Volume 4, No. 4 | July–August 2021

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 4, No. 4 | July–August 2021

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. 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.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Prepare for the Impending Wave of Facial Recognition Technology Regulation—Before It's Too Late

David J. Oberly*

The ability of companies to use facial recognition in a safe and responsible manner has become a paramount concern for consumers, lawmakers, and regulators alike. As a result, new laws specifically targeting facial recognition have steadily increased across the nation in recent years. The author of this article discusses the laws pertaining to facial recognition technology and steps companies should consider implementing to comply with these laws.

At the present time, regulation over the use of facial recognition technology remains limited to a relatively few number of state and local laws. Consequently, a large number of companies that are not currently subject to any facial recognition regulation continue to operate under the assumption that they need not worry about developing a biometric privacy compliance program to ensure compliance with today's facial recognition-related requirements and restrictions.

A word of caution: operating in this fashion is a recipe for disaster.

As the legal and privacy risks continue to increase in connection with the use of facial biometrics, and as lawmakers seek to impose tighter controls over the use of this especially sensitive type of biometric data, companies that utilize facial recognition technology—but do not fall under any current facial recognition laws or regulations—are well advised to take proactive steps to build out their facial biometrics compliance programs at this time. By doing so, companies can get a head start on addressing the issues raised by the impending wave of biometric privacy laws targeting facial biometrics, as it is only a matter of time before facial recognition regulation reaches the locations where they conduct business.

Robotics, Artificial Intelligence & Law / July–August 2021, Vol. 4, No. 4, pp. 271–276.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

Facial Recognition Technology Explained

Facial recognition technology involves the process of using "biometrics" (i.e., individual physiological 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 verify their identity or to identify that individual.

Legal Landscape Overview

At this time, there are only three active targeted biometric privacy laws on the books in the United States: Illinois' Biometric Information Privacy Act ("BIPA"), Texas' Capture or Use of Biometric Identifier Act ("CUBI"), and Washington's HB 1493. All three laws govern the use of facial biometrics.

Illinois' BIPA has become a household name in the area of privacy and data protection law, and for good reason. BIPA mandates notice, consent, and data security requirements on companies that collect and use facial template data. BIPA is also the only state-level biometric privacy law that includes a private right of action permitting the recovery of statutory damages ranging from $1,000 to $5,000 for "each violation" of the law.

Importantly, in early 2019 the Illinois Supreme Court ruled that BIPA does not require plaintiffs to allege any actual injury or damage to recover statutory damages under the law. Not surprisingly, this decision immediately led to a tsunami of bet-the-company class action litigation, which has continued apace into 2021—with no signs of slowing down any time soon.

Recent Efforts to Impose Greater Regulation Over Facial Recognition Technology

Recently, states from coast to coast (and some cities) have taken a keen interest in imposing strict requirements and limitations over the use of facial recognition technology. In 2020 alone, multiple states introduced bills that directly targeted facial biometrics exclusively, including:

- Idaho (HB 492);
- California (AB 2261);
- Maryland (HB 1578); and
- Louisiana (HB 662).

Although none of these bills was enacted in 2020, lawmakers' awareness of the need for greater regulation over facial biometrics is clear.

New Wrinkles in the Legal Landscape

Two facial recognition bills that did make their way into law in 2020 will likely have an oversized impact on the landscape of facial biometrics regulation for years to come.

In September 2020, the City of Portland enacted a new type of biometric regulation—an outright ban over the use facial recognition technology by private entities. While several other cities have enacted public-sector bans, the Portland law—which went into effect at the start of 2021—is noteworthy because it goes one step further by applying a blanket ban to the private sector. In addition, the law also contains a private right of action that gives the ban teeth by permitting class action litigation and the recovery of damages in the amount of "$1,000 per day for each day of violation," as well as attorneys' fees.

New York City also heeded the call for greater regulation over facial biometrics by recently approving a new biometric privacy law of its own directly impacting the use of facial recognition software. This law—which goes into effect on July 9, 2021—bans companies from selling, sharing, or otherwise profiting from consumers' biometric data, and also requires commercial establishments to post visible signage near all public entrances notifying consumers of the use of facial recognition technology. Like Portland, the New York City law also features a private right of action that allows for the recovery of statutory damages.

