IBIA
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 groups[2]

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 shortcoming 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

IBIA

International
Biometrics+Identity
Association

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

202.888.0456 | IBIA.ORG