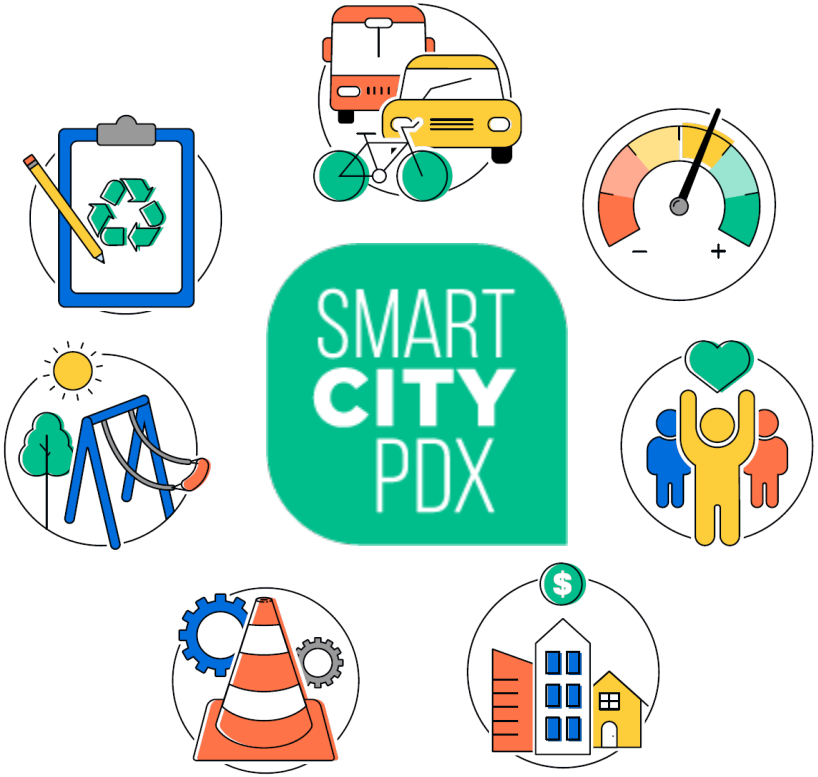
SMART CITY PDX

How has Portland redefined smart cities?

- Smart City PDX was created in 2017 in the Bureau and Planning and Sustainability to use data and technology to improve people's lives, particularly in underserved communities.

- Partners with the Office of Equity and Human Rights and Portland communities to proactively prepare for emergent technology to promote community-driven goals and values.

- Build a policy/process foundation for better use of data and technology, improved decision-making and evaluation, and the modernization of City services.



The work so far

- Open Data and Data Governance (2017)
  - Develop a program for increasing publication, open access, and widespread sharing of data.
  - Ordinance and Exhibit A as single link
- Smart City PDX Priorities Framework (2018)
  - Recognize technology advancement benefits are not accessible by all due to existing disparities and inequities driven by racism and other systems of discrimination. Data collection and technology can also create new harms.
  - Resolution and Exhibit A
- Privacy and Information Protection Principles (2019)
  - Seven principles to guide all City staff to protect privacy when managing data. Direction to work with Office of Equity and Human Rights to create more robust privacy policies.
  - Resolution and Exhibits
- Face Recognition Bans (2020)
  - Ban the use of face recognition by the City and private entities in places of public accommodation. Developed using participatory practices with communities and led with protection of Black, Indigenous, and people of color communities.
  - Ordinance to prohibit City acquisition and use
  - Ordinance to prohibit use by private entities in places of public accommodation

