AGENDA ITEM 610 **TESTIMONY** **2:45 PM TIME CERTAIN**

37437-1

Establish Privacy and Information Protection Principles to guide how City collects, uses, manages and disposes of Data and Information

If you wish to speak to Council, please print your name, address and email

Name (PRINT)	Address and Zip Code (*Optional*)	Email (*Optional*)
✓ Brian King		
Chris Bushick		
Ala-Hyslib		

Date 6-19-19

37437

PDX Privacy

June 19, 2019

Mayor Ted Wheeler and Portland City Council
Portland City Hall
1221 SW 4th Avenue, Room 130
Portland, OR 97204

Mayor Wheeler and City Council Commissioners:

PDX Privacy, an organization composed of local residents, advocates for privacy, transparency, and digital rights in the Portland Metro Area. We care deeply about issues related to the collection, use, and potential abuse of personal data by both businesses and government. Therefore, we respectfully submit these comments in support of the Privacy and Information Protection Resolution coming before Portland City Council on June 19, 2019.

Data collected from residents may potentially yield valuable insights to the City, such as the most popular transit routes or ways in which the City can improve its services. Without thoughtful planning and oversight, however, personal information can also be misused or stolen, harming the City's residents and the City's future as an open, transparent, and equitable place to live.

Current technology offers considerable opportunities to accumulate a wide variety of personal data. When combined, the information can provide a detailed picture of a person's life–gender, health, sexual preferences, religious affiliations, travel habits, and relationships, among other aspects. Misuse could lead to a person being manipulated, surveilled, or otherwise mistreated; indeed, marginalized communities are especially at risk for abuse since they don't have as many choices as more affluent persons.

Having guidelines and policies in place related to the collection, secure handling and storage, and timely deletion of data will help to ensure that the City is a good steward of its residents' and visitors' information and will promote trust in the City and its efforts towards privacy and data protection.

PDX Privacy commends the City's efforts in taking proactive steps towards privacy and information protection in the absence of guidance on this issue from the state and federal levels. While we would like to see residents have actionable privacy rights, we believe that the principles outlined in the Privacy and Information Protection Resolution are an important and needed step towards protection of residents' personal information. Therefore, we endorse this resolution.

Sincerely,

Chris Bushick and Michael Miller
on behalf of PDX Privacy

P.O. Box 3431 Portland, OR 97208
info@pdxprivacy.org

37437-1

Brian King
Chair, Information Technology Working Group
Portland Democratic Socialists of America
info@portlanddsa.org

Privacy is a human right. Information privacy protects us from theft, harassment, and abuses of private and government power. We welcome Portland City council's approval of the "Privacy and Information Protection Principles" resolution. Implementing these principles will require follow-on ordinances and new policy to ensure transparency, accountability, and public control of data collection.

In 2015, Portland Police Capt. Mark Kruger acknowledged that Portland Police have access to a stingray[i], a device that mimics a cell phone tower so that it can gather location data on phone users in a wide area. In 2017, the D.C. Court of Appeals ruled that warrantless use of a "stingray" violates Fourth Amendment privacy rights[ii].

In 2017, the Willamette Week reported that Portland Police (PPB) failed to delete photos of protesters' IDs, despite having committed to doing so "pursuant to PPB policy"[iii]. However, an Independent Police Review found that PPB had no such policy for digital images. No discliplinary actions were reported over the privacy violations.

Vigilant Solutions runs a national database of Automated License Plate Reader (ALPR) data collected by law enforcement agencies. Vigilant Solutions has a data sharing ageement with ICE (Immigration and Customs Enforcement). The ACLU obtained ICE search records, and found that ICE agents use license plate data to track the daily movements of suspects, and that they also conduct searches on the families of suspects, on U.S. citizens, and conduct searches which the ACLU called "vague and arbitrary"[iv]. PPB has license plate readers on some patrol cars. If PPB is sharing its license plate data with Vigilant Solutions, this would contribute to ICE's violations of privacy which could violate Oregon's anti-profiling laws.

President Trump has issued orders which condition federal funding on cooperation with investigations by DHS and ICE[v]. Local governments are asked to share information about undocumented immigrants so that they can be targeted for deportation. Our Federally funded data fusion center in Salem violated anti-profiling laws by tracking "Black Lives Matter" protests[vi]. Our local law enforcement database, RegJIN, shares data through a network of regional and national law enforement databases that ICE has access to[viiviiiix]. The executive order may put Portland in a dilemma. Do we accept Federal money and share data that may violate anti-profiling laws, or do we protect our residents by refusing funding and disengaging from abusive Federal agencies?

