

ORDINANCE No.

Prohibit the use of Face Recognition Technologies by private entities in places of public accommodation in the City (Ordinance; add Code Title 34)

The City of Portland ordains:

Section 1. The Council finds:

1. Portland residents and visitors should enjoy access to public spaces with a reasonable assumption of anonymity and personal privacy. This is true for particularly those who have been historically over surveilled and experience surveillance technologies differently.
2. The City of Portland must be a welcoming city, a sanctuary city, and an inclusive city for all, including residents and visitors, according to the City Council Resolution 37277.
3. City Code Chapter 23.01 on Civil Rights decrees the elimination of discrimination, that every individual shall have an equal opportunity to participate fully in the life of the City and that discriminatory barriers to equal participation be removed.
4. 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.
5. 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.
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 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. Black, Indigenous and People of Color communities have been subject to over surveillance and disparate and detrimental impact of the misuse of surveillance.
9. Face Recognition Technologies have been documented to have an unacceptable gender and racial bias. The City needs to take precautionary actions until these technologies are certified and safe to use and civil liberties issues are resolved.
10. At the moment, the City does not have the infrastructure to evaluate Face Recognition Technologies. Indiscriminate use of these technologies will degrade civil liberties and enable spaces or services that may be unfair to Black, Indigenous and People of Color. These existing issues would result in barriers to access services or public spaces where Face Recognition Technologies are required.
11. Surveillance Technologies means 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.
12. Surveillance Technologies, including Face Recognition, must be transparent, accountable, and designed in ways that protect personal and collective privacy, particularly information from children and vulnerable and marginalized groups.
13. 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.
14. While uses of Face Recognition Technologies may have benefits, the risk for misidentification and misuse is always present. Safe use of these technologies requires adequate due process, transparency, and oversight measures to be trusted. Implementing this infrastructure needs investment in development of rules and structures that allow appropriate uses of Face Recognition Technologies.

15. Public participation in policy making, particularly frontline perspectives and bringing diverse life perspectives, enhance our City values of equity and anti-discrimination, keeping processes open, inclusive, and engaging.
16. 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 B.

NOW, THEREFORE, the City Council directs:

- a. Code Title 34 Digital Justice is added effective January 1, 2021 as shown in Exhibit A.
- b. From the ordinance effective date until the implementation date of January 1, 2021, the Bureau of Planning and Sustainability, the Office of Equity and Human Rights, and the City Attorney's Office in collaboration with other City bureaus will develop a plan for creating public awareness on impacts and uses of Face Recognition Technologies particularly around children, Black, Indigenous and People of Color, people with disabilities, immigrants and refugees, and other marginalized communities and local businesses.
- c. The Bureau of Planning and Sustainability and the Office of Equity and Human Rights will coordinate communications with other jurisdictions and convene an effort to support and promote digital rights, including privacy and information protection regarding the collection of information by Face Recognition Technologies.
- d. The Bureau of Planning and Sustainability and the Office of Equity and Human Rights will coordinate effective and meaningful public participation after the code provisions are approved. This effort should represent a diverse set of voices, expertise, and life experiences on issues around Face Recognition and other surveillance technologies, including the development of a comprehensive surveillance technologies policy.
- e. The prohibitions stated in Chapter 34.10 shall remain in effect until the City adopts or revises an appropriate model for the regulation of Face Recognition Technologies.

Passed by the Council:
Mayor Ted Wheeler
Commissioner Joann Hardesty

Mary Hull Caballero
Auditor of the City of Portland
By

Deputy

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

704
 Agenda No.
ORDINANCE NO.
 Title

Prohibit the use of Face Recognition Technologies by private entities in places of public accommodation in the City (Ordinance; add Code Title 34)

INTRODUCED BY Commissioner/Auditor: Mayor Wheeler	CLERK USE: DATE FILED <u>9/1/20</u>
COMMISSIONER APPROVAL Mayor—Finance & Administration - Wheeler	Digitally signed by Mustafa Washington Date: 2020.09.01 12:21:36 -07'00' Mary Hull Caballero Auditor of the City of Portland
Position 1/Utilities - Fritz	Digitally signed by Keelan McClymont Date: 2020.09.02 11:26:10 -07'00' By: Keelan McClymont Deputy
Position 2/Works - Vacant	
Position 3/Affairs - Hardesty	
Position 4/Safety - Eudaly	
BUREAU APPROVAL Bureau: Planning and Sustainability Bureau Head: Andrea Durbin	ACTION TAKEN:
Prepared by: Hector Dominguez Aguirre Date Prepared: 7/30/20	Digitally signed by Andrea Durbin Date: 2020.08.20 17:43:05 -07'00'
Impact Statement Completed <input checked="" type="checkbox"/> Amends Budget <input type="checkbox"/>	Digitally signed by Esin Onart Date: 2020.08.19 11:29:36 -07'00'
Portland Policy Document If "Yes" requires City Policy paragraph stated in document. Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
City Auditor Office Approval: DB required for Code Ordinances	
City Attorney Approval: Esin Onart required for contract, code, easement, franchise, comp plan, charter	
Council Meeting Date 9/9/20	

AGENDA
TIME CERTAIN <input checked="" type="checkbox"/> Start time: <u>2:00 PM</u> Total amount of time needed: <u>2 hours</u> (for presentation, testimony and discussion)
CONSENT <input type="checkbox"/>
REGULAR <input type="checkbox"/> 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

TITLE 34 DIGITAL JUSTICE

Chapter 34.10, Prohibit the use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City of Portland

34.10.010 Purpose.

The purpose of this Chapter is to prohibit the use of Face Recognition Technologies in Places of Public Accommodation by Private Entities within the boundaries of the City of Portland.

Face Recognition Technologies have been shown to falsely identify women and People of Color on a routine basis. While progress continues to be made in improving Face Recognition Technologies, wide ranges in accuracy and error rates that differ by race and gender have been found in vendor testing.

Community members have raised concerns on the impacts of Face Recognition Technologies on civil liberties and civil rights. In addition, the collection, trade, and use of face biometric information may compromise the privacy of individuals even in their private setting. While these claims are being assessed, the City is creating safeguards aiming to protect Portlanders' sensitive information until better infrastructure and policies are in place.

Portland's commitment to equity means that we prioritize the safety and well-being of communities of color and other marginalized and vulnerable community members.

34.10.020 Definitions.

As used in Sections 34.10.020 through 34.10.050, the following terms have the following meanings:

- A. "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.
- B. "Face Recognition Technologies" means automated or semi-automated processes using Face Recognition that assist in identifying, verifying, detecting, or characterizing facial features of an individual or capturing information about an individual based on an individual's face.
- C. "Government Agency" means:
 - 1. The United States Government; or
 - 2. The State of Oregon including any office, department, agency, authority, institution, association, society, or other body of the state, including the legislature and the judiciary; or

3. Any political subdivision of the State of Oregon or any county, city, district, authority, public corporation, or public entity other than the City.

D. “Places of Public Accommodation”

1. means: Any place or service offering to the public accommodations, advantages, facilities, or privileges whether in the nature of goods, services, lodgings, amusements, transportation or otherwise.
2. does not include: An institution, bona fide club, private residence, or place of accommodation that is in its nature distinctly private.