Privacy principles (2019) and Portland values

Transparency and accountability

Equitable data management

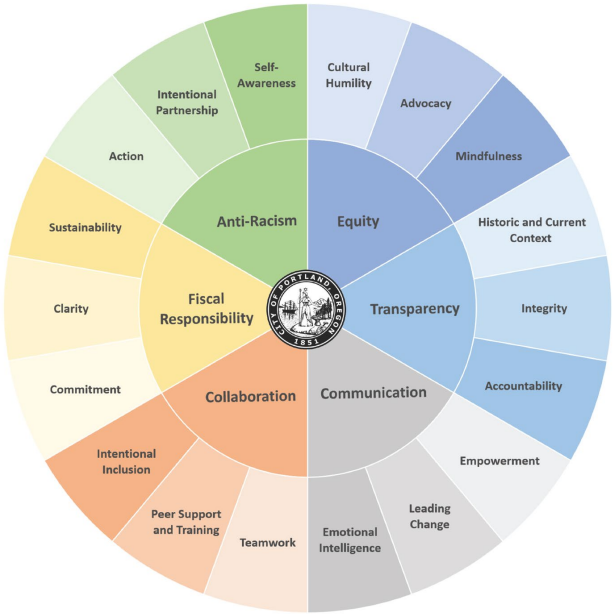
Full lifecycle stewardship

Data openness

Automated decision systems

Data utility

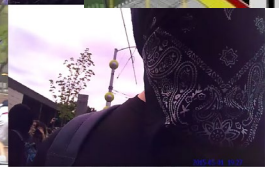
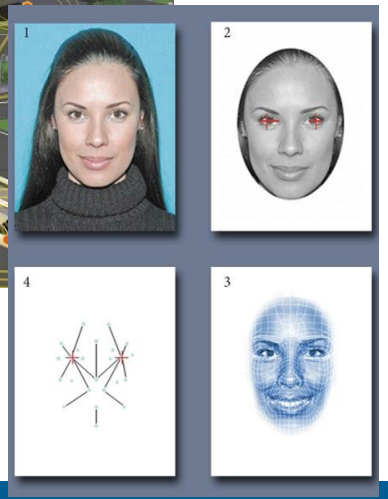
Ethical and non-discriminatory use of data



DIGITAL JUSTICE

What are surveillance technologies?

Surveillance technologies monitor and track behavior, activities, or information from a **specific** individual or group for the purpose of gathering information, influencing, managing or providing direction.*

Developing the policy

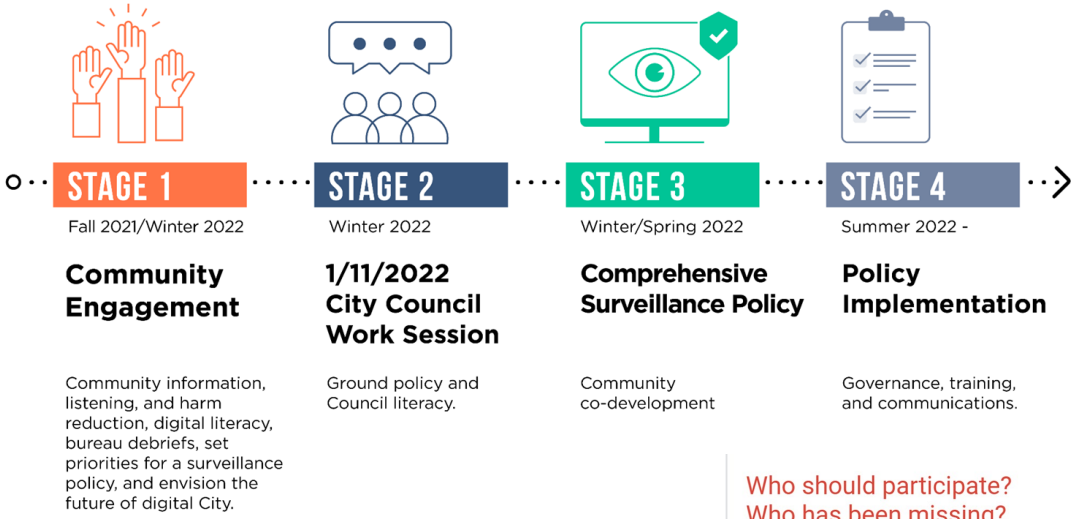
This initial policy is focus only on City use of surveillance technologies and it will consider existing policies, procedures, and ongoing work applicable to surveillance technologies.

Bureaus involved:

- Smart City PDX (BPS)
- Office of Equity and Human Rights
- City Attorney's Office
- BTS - Information Security

Community engagement plan:

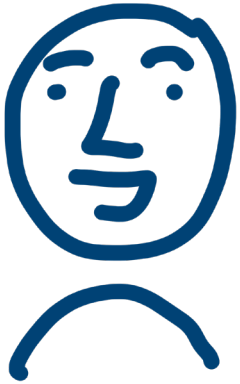
June 21, 2021 – Community kickoff event
October 9, 2021 - Surveillance and Digital Rights panel
December 13, 2021 - Codesign event on Surveillance Technologies & Information



SURVEILLANCE TECHNOLOGIES STORIES

Porch cameras are everywhere now. Can they be used in a way that causes harm to the community?

