ORDINANCE No.

*Prohibit the acquisition and use of Face Recognition Technologies by City bureaus (Ordinance).

The City of Portland ordains:

Section 1. The Council finds:

1. On May 3, 2017, City Council Ordinance 188356 established an Open Data Policy and Program committed to the publication, accessibility, and equitable sharing of data collected by the City of Portland and partners and directed the development of a team to provide data governance guidance for Open Data Program. Through development and implementation of this work, the team identified the need for privacy assessment and comprehensive structure to address tensions with transparency.

2. On June 21, 2018, City Council Resolution 37371 created the Smart City PDX Priorities Framework to prioritize addressing inequities and disparities when using data and investing in technologies that improve people's lives, with a specific focus on communities of color and communities with disabilities.

3. On June 19, 2019, City Council Resolution 37437 established Privacy and Information Protection Principles to serve as guidance for how the City of Portland collects, uses, manages and disposes of data and information, and directed staff at the Bureau of Planning and Sustainability and Office of Equity and Human Rights to identify and develop policies and procedures that promote these Principles.

4. The Privacy and Information Protection Principles center equity and human rights in privacy strategy development and acknowledge that underserved communities are most at risk in the digital age. Human rights principles such as privacy and freedom of expression must guide the use of the City of Portland’s data and digital services.

5. Surveillance Technologies are defined as 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.

6. Face Recognition means the automated searching for a reference image in an image repository by comparing the facial features of a probe image with the features of images contained in an image repository (one-to-many search). A Face Recognition search will typically result in one or more most likely candidates—or candidate images—ranked by computer-evaluated similarity or will return a negative result.

7. Face Recognition Technology means an automated or semi-automated process using Face Recognition that assists in identifying, verifying, detecting, or characterizing facial features of an individual or capturing information about an individual based on an individual's face.

8. It is essential to have an informed public discussion about decisions related to the City of Portland's acquisition and use of Surveillance Technologies including Face Recognition Technologies.

9. The use of Face Recognition Technologies raises general concerns around privacy, intrusiveness, and lack of transparency. The lack of transparency and accountability, in addition to biased technologies -- particularly in the context of false positives in law enforcement -- can create devastating impacts on individuals and families.

10. United States federal law does not currently regulate Face Recognition Technologies, and Oregon state law only prohibits its use by law-enforcement agencies to analyze recordings obtained through the use of body-worn cameras (see ORS 133.741(1)(b)(D)). There are no other laws addressing Face Recognition Technologies applicable to the City of Portland.

11. Existing methodologies assessing bias in Face Recognition Technologies show progress on their performance. However, there is still not a formal certification process available to cities that includes the full lifecycle of sensitive information collected from individuals.

12. Smart City PDX is currently developing a scope for a comprehensive Data Governance and Privacy and Information Protection framework for the City of Portland. It is essential that such frameworks include impacted communities and transparent decision making authority to regulate and oversee that the use of Surveillance Technologies and sensitive information from Portlanders and visitors, like Face Recognition Technologies, do not harm civil rights and civil liberties.

13. The City recognizes the rapid evolution of technologies demand more frequent revisions of existing technology related policies, in order to make sure policies still fulfill their purpose.

14. The City has received public comments of drafts publicly released through the development of this policy. These comments have enriched this ordinance and are attached in Exhibit A.

15. The City desires to adopt a ban on the City's acquisition and use of Face Recognition Technologies and information derived from such technologies.

NOW, THEREFORE, the City Council directs:

a. Each bureau director shall require bureau staff to review and assess whether bureau staff are using Face Recognition Technologies. Each bureau will complete this assessment and provide it to the Bureau of Planning and Sustainability's Smart City PDX Open Data Coordinator within 90 business days after the effective date of this ordinance. This report will be made publicly accessible.

b. Bureaus shall not acquire, evaluate or use Face Recognition Technologies, except as expressly provided in Section (f). This prohibition applies to Face Recognition Technologies that are procured by any means with or without the exchange of monies or other consideration. For purposes of clarity, this means bureaus shall not purchase, lease or accept a donation or gift of Face Recognition Technologies.

c. Bureaus shall not knowingly acquire, request, use, access or retain any information (unless required by public record retention rules) derived from Face Recognition Technologies or intentionally collect information to be used for Face Recognition Technologies, except as expressly provided in Section (f).

d. Bureaus shall not direct a non-City entity to acquire or use Face Recognition Technologies on the City's behalf unless such acquisition or use would be otherwise allowed for bureaus under this ordinance.

e. Bureaus shall not knowingly allow a non-City entity to use Face Recognition Technologies on City owned property unless such use would be otherwise allowed for bureaus under this ordinance.

f. Bureaus may only use Face Recognition Technologies for the following purposes:

1. For verification purposes for bureau staff to access their own personal or City issued personal communication and electronic devices. For example, bureau staff may use Face Recognition Technologies to unlock their own or assigned mobile phones or tablets;
2. In automatic face detection services in social media applications. Bureau staff activity in social media is regulated by the policy HRAR 4.08A; and
3. In detecting faces for the sole purpose of redacting a recording for release or disclosure outside the City to protect the privacy of a subject depicted in the recording.

g. If a bureau inadvertently or unintentionally receives, accesses or uses information obtained from Face Recognition Technologies, it shall not be a violation of this ordinance provided the bureau follows the requirements of this section:

    1. The bureau immediately ceases using the information as soon as it learns that the information was obtained from Face Recognition Technologies;
    2. The bureau documents its receipt, access or use of the information in an impact report;
    3. The impact report contains the following information: (i) date the information was received, accessed, or used; (ii) source of the information; (iii) a description or summary of the incident; (iv) whether the bureau accessed or used the information in the course of its operations; and (v) corrective measures taken by the bureau to prevent the further transmission or use of any information inadvertently or unintentionally obtained through the use of Face Recognition Technologies. The impact report shall not include the information involved in the incident or any personally identifiable information or other information prohibited by law;
    4. The impact statement is submitted to the City Council at a regularly noticed public hearing, within 60 days of the discovery; and
    5. The bureau retains the information no longer than the applicable retention period or as otherwise required by law.

h. The Bureau of Planning and Sustainability's Smart City PDX Open Data Coordinator will convene a temporary group to serve as a resource to all bureaus to assess whether a technology constitutes Face Recognition Technologies and explore whether any changes are necessary to other existing City policies or administrative rules. This temporary group will include representatives from bureaus, including but not limited to, the Bureau of Planning and Sustainability; the

Bureau of Technology Services; the Portland Police Bureau; the Bureau of Human Resources; the City Attorney's Office; and the Office of Equity and Human Rights.

i. As part of the work directed by City Council Resolution 37437, the Bureau of Planning and Sustainability is directed to explore the adoption of a comprehensive Data Governance and Privacy and Information Protection framework that addresses the appropriate use or prohibition of Surveillance Technologies, including Face Recognition Technologies and the information derived from Face Recognition Technologies. This includes assessing staff and budget resources needed to: establish new Citywide privacy policies and procedures; develop effective privacy assessment tools; create guidelines for acquiring, using or sharing information derived from Surveillance Technologies; design and implement public engagement processes, with a focus on underserved communities; and create decision-making structures for managing City data.

j. The Bureau of Planning and Sustainability and the Office of Equity and Human Rights shall address public use of Face Recognition Technologies in coordination with other local jurisdictions such as TriMet, Multnomah County, and Portland Public Schools, to ensure that community members do not develop a false sense of security because of the limitations of this ordinance.

k. The prohibitions stated in this ordinance shall remain in effect until the City adopts or revises a comprehensive Data Governance and Privacy and Information Protection framework that addresses the appropriate use or prohibition of Face Recognition Technologies and the information derived from Face Recognition Technologies.

l. Violations of this ordinance are subject to the following remedies:
    1. A person injured by a material violation of this ordinance may institute proceedings against the City in a court of competent jurisdiction for injunctive relief, declaratory relief, or writ of mandate to enforce this ordinance.
    2. Prior to the initiation of any legal proceeding under subsection (1), the City must be given written notice via the City Attorney’s Office of the violation(s), and the bureau who is alleged to have violated the ordinance will have 30 days from receipt of the notice to correct such violation(s).
    3. If the alleged violation(s) is substantiated and subsequently corrected, a notice shall be posted in a conspicuous space on the City’s website that describes the corrective measure(s) taken to address the violation(s).

m. Each bureau director is responsible for enforcing this policy within its bureau.

n. This ordinance is binding City policy applicable to all bureaus and Council/elected offices.