E. “Private Entity” means any individual, sole proprietorship, partnership, corporation, limited liability company, association, or any other legal entity, however organized. A Private Entity does not include a Government Agency.

34.10.030 Prohibition.

Except as provided in the Exceptions section below, a Private Entity shall not use Face Recognition Technologies in Places of Public Accommodation within the boundaries of the City of Portland.

34.10.040 Exceptions.

The prohibition in this Chapter does not apply to use of Face Recognition Technologies:

- A. To the extent necessary for a Private Entity to comply with federal, state, or local laws;
- B. For user verification purposes by an individual to access the individual’s own personal or employer issued communication and electronic devices; or
- C. In automatic face detection services in social media applications.

34.10.050 Enforcement and Remedies.

Violations of this Chapter are subject to the following remedies:

- A. Any person injured by a material violation of this Chapter by a Private Entity has a cause of action against the Private Entity in any court of competent jurisdiction for damages sustained as a result of the violation or \$1,000 per day for each day of violation, whichever is greater and such other remedies as may be appropriate.
- B. In an action brought to enforce this Chapter, a court may award to the plaintiff who prevails in such action, at trial and on appeal, a reasonable amount to be fixed by the court as attorney fees if the court finds that written demand for the payment of such claim was made on the defendant, and on the defendant’s insurer, if known to the plaintiff, not less than 30 days before the commencement of the action or the filing of a formal complaint. However, no attorney fees shall be allowed to the plaintiff if the court finds that the defendant tendered to the plaintiff, prior to the commencement of the action or the filing of a formal complaint an amount not less

than the damages awarded to the plaintiff, exclusive of any costs, interest, and prevailing party fees.

Exhibit B

Public feedback received by July 24, 2020 to the policy draft to “prohibit the use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City” made available on July 1st, 2020.

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

submitter	organization	date received	city
Larry Kirsch	Portland	7/6/2020	Portland, OR
Emerald Boege	Port of Portland	7/14/2020	Portland, OR
John Nurse'Mayes	Resident of Cully neighborhood	7/20/2020	Portland, OR
Mariah Linden	Resident of Cully neighborhood	7/20/2020	Portland, OR
Kaitlin Carpenter	Resident of Portland	7/21/2020	Portland, OR
Boaz Ally-Feuer	Resident of Portland	7/21/2020	Portland, OR
Jessica Beckart	Resident of Portland	7/21/2020	Portland, OR
Katherine Noble	Resident of Portland	7/21/2020	Portland, OR
Sean Gamble	Resident of Portland	7/21/2020	Portland, OR
Kelly Orthel	Resident NorthEast Portland	7/22/2020	Portland, OR
Jill W-S	Resident North Portland	7/22/2020	Portland, OR
Emilien Shireen Press	Resident of Cully neighborhood	7/22/2020	Portland, OR
Alison Kavanagh	Resident of John's Landing, Portland	7/23/2020	Portland, OR
Tovah LaDier	IBIA group	7/24/2020	Washington DC
Kelsey Finch	Future of Privacy Forum	7/24/2020	Seattle, WA
Kevin T. Christiansen	Oregon Bankers Association	7/24/2020	Salem, OR
Drake Jamali	Security Industry Association (SIA)	7/24/2020	Silver Spring, MD
Jon Isaacs	Portland Business Alliance	7/24/2020	Portland, OR
Brian Hofer	Secure-Justice	7/26/2020	Oakland, CA

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. Overview

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. Areas of Agreement

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 application. 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

████████████████████

(617) 731 2600

Portland, OR 97209

July 14, 2020

Hector Dominguez
c/o Bureau of Planning and Sustainability
1900 SW 4th Ave, Suite 7100
Portland, OR 9720

Dear Hector,

Thank you for the thoughtful and collaborative approach you and your colleagues have led in crafting the city's bold set of actions on facial recognition technology. Through every step, you have been open to questions and concerns – while keeping the driving values central in each discussion.

As we have discussed, there are principled and good reasons for concern over the private use of facial recognition technology. That said, there is a distinct difference between the general public use of “facial recognition technology” and the limited “facial authentication” processes being implemented at airports. Both technologies rely on biometrics, but they have very different purposes and outcomes.

Unlike use of the technology in other venues (retail stores or street surveillance, for example), passenger processing is different in that it is used for *authentication and verification* – the process of confirming that a traveler is who they say they are.

The process uses a single image captured at the time of travel, which is immediately compared with a previously supplied image in a trusted data source. For example, the facial authentication process for international travelers at Portland International Airport (PDX) works by comparing a picture of the passenger taken at the gate with a picture from a passport or visa within a federal data base, for the sole purpose of confirming identity and allowing the passenger to proceed.

Most travelers can opt out if they so choose (federal law requires it be used for foreign nationals), a right they are explicitly informed of. Should a traveler opt-out, or if the system fails to verify identity - the traveler is screened the traditional way (by handing the gate agent a boarding pass and identification).

To improve security, federal law guides the use of facial authentication technology for the screening of international travelers, and this technology is being deployed at airports across the country – including PDX. Under current protocols, neither an airline or airport operator keeps any data connected with the passenger screening process; in fact, Customs and Border Protection requires that the local data be purged.

Airports are publicly owned, but the functions within are carried out by both public and private partners. Whether it's the port, the FAA, the TSA, or the airlines – all parties coordinate to carry out the safety and security of air travel. The emergence of COVID-19 added a whole new layer to the discussion of safety in air travel. In order to be and feel safe traveling, travelers need to move through airport systems quickly, pass fewer items back and forth and have as little physical contact as possible with other people. As we

contemplate how to safely accommodate return to travel, facial authentication systems are an important tool to keep in protecting the health of travelers and workers alike.

For these reasons, we are requesting a minor modification to your proposed code language. The exemption for verification should be modified to read: “For verification purposes to access personal communication and electronic devices, or for air carrier passenger processing;”. This is a narrow exemption that would not apply to other functions within the airport. Thank you again for helping us think through this exemption. It feels like the right solution in that it accommodates essential functions while not undermining the very solid rationale behind the city’s policy.

Sincerely,

Emerald Bogue
Director, Regional Government and Community Affairs

CC: Derek Bradley, Office of Commissioner Hardesty
Christine Kendrick, Bureau of Planning and Sustainability
Kevin Martin, Bureau of Planning and Sustainability
Judith Mowry, Office of Equity and Human Rights
Esin Orart, Office of the City Attorney
Khanh Tran, Office of Mayor Wheeler
Ian Whitlock, Port of Portland

Dominguez Aguirre, Hector

From: Leah and John Mayes'Nurse [REDACTED] >
Sent: Monday, July 20, 2020 10:56 PM
To: Dominguez Aguirre, Hector
Subject: Facial recognition

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

Hello,

As a Portland resident, I was very excited to learn of the upcoming legislation to ban facial recognition from our city. I have just heard that the legislation might be weakened to provide an exception for airlines to collude with Customs and Border Protection.

I am writing you to ask that you please do not weaken the legislation. We do not need loopholes. We need a strong, firm ban on the use of facial recognition. We need our city to defend ALL its citizens from CBP's overreach.

Please do not create an exception for airlines in the bills to ban facial recognition.