When I use Biketown or Parking Kitty, I wonder if my personal information is being stored or shared.



Eye tracking software being used in schools concerns me.

My friend's employer records her on camera to make sure she is being productive at work. That seems invasive.

I attended a protest downtown and I heard that the police were taking drone footage of the crowd.

About this work session

This work session will inform City Council about surveillance technologies and data collection, how communities are impacted by them, and how cities are implementing local policies and strategies to use technologies responsibly.

Commissioners will have the opportunity to discuss these topics and provide guidance to the Smart City PDX and Office of Equity team for the City's surveillance technologies policy.

Ginger Armbruster
Chief Privacy Officer
- City of Seattle

Brian M. Hofer
Chair Commissioner
- Oakland Privacy Advisory Commission

Invited community members connected with privacy and civil rights and liberties organizations will follow

Ginger Armbruster
Chief Privacy Officer – City of Seattle

Privacy Office

Increasing transparency and accountability about data collection and use

City of Seattle

Division Overview

	Program Function
Privacy Program	The Privacy Program provides structure & guidance essential for City departments to incorporate appropriate privacy practices into daily operations, and to build public trust in how we collect and manage the public's personal information.
Surveillance Program	The Surveillance Program is responsible for ensuring compliance with the City's Surveillance Ordinance, and ordinance designed to provide greater transparency to City Council and the public when the City acquires any technology that meets the City's definition of surveillance.
Open Data	Making City data openly available to the public for the purpose of increasing the quality of life for our residents; increasing transparency, accountability and comparability; promoting economic development and research; and improving internal performance management.
CPRA Program/ eDiscovery	The Citywide Public Records Act Program ensures compliance with the state Public Records Act. Responsibilities include leading the development and implementation of consistent operational policies and procedures.
Data Governance Program	Enabling the use of data as a strategic City asset while addressing associated data management and protection obligations.

Privacy Program Desired Outcomes

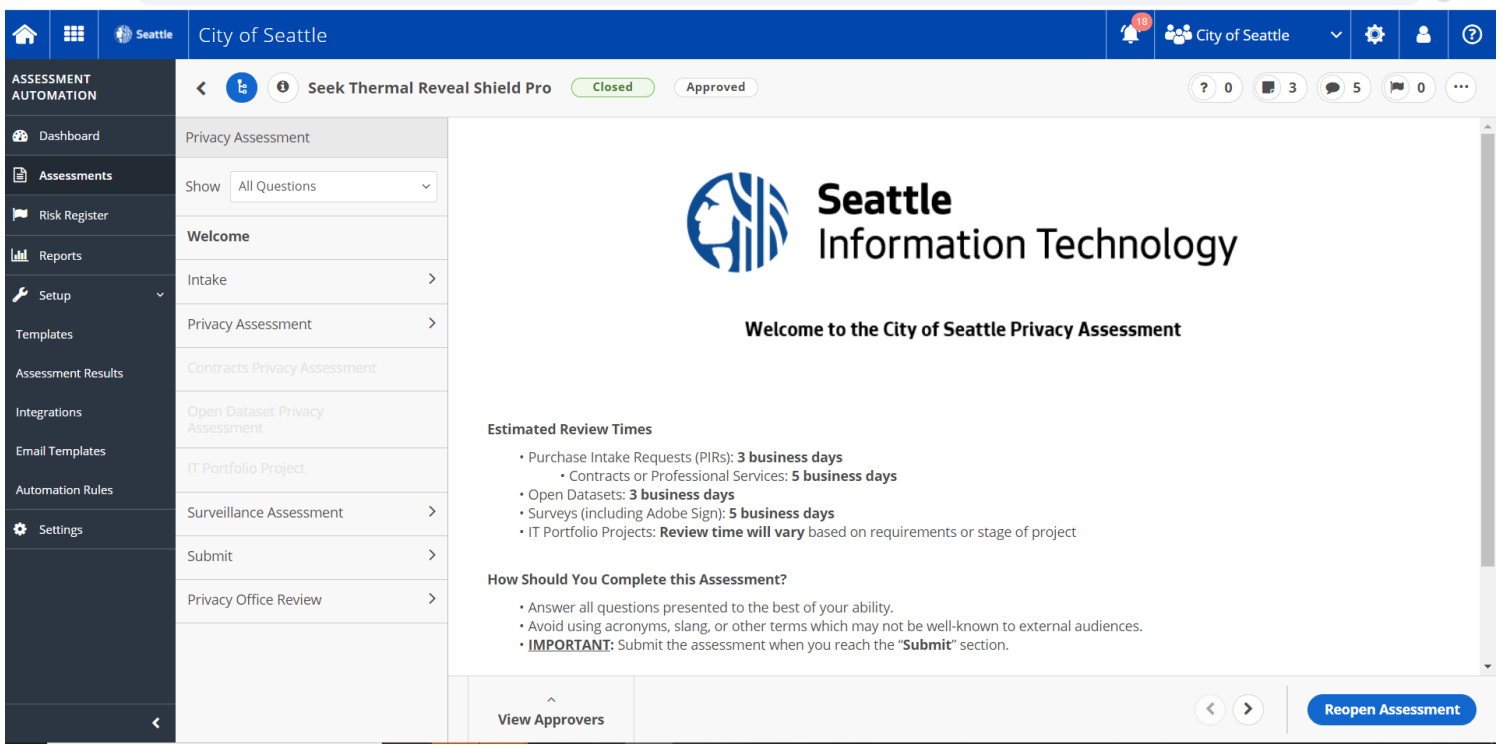
Mission: Build public trust about the use and management of the public's personal information