Section 2. The Council declares that an emergency exists because of the need to respond to the immediate concerns of Black, Indigenous and People of Color (BIPOC) and to center the safety and well-being of BIPOC communities. Therefore, this ordinance shall be in full force and effect from and after its passage by the Council.

Passed by the Council:
Mayor Ted Wheeler
Commissioner Joann Hardesty

Prepared by: Hector Dominguez
Date Prepared: 08-03-2020

Mary Hull Caballero
Auditor of the City of Portland By

Deputy

703

Agenda No.

ORDINANCE NO.

Title

*Prohibit the acquisition and use of Face Recognition Technologies by City bureaus (Ordinance)

INTRODUCED BY
Commissioner/Auditor:
Mayor Wheeler

CLERK USE: DATE FILED 9/1/20

COMMISSIONER APPROVAL

Mayor—Finance & Administration - Wheeler — Mustafa Washington — Digitally signed by Mustafa Washington Date: 2020.09.01 12:19:03 -07'00'

Position 1/Utilities - Fritz

Position 2/Works - Vacant

Position 3/Affairs - Hardesty

Position 4/Safety - Eudaly

Mary Hull Caballero
Auditor of the City of Portland

By: Keelan McClymont — Digitally signed by Keelan McClymont Date: 2020.09.01 15:34:25 -07'00'
Deputy

ACTION TAKEN:

BUREAU APPROVAL

Bureau: Planning and Sustainability
Bureau Head: Andrea Durbin — Digitally signed by Andrea Durbin Date: 2020.08.20 17:42:04 -07'00'

Prepared by: Hector Dominguez Aguirre
Date Prepared: 7/30/20

Impact Statement
Completed ☑ Amends Budget ☐

Portland Policy Document
If "Yes" requires City Policy paragraph stated in document.
Yes ☑ No ☐

City Auditor Office Approval:
required for Code Ordinances

City Attorney Approval:
required for contract, code, easement, franchise, comp plan, charter — Esin Onart — Digitally signed by Esin Onart Date: 2020.08.19 11:30:36 -07'00'

Council Meeting Date 9/9/20

AGENDA

TIME CERTAIN ☑
Start time: 2:00 PM
Total amount of time needed: 2 hours
(for presentation, testimony and discussion)

CONSENT ☐

REGULAR ☐
Total amount of time needed: _____
(for presentation, testimony and discussion)

FOUR-FIFTHS AGENDA	COMMISSIONERS VOTED AS FOLLOWS:	YEAS	NAYS
1. Fritz	1. Fritz		
2. Vacant	2. Vacant		
3. Hardesty	3. Hardesty		
4. Eudaly	4. Eudaly		
Wheeler	Wheeler		

Exhibit A

Public feedback received by July 24, 2020 to the policy draft to “prohibit the acquisition and use of Face Recognition Technologies by the City of Portland bureaus” made available since January 28, 2020.

Note: Comments were redacted according to current public records exceptions.

submitter	organization	date received	city
Sean Patrick	Portland resident	5/8/2020	Portland, OR
EFF About face campaign	Electronic Frontier Foundation	6/15/2020	Portland, OR
Larry Kirsch	Portland	7/6/2020	Portland, OR
Boaz Ally-Feuer	Portland	7/21/2020	Portland, OR
Dan Handelman and other members of portland copwatch	portland copwatch	7/23/2020	Portland, OR
Kelsey Finch	Future of Privacy Forum	7/24/2020	Seattle, WA
Brian Hofer	Secure-Justice	7/26/2020	Oakland, CA

Smart Cities PDX
c/o Portland Bureau of Transportation
1120 SW 5th Ave.
Portland, OR 97204

May 8, 2020

Dear persons:

After reviewing information available online through the "Smart Cities PDX" website, I am writing today to express my strong support for an outright ban on face recognition technology in the city of Portland.

I agree with the ACLU and other civil rights and civil liberties organizations when they express grave misgivings over how this technology could (even inadvertently) be misused with respect to poor communities, at-risk communities and communities of color.

If it is ever to be used in any way, we must start from a position of **outright ban**. This is the only way to ensure justice in Portland, as Commissioner Jo Ann Hardesty eloquently states in her transcripted remarks on the subject.

However, I firmly believe that face recognition technology is a terrible danger to *all* citizens, regardless of background.

First of all, in Oregon, citizens are not required to present identification or establish their identity in any way, *unless they are reasonably suspected of a crime.*

The spirit of this law clearly supports the corollary that Oregon citizens **have the right to remain unidentified in public spaces**. The purpose of this law is obvious from my perspective. It places the balance of power firmly in the citizen's hands and ensures that justice is served throughout the state such that citizens cannot be targeted (as easily) through extrajudicial profiling and abuse.

After all, if police and officials do not know who you are, then they cannot retaliate against you for doing legal things that they find distasteful.

The use of public face recognition technology removes this right and shifts the balance of power directly into the hands of the police and government. It places undue burden on citizens to hide or otherwise obscure their physical appearance in order to exercise this clearly intended freedom and makes its free and unfettered expression practically impossible.

The state of Oregon has already removed (what I believe to be) the basic human right to avoid biomettrics collection by implementing the **collection of facial biometrics** in the ID system of the state. This is a direct violation of the spirit of the law I described.

However, it is this law *in combination* with face recognition technology, public or private, that creates a system **turn-key ready** for abuse.

First and foremost, we must protect our poor communities and communities of color from what we have clearly seen can be (sometimes unconscious?) profiling and abuse from the "stop-and-frisk" use of this technology in other parts of the country.

But in more general terms, how might it chill democracy?

When activists, citizens and citizen-journalists know that their attendance at a rally or investigation process around town will be attached directly to their names and data, this might change the way they operate. Or to whom they speak.

How might it chill their participation levels and contributions to oversight in our system?

How might people in positions of power benefit from this chilled environment and how might this be used "under-the-radar" to support injustices in our community?

I am deeply sympathetic to the difficulties officers of the law face as they seek to investigate crime and do what they believe will help our communities remain safer. But we must not sacrifice our collective freedoms to make this task easier, as much as we would like to see it become so. The risks for abuse are too great, especially as technology (of all kinds) continues to develop in unexpected and powerful ways.

And while public face recognition technology is a clear danger in this way, allowing the private sector to engage in using it **could be just as damaging**.

The 3rd-party doctrine (an archaic legal opinion from the 1970s that could not have predicted the widespread private data collection practices we now face) can be construed to allow unfettered access to nearly any data collected by private entities.

With a simple "I agree" check box on an employment or electronic application website, a massive (though disparate) database accessible to government actors could be created. And who would actually read the fine print in order to opt-out of this kind of data collection? And even if they *did* read into it, who would be willing to turn down a job or a special sale in order to opt-out?

The alternative to this dangerous scenario is an outright ban.

But as dangerous as this technology might be here in the present, my concerns run deeper.

We live in an increasingly authoritarian-leaning world supported by wildly inflamed socio-political divisions. The election of Donald Trump and the sudden shift in electoral politics that we all witnessed in his rise have made the illusion of stability in our political system obvious.

The deepest danger of face recognition technology is not how that technology might be used today. The deepest danger, in my opinion, is how this technology might be used *in the future*.

I believe that our current council members have nothing but the best of intentions for the city and its inhabitants, but who will be in power 10 years from now? In 20 years?

In our populist-leaning political climate, it is difficult to predict just what forces might be placed in office. It is the job of this council then to ***future-proof*** **this technology**.

The COVID-19 pandemic has illustrated how quickly and easily an "emergency" can be called and just how vast the expansion of state powers can be in those situations. I am not entirely opposed to the current handling of the pandemic, but to see the sweeping powers of the executive branch in action is, at the very least, breath-taking.