Thank you,
John Nurse'Mayes
A resident of the Cully neighborhood

Dominguez Aguirre, Hector

From: Mariah76 [REDACTED]
Sent: Monday, July 20, 2020 10:23 PM
To: Dominguez Aguirre, Hector
Cc: Commissioner Hardesty
Subject: No facial recognition at all. This Portland not China

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

As a Portland resident, I was very excited to learn of the upcoming legislation to ban facial recognition from our city. I have just heard that the legislation might be weakened to provide an exception for airlines to collude with Customs and Border Protection.

I am writing you to ask that you please do not weaken the legislation. We do not need loopholes. We need a strong, firm ban on the use of facial recognition. We need our city to defend ALL its citizens from CBP's overreach.

Please do not create an exception for airlines in the bills to ban facial recognition.

Thank you,
Mariah Linden
A resident of (cully)

Dominguez Aguirre, Hector

From: Kaitlin Carpenter [REDACTED]
Sent: Tuesday, July 21, 2020 8:59 PM
To: Dominguez Aguirre, Hector
Subject: Request to not weaken facial recognition ban

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

As a Portland resident of the Hawthorne neighborhood, I was interested in the upcoming legislation to ban facial recognition from our city. I've also learned that the legislation might be weakened to provide an exception for airlines and Customs and Border Protection.

I am writing you to add my voice to the requests not to weaken the legislation. We need a strong, firm ban on the use of facial recognition. We need our city to defend ALL its citizens from CBP's overreach.

Please do not create an exception for airlines in the bills to ban facial recognition.

*Thank you,
Kaitlin Carpenter*

Dominguez Aguirre, Hector

From: Jessica Beckhart [REDACTED]
Sent: Tuesday, July 21, 2020 2:37 PM
To: Dominguez Aguirre, Hector; Commissioner Hardesty
Subject: Ban Facial Recognition

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

Hello,

As a Portland resident, I was very excited to learn of the upcoming legislation to ban facial recognition from our city. I have just heard that the legislation might be weakened to provide an exception for airlines to collude with Customs and Border Protection.

I am writing you to ask that you please do not weaken the legislation. We do not need loopholes. We need a strong, firm ban on the use of facial recognition. We need our city to defend ALL its citizens from CBP's overreach. Let's continue to use Portland as an example of resistance and set a gold standard to defend us from the surveillance state

Please do not create an exception for airlines in the bills to ban facial recognition.

Thank you,

Jessica Beckhart

A concerned resident in Portland

Jessica Beckhart
c: [217-369-1206](tel:217-369-1206)
[REDACTED]

Dominguez Aguirre, Hector

From: Katherine Noble [REDACTED]
Sent: Tuesday, July 21, 2020 11:32 AM
To: Dominguez Aguirre, Hector; Commissioner Hardesty
Subject: Don't Weaken the Facial Recognition Ban!

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

To Whom it May Concern,

I am a Portland resident and writing to you out of concern for the possible exception for airlines that may be included in the upcoming facial recognition legislative ban. By allowing an exception for airlines, this will allow collusion with Customs and Border Protections and drastically weaken this legislation.

This loophole would significantly increase risk to a large portion of our population and we need our city to defend EVERYONE against Custom and Boarder Protections overreach.

Please do not allow this exception for airlines to be included in the ban against facial recognition.

Thank you,

Katherine Noble
Portland City Resident, 97214

Dominguez Aguirre, Hector

From: Sean Gamble [REDACTED]
Sent: Tuesday, July 21, 2020 11:26 AM
To: Dominguez Aguirre, Hector
Subject: Facial Recognition technology legislation

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

Greetings Mr. Dominguez;

It is my understanding that some legislation is being considered that will ban facial recognition software from being used in Portland. This is very important to me, and I am thrilled to hear that it may become law.

I am a bit concerned, however, that the proposed legislation may be altered to include an exception for its use to be allowed at the airport, which is very problematic both ethically and in terms of potential 4th amendment rights violations.

Considering the current climate of resistance to increased surveillance on the citizenry, I would ask that you please leave the legislation ironclad, and do not allow any company or agency to use facial recognition software anywhere, for any reason, within your area of influence.

Thank you so much,

Sean Gamble

Dominguez Aguirre, Hector

From: Kelly Orthel [REDACTED]
Sent: Wednesday, July 22, 2020 4:07 PM
To: Dominguez Aguirre, Hector; Commissioner Hardesty
Subject: Facial recognition legislation

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

Hello,

I just learned that there is legislation in the works that will ban facial recognition technology. This is something that I fully support. Facial recognition is a powerful technology with far reaching privacy risks. I have also been informed that there is the potential that the legislature will be weakened by adding an exception to allow airlines and Border Patrol to still use it. As a resident of Portland, I ask you to please not weaken the legislature.

We need our city to defend ALL its citizens from CBP's overreach.

Please do not create an exception for airlines in the bills to ban facial recognition.

Thank you

Kelly Orthel
A resident of North East Portland.

Dominguez Aguirre, Hector

From: Jill W-S [REDACTED]
Sent: Wednesday, July 22, 2020 3:14 PM
To: Dominguez Aguirre, Hector
Subject: No Exception for airlines to ban facial recognition

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

Hello,

As a Portland resident, I was very excited to learn of the upcoming legislation to ban facial recognition from our city. I have just heard that the legislation might be weakened to provide an exception for airlines to collude with Customs and Border Protection.

I am writing you to ask that you please do not weaken the legislation. We do not need loopholes. We need a strong, firm ban on the use of facial recognition. We need our city to defend ALL its citizens from CBP's overreach.

Please do not create an exception for airlines, or for any entity, in the bills to ban facial recognition.

Thank you,

Jill

A resident of North Portland

Dominguez Aguirre, Hector

From: [REDACTED]
Sent: Wednesday, July 22, 2020 11:01 AM
To: Dominguez Aguirre, Hector; Commissioner Hardesty
Subject: Facial Recognition

Follow Up Flag: Follow up
Flag Status: Flagged

Hello,

As a Portland resident, I was relieved to learn of the upcoming legislation to ban facial recognition from our city. I have just heard that the legislation might be weakened to provide an exception for airlines to collude with Customs and Border Protection.

I am writing you to ask that you please do not weaken the legislation. We do not need loopholes. We need a strong, firm ban on the use of facial recognition. We need our city to defend ALL its citizens from CBP's overreach.

Please do not create an exception for airlines in the bills to ban facial recognition.

Thank you,

Emilie Shireen Press
A resident of Cully

Dominguez Aguirre, Hector

From: Alison Kavanagh [REDACTED]
Sent: Thursday, July 23, 2020 11:27 PM
To: Dominguez Aguirre, Hector; Commissioner Hardesty
Subject: Facial recognition ban

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Policy

Hello,

As a Portland resident, I was very excited to learn of the upcoming legislation to ban facial recognition from our city. I have just heard that the legislation might be weakened to provide an exception for airlines to collude with Customs and Border Protection.

I am writing you to ask that you please do not weaken the legislation. We do not need loopholes. We need a strong, firm ban on the use of facial recognition. We need our city to defend ALL its citizens from CBP's overreach.

Please do not create an exception for airlines in the bills to ban facial recognition.