- Increase transparency
- Create internal data governance
- Ensure legal compliance
- Increase third-party data accountability
- Comply with Surveillance Ordinance

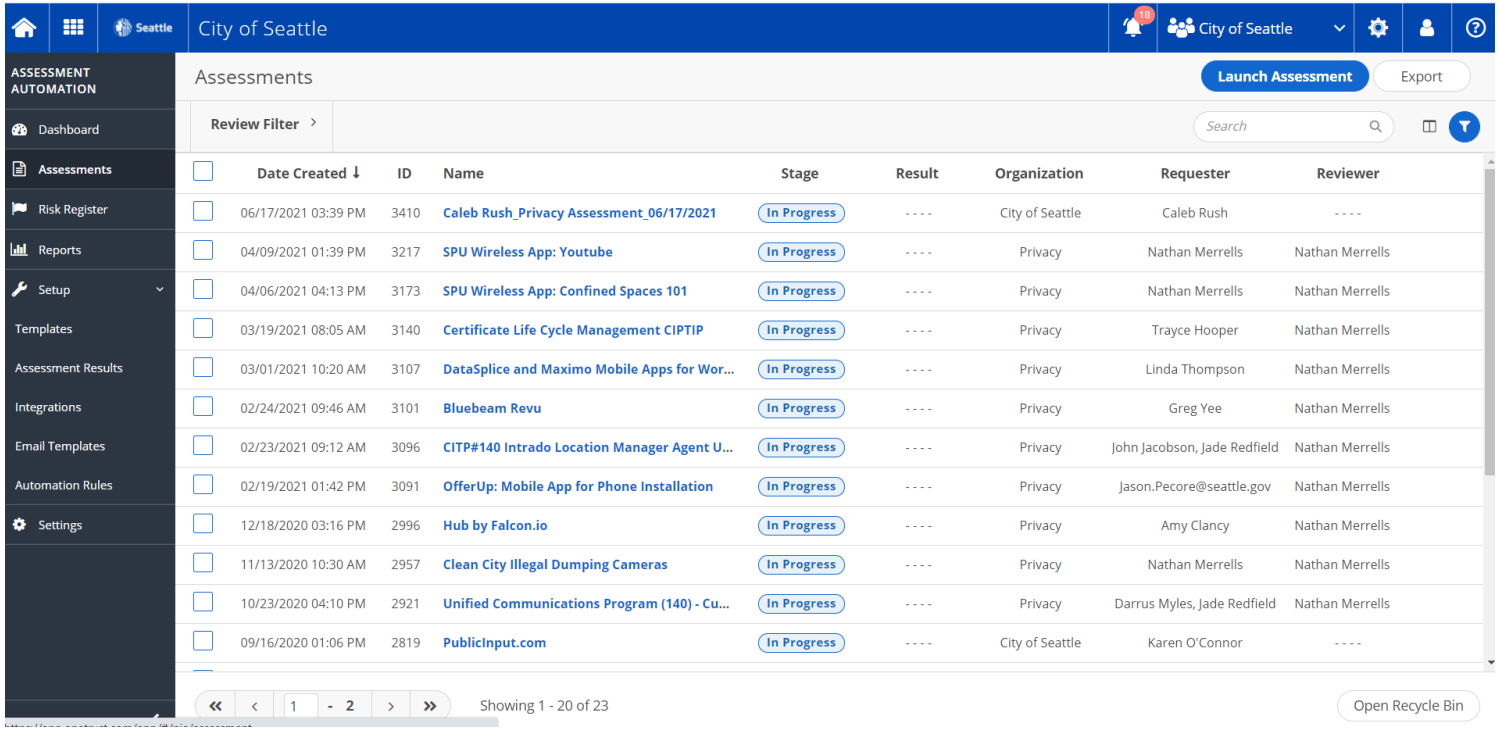
2021 Privacy Program by the Numbers

*All numbers for 2019 as of 9/2019

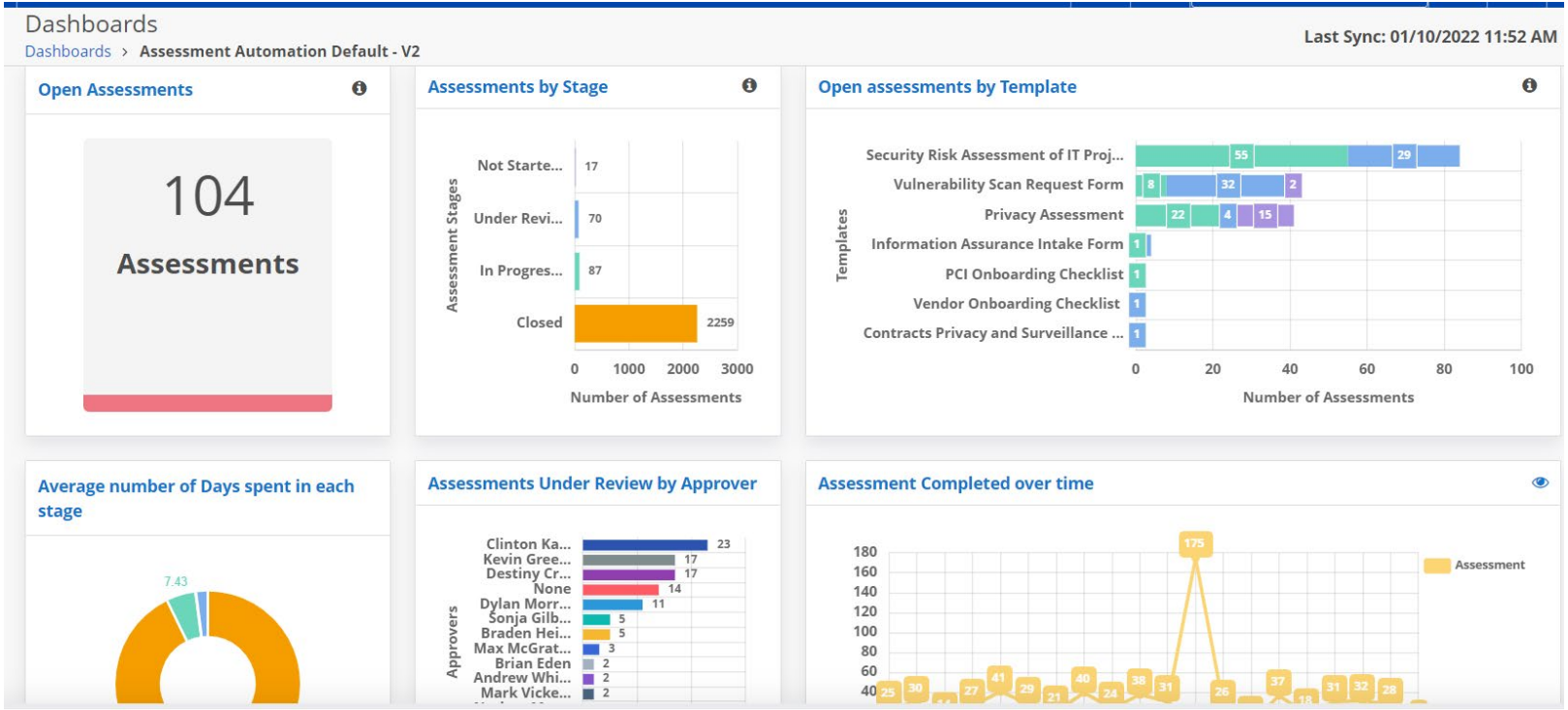
OneTrust: Privacy Review Solution



Consistent Documentation



Program Insights



Privacy Program Resources

- 4 FTE: $690K
- OneTrust Software: $60K
- Surveillance: 4000+ hours annually
- Retroactive reviews: 4 years, 23/27 completed
- Audits: Annual requirement (OIG, Auditor’s Office)
- New technologies: On hold

Questions?

Brian Hofer
Chair of the City of Oakland's Privacy Advisory Commission

December
2021

OAKLAND'S PRIVACY ADVISORY COMMISSION

History, and Process

Brian Hofer

Executive Director, Secure Justice

Chair, City of Oakland's Privacy Advisory Commission

The Opportunity

Oakland contemplated building-out a multi-faceted surveillance apparatus

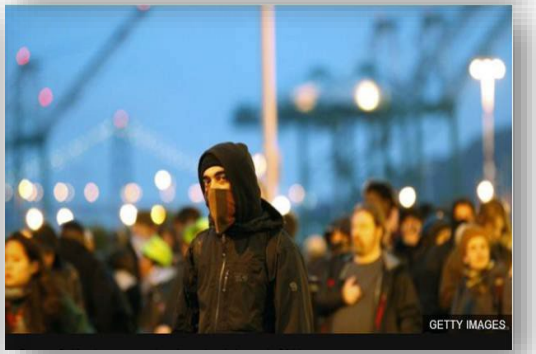
- In 2013, Oakland was given the opportunity to expand its Port's **Domain Awareness Center**