These examples show there is much to be done. Two endorsers of this resolution, the Sunlight Foundation and Oakland's Privacy Advisory Commission, show the way forward.

The Sunlight Foundation recommends adopting further accountability measures, including "Establishing regular public reporting requirements", and "Creating public disclosure requirements around partnership agreements and contracts". The Sunlight Foundation recommends that cities not share data with less protective third parties.[x] We agree with these recommendations.

The Oakland Privacy Advisory Commission is responsible for oversight of Oakland's new "Surveillance and Community Safety Ordinance"[xi]. That ordinance provides whistleblower protections,

strong accountability measures for privacy violations, and covers technology like stingrays, facial recognition, and social media surveillance. We believe it should be a model for Portland's privacy ordinances.

Information privacy is a large topic, and we only begin to cover it today. We hope to work with commissioners in the future on securing the information privacy rights of Portland residents.

i https://www.wweek.com/news/2015/12/16/somebodys-watching-you/

ii https://www.cbsnews.com/news/d-c-court-rules-warrant-is-required-for-stingray-cell-phone-tracking/

iii https://www.wweek.com/news/courts/2018/05/31/city-review-reveals-portland-police-did-not-delete-photos-of-protesters-ids-despite-promises-to-do-so/

iv https://www.aclunc.org/blog/records-reveal-ice-agents-run-thousands-license-plate-queries-month-massive-location-database

v https://sunlightfoundation.com/2017/02/10/protecting-data-protecting-residents/

vi https://www.opb.org/news/article/oregon-department-of-justice-intelligence/

vii https://www.portlandoregon.gov/police/article/679605

viii https://publicintelligence.net/ice-pattern-analysis-and-information-collection-icepic-system/

ix https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_icepic-4a.pdf

x https://sunlightfoundation.com/2017/02/10/protecting-data-protecting-residents/

xi https://www.eff.org/files/2018/05/17/oaklandccops.pdf

FILED
OFFICE OF THE CITY CLERK
OAKLAND

2018 APR 26 PM 3:03

37437

APPROVED AS TO FORM AND LEGALITY

CITY ATTORNEY'S OFFICE

AMENDED AT THE APRIL 24, 2018 PUBLIC SAFETY COMMITTEE

OAKLAND CITY COUNCIL

ORDINANCE NO. _____ C.M.S.

ORDINANCE ADDING CHAPTER 9.64 TO THE OAKLAND MUNICIPAL CODE ESTABLISHING RULES FOR THE CITY'S ACQUISITION AND USE OF SURVEILLANCE EQUIPMENT

WHEREAS, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to the City of Oakland's ("City") acquisition and use of surveillance technology; and

WHEREAS, the City Council finds that, while the use of surveillance technology may threaten the privacy of all citizens, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and

WHEREAS, while acknowledging the significance of protecting the privacy of citizens, the City Council finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also may include technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and

WHEREAS, the City Council finds that no decisions relating to the City's use of surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions; and

WHEREAS, the City Council finds that any and all decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight in policy decisions; and

WHEREAS, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any City surveillance technology is deployed; and

WHEREAS, the City Council finds that if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF OAKLAND DOES ORDAIN AS FOLLOWS:

SECTION 1. This Ordinance shall be known as the Surveillance and Community Safety Ordinance.

SECTION 2. Oakland Municipal Code Chapter 9.64, is hereby added as set forth below (chapter and section numbers are indicated in **bold type.**

Chapter 9.64 REGULATIONS ON CITY'S ACQUISTION AND USE OF SURVEILLANCE TECHNOLOGY

9.64.010. DEFINITIONS. The following definitions apply to this Chapter.

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:

   A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
   B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
   C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such

hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each Police Area in the relevant year;
E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties.
F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.
G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;
J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

2. "City" means any department, agency, bureau, and/or subordinate division of the City of Oakland as provided by Chapter 2.29 of the Oakland Municipal Code.

3. "City staff" means City personnel authorized by the City Administrator or designee to seek City Council Approval of Surveillance Technology in conformance with this Chapter.

4. "Continuing agreement" means an agreement that automatically renews unless terminated by one party.

5. "Exigent circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.