Thank you,

Alison Kavanagh, J.D.
a resident of John's Landing, Portland
[REDACTED]



International
Biometrics+Identity
Association

**IBIA Comments on
City of Portland Draft Bills
Prohibiting Public and
Private Use of Facial Recognition
Technology**



The International Biometrics + Identity Association (IBIA) is the leading voice for the biometrics and identity technology industry. It advances the transparent and secure use of these technologies to confirm human identity in our physical and digital worlds. #identitymatters

Overview

The International Biometrics + Identity Association (IBIA) is the leading voice for the biometrics and identity technology industry. It promotes the transparent and lawful use of technologies to confirm and secure human identity in our physical and digital worlds. Our [membership](#) includes researchers, developers, providers, and users of biometric technologies around the world.

IBIA appreciates the opportunity to present these comments on the pending facial recognition legislation in Portland. IBIA supports the Committee's goals of transparency, accountability and standards for the use of all biometrics, including facial recognition.

IBIA believes that a ban on the use of facial recognition is not in the best interests of any jurisdiction, and will have adverse consequences for the public, business, and all levels of government. IBIA respectfully urges that the draft ordinances be rejected as drafted.

IBIA believes there are other options, short of a facial recognition ban, to develop principles for the transparent, secure, and trustworthy use of facial recognition, including addressing specific problems that may exist

IBIA Comments

Underlying rationale for the ordinances is unsupportable

The definitions and the enumerated Findings, which outline the rationale for the draft ordinance, are based on erroneous facts, bad science, and do not include information critical to understanding facial recognition, the current state of the technology and its risks and benefits:

- Latest NIST test results on performance among demographic groups that show that top performing algorithms have undetectable differences among demographic groups,¹ the algorithms that should be used by government and business.
- Benefits of facial recognition.
- Serious risks of an open-ended moratorium on facial recognition to public safety and national security.
- The definition of facial recognition not supported by science and experts.

NIST test results on facial recognition algorithm performance across demographic groups show that top performing algorithms have undetectable false positive accuracy differences in performance among demographic groups²

The National Institute of Science and Technology (NIST) is the global gold standard for facial recognition performance testing, as well as all other biometrics. For reasons that are not clear, Portland City Council appears to have ignored key NIST testing results in drafting its ordinances and the ordinance does not reveal the testing sources supporting its statements that facial recognition is routinely 'biased'.

- Key Findings of NIST Testing on algorithm performance across demographic differences:
 - NIST tested 189 algorithms from laboratories and vendors around the world (a large number because the NIST testing is open to anyone who wants to submit algorithms for testing).³

1 Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. NISTIR 8280, (pp. 1–79). doi: 10.6028/nist.ir.8280 Re

2 Op. cit.

3 Op. cit. (p. 1)

- The test results, as expected, show wide variations in algorithm performance with respect to demographic differentials. NIST explicitly states that it is not accurate to draw generalizations about algorithm performance.⁴ Some perform very well; others do not.
- The low performing algorithms show significant performance differences among demographic groups.
- The most accurate high-performing identification algorithms (a one-to-many search in which an image is used to search a database of images to find potential matches) display ‘undetectable’ differences among demographic groups;⁵ more than 30 of the 189 identification algorithms NIST tested have false non-match rates (misses) less than three per thousand,⁶ providing far greater accuracy than humans could ever achieve.
- The most accurate high-performing verification algorithms (a one-one verification search where 2 images are compared to each other to determine similarities of the faces) display both low false positives and false negatives. More than 50 tested algorithms have false non-match rates (misses) less than three per thousand,⁷ and false match rates (erroneous matches) less than one per hundred thousand,⁸ again, greater accuracy than humans could ever achieve.
- Performance variations does not mean ‘bias’ has been introduced into facial recognition algorithms
 - NIST uses the term ‘demographic differences’ (not ‘bias’) to describe performance variations, which conveys that variation is technical and scientific.
 - Differences in algorithm performance most likely result from natural variations among people in facial bone structures, skin tones, and image capture. The NIST testing shows researchers have made significant progress reducing performance variation across the board, and ongoing efforts will continue this trend. There is little reason to believe that computer vision technology is yet approaching performance boundary conditions.
 - This is precisely what happened with fingerprint matching of Asian women.
 1. With smaller surface area, thinner skin, and more closely spaced and thinner ridge structure in their fingerprints, it was difficult to capture and match those fingerprints, a fact about which the researchers were unaware, a short-coming in human knowledge.
 2. When these natural variations became known, researchers fine-tuned the algorithms to address and resolve the issue, confirming the value of continuing research to improve algorithms and for ongoing NIST testing to spur further improvement in algorithms and to identify flaws.
 - That developer ‘bias’ connotes unfounded prejudice is highly unlikely.
 1. Machines do not have emotions and do what they are programmed to do.
 2. Commercial entities in this space, especially the more successful ones, are international entities offering their products all over the world.
 3. To be successful those products need to work well with every demographic.
 4. Many leading algorithm developers in both academia and industry are themselves minorities, as is the case also in management.

4 Op. cit.

5 Op. cit. (pp. 3, 8)

6 Op. cit. (pp. 64, 65)

7 Op. cit. (pp. 54, 58)

8 Op. cit. (pp. 56, 57)

Automated facial recognition is more accurate and less biased than human recognition, the pertinent issue in the real world

- Measured accuracy of human visual passport inspection is notoriously low, determined by some to be in the 80% range or less (for example, Passport Officers' Errors in Face Matching).⁹
- The top performing algorithms outperform mean performance of all human groups including skilled forensic face examiners.
- Algorithm performance for the high performers, across the board, is more than 20 times better than skilled professional examiners.
- NIST's January 2020 FRVT Verification Report lists five algorithms, under suitable conditions with good lighting and photos have an accuracy rate of 99.9% or better. Otherwise, the accuracy, for high performing algorithms is in the 98-99% range, and algorithm performance continues to rapidly improve.¹⁰

Automated facial recognition can do things that humans cannot do

- Machines can memorize millions of faces, humans only thousands; this enables machines to do things unaided that humans cannot, including:
 - Identifying missing children who do not know their names
 - Identify exploited children in dark web pornography
 - Identifying disoriented (amnesia, Alzheimer's, etc.) adult
 - Flagging likely driver license application fraud for human review

Facial recognition is also critical in real time in cases of mass shootings, bombings, and other disasters. The technology has improved by orders of magnitude and facial recognition now is a crucial element in counterterrorism and law enforcement around the country and the world. Instead of banning or seriously restricting law enforcement and other public-sector uses of facial recognition, legislative efforts should aim to ensure that existing Constitutional and civil liberties protections apply to public-sector uses of facial recognition.

Any facial recognition technology ban poses substantial risks to law enforcement and public safety where facial recognition technology has proven essential

- For many critical public safety activities, it is not acceptable to limit performance to human capability, or alternatively to delay the use of and the implementation of upgrades and improvements for an undefined period of time.
- A ban on facial recognition will preclude its use in forensic analysis, severely limiting the capability of law enforcement officials to solve crimes.
- A ban also assumes that the current system of human recognition is accurate and unbiased. In fact, as previously pointed out, human recognition alone is far less accurate than when augmented by automated facial recognition, and eyewitness testimony is notoriously biased.
- Banning facial recognition will only result in foregoing improvements in our flawed existing law enforcement system and, in some cases, it may be tantamount to deciding not to investigate crime.