How might face recognition be used to lock down our country against the will of its people for less-benign reasons? As state and federal powers are continuing to be aggregated into the executive branch, do we trust the "*next Trump"* (elected 10 or 20 years from now) to implement such powers judiciously and prudently?

(*Of course, if your "Lesser of Two Evils" looks different than mine, please feel free to substitute any political figure you find distasteful into that previous statement. The spirit of its concern remains intact.*)

In addition, as we enter the "AI era," we must be aware of how future administrations might make use of face recognition technology in the process of **retroactive surveillance**.

Retroactive surveillance is the process of mining datasets, created over time, in order to build patterns of behavior and association that identify every possible influence, person, organization and structure that supported a dissident in becoming difficult in the present moment.

Retroactive surveillance requires the creation of datasets that can be analyzed at some point in the future. Face recognition technology enables and greatly enhances the potential creation of these datasets.

How Face Recognition Technology Enhances the Potential for Dataset Collection

When face recognition technology is being used, the potential for the creation of a dataset of citizen activity *over time* is greatly enhanced. This data and can be used to identify a person's whereabouts, their contacts and activities, especially when combined with the huge amount of data already collected in our society at the present time.

Even if this information is not recorded actively by the city, **the potential for other non-city actors** to do so surreptitiously is a clear and present danger.

Through their testimony to our very own Senator Ron Wyden, we have witnessed the NSA *lie under oath* about their collection of data of this sort. Even with powerful debate on Section 215 of the USA

PATRIOT act, it is very likely that it will be renewed and this kind of (unconstitutional?) data collection will continue.

But, even if Section 215 *were* struck down, the secretive continuation of these practices can not be ruled out. The NSA made that clear when refusing to be transparent with Mr. Wyden in front of congress.

However, the danger of creating datasets that can be used for retroactive surveillance is not limited to the actions of public entities.

As private companies, contractors and tech-giants continue to track citizens in ever more complex and difficult-to-trace ways, the potential for deep profiles of data about our citizenry is a very real threat.

How so?

Under the USA PATRIOT Act, "terrorism" has been defined in exceedingly broad terms. Most often domestically, since 9/11, it has been attached to environmental activists and peaceful protestors.

There is **no public burden of proof** required to define suspicion of "terrorism" and the level of enhanced government surveillance this "suspicion" enables is huge.

Under the PATRIOT Act, datasets can be requested and compiled through an enhanced National Security Letter (NSL) system, without the public oversight of a judge. In addition, they can be delivered to nearly any private entity and come **attached to a gag order** (although this gag order now must be substantiated legally, but only when directly challenged by the recipient).

When combined with the *3rd Party Doctrine* outlined earlier, these Patriot Act powers make private face recognition systems an avenue for deep dataset collection.

These datasets, despite the best intentions of their creators, can be used to reveal citizen activity data to the government now and into the future.

The Dangers of Retroactive Surveillance With Citizen Datasets

Face recognition technology removes the ability for law-abiding citizens to move about the country freely without fear of data-collection and profiling. **They cannot reasonably "opt-out."**

Once this data has been aggregated, it can be retained far into the future. Perhaps "forever." This makes it susceptible to use in retroactive surveillance.

But how could retroactive surveillance actually work?

Consider the following example.

In the future, a more civil-liberties averse administration could use the vast datasets created (by FRT and other technologies) to track a person's behavior and associations "backward in time."

Imagine a peaceful, environmental activist that has become inconvenient to a future, more authoritarian-friendly administration. Let's say, one of our children's friends that has become interested in the more extreme effects of global climate change, maybe 10 or 15 years from now.

Without a warrant, under the PATRIOT Act, this future administration could easily access data collected by private *and* public entities about them. In addition, this administration may already have access to a great deal of this data, as it may have been collected by the NSA or other organizations once enabled by local face recognition systems.

This more authoritarian administration could then analyze every aspect of their behavior and the way they developed their ideas and associations over time.

If they were deemed inconvenient to said administration, networks of law abiding citizens, associates or sympathizers could be easily ferreted out through this analysis. **Our child might be among them.** In addition, the activities and processes by which they built their associations can be analyzed and identified as well.

We know that some administrations will stop at almost nothing to protect their interests. And the administrations that come after tend to immunize them against prosecution.

What might happen to these peaceful, forward thinking people?

Perhaps nothing.

Or maybe the unthinkable.

Something in between?

It's certainly not outlandish to imagine that the quiet suppression of their democratic rights to express themselves might at least, be endangered.

And in broader terms, how might our society be affected?

How might communities of color resisting gentrification and abuse be targeted quietly?

What might happen to journalists reporting uncomfortable truths?

To citizens that ask difficult questions and those that support them?

At the very least, information of this sort could be a treasure trove of data for micro-targeted ads and manipulation by internal and external actors to shift public opinion, as we have already seen with citizen data sold by Facebook to Cambridge Analytica.

The potential to permanently enshrine an authoritarian regime, system, administration or process in this way is enormous, in my opinion.

*(An example of how electronic data has **already been used** in Britain to quell and prevent protest can be found near the end of this documentary: Terms and Conditions May Apply, a New York Times "Critic's Pick" from 2013).*

Drowning In Data: Why This Is Not a Protection

Currently, the government is "drowning in data," and the argument has been made that this invalidates any concerns about the use of it in the future. Or fears of creating additional systems by which it might be collected.

If this is true, however, why is the NSA so insistent on retaining it?

Perhaps because there is an expectation that the ability to analyze it effectively will exist at a later date.

The specificity and implementation of artificial intelligence is improving in power and scope every day. Indeed, face recognition, the very technology we are discussing here, was nearly *unthinkable* 15 years ago. It is the advancement in AI that has made it possible.

Where will this technology be in the *next* 15 years?

Or 30?

Do we believe that the reach and abilities of AI have topped out as it continues to advance in surprising ways?

The artificial intelligence of today is **already** giving businesses and organizations unprecedented abilities to work with *past data*. This has been extensively documented and clearly described.

And, as **threat detection** is *already* a common task for AI (defined here as machine learning), as it continues to develop, how will future administrations choose to define a "threat?"

Will we create a system that allows our children and their expression of democratic growth and freedom to be fodder for analysis that chills their abilities to express themselves?

Personally-identifying data collection and retention in the dawning era of AI is a danger to the future of our democratic republic. Face recognition technology **greatly enhances** this threat, violates the spirit of our freedoms here in Oregon and places the future of our children and their communities at risk.

Once in place, we **cannot reasonably "opt out"** of face recognition systems. Public or private.

In closing, I strongly support an outright ban on this technology in the City of Portland, and give my strongest thanks and support to Jo Ann Hardesty for embracing this position.

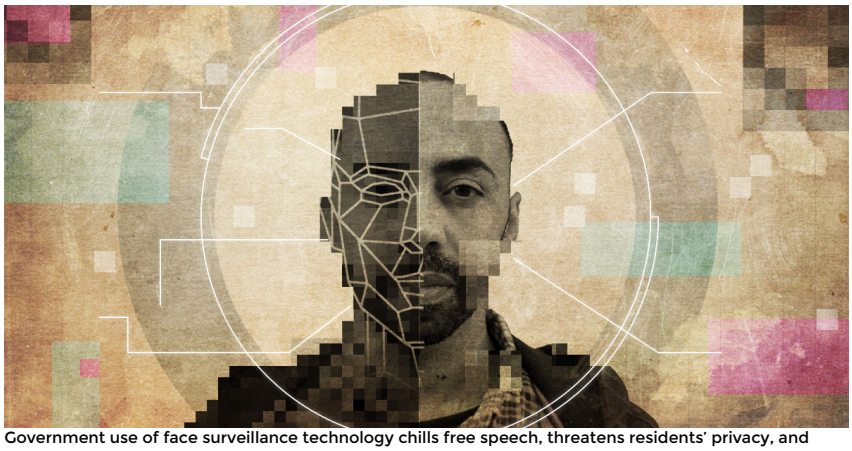
In democratic expression,

Sean Patrick

(/)

PRIVACY

About Face



Government use of face surveillance technology chills free speech, threatens residents' privacy, and amplifies historical bias in our criminal system.

From San Francisco, California to Somerville, Massachusetts, communities are coming together to demand an about-face on the proliferation of government use of this especially pernicious form of surveillance and biometric data collection.