  - DHS would foot the $10.9M bill to build out a city-wide surveillance apparatus to fight terrorism and improve security
  - City council voted to proceed

Community Response

Community backlash was swift and certain

OAKLAND PRIVACY

..... I'VE BEEN WATCHING YOU WATCHING ME



Prompted Oakland residents to organize, protest, and to publically assert a three-part right to privacy:

1. **Secrecy** - *our ability to keep our opinions known only to those we intend to receive them. Without secrecy, people may not discuss affairs with whom they choose, excluding those with whom they do not wish to converse*;
2. **Anonymity** - *Secrecy about who is sending and receiving an opinion or message*; and
3. **Autonomy** - *Ability to make our own life decisions free from any force that has violated our secrecy or anonymity*.

Oakland's Reaction?

The City Council listened to residents

Resolution No.85638
C.M.S. on June 2, 2015

- Voted to **restrict DAC to a Port-focused operation**, removing citywide traffic cameras and ShotSpotter maps from the system;
- Established an **ad hoc Privacy Advisory Committee** to develop a DAC Privacy and Data Retention Policy; and
- Created a permanent **Privacy Advisory Commission** to provide advice to the City of Oakland on best practices to protect Oaklanders' privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores our data

PAC Motivation:

- Surveillance efforts to be guarded against include not just technology capable of accessing non-public places or information (such as wiretaps), ***but also technology which aggregates publicly available information***, providing the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations.
- The use of surveillance technology may threaten the privacy of all citizens, ***including communities defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective.***

Volunteer commissioners from each city council district:

District 1	Reem Suleiman
District 2	Chloe Brown
District 3	Brian Hofer (Chair)
District 4	Lou Katz
District 5	Omar De La Cruz
District 6	Gina Tomlinson
District 7	Robert T. Oliver
At Large	Henry Gage III (Co-Chair)
Mayoral	Heather Patterson