9 White D, Kemp RI, Jenkins R, Matheson M, Burton AM (2014) Passport Officers' Errors in Face Matching. PLoS ONE 9(8): e103510. <https://doi.org/10.1371/journal.pone.0103510>

10 "Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification," Grother P, Ngan M., and Hanoka K., 2020/01/22, Pp 26-29

The draft ordinances' definitions of facial recognition technology and other terms do not reflect an accurate understanding of the technology

Facial recognition and surveillance are two different processes

The public-sector ordinance defines a 'surveillance technology' to include 'facial recognition technology', conflating two entirely different processes. Facial recognition and surveillance are not the same. Conflating them is a misconception based on hypothetical statements, not facts.

- Facial recognition is only about the identification of a human face and the ability to match it to a single known person. Facial matching is only useful to match against a known gallery of quality facial images to those submitted to it for matching. There is no database of all faces in the U.S. so an unknown individual will still remain anonymous after a non-match.
- Facial recognition is usually understood to be 1:1 verification and 1:N identification, which are significantly different applications with very different privacy concerns. Facial recognition is normally a **passive** activity, where action is taken on-demand (1:1) for various types of access, or post-event (1:N) for investigation.
- Video surveillance cameras are in wide use today and capture entire scenes for later playback, if needed.
- Surveillance is the **active** watching of people, places, and things. It can be done with recorded video and human review, or more recently technology has evolved so that video analytics can look for specific listed persons in recorded material or even real-time. Some people have raised the strawman of massively surveilling the U.S. population. As far as we know, there are no existing surveillance systems based on facial recognition in the U.S. or anyone thinking of implementing such a system. The cost of extending facial recognition to general surveillance would require a substantial appropriation action. No agency has sufficient discretionary funds to initiate such a huge effort, which means that Congressional authorization and appropriations, as well as OMB approval, would be required to set up a facial recognition surveillance system.

IBIA agrees that surveillance is an important issue to address and IBIA supports principles with respect to ensuring appropriate use of surveillance technologies. However, the proper way to do so is to address the issue of surveillance separately, not by conflating it with all facial recognition and banning facial recognition.

Conflating facial recognition with surveillance or suggesting that facial recognition surveillance systems are in use, or planned, only serves to confuse a complicated issue and might have the unintended consequence of discrediting the use of facial recognition technology that provides substantial benefits to public safety and security.

Facial recognition technology does not provide information about an individual's characteristics

Facial recognition algorithms as a source of information about an individual's characteristics is not science. One cannot infer emotion, patriotism, criminal inclinations, sexual orientation, or other characteristics from a mathematical template of the face. This is **NOT** facial recognition.

Conflating this with facial recognition only confuses the issues and will certainly preclude an informed discussion on the public safety and security benefits of facial recognition technology.

Conclusion

IBIA appreciates the opportunity to comment on the Portland ordinances. In summary, the rationale for the Portland ordinances is not supported by facts or science. The ordinances should not be enacted as they are drafted.

NIST facial recognition testing completely debunks the basic argument that facial recognition technology has been documented to have an unacceptable gender and racial bias and routinely falsely identify women and people of color on a routine basis.

On the contrary, the NIST test results on performance among demographic groups shows that top performing algorithms have undetectable differences among demographic groups.¹¹ These high-performing algorithms should be available to governments and businesses that can use them in a wide variety of beneficial ways.

¹¹ Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. NISTIR 8280, (pp. 1–79). doi: 10.6028/nist.ir.8280 Re

#identitymatters



International
Biometrics+Identity
Association

1325 G Street, NW, Suite 500
Washington, DC 20005

202.888.0456 | IBIA.ORG

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 24, 2020

Sent Via Electronic Delivery: Hector.DominguezAguirre@portlandoregon.gov

City of Portland
Attn: Hector Dominguez
1900 SW 4th Avenue
Portland, Oregon 97201

Re: Proposed City of Portland Facial Recognition Ban

Dear Mr. Dominguez:

On behalf of the Oregon Bankers Association (“OBA”) and our membership of state and nationally-chartered, FDIC-insured banks, we appreciate the opportunity to comment on the proposed City of Portland (“City”) ban on the use of facial recognition technology (“FRT”). OBA is a full-service trade association for the banking industry throughout the State of Oregon. Our organization represents banks of all sizes and is the voice of Oregon banking before federal, state, and local government entities.

Comments

We commend the City for reaching out to stakeholders to gather feedback with respect to the proposed ban. FRT is a valuable tool that our banks utilize to provide security to their customers and employees. It also allows for faster and more efficient customer service that our customers want.

We are very concerned about the proposed ban on FRT. Like the City, our banks share and understand the concerns raised with FRT, including the need for transparency, avoiding misidentification, and protecting privacy. These concerns, however, must be balanced against the benefits provided by FRT. As currently drafted, the FRT ban is very broad in its scope and will likely include technologies that have an important role to play in keeping our banks and their customers and employees safe. This ban could stifle future innovation. In light of these considerations, we strongly encourage you to weigh the following in moving forward:

1. A Bank Exemption

Security, is of paramount importance to all of our banks. Unlike other private entities, banks must safeguard the public’s financial resources and sensitive customer data. Banks must also protect the physical safety of their customers and employees. Robbery, theft, fraud, and other crimes are, unfortunately, issues that banks must contend with and take steps to avoid. When crimes are committed, banks must take action. To those ends, the FDIC promulgated 12 CFR Section 326.3 which provides:

§ 326.3 Security program.

(a) *Contents of security program.* The security program shall:

- (1) Establish procedures for opening and closing for business and for the safekeeping of all currency, negotiable securities, and similar valuables at all times;
- (2) Establish procedures that will assist in identifying persons committing crimes against the institution and that will preserve evidence that may aid in their identification and prosecution; such procedures may include, but are not limited to:
 - (i) Retaining a record of any robbery, burglary, or larceny committed against the institution;
 - (ii) Maintaining a camera that records activity in the banking office; and
 - (iii) Using identification devices, such as prerecorded serial-numbered bills, or chemical and electronic devices;
- (3) Provide for initial and periodic training of officers and employees in their responsibilities under the security program and in proper employee conduct during and after a robbery, burglar or larceny; and
- (4) Provide for selecting, testing, operating and maintaining appropriate security devices, as specified in paragraph (b) of this section.

(b) *Security devices.* Each institution shall have, at a minimum, the following security devices:

- (1) A means of protecting cash or other liquid assets, such as a vault, safe, or other secure space;
- (2) A lighting system for illuminating, during the hours of darkness, the area around the vault, if the vault is visible from outside the banking office;
- (3) An alarm system or other appropriate device for promptly notifying the nearest responsible law enforcement officers of an attempted or perpetrated robbery or burglary;
- (4) Tamper-resistant locks on exterior doors and exterior windows that may be opened; and
- (5) Such other devices as the security officer determines to be appropriate, taking into consideration:
 - (i) The incidence of crimes against financial institutions in the area;
 - (ii) The amount of currency or other valuables exposed to robbery, burglary, and larceny;
 - (iii) The distance of the banking office from the nearest responsible law enforcement officers;
 - (iv) The cost of the security devices;
 - (v) Other security measures in effect at the banking office; and
 - (vi) The physical characteristics of the structure of the banking office and its surroundings.