Join us in ending government use of face surveillance in our communities.

[Can't find your town listed? Contact your state representatives (https://action.eff.org/o/9042/p/dia/action4/common/public/?action_KEY=10946).]

June 15, 2020

Use of face surveillance by law enforcement and other government agencies invades Fourth Amendment freedoms of privacy and chills First Amendment freedoms of speech and association.

Face surveillance technology has already been used to target individuals engaged in First Amendment-protected activity. And the threat of this especially pernicious form of surveillance extends far beyond political rallies. Images captured outside houses of worship, medical facilities, schools, community centers, and homes would reveal familial, political, religious, and sexual partnerships.

Data theft is another threat. Digital security professionals regularly warn that it's not a matter of if a given system will be breached, but when. Government agencies have a notorious history of failing to adequately secure from theft the sensitive personal information and biometric data that government stockpiles. Unlike a driver's license or social security number, when a breach occurs, our faces can not be reissued.

As community members concerned with our own privacy and safety, as well as that of our families and neighbors, we stand together in committed support of an immediate end to the government's use of face surveillance.

SIGNED

Your Name

Learn More

TAKE ACTION

Your name and affiliations will be published on our site.

2,800 signatures

If you are a human, ignore this field

(/)

Email

First Name

Last Name

City

I am a...

+ Add another city

Zip Code (optional)

OUTSIDE THE US?

Yes! I would like to join EFF's mailing list for EFF news, events, campaigns, and ways to support digital freedom.

How will EFF use this information? ?

TAKE ACTION

Signatures

Portland, OR

FILTER

remove filter (/action/about-face)

Portland, OR

155 Signatures

MacKenzie Stout Business Owner	14 DAYS AGO
Austin Millan Technologist	14 DAYS AGO
Cleo Forman Resident	16 DAYS AGO
Joseph Corrado Resident	16 DAYS AGO
Melba Dlugonski Resident	16 DAYS AGO
Michele Unger Resident	16 DAYS AGO
DR Gaylord Skip King Technologist	17 DAYS AGO
Janice Coleman Resident	17 DAYS AGO
David Hermanns Resident	17 DAYS AGO

← Previous *1* 2 (/Action/About-Face/Portland-Or?Page=2) 3 (/Action/About-Face/Portland-Or?Page=3) 4 (/Action/About-Face/Portland-Or?Page=4) 5 (/Action/About-Face/Portland-Or?Page=5) 6 (/Action/About-Face/Portland-Or?Page=6) 7 (/Action/About-Face/Portland-Or?Page=7) 8 (/Action/About-Face/Portland-Or?Page=8) 9 (/Action/About-Face/Portland-Or?Page=9) … 17 (/Action/About-Face/Portland-Or?Page=17) 18 (/Action/About-Face/Portland-Or?Page=18) Next → (/Action/About-Face/Portland-Or?Page=2)

(https://www.eff.org)
(/)

☰

THANKS (HTTPS://WWW.EFF.ORG/THANKS)
RSS FEEDS (HTTPS://WWW.EFF.ORG/RSS)
COPYRIGHT POLICY (HTTPS://WWW.EFF.ORG/COPYRIGHT)
PRIVACY POLICY (HTTPS://WWW.EFF.ORG/POLICY)
OPEN SOURCE (HTTPS://GITHUB.COM/EFFORG/ACTION-CENTER-PLATFORM)
CONTACT (HTTPS://WWW.EFF.ORG/ABOUT/CONTACT)

Dominguez Aguirre, Hector

From: Larry Kirsch [redacted]
Sent: Monday, July 6, 2020 9:03 AM
To: Wheeler, Mayor; Commissioner Hardesty; Commissioner Fritz; Crail, Tim; Carrillo, Yesenia; Commissioner Eudaly; Runkel, Marshall; Weeke, Margaux; Bradley, Derek; Tran, Khanh; Grant, Nicole; Park, Eileen; Dominguez Aguirre, Hector; Martin, Kevin; Llobregat, Christine; Taylor, Kalei; Smith, Markisha
Subject: Comments in OPPOSITION to Portland's Proposed Ordinances on FACIAL RECOGNITION TECHNOLOGY
Attachments: COMMENTS on Facial Recognition Ordinances-July 2020.docx

Dear Mr. Mayor, City Council Members, and Other City Officials Concerned With the Facial Recognition Technology Ordinances,

In anticipation of the PDX City Council's August 13th Hearing on this matter, I attach extensive comments that acknowledge and support the precautionary purposes of the proposed ordinances and new city code but oppose both the public and private sector open-ended bans contained, therein.

I appreciate all the work you have done on this important issue and thank you for the opportunity to present my views for your consideration.

In my opinion, the ordinances go too far because they are predicated more on fears than on facts on-the-ground. On the other hand, they don't go far enough because they do virtually nothing to validate their assumptions and to objectively test the possibility that useful and safe applications could be developed in the public interest through a "Responsible Use Framework".

In lieu of the proposed ordinances, I recommend that the Council adopt a temporary moratorium together with an inclusive public-industry-community process for developing a "Responsible Use Framework" of product and usage standards, testing procedures, and compliance.

The current proposals before City Council would completely ban adoption and use of Facial Recognition by city agencies and most private sector entities based on concerns relating to accuracy, racialized use, privacy, intrusiveness, and other fundamental human rights/civil liberties issues. Although each of these concerns is deserving of the most serious public scrutiny, a time-limited moratorium would provide all the protections necessary for public safety while allowing the development of a standard setting and testing process to determine if beneficial uses could be approved while objectionable uses were screened out.

It is my view that if City Council decides to pursue both a public and private sector ban approach based on the evidence now before it, it unnecessarily jeopardizes Portland's reputation as a technology hub, lends credence to a label of Luddite city, fails to recognize the availability of better options, and invites implementation challenges on various grounds.

I will be happy to clarify or assist you with your ongoing work on this matter.

Respectfully submitted with all best wishes,

:Larry Kirsch
Portland

(617) 731 2600

July 8, 2020

COMMENTS TO THE PORTLAND CITY COUNCIL ON PROPOSED ORDINANCES AND CODE BANNING THE USE OF FACIAL RECOGNITION TECHNOLOGY BY THE CITY OF PORTLAND AND IN PLACES OF PUBLIC ACCOMMODATION WITHIN THE CITY OF PORTLAND

Personal Introduction

By way of brief introduction, my name is Larry Kirsch. I am a resident of Portland, an economist, retired university faculty (health economics and policy), and consumer protection consultant/author. I have absolutely no interest (financial, professional, legal, or otherwise) or connection of any sort to any person or entity involved in the facial recognition and/or biometric surveillance business or similar. I claim no firsthand technical expertise in the fields of facial recognition technology, software, or hardware systems. My perspective on this matter centers exclusively on the process of public policy development associated with the Council's scheduled review of the proposed bans on facial recognition technology.

I have participated in various forums convened by Smart City PDX (a lead agency designated by the City Council) and have shared informal, preliminary observations with that team and with others engaged in this issue. I have reached no firm conclusions about the ultimate merits and/or limitations of facial recognition technology but I do have several observations and recommendations to offer in conjunction with the process of policy development in this matter.

I acknowledge and fully support the general concerns that have given rise to the proposed ordinances, namely, human rights, civil liberties, non-discriminatory application, and operational integrity of the technologies. I welcome the City's involvement as a matter of public interest and appreciate its commitment to provide residents of the City of Portland procedural and substantive safeguards.

I disagree, however, with the comprehensive, open-ended ban the ordinances would invoke. As my comments will show, I believe there are more effective ways to address the City's enunciated concerns and to simultaneously develop robust standards of "responsible use". Finally, I question the justifications put forth by the City for both ordinances and also its authority to implement the proposed public accommodation ordinance at this time.

Section I. <u>Overview</u>

1. Portland City Council (City Council or City) has docketed two draft Ordinances and a new Code section that would prohibit acquisition, evaluation, retention, and utilization of Facial Recognition Technology (FR Technology) for an unspecified period of time. One ordinance would apply to Portland City government; the other to defined Public Accommodations including retail stores, hotels and restaurants, private universities, etc. The City Government ban would take immediate effect; the Public Accommodation Ban would take effect on January 1, 2021. [1]

   If adopted, Portland will join a handful of other cities (including San Francisco and Boston) that have already enacted ordinances banning the adoption and utilization of FR Technology by municipal agencies. It would be the first one to extend its ban to public accommodations.