Privacy Advisory Commission

Duties of the Commission

Resolution No.85638
C.M.S. on June 2, 2015

1. **Provide advice and technical assistance** to the City of Oakland on best practices to protect citizen privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores citizen data.
2. **Draft for City Council consideration, model legislation relevant to privacy and data protection**, including a Surveillance Equipment Usage Ordinance.
3. **Submit annual reports and recommendations to the City Council** regarding: (1) the City's use of surveillance equipment, and (2) whether new City surveillance equipment privacy and data retention policies should be developed or such existing policies be amended.
4. **Provide analyses to the City Council of pending federal, state and local legislation** relevant to the City's purchase and/or use of technology that collects, stores, transmits, handles or processes citizen data.
5. **Conduct public hearings, make reports, findings and recommendations** either to the City Administrator or the City Council as appropriate, including an annual report to be presented in writing to the City Council.
6. **Review and make recommendations to the City Council regarding any proposed changes to the operations of the Domain Awareness Center ("DAC")** and/or proposed changes to the City's Policy for Privacy and Data Retention for the Port Domain Awareness Center ("DAC Policy").

Surveillance and Community Safety Ordinance

"Surveillance Ordinance" passed May 2018

Ordinance adding Ch. 9.64 to the Municipal Code Establishing Rules For the City's Acquisition and Use of Surveillance Tech

- **Purpose:** Establish a public approval process for surveillance technologies used by the city; lay the groundwork for the City Council to decide whether the benefits of using the technology outweigh the costs to privacy.
- **City obligations:** City agencies must submit **a "technology impact report"** and a **use policy** to Oakland's Privacy Advisory Commission if they plan to implement new surveillance technologies, like license plate readers or cellphone trackers.
- **"Surveillance Technologies":** Any software, electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group.
- **Differentiated from other cities**: 1) Standardized public format for evaluation and approval; 2) Prohibits secret contracts or non-disclosure agreements between cities and third parties; 3) Provides whistleblower protections to employees who report violations.

How does the Surveillance Ordinance work in practice? Process for city to acquire or use a surveillance technology

Notification

- City entity **notifies** PAC Chair of its wish to acquire new surveillance technology.

Report Submission

- City entity submits a **Surveillance Impact Report** and proposed **Surveillance Use Policy** to the Privacy Advisory Commission for its review at a regularly noticed meeting.

PAC Evaluation

- PAC reviews documentation, works with City entity to revise Impact Report and Use Policy
- Recommends that the City Council **adopt**, **modify**, or **reject** the proposed Surveillance Use Policy.

Public Notice

- City Council provides **public notice** that will include the Surveillance Impact Report, proposed Surveillance Use Policy, and Privacy Advisory Commission recommendation at least fifteen (15) days prior to the public hearing.

Public Hearing

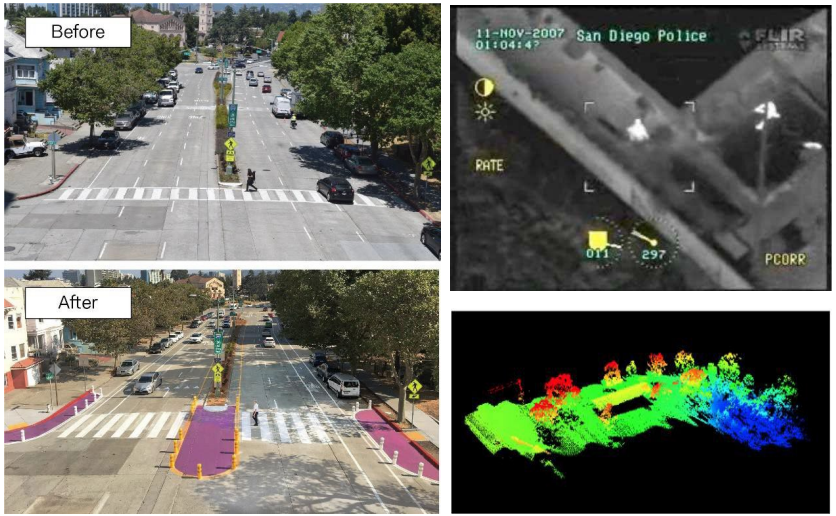
- City Council determination: 1) benefits to the community outweighs the costs; 2) proposal will safeguard civil liberties and civil rights; and 3) no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Illustrative Examples

Types of requests include:

- DOT acquisition of **Unmanned Arial Vehicles (UAVs)** to document transportation improvement projects;
- DOT Parking and Mobility using vehicle-mounted **Automatic License Plate Recognition (ALPR)** to "virtually chalk" vehicles in time-limited spaces, verify permit parking, monitor "pay by phone" parking payments;
- District Attorney' use of **surveillance video** to monitor illegal dumping;
- Police Dept. use of **cell site simulators** to locate missing persons and apprehend fugitives;
- . . .