(emphasis added). Banks are regularly examined and are required to comply with these standards. Given the paramount importance of security, we would ask that the City create a specific bank exception to the FRT ban.

If the City is unwilling to grant a bank exception, we request that the City narrow the broad language of the FRT ban to ensure banks are able to operate safely. It is difficult to present an exhaustive list of the security utilized by banks that may, inadvertently, be captured by the ban. We have reached out to our members to

try to identify the kinds of items that need to be excluded from the FRT ban. The following is a non-exhaustive list of those items:

- As required by FDIC regulation (see above), banks utilize cameras and surveillance equipment in their lobbies and ATM's. In high value areas of the bank largely not subject to public access (e.g., data storage areas, vaults) other cameras or biometric-related devices (e.g., fingerprint readers, retinal scanners) may be used.
- This first group of cameras and surveillance equipment is often related to FRT. Banks using this FRT enroll their employees for access control to certain areas of the bank and customers for ATM and account identification. An employee using FRT equipped access control entry points, or customers using ATM's or accessing an account, would have an image obtained via the surveillance system compared to the image captured during the employee or customers enrollment process. The image is stored on an internal bank database that is not part of a broader system (e.g. Amazon, social media). This enables the bank to use photos or videos of the employees and customers to confirm they are who they say they are. This comparison, especially at an ATM, is often done manually by bank staff. This system is for internal security and customer service.
- The second group of cameras and biometric-related devices, although not yet employed by many banks in Portland, electronically compare images or biometric data to an existing internal database. These areas are generally not accessible to the public, although issues may arise with safe-deposit boxes (which are not directly accessible without assistance from a bank employee). These devices are employed for security purposes.
- To meet customer demand, some banks are beginning to explore the use of FRT to identify a customer trying to access on-line banking through a mobile application. Others are exploring a "selfie-scan" for purposes of online new account origination and to help prevent identification theft. Concern was raised that these items may be deemed FRT and subject to the City ban.

Our banks request that in the absence of a full bank exception that the City allow exceptions from the ban for the above kinds of security and customer service measures. Protecting our customers, their hard-earned money and property, and our employees is a top concern and we encourage the City not to create unnecessary burdens for our banks to do so.

2. Public Accommodation

The ordinance is unclear as to what is meant by "public accommodation". It appears that the definition of "places of public accommodation" was taken from ORS 659A.400 which concerns unlawful discrimination in places of public accommodation. Although it is not clear, it appears that the City is attempting to limit the FRT ban to only those areas of a Private Entity's premises that are not accessible to the public. If that is the case, we would encourage the City to clarify its language so that it is understood the ban does not apply to a Public Entity's premises where the public is not generally allowed to go (e.g., back offices, storage facilities, vaults), or at least not without explicit permission from the Private Entity.

3. Enforcement and Remedies

The language in the Enforcement and Remedies section of the ordinance is extremely vague. It is unclear what is meant by being "aggrieved by a Private Entity's noncompliance". What does "aggrieved" mean? Must a person show actual damages to be "aggrieved"? This needs further clarification.

The ordinance also calls for damages and “such other remedies as may be appropriate” for violation of the ordinance. What is meant by “other remedies”? The plain language of the ordinance appears to require actual damages, but it is unclear what other remedies a plaintiff may be able to recover.

We would encourage the City to remove the private right of action for purported violations of the ordinance and allow enforcement of alleged violations by the City itself or other public body.

Finally, it is unclear what the statute of limitations would be with respect to claims brought under this ordinance. A specific statute of limitation should be identified in the ordinance or, if there is another law or ordinance providing an applicable statute of limitation, a citation or reference to that law or ordinance.

4. Ban Versus Moratorium

Rather than a permanent ban on FRT, we would encourage to the City to consider a moratorium, subject to periodic review, to examine and study the state of FRT. As FRT continues to evolve and improve, it will present opportunities to improve safety as well as customer service for not only banks, but also other public entities.

Conclusion

We appreciate the opportunity to comment on the above-referenced FRT proposal. We would strongly encourage the City to narrow and refine its ban to accommodate the important security and customer service concerns set forth above. The OBA is ready to assist with this issue. If you have any questions, please feel free to contact me at (503) 576-4123 or kchristiansen@oregonbankers.com.

Very best regards,



Kevin T. Christiansen
Vice President and Government Affairs Director
Oregon Bankers Association & Community Banks of Oregon



July 24, 2020

The Honorable Mayor Tom Wheeler
City of Portland
1221 SW 4th Ave
Room 340
Portland, OR97204

Dear Mayor Wheeler, and Members of the City Council:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with the proposed ordinances banning the use facial recognition technology by both private entities, including individuals, and government entities within the City of Portland.

SIA is a nonprofit trade association representing businesses providing a broad range of security products and services in the U.S, including throughout Oregon. SIA represents many of the leading developers of facial recognition technology as well as companies offering products that incorporate this technology for a wide variety of security and public safety applications.

Facial recognition technology offers tremendous benefits when used effectively and responsibly. Like many other technologies, facial recognition could be misused, and we would strongly support policies ensuring that facial recognition is only used for appropriate purposes and in acceptable ways. Instead of banning the technology and depriving the public of the benefits that facial recognition technology can produce now and in the future, we urge you to consider working with local stakeholders to enact tailored use restrictions and procurement policies that address application-specific concerns without unduly impeding widely accepted uses.

Here are just some of the benefits that would be eliminated under the private-sector ban. As a means of digital identification, facial recognition can be a vital enabler for commerce by improving security, protecting identity, safeguarding our personal devices, and ensuring more seamless travel and customer experiences. In the security field, facial recognition solutions help businesses keep their facilities, employees, and patrons safe. More accurate security solutions can reduce unnecessary interactions with law enforcement by limiting the role that human bias plays in detecting allegedly suspicious activity. Furthermore, touchless access control solutions are more important than ever as we work to protect essential workers during the COVID-19 pandemic. In health care facilities, facial recognition technology can reduce contact during patient check-in and provide touchless access control that helps ensure that only trained and authorized personnel can enter sensitive areas like "clean rooms" in order to decrease the risk of contamination. Facial recognition and other biometric technologies can also provide a way to identify unconscious patients in need of emergency assistance.

In the public sector, the technology has been used for over a decade to detect identity fraud against government programs that fuels criminal activity. It also been used to help find and rescue human trafficking victims, thwart potential terrorist attacks, solve hate crimes against the LGBTQ community and crack cold cases. We have highlighted a number of success stories we urge you to consider.¹

¹<https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/>

We understand that there are legitimate concerns that in some applications, use of facial recognition technology might negatively impact women and minorities, and these concerns are reflected in the draft ordinances. Using accurate technology matters, and public policy should seek to ensure use of the facial recognition technology that is most accurate overall and across demographic groups. However, especially considering that high-quality facial recognition technology can identify individuals more accurately than most people can, banning all facial recognition technology would eliminate an important tool for checking and mitigating human bias.

