AN A.S. PRATT PUBLICATION
FEBRUARY-MARCH 2022
VOL. 8 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 2** **February-March 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [2] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Complying with Portland's Private-Sector Facial Recognition Ban

By David J. Oberly*

The author of this article discusses Portland's ban on facial recognition technology and advises companies operating there to take immediate action to ensure compliance.

The city of Portland, Oregon, made headlines when it became the first jurisdiction in the nation to enact a blanket ban on the use of facial recognition technology ("FRT") by all private entities physically located within its city limits. While many cities have banned the use of face biometrics by law enforcement and parts of the public sector, the Portland ordinance is noteworthy because it drastically expanded the scope of this new type of regulation to also reach the private sector.

Since that time, the city of Baltimore, Maryland, followed suit with a similar private-sector facial biometrics ban of its own. More jurisdictions, including both cities and potentially states as well, are likely to add new laws mirroring those of Portland and Baltimore in the immediate future, especially as facial recognition continues to receive regular negative media coverage highlighting its claimed shortcomings, including potential accuracy and bias problems.

Combined, all companies that operate in Portland and use any type of software or other technology that may capture images of individuals' faces should evaluate whether the new ordinance applies to them and, if so, take immediate action to ensure compliance with the law. And from a broader perspective, as this draconian type of biometric privacy regulation is likely expand to additional parts of the country moving forward, companies that use or intend to use any type of facial recognition technology need to familiarize themselves with this new type of biometrics regulation and consider taking proactive steps to minimize their anticipated liability exposure.

OVERVIEW

- *Scope/Applicability*: The Portland ordinance bars the use of "facial recognition technologies" by "private entities" in "places of public accommodation" within the City of Portland.
- "*Private Entity*": The ordinance defines the term "private entity" in similar fashion to the Illinois Biometric Information Privacy Act ("BIPA") as "any

* David J. Oberly is an associate at Blank Rome LLP focusing his practice on counseling, advising, and representing clients in a broad range of biometric privacy, data privacy, and data security/cybersecurity compliance, risk management, and class action litigation matters, as well as providing data breach rapid incident response and crisis management services. He may be contacted at david.oberly@blankrome.com.

individual, sole proprietorship, partnership, limited liability company, association, or any other legal entity, however organized."

- "*Face Recognition Technologies*": 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."

- "*Face Recognition*": 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)."

- "*Places of Public Accommodation*": "Places of public accommodation" is defined broadly to mean "[a]ny place or service offering to the public accommodations, advantages, facilities, privileges whether in the nature of goods, services, lodgings, amusements, transportation or otherwise."

EXEMPTIONS

- *Certain Places of Public Accommodation*: Excluded from the scope of the ordinance are "institution[s], bona fide club[s], private residence[s], [and] place[s] of accommodation that [are] in [their] nature distinctly private."

- *Legal Compliance*: The ordinance does not apply to the use of FRT to the extent necessary to comply with federal, state, or local laws.

- *User Verification*: The ordinance does not apply to the use of FRT for user verification purposes, but only in the narrow context of allowing an individual to access his or her individual or employer-issued communication or electronic device.

- *Automatic Face Detection*: Finally, the ordinance does not apply to the use of FRT "[i]n automatic face detection services in social media applications."

CORE COMPLIANCE REQUIREMENT

- *Prohibition on FRT Use*: Under the ordinance, private entities are barred from using face recognition technologies in places of public accommodation within city limits.

ENFORCEMENT AND REMEDIES

- *Private Right of Action*: Any person "injured" by a material violation of the ordinance may pursue class action against the offending private entity.

- *Recoverable Damages*: A person injured by a violation of the ban can recover $1,000 per day for each day of the violation or actual damage sustained as a result of the violation, whichever is greater, as well as "such other remedies as may be appropriate."

- *Attorneys' Fees*: Attorneys' fees are also recoverable, but only if certain actions are taken by the injured person before filing suit. Specifically, a plaintiff must submit a written demand for the payment of a claim on the offending private entity and its insurer (if known to the plaintiff) at least 30 days before the filing of the complaint. Where this is completed, a court may award to a prevailing plaintiff a "reasonable amount" of attorneys' fees. Conversely, a plaintiff cannot recover attorneys' fees if, before suit was filed, the offending private entity tendered to the plaintiff an amount that is at least equivalent to the damages awarded to the plaintiff in the litigation, exclusive of any costs, interest, and prevailing party fees.

PRACTICAL COMPLIANCE TIPS AND BEST PRACTICES

For companies operating in Portland, immediate action should be taken if not already done so to ensure compliance with the city's FRT ban. Companies should consider the following action steps to determine the applicability of the ban to their operations and to come into compliance with the Portland ordinance if the organization falls under the scope of the law:

- *Determine Whether Technology Falls under Scope of Law*: First, companies should determine if their technology falls under the scope of the law. To do so, the system must engage in identifying, verifying, detecting, or characterizing facial features or capture information about an individual based on his or her facial features.

- *Evaluate Applicability of Exceptions to Ban*: If the technology is found to fall under the scope of the ban, the next step is to evaluate whether any of the limited exemptions offered by the ordinance can be satisfied to allow the company to continue its use of the technology.

- *Cease All Use of FRT If No Exceptions Apply*: If none of the exceptions apply, the company must immediately cease all use of its FRT technology.

- *Identify Availability of Any Suitable Alternative Technologies*: At the same time, companies that are no longer permitted to use their current FRT technology should evaluate whether any alternative technologies can be implemented to accomplish the same objectives – such as identification, verification/authentication, or security – for which facial recognition was used.