E.g., Pending DOT request:



- **Data types and sources:** Optical cameras, IR cameras, LIDAR, mapping software
- **Potential impacts:** Capturing PII without notice or consent; Enabling targeted voyeurism; Data use and retention uncertainties
- **Mitigations:** Deploy only in public and with notice where possible; obfuscate faces and license plates. Two-person team; focus must remain on project

Elements of the Required Documents

(Heart of the ordinance)

Surveillance Impact Report:

A. Description of the technology
B. Proposed use(s)
C. Location to be deployed
D. Impact on civil rights and liberties
E. Mitigations
F. Data types and sources
G. Data security
H. Fiscal cost(s)
I. Third-party dependence
J. Alternative methods
K. Track record

Surveillance Use Policy:

A. Purpose of the use
B. Authorized use(s)
C. Data collection
D. Data access
E. Data protection
F. Data retention
G. Public access
H. Third party data sharing
I. Training
J. Auditing and Oversight
K. Maintenance

Elements of the Required Documents

(Heart of the ordinance)

- **Annual Report:**
  A. Summarize how tech was used
  B. Data shared with third parties
  C. Describe deployment practices
  D. Breakdown geographic deployment
  E. Summary of community complaints
  F. Results of internal audits
  G. Information about any data breaches
  H. Efficacy
  I. Summarize public record requests
  J. Total Annual Costs
  K. Suggested Policy Amendments

It is important for law enforcement to understand that this is a summary – there is no expectation that raw data will be provided here, nor is there an obligation to provide information so specific as to interfere with active investigations or deployment practices.

Not all categories will be applicable to all surveillance technologies.

The annual review will ideally confirm that the stated goals (provided during the up-front vetting stage) were achieved, whether policy amendments are needed to better achieve those goals, or whether use should discontinue because the technology was either ineffective at achieving its stated goal or was too intrusive and ripe for abuse.

Researching City-wide Privacy Principles

- Design And Use Equitable Privacy Practices
- Limit Collection And Retention Of Personal Information
- Manage Personal Information With Diligence
- Extend Privacy Protections To Our Relations With 3rd Parties
- Safeguard Individual Privacy In Public Records Disclosures
- Be Transparent And Open
- Be Accountable to Residents

How We're Addressing These Challenges

Communicating with technology companies to assess opportunities for protecting privacy

A variety of interesting solutions, depending on use case:

- Data de-identification
- Differential privacy
- Selective sharing of data across silos while assuring confidentiality and privacy
- Tools to enable data obfuscation

Pictures Collected by an AI system before and after applying facial blur policies

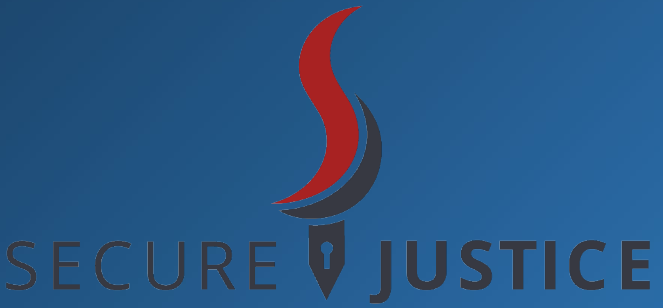
Questions?
Interested in engaging?

Please reach out!
We'd love to
hear from you.

brian@secure-justice.org

@b_haddy

@SecureJustice



5 minutes break

Community guest speakers

Sarah T. Hamid
Carceral Tech Network

Alan Hipolito
SUMA

Romeo Sosa
Portland Immigrants Rights Coalition

Questions?

Closing Statements

- Privacy is a human right.
- Surveillance technologies impact in black, indigenous and people of color communities in disproportionate forms.
- A surveillance policy will help city bureaus to understand these risks and impacts and create more transparency
- Impacted community is part of the development of this policy.
- People want to know how information that the city collects is being used.
- Technology can be a good instrument to support the City goals and the community.

Discussion