2. The pending ordinances assert that the use of FR Technology "raises general concerns" and "can create devastating impacts". They identify transparency, privacy, intrusiveness, inaccuracy, racial and other invidious disparities, and inequities as among the main characteristics of concern to the City. They make no factual determinations, however, that FR Technology, in general, nor any specific brands or models of FR Technology, in particular, do, in fact, pose

[1] The effective date of the Public Sector ordinance is a bit ambiguous and should be addressed; the Public Accommodation ordinance is more clearly defined.

threats that justify an immediate, time-unlimited prohibition. To the contrary, the Public Accommodation ordinance stipulates that the City does "not have the infrastructure to evaluate Facial Recognition Technology". In sum, then, the proposed ban is precautionary and is driven by general concerns about the safety and accuracy of the technology as well as applications that could impinge on important civil and human rights.

3. The City asserts that these ordinances are needed to manage the acquisition and use of FR Technology and to address the threat of adverse or inequitable impacts on minority groups, marginalized communities, genders and ages.

4. The City states that there are no statutes currently in-force to carry out this oversight function in Portland.

5. The proposed ordinances explicitly recognize a need for informed public discussion about the acquisition and use of FR Technology. Indeed, the Public Accommodation Ordinance is replete with discussion of plans and procedures for public engagement and consultation. This comment is an attempt to contribute to such a public debate.

6. After a general summary section, the comment goes on to address four issues central to the current proposal: (a) the immediate, open-ended ban on the private sector's and the City's acquisition and use of all FR Technology, (b) the alternative of a time-limited moratorium, (c) a "responsible use framework" process, and (d) elements of "responsible use" guidelines. It concludes with recommendations.

Section II. <u>Areas of Agreement</u>

7.a. I agree that the City has stated valid public concerns relevant to FR Technology and its application. They include: (1) transparency, (2) intrusiveness, (3) accuracy,

(4) privacy, (5) biased data—collection and utilization, and (6) possible misuse in conjunction with surveillance of persons and populations.

7.b. I agree with the City's goal of addressing issues related to FR Technology on a prospective basis.

7.c. I agree that the City is right to accord priority attention to the potential impact of FR Technology on minority and marginalized communities.

Section III. Areas of Dispute

8.a.1. I do not believe the City has set forth a sufficient factual basis for invoking an open-ended ban on the acquisition, evaluation, retention, and use of all FR Technology—either by city bureaus or public accommodations.

8.a.2. The ordinances are predicated on hypotheses, assumptions, and worst case scenarios about the performance of products subsumed under the label of FR Technology. The City does not have the infrastructure to evaluate FR products. It has not developed or adopted any product guidelines, standards or criteria that would permit it to objectively evaluate the operating performance of any or all brands or models in the FR Technology class and to reach factual conclusions about their safety and appropriateness in areas of concern.

8.a.3. The City has not objectively tested or examined any brands or models of FR Technology to determine how they actually perform in the areas of concern. While there is limited anecdotal evidence and a few objective performance tests focusing on accuracy, the City has not cited any comprehensive evaluations that reach all of the areas of concern. Nor has it put forth expert evidence on product safety and/or other dimensions that would permit it to conclude, reasonably, that a given model or brand could be presumed (un)safe.[2]

[2] I have in mind a model analogous to the Food and Drug Administration's GRAS (Generally Recognized as Safe) standards for determining the presumptive safety of food additives.

8.a.4. Although the ordinances pay lip service to the need for standards, criteria, and testing of FR Technology, brands, and models, they do not undertake to make an investment in developing the required infrastructure. [3] Instead, the ordinances focus extensive attention on procedures for facilitating public engagement as if that input, alone, can be assumed to result in an objective, fact-based evaluation of safe products and responsible applications. In my opinion, that assumption is totally unrealistic.

8.a.5. The City has not made out a case of dire necessity or emergency to justify immediate imposition of a generalized, open-ended ban.

8.a.6. As to the proposed Public Accommodation ban applicable to all brands and models of FR Technology, I seriously question whether the City has demonstrated real-- as opposed to theoretical or potential harms—sufficient to satisfy pertinent legal requirements for the use of its police powers. Moreover, as I understand the proposal, there is no way for a producer to overcome the negative inference that it's brands/models are not safe enough to meet the City's concerns or that its conditions of use are not sufficiently protective to address the City's goals.

Section IV. A Time-Limited Moratorium

9.a.1. I believe a time-limited moratorium (as distinct from an outright ban) on the acquisition, evaluation, retention, and use of FR Technology would provide a reasonable, appropriate, and effective approach for managing the City's legitimate concerns about the potential threats of the technology and its applictation. Along similar lines, some leading members of the FR Technology industry have recently announced their decision to temporarily pause sales to police departments (or more generally). Thus, a time-limited moratorium adopted by the City would be compatible with those actions. All FR Technology products (brands and models)

[3] "While FRT uses may have benefits, the risk for misidentification and misuse is always present. This technology requires proper due process, transparency and oversight measures to be trusted. This requires investment in development of rules and structures that allow appropriate uses of FRT." (Public Accommodation Ordinance, §1.13)

would remain subject to the moratorium until such time as the City authorized their use. [4]

9.a.2. As stated in § 8.a.2 and §8.3 the City has not adopted any specific product safety standards or utilization guidelines nor has it tested any FR Technology products to determine their actual performance against such norms and standards. As a result, it cannot make the claim that an outright ban on FR Technology is solidly grounded in fact.

9.a.3. The moratorium would provide a landmark opportunity for the City to bring stakeholders (City, community, industry, experts, privacy advocates) to the table to craft community guidelines for "responsible use" of FR Technology and a protocol to test products for compliance. [5] I will refer to this as a "Responsible Use Framework". The Responsible Use Framework would incorporate product standards, testing requirements, guidelines for the safe application and fair use of the technology, compliance provisions, and other features of comprehensive oversight. The Responsible Use Framework would apply to both public and private uses and would be subject to City Council approval. No brands or products that were inconsistent with the Framework could be utilized or licensed for sale in the City.

9.a.4. Although there can be no guarantee that a Responsible Use Framework would be feasible in Portland, I offer at least several grounds for qualified optimism.

First, some major industry players, most outspokenly Microsoft, have recognized the legitimacy of community concerns for the transparency and accountability of FR Technology, the need for public safeguards against exploitation, and the vital need to establish community trust about protections against unchecked surveillance based on FR Technology. The State of Washington is the first in the country to have enacted a statute that would define a framework for regulating public use of the technology (effective July 2021). [6] Although supporters and critics of the statute

[4] One general approach the City might consider would be a licensing model the details of which are well beyond the scope of this Comment.

[5] See §8.4 above.

[6] Washington State Engrossed Substitute Senate Bill SB 6280 (enacted March 12, 2020)

hold different views about its sufficiency and particular provisions, it represents a first publicly- supported starting point for engaging stakeholders in a critical assessment of acceptable and workable technology performance standards. [7]

Second, there is no current indication that Oregon's Governor or state legislature or the federal government has the intent to initiate a Responsible Use Framework. [8] Thus, the potential for conflicts to arise between levels of government is minimal and a strategy that would defer City action pending state or federal activity is highly questionable. Moreover, since issues of nondiscriminatory application of FR Technology at the community level have come to dominate public discussion in Portland, the creation of a local process involving the City's communities would be more responsive than a state or federal solutions.

Third, Portland is a hub of tech sector activity and has the capacity to mobilize public and private sector resources at a level necessary to engage the complex spectrum of issues related to FR Technology. As an example, Intel and other area tech companies are prominent in this field; individual universities or a consortium would have the range of intellectual and technical resources needed to contribute to the analytic aspects of the issue, the City has organized itself to focus on FR Technology, and community organizations, privacy advocates, and other civil society groups have become actively engaged as well.

