BLANKROME

Biometric Privacy

SEPTEMBER 22, 2020 • NO. 1

City of Portland Enacts Nation's First Private-Sector Facial Recognition Ban

On September 9, 2020, the City of Portland, Oregon, became the first jurisdiction in the United States to issue a sweeping ban prohibiting the use of facial recognition technology by private entities, which will go into effect January 1, 2021. The ban corresponds with a similar ordinance enacted by Portland prohibiting the use of this technology by city officials, which went into effect immediately.

The new Portland facial recognition ban is noteworthy, as it highlights the aggressive manner lawmakers across the nation are seeking to enact strict regulation over the use of facial recognition software. In addition, the ordinance may serve as a template for other cities and states to enact bans.

As such, companies that incorporate facial recognition into their operations (or intend to do so) should take proactive measures to develop and implement facial recognition biometrics compliance programs to ensure continued organizational compliance with today's increasingly complex web of biometric privacy laws and to minimize potential exposure.

OVERVIEW OF FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology involves the use of "biometrics" (*i.e.,* individual physical characteristics) to digitally map an individual's facial "geometry." These measurements are then used to create a mathematical formula known as a "facial template" or "facial signature." This stored template or signature is then used to compare the physical structure of an individual's face to confirm their identity or uniquely identify that individual.

KEY ELEMENTS OF PORTLAND'S PRIVATE-SECTOR FACIAL RECOGNITION TECHNOLOGY BAN

Under the Portland ordinance, "private entities" are barred from using "facial recognition technology" in any "places of public accommodation" within the boundaries of the City of Portland.

"Facial recognition technology" is defined under the ordinance to mean "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."

"Face recognition," in turn, is defined as "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 negatives result."

Importantly, the ban defines "private entities" extremely broadly as "any individual, sole proprietorship, partnership, corporation, limited liability company, association, or any other legal entity, however organized."

Similarly, the scope of the ban is also extensive due to the term "places of public accommodation" being defined as "[a]ny place or service offering to the public accommodations, advantages, facilities, or privileges whether in the nature of goods, services, lodgings, amusements, transportation or otherwise."

Thus, the ban encompasses essentially all types of businesses—including banks, hotels, convenience stores, and even airports—that will no longer be able to use facial recognition for any purpose.

The ordinance provides three limited exemptions from the ban whereby facial recognition may be use: (1) to the extent necessary for a private entity to comply with federal, state, or local laws; (2) for user verification purposes by an individual to access their own personal or employer-issued communication and electronic devices; and (3) in automatic face detection services in social media applications.

PENALTIES & ENFORCEMENT

Importantly, the ordinance contains a private right of action permitting any person "injured" by a "material violation" of the law to pursue litigation and recover liquidated damages in the amount of "$1,000 per day for each day of violation," as well as attorney's fees in some instances.

KEY TAKEAWAYS

The most direct takeaway from the Portland private sector facial recognition ban is that companies operating in Portland will no longer be able to use facial recognition beginning at the start of 2021.

With that said, the impact of the private sector ban will likely extend well beyond the borders of Portland.

Currently, states and cities from coast to coast—and even the federal government—are attempting to enact biometric privacy legislation of their own, many of which take direct aim at facial recognition technology. Until now, jurisdictions that have enacted laws outlawing the use of facial recognition technology have limited the scope of their bans to the public sector, and law enforcement in particular. Portland, however, has taken a significant step further by applying its ban to the private sector as well.

Importantly, Portland's success in enacting a sweeping, across-the-board private-sector ban may influence lawmakers in other parts of the country to try their hand in enacting similar laws barring private entities from using facial recognition or other forms of biometrics.

Even if lawmakers are not successful in passing outright bans, the recent move by Portland will provide strong encouragement to lawmakers who may be contemplating the prospect of enacting robust requirements and limitations over the use of this technology to push forward with related biometric privacy laws.

To further complicate matters, facial recognition has recently received a significant amount of negative media coverage over potential accuracy and bias problems. Of particular concern is the fact that today's technology is less accurate in identifying people of color and women—thereby creating an enhanced risk of misidentification of minorities.

Facial recognition has also garnered a significant amount of recent publicity stemming from controversial uses of the technology. At the start of 2020, news broke regarding the alleged practices of facial recognition startup Clearview AI, which built a massive database of facial templates of millions of individuals across the world and then sold access to its database to both law enforcement and private entities.

Since that time, other companies have also made headlines after reports surfaced regarding their purported practices involving the deployment of facial recognition technology for security and surveillance purposes without disclosing their use of facial recognition to patrons and customers.

This sustained news coverage relating to alleged improper and controversial uses of this technology will only add to the pressure put on lawmakers to make stringent regulation over facial recognition software a reality sooner than later.

Taken together, it is clear potential exposure stemming from the use of facial recognition biometrics will steadily—if not drastically—increase in the immediate future.

WHAT TO DO NOW

Due to the rapidly expanding risk associated with the use of facial recognition technology, if your organization currently utilizes this form of biometrics—or is contemplating doing so—the best course of action is to speak with experienced counsel to ensure you are able to minimize risk to the greatest extent possible.

For companies operating in Portland, immediate action should be taken to ascertain whether any form of facial recognition software is being used and, if so, whether any of the limited exemptions in the ordinance can be utilized to permit continued use of the technology into 2021. Those companies that do not fall under any of the limited exemptions should evaluate whether alternative technologies can be implemented to accomplish the same objectives—such as identification, authentication, or security.

At the same time, companies operating outside Portland should take proactive measures by building out their biometric privacy compliance programs to get a step ahead on the anticipated facial recognition laws governing the use of this technology, as it is only a matter of time before similar regulatory controls and limitations over the use of facial recognition biometrics are enacted in other parts of the country.

HOW WE CAN HELP

As leaders in the biometric privacy space, Blank Rome's dedicated Biometric Privacy Team can assist with providing key counseling and guidance regarding issues or concerns relating to the use of facial recognition technology and/or today's new wave of biometric privacy laws. We can also assist in developing tailored, comprehensive facial recognition and biometric privacy compliance programs that ensure continued, ongoing compliance not just with current biometrics regulation, but anticipated laws as well—allowing you to stay ahead of this constantly-evolving legal landscape.

For additional information, please contact:

Jeffrey N. Rosenthal, Philadelphia Office
Partner and Team Lead, Biometric Privacy
215.569.5553 | rosenthal-j@blankrome.com

David J. Oberly, Cincinnati Office
Associate, Biometric Privacy
513.362.8711 | doberly@blankrome.com