These laws enacted by Portland and New York City will likely have a widespread impact. First, the success seen by Portland and New York City in enacting strict regulation over the use of facial recognition technology may encourage lawmakers in other cities and states to follow suit by enacting blanket bans of their own. At the same time, these laws may provide strong encouragement to

lawmakers contemplating the prospect of enacting robust regulation over the use of this technology—but who do not have an appetite for passing an outright ban—to push forward with strict regulation paralleling that of Illinois' BIPA.

Efforts at the Federal Level

Lawmakers in Washington, D.C., have also become increasingly interested in enacting a national biometric privacy law that would regulate facial recognition technology and other forms of biometrics in a uniform fashion across all 50 states.

Over the course of the past two years, several federal legislative proposals seeking to regulate facial recognition technology were introduced in Congress, including the Commercial Facial Recognition Privacy Act of 2019 (S. 847), the National Biometric Information Privacy Act of 2020 (S. 4400), and the Data Accountability and Transparency Act of 2020.

While these bills all failed during the legislative process, it is expected that some, if not all, of these bills will be reintroduced during the current legislative session.

Importantly, the likelihood of success in enacting nationwide biometric privacy legislation is precipitously higher in 2021 as compared to prior years because of the new Biden administration now occupying the White House and Democratic control of both chambers of Congress. Together, the prospect of a federal biometric privacy statutory scheme being enacted over the course of the next 12 months is a distinct reality.

The Federal Trade Commission's New Priority Focus: Policing Facial Biometrics

In addition to increased legislative activity, the Federal Trade Commission ("FTC") has stepped up and taken an active role in policing improper facial recognition practices. In January 2021, the FTC reached a proposed settlement with photo app developer Everalbum Inc. stemming from the company's alleged deceptive facial recognition practices. Notably, the Everalbum settlement represents the first FTC case specifically targeting facial recognition

technology. In announcing the settlement, the FTC also noted that ensuring companies utilize facial recognition in a proper fashion will remain a "high priority" for the agency moving forward.

What This Means for Companies Utilizing Facial Recognition Technology

With more jurisdictions seeking to enact targeted facial recognition laws of their own and the FTC aggressively pursuing enforcement actions against companies for improper facial biometrics practices, it is imperative that all companies utilizing this technology devote the necessary time, effort, and resources to get a head start on complying with the laws that will inevitably be enacted as biometric privacy rights continue to expand across the country, as well as to mitigate liability exposure in connection with the FTC.

In particular, companies should consider implementing the following action steps where feasible:

- Complete pre-deployment testing of facial recognition technology to ensure its effectiveness and accuracy prior to its use in real-time situations;
- Implement a publicly available, detailed facial recognition-specific privacy policy;
- Provide advance written notice to all individuals of the company's facial recognition practices;
- Obtain signed, written releases from all individuals providing consent for the company to collect, use, and share their facial template data;
- Permit individuals to opt out of the collection of their facial template data;
- Implement data security measures to protect and secure facial template data;
- Maintain an explicit policy strictly barring the use of facial recognition technology by the company, its employees, and contractors/vendors for discriminatory purposes; and
- Consult with experienced biometric privacy counsel to ensure compliance with today's constantly evolving biometric privacy legal landscape.

Conclusion

The ability of companies to use facial recognition in a safe and responsible manner has become a paramount concern for consumers, lawmakers, and regulators alike. As a result, new laws specifically targeting facial recognition have steadily increased across the nation in recent years.

Looking ahead, the scope of liability exposure will only broaden further as additional cities, states, and Washington, D.C., look to impose greater regulation over the use of facial recognition and other types of biometrics, and as the FTC continues to aggressively police improper facial recognition practices.

As such, companies that are not subject to any facial recognition regulation at this time can get ahead of the compliance curve by taking proactive measures to develop and implement facial recognition biometrics compliance programs that encompass the principles and practices described above.

Note

* David J. Oberly is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Biometric Privacy, Privacy Class Action Defense, and Cybersecurity & Data Privacy groups. His practice encompasses both defending clients in biometric privacy, privacy, and data breach class action litigation, as well as counseling and advising clients on a wide range of biometric privacy, privacy, and data protection/cybersecurity matters. He can be reached at doberly@blankrome.com.