Finally, to the extent Portland becomes the first city in the country to ban private sector use of FR Technology, I believe City Council takes the needless reputational risk of establishing the City as a Luddite foe of technology. That is certainly the

[7] Lostri, Eugenia, "Washington's New Facial Recognition Law". Center for Strategic and International Studies (April 3, 2020) https://www.csis.org/blogs/technology-policy-blog/washingtons-new-facial-recognition-law

[8] Several bills have been introduced in Congress but as of now they haven't progressed very far. See, for instance, the Markey-Merkley moratorium bill https://www.markey.senate.gov/imo/media/doc/acial%20Recognition%20and%20Biometric%20Technology%20Moratorium%20Act.pdf

case where other less extreme measures are available to deal with the public concerns outlined in the ordinances.

9.a.5. A temporary moratorium linked to a responsible use framework would not, of course, guarantee favorable results. For that reason, City Council should retain authority to terminate or extend the moratorium at its discretion and to revisit prohibition legislation, as necessary. The incentives for best efforts, however, are strongest where the costs of failure are clear and well known from the outset.

Section V. FR Technology and the Adoption of a Responsible Use Framework

A. Background

10.a.1. On June 21, 2018, City Council Resolution 37371 created a Smart City PDX Priorities Framework as a guide to the City's use and investment in technology. The Framework emphasized the City's interest in safeguarding the equitable and non-discriminatory adoption of technologies, specifically mentioning communities of color and disability communities.

10.a.2. On June 19, 2019, City Council Resolution 37437 established Privacy and Information Protection Principles and assigned primary responsibility to the Bureau of Planning and Sustainability and the Office of Equity and Human Rights (the lead agencies) for the development of policies and procedures to implement the principles.

10.a.3. Facial Recognition is an emerging and controversial technology. It embodies numerous current uses ranging from public safety and medical diagnosis to consumer services and political research. It is generally considered to have additional applications that are still opaque. FR Technology is also considered to pose potential risks to the public interest especially in areas relating to privacy, equity, and human rights.

10.a.4. Facial Recognition's status as an emerging technology with potential benefits as well as risks demands strict public oversight of its adoption and use. An

effective public oversight process has won general acceptance among major public interest advocacy groups as well as leading industry representatives. [9]

10.a.5. If the Council now decides to adopt prohibitory ordinances before the lead agencies have presented a fully developed factual basis for an immediate and time-unlimited ban and justification for declining a less extreme alternative, that decision would represent a classic case of putting the regulatory cart before the fact-finding horse.

10.a.6. A Responsible Use Framework would represent an example of a public interest alternative to a comprehensive ban.

B. A Responsible Use Framework: Elements and Process

10.b.1. The quintessential elements of a public oversight process would include (a) identification of product performance features inclusive of product features and conditions of use that would demonstrably endanger safety, privacy, and other human and civil rights interests, (b) definition and quantification of maximum acceptable risks levels associated with each feature, (c) provisions for verifying product test data and objectively testing product brands and models, (d) a means of assuring compliance with the elements of the Framework, and (e) methods for approving the acquisition and use of FR Technology via a system of licensing or other means.

10.b.2. Recognizing the budgetary and capacity constraints facing the City, development of the Responsible Use Framework could be contracted to an independent third party (such as a university) working in close coordination with the lead agencies designated by City Council. A prime responsibility of the City and the Contractor would be to convene and manage a broad-based process of

[9] See letter to Reps. Elijah Cummings and Jim Jordan from the ACLU and other organizations https://www.aclu.org/sites/default/files/field_document/2019-06-03_coalition_letter_calling_for_federal_moratorium_on_face_recognition.pdf. Also see the statements of Microsoft's president, Brad Smith https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/; https://blogs.microsoft.com/on-the-issues/2020/03/31/washington-facial-recognition-legislation/

community, industry, civil society, and technical engagement that would be involved in each phase of the project.

10.b.3. The lead agencies in collaboration with the Contractor would seek suitable external funding for a Framework development project. Among other things, funding should be requested to facilitate informed civic engagement in the complete planning process.

10.b.4. The lead agencies could be requested to brief the Council, periodically, on the status of the project. They would submit a final proposed Responsible Use Framework to City Council for its approval. Any agreements between the City, funding sources, contractors, or other parties should recognize the possibility that the project could be restructured or terminated by City Council.

Section VI. Recommendations

In view of the above, I respectfully recommend that the City Council: (a) withhold approval of the two proposed ordinances and new Code section currently before it for action; (b) request that the designated lead agencies prioritize development and submission of a proposal to City Council for a Responsible Use Framework along the lines outlined in these Comments, and (c) adopt an ordinance that would place a time-limited moratorium on City of Portland and Public Accommodation FR Technology pending a subsequent decision to adopt a Responsible Use Framework approach.

In conclusion, I appreciate the opportunity to submit these comments and to participate in the public discussion of FR Technology in the City of Portland. I stand ready to help clarify these comments and to assist the City move forward on this matter of vital public importance.

Respectfully submitted,

Larry Kirsch

[redacted]

(617) 731 2600

Portland, OR 97209

Dominguez Aguirre, Hector

From: Boaz Allyn-Feuer [redacted]
Sent: Tuesday, July 21, 2020 8:19 PM
To: Smart City PDX
Subject: Comments: facial recognition

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

Below are my comments regarding the:

Draft of the public use of Face Recognition Technologies Ordinance (Public draft 07-01-2020)

The exception "In social media applications, which is regulated by the Social Media Policy: HRAR 4.08A" is overly broad. What, specifically, motivates a desire to include such an exception? Whatever it is, the exception should be written so as to be narrowly tailored to that purpose. As currently written, this exception covers a huge category of potential use of facial recognition technology by city bureaus.

Moreover, HRAR 4.08A does not appear to regulate bureau activity at all, as it seems to apply only to personal use of social media by bureau employees. What's more, HRAR 4.08A as written violates the First Amendment rights of city employees.

The exception "For the sole purpose of redacting a recording for release or disclosure outside the City to protect the privacy of a subject depicted in the recording" is clearly unnecessary. This kind of redaction should be done by hand and no use of facial recognition technology is necessary or appropriate.

The phrases "unless required by retention rules" and "no longer than the applicable retention period or as otherwise required by law" are also potentially problematic. What retention rule requires a bureau to retain information it should never have acquired in the first place?

Is there a reason relief in a civil suit is limited to injunctive relief, declaratory relief, or writ of mandate? Why not monetary damages in addition to these remedies?

This draft of the ordinance suggests that some use of facial recognition technology by city bureaus may be allowed at some point in the future. I would write the ordinance as a clean, total and permanent ban of the use of facial recognition technology by city bureaus.

Dominguez Aguirre, Hector

From: Portland Copwatch <copwatch@portlandcopwatch.org>
Sent: Thursday, July 23, 2020 12:33 PM
To: Dominguez Aguirre, Hector
Cc: Smart City PDX
Subject: Re: update on date for feedback to Portland's FRT policies

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

Mr. Dominguez
Thank you for taking the time to talk with Portland Copwatch members about the digital justice legislation being proposed in Portland.

We raised a few concerns during the call which we'd like to remind you about here.

For the public use ordinance, the question about social media applications is deferred to a Human Resources policy. However, it is not clear from the context whether that policy prohibits the use of facial recognition on social media as a means for law enforcement to circumvent the broader ordinance. We hope not, and suggest a clarification and/or change to the HR policy. (Council Directs section [e], 7/1 draft)

That document also does not explicitly call for employees who violate the code to be disciplined. It is implicit in sections [l] and [m] (especially in that [m] says "each bureau director is responsible for enforcing this policy") but we would like to see it be explicit.

We also noted that the public should be made aware that the City of Portland does not have the ability to regulate state or other jurisdictions on this matter, meaning that for instance the Oregon Dept of Transportation could use the technology in their cameras, Oregon State Police or even the Multnomah Sheriffs could use the technology.
Or, for that matter, the federal police who've been in our streets the last 2-3 weeks.

The public use draft implies that a city agency receiving information identifying a person needs to verify that it was not ascertained through facial recognition. This could also be more explicit. Moreover, the private use code should explicitly tell private actors that they are not allowed to use the technology to identify people to any City agency including the Portland Police.

