CBA Report

Cincinnati Bar Association

November/December 2020

INTENTIONAL RACIAL EQUITY
pg. 15

BIOMETRIC DATA AND COVID
pg. 7

WORKING FROM HOME
pg. 10

Biometric Data and COVID19 in the Workplace

Beware potential privacy implications of touchless technology

By David J. Oberly

As the country begins to shift back to traditional work environments during the return-to-work phase of the COVID-19 pandemic, employers will implement a range of risk mitigation measures designed to combat community spread of the virus in the workplace. In particular, many employers will turn to devices that incorporate facial recognition technology, which can be utilized in a variety of ways to enhance workplace safety and minimize the health risks associated with the virus. While this cutting-edge technology offers a range of benefits, its use also implicates a growing patchwork of biometric privacy laws that can leave employers vulnerable to significant liability exposure if not addressed properly. As such, employers that opt to implement policies featuring facial recognition software must ensure they take the appropriate measures to harness the benefits of this technology in a manner that also ensures compliance with current (and future) biometric privacy regulation.

Overview of Facial Recognition Technology

Facial recognition technology involves the process of using "biometrics" (*i.e.*, individual physical characteristics) to digitally map an individual's facial "geometry"— such as the distance between an individual's eyes, between the forehead and chin, and the width of the nose. 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 to uniquely identify that individual.

The Role of Facial Recognition Technology in Combating COVID-19

Facial recognition technology has significantly enhanced the operations of businesses across all industries in a myriad of different ways — including with respect to security and identity fraud prevention; access and authentication; and accessibility to accounts and services. In the specific context of COVID-19, facial recognition technology can be deployed in a variety of ways to combat the spread of the virus.

First, facial recognition technology may play a vital role in time and attendance. In recent years, many employers have replaced traditional paper-based timecards with biometric fingerprint readers to address fraudulent employee time and attendance issues, which have bilked organizations out of billions of dollars over the years. Importantly, however, fingerprint timeclocks require employees to physically place their finger on the biometric scanner each time they clock-in or clock-out, making them one of the most heavily utilized touch points in the workplace. Facial recognition timekeeping systems, on the other hand, offer a contactless time and attendance solution, while still providing the significant fraud-related benefits offered by their fingerprint counterpart.

Second, facial recognition may also serve an important role in access control. Access control systems restrict entrance to certain areas of a property or facility. To reduce the number of touchpoints in the workplace, many employers will seek to replace their traditional lock and key or employee badge ID access systems with systems controlled by facial recognition software, which not only offer a contactless method of access control, but also provide significant security enhancements as well.

Lastly, facial recognition may also play a part in certain COVID-19 temperature screening programs. Although most types of temperature screening devices do not implicate biometric privacy issues, some of the more advanced devices — particularly contactless infrared thermal temperature scanners — also capture facial geometry, triggering obligations to comply with applicable biometric privacy regulation.

The Legal Landscape of Biometric Privacy Law

Lawmakers across the country have sought ways to stringently regulate the use of facial recognition technology and similar forms of biometric software.

First, to combat the risks posed by facial template data and other biometric data, several states have enacted targeted biometrics laws, focusing directly on regulating the collection and use of facial recognition technology by employers and other business entities.

Currently, there are only three active, domestic biometric privacy laws on the books: Illinois's Biometric Information Privacy Act ("BIPA"), Texas's Capture or Use of Biometric Identifier Act ("CUBI"), and Washington's H.B. 1493.

Of these laws, BIPA has been the one to garner the most headlines to date — and for good reason. BIPA prohibits private entities from collecting, using, storing, or disclosing biometric data without first providing notice and obtaining a written release from the individual. Importantly, BIPA is the only biometrics law to offer a private right of action, which permits the recovery of statutory damages of $1,000 to $5,000 for "each violation" of the law. These high damages awards — combined with a low bar for establishing BIPA claims — led to an explosion of bet-the-company BIPA class litigation in 2019, which has continued apace into 2020 with no signs of slowing down.

As just one example, after several significant setbacks, Facebook agreed to pay $650 *million* to settle a long-standing BIPA dispute over allegations that the social media giant violated BIPA in connection with its photo "tagging" feature.

Second, legislators have sought to add facial template data to the types of protected "personal information" which, if compromised, triggers breach notification obligations by impacted entities.

Third, new state consumer laws — most particularly the California Consumer Privacy Act of 2018 ("CCPA") and the New York Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") — also include facial template data (and other forms of biometric data) within their definitions of "personal information." Beyond that, the CCPA also requires covered entities provide notice to consumers as to how facial template data is used and provides a private right of action if facial template data is involved in certain data breach events.

In addition, many states without laws regulating facial recognition technology have ramped up their efforts in 2020 to enact similar laws of their own, many of which are modeled heavily after the draconian BIPA.