Industry is striving to provide technology that is as effective and accurate as possible across all types of uses, deployment settings and demographic characteristics. In safety and security applications, biometric technologies like facial recognition ultimately increase their effectiveness and help protect people from harm. Any significant bias in technology performance makes it harder to achieve this goal. The National Institute of Standards and Technology (NIST), the world's leading authority on this technology, found last year that the highest performing technologies had "undetectable" differences across demographic groups - accuracy rates well above 99% and undetectable false positive differences across demographics, even when tested against galleries of up to 12 million images. While some commentary on this report focused on the very lowest-performing algorithms, most performed far more consistently than had been widely reported in the media and a few non-scientific tests.²

Additionally, the extension to private entities and individuals of the private right of action in the ordinance could have catastrophic consequences for small local businesses subjected to frivolous lawsuits that are already struggling during a global pandemic and economic downturn. This approach to regulating private sector use of biometric information has had wide-ranging negative consequences where it has been implemented, for example, the Biometric Information Privacy Act (BIPA)-in Illinois. We urge the City Council not to advance the ordinance in its current form. Instead, we ask that the issue of addressing private sector use of biometric data be thoroughly and thoughtfully studied before any rules or regulations restricting its use are passed.

On behalf of SIA and its members, we share your goal of ensuring the responsible use of advanced technology. We urge the City Council to make significant changes to these proposals that address these significant issues and stand ready to provide any additional information or expertise that you may need.

Sincerely,



Don Erickson
Chief Executive Officer
Security Industry Association

Staff contact: Drake Jamali, djamali@securirtyindustry.org

CC: Members of the Portland City Council, Tom Wheeler, Mayor, City of Portland

² <https://www.securityindustry.org/report/what-nist-data-shows-about-facial-recognition-and-demographics/>



July 24, 2020

Smart City PDX
Bureau of Planning & Sustainability
City of Portland
1900 Southwest 4th Avenue, Suite 7100
Portland, OR, 97201

RE: Draft Ordinances regulating the use of facial recognition technology

The Portland Business Alliance (the Alliance) is greater Portland's Chamber of Commerce and represents the largest, most diverse network of businesses in the region. The Alliance advocates for business at all levels of government to support commerce, community health and the region's overall prosperity. We represent nearly 1,900 members, from 27 counties, 13 states and virtually every industry sector. More than 80% of our members are small businesses.

The Technology Association of Oregon (TAO) is a nonprofit member-based organization whose mission is to support entrepreneurs, connect tech professionals to one another and to resources, and develop programs and policies to establish Oregon as a global hub for inclusive innovation.

On behalf of our members, we thank you for the opportunity to submit this joint comment on the draft ordinances regulating the use of facial recognition technology.

First, we would like to reiterate the principles we submitted to the City Council at the work session on January 28, 2020:

- 1. Technology is not inherently good or bad. It has specific potential uses, which can be problematic, and may need to be regulated.** The Alliance encourages you to design any proposal to focus on the inappropriate uses of a technology, and not an outright ban. Focusing on regulating technology uses we all agree are not acceptable still allows the city and the community to realize the benefits of certain technologies. Banning specific technologies can be a fast and slippery slope leading to more bans on technologies that government officials do not yet fully understand. This approach can be minimally effective since technological innovation and development moves faster than public policy.
- 2. Consider the impact on our rapidly expanding local technology industry.** Portland has a strategic advantage in technology and innovation. After years of struggling to retain these companies locally, high growth companies are finally able to raise significant investment dollars without succumbing to pressure to leave Portland. A ban on any technology will be viewed as an anti-tech industry action and will have a negative impact on the perception of Portland as a growing hub for technology and innovation.
- 3. Technology that is used to discriminate or is not capable of avoiding bias based on any human characteristic is not acceptable.** The Alliance would support a proposal that focuses on preventing this use.
- 4. Data should not be collected and used for commercial purposes without consent.** We agree that Portland residents should not have to worry that their biometric data being unknowingly collected for commercial use in

the public right of way. We would support a proposal that prevents the use of biometric technology for these purposes.

5. **Any use of facial recognition technology should be regulated, not banned, in private places of business.** Our members strongly believe their customers, as well as the general public, expect and support the use of the most modern technology to ensure safety and the best experience while in a private business. However, in addition to preventing certain uses, they agree the use of surveillance or biometric technology should be transparent, and the data collected should be kept private. We would support a proposal that requires the disclosure of the use of surveillance technology, and how data is being stored and used. Our members are not supportive of any proposed regulation of the use of this technology by private residents.

Comments specific to draft ordinances released on July 7, 2020:

I. The draft ordinances are harmfully too broad. We can address the public's concerns about facial recognition technologies' impact on privacy, security, and racial justice without depriving the public of the benefits that facial recognition can bring.

1. We continue to have concerns that the city is seeking to permanently prohibit a technology rather than focus on the prohibition of the specific uses that we agree are not appropriate. Additionally, an update in April informed us that the ordinances would be structured to function as a moratorium until the City of Portland develops public-sector and private-sector privacy/data management principles that apply to technology use broadly, including facial recognition. The public sector ordinance appears to take this approach, while the private sector ordinance acts as a permanent ban.

Given that facial recognition surveillance technologies are the technologies about which the public seems most concerned, the private-sector and public-sector draft ordinances should impose a moratorium only on facial recognition surveillance technologies. This targeted approach would prevent the government or private entities from using facial recognition to track individuals' movements, while allowing consumers to benefit from convenient customer experiences, childcare facilities to identify known sex offenders, and law enforcement officers to identify child trafficking victims and perpetrators on the dark web,

A targeted moratorium could alleviate public concerns about using the technology without a governance framework and would give the City of Portland time to work with individual community members, privacy groups, racial justice advocates, academic researchers, and industry experts to develop privacy/data management principles that support case-specific uses, and risk-based facial recognition governance framework.

2. As we have agreed, certain valid concerns exist about how to populate a gallery with facial templates in a manner that promotes social justice, privacy, and data security. An ordinance can be drafted to restrict gallery creation and management without banning the sale or use of the technology itself. Banning facial recognition technologies is a disproportionate response to gallery creation and management concerns, and bans fail to address the root issues related to making databases of sensitive personal information private, secure, and unbiased.
3. We have also acknowledged that valid concerns exist about the accuracy of the technology, particularly across demographic groups. In December 2019, the National Institute of Standards and Technology (NIST) released its highly anticipated [FRVT Part 3: Demographic Effects \(NISTIR: 8280\)](https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf)¹ report, which provided insight into how different vendors' facial recognition algorithms performed across demographic groups. The NIST testing results varied greatly among the 189 algorithms that 99 vendors submitted for testing. Some low-quality algorithms had large false positive accuracy differentials, but the most

¹ <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>

accurate algorithms had false positive accuracy differentials across demographic groups based on race and sex that were so small as to be “undetectable.”

Instead of banning facial recognition technologies, the City could take action to ensure that Portlanders only use high-performing facial recognition technologies in ways that would reduce, rather than exacerbate, racial bias. For example, the City could impose procurement restrictions based on NIST testing results, mandate performance audits, require training for individuals using facial recognition technologies, require humans to review facial recognition match results before acting based on those results, and/or create oversight mechanisms to promote accountability.