Thank you again and keep us posted
--dan handelman and other members of
portland copwatch

Dominguez Aguirre, Hector

From: Kelsey Finch <kfinch@fpf.org>
Sent: Friday, July 24, 2020 4:59 PM
To: Smart City PDX
Cc: Dominguez Aguirre, Hector; Brenda Leong
Subject: FPF comments on the Face Recognition Policies for the City of Portland

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

Dear Hector & Smart City PDX team,

Thank you for the opportunity to submit comments for Portland's Draft Ordinances regarding the public and private use of face recognition technologies (FRT) in places of public accommodation. We appreciate the extent to which Smart City PDX has directly and thoughtfully engaged diverse members of the Portland community in the development of these local policies.

In light of Future of Privacy Forum's experience on these issues, including our infographic Understanding Facial Detection, Characterization, and Recognition Technologies and report on Privacy Principles for Facial Recognition Technology in Consumer Applications, FPF would like to recommend that Smart City PDX consider additional clarification around:

Public Use Ordinance:

- Whether there are situations in which "detection" systems should be treated differently from FRTs that identify, characterize, and recognize particular individuals. All are currently equally categorized as "Face Recognition Technologies," which means the ordinance treats the one-to-many identification of an unknown person as equal to counting the undifferentiated number of people entering a stadium or shopping center. As the risks of these systems, some of which do not collect any personal information at all, vary so greatly, it might be useful to impose more nuance in the definitions in order to target restrictions in a more granular and effective way.
- Per section (e) on permitted uses of FRT, are there other publicly owned facilities that currently use facial recognition technologies for access or security monitoring, such as parking garages, that should also be excepted from the ban? While there may not be any such systems currently in use in Portland, they are not uncommon and should be explicitly considered, if there is a decision to exclude them in the future.
- Per section (f)(3), the requirement to collect and report a fairly broad set of information per incident may create circumstances in which the lead agencies may end up needing to collect more personal information than was already present with the "inadvertent" collection of FR data.
- It may be important to expressly consider and describe how Smart City PDX intends to address "public" uses of FRT outside of the City of Portland's specific jurisdiction (such as county or state equipment that may transit Portland, or federal facilities, or in private spaces not for public accommodation). We encourage Smart City PDX to support additional educational and transparency measures to ensure that community members do not develop a false sense of security because of the ordinance, when the possibilities for FRT in other public spaces may remain a possibility, even if on a much less common basis.

Private Use Draft Code:

- Unlike the Public Ordinance draft code, this draft adds a second definition to make a distinction between the more narrow definition of "Face Recognition" focused on "one-to-many search"

identification activities and “Face Recognition Technology,” which still includes the full range of detection, characterization, and verification activities in addition to one-to-many identifications. Is the intent to only ban the narrow FR systems in public space accommodations? Will the public understand these distinctions of risk in different spaces open to them?

- For private entity spaces, it might be useful to consider more existing or potential applications that would be allowed (as exceptions). As with public spaces, there is the potential for the use of FRT for facility access (such as may be used by parking garages, retailers, or sport/event venues). In addition, some products or services offered or occurring in public space accommodations may innately include FRT in their functions. Examples include photos at school events that may be used for yearbooks or other purposes; weddings and other events that include photography and associated sorting programs; or professional photographers’ services. There may be others that are not limited to social media or that would otherwise fall in the existing exceptions.

We thank Smart City PDX for its commitment to equity, privacy, and public engagement in the context of emerging technologies, and look forward to remaining engaged as the City of Portland continues to address these important topics.

Sincerely,

Kelsey Finch, Senior Counsel, Future of Privacy Forum

Brenda Leong, Senior Counsel and Director of Artificial Intelligence and Ethics at Future of Privacy Forum

--

Kelsey Finch,
Senior Counsel, Future of Privacy Forum
(571) 445-4856 | kfinch@fpf.org | www.fpf.org | PO Box 14051, Seattle, WA 98144
Check www.privacycalendar.org for events!

Subscribe to our monthly newsletter!

July 26, 2020

VIA E-MAIL ONLY

Hector Dominguez
Open Data Coordinator – Smart City PDX
Bureau of Planning & Sustainability
E-Mail: smartcitypdx@portlandoregon.gov

Re: **Prohibition on Facial Recognition Technology**

Dear Mr. Dominguez:

On behalf of Secure Justice, thank you for allowing us to provide commentary on the proposed ordinances pertaining to surveillance, public privacy, and facial recognition technology.

Secure Justice is a non-profit organization located in Oakland, California, that advocates against state abuse of power, and for reduction in government and corporate over-reach. We target change in government contracting, and corporate complicity with government policies and practices that are inconsistent with democratic values and principles of human rights. We were part of the team that successfully advocated for prohibitions on city use of facial recognition technology in San Francisco, Oakland, Berkeley and Alameda.

Prohibition on City Use of Facial Recognition Technology[1]

We applaud the intent to prohibit the city's use of dangerous facial recognition technology, and strongly encourage Portland to implement the technology vetting framework described in the ordinance. As Chair of the City of Oakland's Privacy Advisory Commission, I have seen firsthand the importance of a standing body and procurement process that allows for meaningful discussions to occur in public regarding the use of privacy invading and potentially harmful technologies.

Across the country, municipalities like Portland are quickly discovering that facial recognition technology is inappropriate in their respective cites, and several states like California have imposed moratoriums on its use. Beginning with San Francisco and most recently with Boston, large and small governing bodies are listening to their communities as they strongly reject this creepy technology.

We do suggest two amendments to the ordinance. While we understand the intent of the right-to-cure provision and have supported such provisions in our various Bay Area reform efforts, ninety days is far too lengthy when technologies like facial recognition are available. In ninety days, a

[1] The draft we were provided and reviewed is dated July 1, 2020.

bad actor could easily collect and/or identify Portland's entire population. We recommend a shorter period of 30 days.

In addition, the current enforcement mechanism will likely not provide much protection because A) we typically only learn of harm from surveillance long after the fact, and B) this technology works at a distance, in secret, and thus an injured party will almost never discover that they were subject to its use.

We suggest using the private right of action from Oakland's surveillance equipment ordinance (slightly modified for our purposes here):

"Violations of this ordinance are subject to the following remedies:

A. Any violation of this ordinance constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in a court of competent jurisdiction to enforce this ordinance. An action instituted under this paragraph shall be brought against the respective city department, and the City of Portland, and, if necessary to effectuate compliance with this ordinance (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this ordinance, to the extent permitted by law.
B. Any person who has been subjected to facial recognition technology in violation of this ordinance, or about whom information has been obtained, retained, accessed, shared, or used in violation of this ordinance, may institute proceedings in a court of competent jurisdiction against the City of Portland and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars ($1,000.00) or one hundred dollars ($100.00) per day for each day of violation, whichever is greater).
C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs A or B.
D. Violations of this ordinance by a city employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any memorandums of understanding with employee bargaining units." Oakland Municipal Code Chapter 9.64.

On June 25, 2019, the United Nations Special Rapporteur David Kaye released a report on surveillance technology, calling for a worldwide moratorium on invasive technology like facial recognition software. "Surveillance tools can interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation," the Special Rapporteur said in statement. "And yet they are not subject to any effective global or national control."[2]

[2] https://news.un.org/en/story/2019/06/1041231

We believe the Portland City Council should prohibit the city's acquisition or use of facial recognition technology for the following reasons:

1. **The error rate will create a substantial financial liability for the City of Portland, and waste resources instead of conserving them.**

According to the groundbreaking MIT study conducted by Joy Buolamwini, facial recognition technology has an error rate of up to 34.7% for black women, with a greater propensity to misidentify darker skin tones[3]. It would be irresponsible to allow the Portland Police Department, in a diverse city like yours, to use a technology with such a high error rate especially against the darker skins of certain communities that have historically been over-policed and profiled.

Although proponents of this technology put forth a credible argument about new technology's ability to make us faster and more efficient, they are ignoring the high error rate which will necessarily make us less efficient, as we must discard false positives and/or rely on other sources of information to confirm what the computers are telling us, because the results aren't trustworthy. As our coalition learned recently in Oakland from the Police Chief's own report, "most of the time the search does not yield a match." *See* Chief Kirkpatrick June 17, 2019 Report, Pg. 4 ¶2.