For example, in early 2020 Washington's legislature introduced the Washington Privacy Act ("WPA") which, among other things, sought to impose a stringent set of requirements and limitations on use of facial recognition technology. The proposed bill also included a private right of action allowing the recovery of statutory damages awards between $50,000 and $100,000 per violation, which would have provided the highest allowable damages awards in any piece of U.S. data privacy legislation to date. Ultimately, although the WPA failed to become law, it is clear the risk of potential legal liability—with corresponding sky-high damage awards—will increase exponentially in the immediate future.

Fortunately, there are several best practices employers can implement to minimize the risk of becoming embroiled in high-stakes class action litigation stemming from the use of biometric data as part of their efforts to combat the community spread of COVID-19 in the workplace.

Written Privacy Policy

As a starting point, employers should ensure transparency as to how they collect, use, store, disclose, and dispose of facial template data by implementing a detailed facial recognition-specific privacy policy.

Privacy policies should encompass the following issues: (1) notice that facial template data is being collected and/or stored; (2) the current and reasonably foreseeable purposes for which the employer utilizes facial template data; (3) a description of the protective measures used to safeguard facial template data; and (4) the employer's facial template data retention and destruction policies and practices. These policies should also strictly prohibit the disclosure of any individual's facial template data without their consent and should ban the employer and its workers from selling or otherwise profiting from any such data.

This facial recognition privacy policy should be made publicly available, and, at a minimum, entail inclusion in the entity's broader online privacy policy, as well as dissemination of the policy to all employees.

Written Notice

Second, to further transparency, employers should provide conspicuous, advance notice of the use of facial recognition technology before it is implemented. In so doing, employers should offer their workers meaningful notice regarding how facial templates are created, and how such data will be used, shared, and stored by the employer. Where appropriate, or required by law, contextual and just-in-time notices may be necessary.

Written Release

Third, employers must obtain signed, written consent in the form of a written release from employees authorizing the collection, use, storage, and disclosure their facial template data prior to the time any such data is captured or used for any purpose.

In signing the written consent, employees should acknowledge they have read their employer's facial recognition privacy policy, as well as the more specific, written notice. This consent should also make clear the employee consents to those policies and guidelines, as well as to the capture and use of their facial template data, including the employer's ability to share such data with any service providers or third-party vendors.

Data Security Measures

Finally, employers must ensure they implement effective data security safeguards to protect all facial template data from improper disclosure, access, or acquisition. In doing so, employers should ensure they safeguard employees' biometric data: (1) by using the reasonable standard of care applicable to their given industry; and (2) in a manner that is the same or more protective than that in which the employer stores, transmits, and protects other forms of sensitive personal information.

Conclusion

Facial recognition technology will play a supporting, if not significant, role in allowing employers and their workforces to return to work safely by minimizing the significant health risks associated with COVID-19. In doing so, however, employers must take special care to comply with an increasingly complex maze of biometric privacy laws, which

will only become more difficult to navigate moving forward.

As such, employers that incorporate facial recognition technology in their efforts to combat the risk of community spread of COVID-19 (even those operating in jurisdictions where no facial recognition or other biometric laws are on the books) should consider taking proactive measures to create and implement compliance programs that encompass the principles and practices described above. By doing so, employers can ensure they maintain legal compliance to mitigate potential liability exposure. Including experienced counsel in this process remains an important first step that can pay significant dividends.

Oberly is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Cybersecurity & Data Privacy and Privacy Class Action Defense groups. David's practice encompasses counseling and advising sophisticated clients on a wide range of cybersecurity, data privacy, and biometric privacy matters, representing clients in the defense of privacy and biometric privacy class action litigation, and assisting clients with responding to a wide variety of data breach and data compromise events. He can be reached at doberly@blankrome.com.

$ Rare Coins $ Precious Metals $ Paper Money
$ Diamonds $ Jewelry $ Watches
$ Firearms $ Antiques $ Rare Collectables
$ Buy $ Sell $ Trade $ Loan $ Appraisals

American Trading Company
The Original
3236 W Galbraith Rd
Cincinnati, Ohio 45239
1 Block West of Colerain Ave
513-385-6789
www.americantradeco.net

Highest Cash Buyers
Free Verbal Appraisals
Over 100 Years' Experience
Life Member American Numismatic Association
A+ Better Business Bureau
Licensed By The State of Ohio PB # 100642.00
Licensed by The Federal Government
No Deal too Large or Small
One Call Buys and Sells it All

CE-GCI0468135-01

We ran out of red tape in 1982.

TURNS OUT WE DIDN'T NEED IT ANYWAY.

Why are so many banks dedicated to running you through red tape? Making you jump through hoops. Not us. We hate red tape. That's why we work to deliver simple, sophisticated solutions. We remove complications, so you can live with no boundaries.

Break free from red tape.
Let us go to work for you.

LCNB.COM/WEALTH

LCNB | Wealth