4. Banning Portlanders from having access to opt-in customer experience conveniences, whether in retail, health care, or other settings seems to be much broader than the concerns raised around security and surveillance applications. While it has been established that this technology is not in wide use in Portland today, below are several use examples, which already have broad public acceptance, that would fall under this ban. We request that city staff work with the private sector to craft language that focuses on the uses that we agree should be prevented, but allows for positive uses such as:
 - **Airlines** to allow travelers to pass through airports faster.
 - **Banks** to enhance consumer security to verify purchases and access ATMs.
 - **Hotels** to recognize loyal customers, speed check-in and unlock rooms.
 - **Retailers** to speed checkout lines.
 - **Automobiles** to unlock doors, start motors and adjust seats, mirrors, and climate control systems.
 - **Venues** to permit faster, more efficient, and more hygienic ticketless access to concerts and amusement parks.
 - **Healthcare facilities** to verify patient identities while reducing the need for close-proximity interpersonal interaction.
 - **Apps** to assist people suffering from memory loss or prosopagnosia (face blindness) with recognizing friends.
5. Both the public-sector and private-sector facial recognition draft ordinances should more clearly state that they do not apply to PDX airport and other Port authorities. San Francisco’s ordinance, for example, clearly exempts airport and port uses. Additionally, we urge you to work with the Oregon Bankers Association, the Oregon Association of Hospitals and Health Systems, and other heavily regulated industry sectors to ensure these ordinances do not conflict with state and federal regulations.

II. The private-sector draft ordinance is problematically unclear.

6. The definitions in the private sector draft ordinance are confusing, making it very difficult to understand the scope of what the prohibition is attempting to cover. The definition of “face recognition” seems to suggest that there needs to be a type of database “matching” happening, but the definition of “facial recognition technology” is extremely broad and includes face clustering, face detection, and potentially anything involving the use of facial characteristics beyond identification or a use which would require database “matching.” Further, this sentence does not define the term, but rather seems more explanatory, making its utility in the definition questionable. For example, a Face Recognition search will typically result in one or more most likely candidates—or candidate images—ranked by computer, evaluated similarly, or will return a negative result. The conflict between the two definitions will create uncertainty in an area that is trying to do just the opposite.
7. There is a lack of clarity on whether the prohibition intends to include face-related technology generally or if identification and/or matching is required and what it means to “use” face recognition/face recognition technology in places of public accommodation. For example, it is a general expectation of the public that banks have cameras to record transactions at ATM machines if the need arises to verify a transaction, and to prevent theft. These ordinances appear to ban even that use of technology.

8. The private-sector draft ordinances' exemptions make little sense.

- a. The current private-sector ordinance's social media exemption seems to disadvantage small brick-and-mortar establishments that are already facing stiff competition from bigger technology companies that operate online platforms. Facial recognition technologies can improve customer experience in brick-and-mortar settings, and further disadvantaging small businesses by preventing them from using innovative technologies seems especially imprudent and unfair to local businesses during the pandemic and corresponding economic downturn.

Additionally, the social media exemption is confusing. The private-sector prohibition purports to cover use of facial recognition in places of public accommodation, but it is not clear how social media would apply in that case. This should be clarified or removed.

- b. In other states that have successfully worked with stakeholders to pass legislation regulating facial recognition technology, specific language has been included to ensure that the features that use this technology on personal devices may be used in public spaces. For example, many people use the technology on their phone to help them sort photos that could be taken anywhere. The private-sector draft ordinance does not appear to allow for this use. Additionally, as previously noted, the definitions do not distinguish between face related technology and face matching or identification.

9. We have numerous strong concerns about the enforcement mechanisms and proposed remedies in the private-sector ordinance. As we have previously noted, enforcement of this ordinance will be nearly impossible as drafted. The language in the Enforcement and Remedies section of the ordinance is extremely vague. It is unclear what is meant by being "aggrieved by a Private Entity's noncompliance". What does "aggrieved" mean? Must a person show actual damages to be "aggrieved"? This needs further clarification.

The ordinance also calls for damages and "such other remedies as may be appropriate" for violation of the ordinance. What is meant by "other remedies"? The plain language of the ordinance appears to require actual damages, but it is unclear what other remedies a plaintiff may be able to recover.

We strongly encourage the City to remove the private right of action for purported violations of the ordinance and allow enforcement of alleged violations by the City itself.

Finally, it is unclear what the statute of limitations would be with respect to claims brought under this ordinance. A specific statute of limitation should be identified in the ordinance or, if there is another law or ordinance providing an applicable statute of limitation, a citation to that law or ordinance.

II. The public-sector draft ordinance contains problematically imprecise terms.

10. The definition of "Surveillance Technologies" is too broad. Capturing personal information capable of being associated with any individual or group is not surveillance. Merriam-Webster defines "surveillance" as "close watch kept over someone or something (as by a detective)." Merely collecting information does not equate to keeping watch. Keeping watch implies some kind of tracking or continuous monitoring.
11. The definition of "Facial Recognition Technology" is too broad and conflates facial detection, facial analysis, and facial verification with facial recognition. Additionally, in paragraph 7, the public-sector ordinance implies that all facial recognition technologies are surveillance technologies, which is not accurate. Technologies that merely identify an individual by analyzing a single probe image are not surveillance technologies because they are not used to track, watch, or continuously monitor individuals.

Finally, we remain concerned at the speed in which the city is moving to ban this technology. Oregon Attorney General Ellen Rosenblum is expected to bring data privacy legislation to the 2021 session based on input from a diverse stakeholder workgroup. Congress is also currently considering legislation that would establish federal standards for the use of facial recognition and similar technologies. In either case, the adoption of new state or federal laws would pre-empt these ordinances. We advise the city to take the time to work with the private sector, as other jurisdictions have, to develop regulations that can work for the entire community, and will not conflict with what will soon likely be new state or national requirements.

Sincerely,

Jon Isaacs

Vice President, Government Affairs

Portland Business Alliance, Greater Portland's Chamber of Commerce

503-757-5721

jisaacs@portlandalliance.com

Skip Newberry (he/him)

President and CEO

Technology Association of Oregon

503.228.5416

techoregon.org



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 Technology¹

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 cities, 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 tones³. 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 go⁹. 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 Spaces¹¹

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.

Smart City PDX
Facial Recognition
July 26, 2020
Page 6 of 6

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,

A handwritten signature in blue ink that reads "Brian Hofer". The signature is written in a cursive style with a long horizontal stroke at the end.

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

IMPACT STATEMENT

Legislation title: Prohibit the use of Face Recognition Technologies by private entities in places of public accommodation in the City (Ordinance; add Code Title 34)
Contact name: Hector Dominguez
Contact phone: 503-823-2071
Presenter name: Hector Dominguez

Purpose of proposed legislation and background information:

This Ordinance adds a new chapter to City code that prohibits the use of Face Recognition Technologies by Private Entities in places of Public Accommodation under the jurisdiction of the City of Portland.

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

Without clear processes available to cities to assess, evaluate and determine trust in technological solutions using face recognition, there is a risk of discrimination and harm, because Face Recognition Technologies collect sensitive personal information and may lead to different decisions about access for those people for which these technologies are biased against.

As a precautionary action to avoid harm, the City of Portland, in partnership with our communities, has developed this ordinance to ban the private use of Face Recognition Technologies in places where the City has jurisdiction and are of common use for all Portlanders.

Financial and budgetary impacts:

There is no immediate financial or budget impact that would result from adopting this ordinance.

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 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