Earlier this year, Robert Julian-Borchak Williams, a black man in Detroit, was arrested by the Detroit Police Department in front of his wife and young children. Mr. Williams had his mug shot taken, and his fingerprint and DNA data taken and entered into law enforcement databases. During his interview, Detroit PD showed a photo to Mr. Williams that they had run through a facial recognition program. Mr. Williams immediately stated that it obviously was not him. "Do you think all black men look alike?" When the investigating officers realized they clearly had the wrong person, the officers casually replied: "I guess the computer got it wrong."[4] This underscores the danger in relying on surveillance technology in the context of policing. In the follow up discussions at Detroit's City Hall, Detroit Police Chief James Craig admitted that the technology they were using had a 96% error rate.[5] There is a clear liability risk from using this technology, as demonstrated by another recently published story from Detroit, again resulting in the wrongful arrest of a black man.[6] As stewards of Portland's tax dollars, the City council should prohibit use of this dangerous technology.

When the technology does yield a supposed match, the results can be terrifying for an individual mistaken for another. In April, Brown University student Amara Majeed was misidentified as one of the Sri Lankan bombers from the Easter terrorist attack.[7] Teenager Ousmane Bah was

---

[3] http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

[4] https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

[5] https://arstechnica.com/tech-policy/2020/06/detroit-police-chief-admits-facial-recognition-is-wrong-96-of-the-time/

[6] https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/

[7] https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html

misidentified by facial recognition technology and accused of robbing an Apple Store in Boston, a city he has never been to.[8]

2. **Mission creep is historical reality.**

No tool with more than one use ever remains confined to a single use for very long. Just ten years ago, license plate readers were introduced to recover stolen vehicles more effectively, to overcome the "hiding in plain sight" phenomenon. Today, they are used for all criminal investigations, at-risk and witness locates, civil investigations such as insurance and worker's comp fraud, and administrative purposes like neighborhood parking passes and payment of parking fees. We believe that facial recognition is even more versatile than a license plate reader because we cannot separate ourselves from our faces, and thus the impact and mission creep will be larger if you crack open the door for limited uses now. In addition, the expensive part of a citywide mass surveillance system is already in place – cameras are everywhere, typically linked together and remotely viewable. All that remains is the flip of a switch to enable facial recognition.

3. **Facial Recognition Technology is anti-democracy and anti-privacy.**

We have a human right to privacy. The United States Supreme Court has consistently ruled for decades that we have the right to be anonymous in public. As a people, we have never consented to law enforcement tracking and tagging us like cattle, without at least a reasonable suspicion of wrongdoing. We have never been forced to, nor agreed to, carry a visible ID around with us as we move about our lives. We have consistently said we do not need to identify ourselves walking around, yet with this technology, it is the equivalent of forcing us to identify ourselves to others simply by participating in modern day life and walking outside our front door. We do not need to speculate about this threat – China is presently using facial recognition against its minority Muslim Uighur population by tracking certain ethnic facial features, today's equivalent of the yellow star for Jews during Hitler's reign.

If Portland allows for the use of facial recognition technology, the inevitable mission creep will cause it to become ubiquitous, and this is our primary concern: this technology is the most radical, and the most intrusive, that we have ever seen in our lifetimes. If used widely, and certainly by those with police power, it will destroy our first amendment protections due to its chilling effect.

No young person exploring their sexuality will be comfortable exploring a gay bar for the first time. Muslims will be nervous attending their mosques. Inter-racial and same sex relationships, cannabis use, aiding run-away slaves (today, refugees), all these actions occurred in the "underground", requiring privacy, before they became accepted as the new normal and decriminalized. In a world of perfect surveillance, these types of social changes will no longer be possible, because the status quo will become cemented.

[8] https://slate.com/technology/2019/04/a-teenager-is-accusing-apple-of-misidentifying-him-with-a-facial-id-system.html

A March 2019 David Binder Research poll conducted for the ACLU revealed that over 82% of likely California statewide voters, and 79% of likely Bay Area voters, **oppose** the government using biometric information to monitor and track who we are, and where we go[9]. It is likely that our neighbors to the north in Portland share similar views.

On June 27, 2019, Axon publicly issued a statement affirming that they will not use facial recognition technology in conjunction with their body cameras, following the advice of its independent ethics board.[10] Axon now joins Google and Microsoft as major players that are saying no to the use of their technology in harmful, biased ways. The California legislature has prohibited the use of this technology in body cameras statewide.

The health of our democracy depends on our ability to occasionally say no – that this technology, more so than others, is too radical for use in our community. We are already losing our ability to move about and associate freely, without this intrusive, error-prone technology. Our locational history is tracked by license plate readers, Stingrays, and cellphone tower dumps. There are already thousands of cameras in place, just waiting for facial recognition to be coupled with them. We do not have to accept as inevitable that technology will creep further into our lives

Prohibiting the Use of Face Recognition Technology in Public Spaces[11]

We applaud Portland's groundbreaking effort to prohibit the use of this technology in places of public accommodation, and to protect our public privacy interests.

We do suggest that the exceptions in this ordinance match the language used in the ordinance above, as to user verification. Although the intent here is likely to allow an individual to unlock their own personal device using facial recognition technology such as Apple's FaceID, the language could be interpreted to allow private entities to force an individual to unlock their phone using this technology.

We suggest the following amendment: "An individual may use face recognition technology to access their own personal or employer issued or assigned personal communication devices or computers for the sole purpose of user verification."

In addition, we suggest that the private right of action discussed above also be included in this ordinance.

[9] https://www.aclunc.org/docs/DBR_Polling_Data_On_Surveillance.pdf

[10] https://www.engadget.com/2019/06/27/axon-facial-recognition-ai-police-body-cameras/

[11] The draft we were provided and reviewed is dated July 1, 2020.

Portland's leadership and acknowledgment of the concerns regarding these complicated matters is appreciated. We trust that you will recognize the moment that we are in and prohibit the use of such dangerous technology.

Sincerely,

Brian Hofer
Executive Director
(510) 303-2871
brian@secure-justice.org
https://secure-justice.org/

IMPACT STATEMENT

Legislation title: *Prohibit the acquisition and use of Face Recognition Technologies by City bureaus (Ordinance).
Contact name: Hector Dominguez
Contact phone: 503-823-2071
Presenter name: Hector Dominguez

Purpose of proposed legislation and background information:

This Ordinance prohibits the use of Face Recognition Technologies by all City of Portland bureaus. It also directs the Bureau of Planning and Sustainability and the Office of Equity and Human Rights to coordinate actions to create awareness among City bureaus about this policy.

The City of Portland recognizes that Face Recognition Technologies are based on the collection of sensitive information from people, and that biases against Black people, women, and older people in these technologies have been demonstrated.

The use of these biased technologies, particularly in law enforcement, may cause irreversible damage due to false identification from a Face Recognition process. The use of biased technologies in Portland prevents all Portlanders from having fair access to City of Portland services.

Financial and budgetary impacts:
There is no immediate financial or budget impact that would result from adopting this ordinance.

The bureau of Planning and Sustainability will likely seek future budget resources needed to implement a process for more privacy and surveillance governance, and awareness and future work related to these topics.

Community impacts and community involvement:

Face Recognition Technologies are not widely used in places of public accommodation in Portland. However, some local businesses may be impacted by the ban.

This ban exempts uses of Face Recognition Technologies by all Private Entities in order to comply with any local, state or federal regulation.

This ordinance included public involvement at different stages of its development, from initial feedback, providing direct feedback to City Council in the form of a work session, and an open workshop for crafting language included in the final document.

By adopting this Ordinance, City Council directs staff at the Bureau of Planning and Sustainability and Office of Equity and Human Rights to make recommendations to assure community involvement in future surveillance and privacy policies.

100% Renewable Goal:
This resolution does not increase or decrease the City's energy or renewable energy use.

Budgetary Impact Worksheet

Does this action change appropriations?

☐ **YES**: Please complete the information below.
☒ **NO**: Skip this section

Fund	Fund Center	Commitment Item	Functional Area	Funded Program	Grant	Sponsored Program	Amount