Drinker Biddle

February 14, 2018

Buyer Beware: Facial Recognition and the Current Legal Landscape

By Kathryn E. Deal, Matthew J. Fedor, Justin O. Kay and Meredith C. Slawe

Vendors are pitching retailers on a range of innovative technology tools that appear to be straight out of the Steven Spielberg science-fiction movie, "Minority Report." Last month, many of these products were featured by more than 500 exhibitors at the Javits Center in New York at the National Retail Federation's ("NRF") Annual Convention and Expo. From artificial intelligence to facial recognition to virtual reality to scheduling/traffic analytics to streaming signage, technology is poised to transform the customer experience, increase familiarity with individual consumer preferences, alter the concept of payment/POS mechanisms, revolutionize supply chain and logistics, and solve a host of challenges through big data, predictive analytics, and robotics. Vendors are understandably excited to share information about and provide demos of their respective technology solutions to prospective retail clients. Many of them, however, have not anticipated the significant legal and compliance challenges that accompany implementation of their tools, or they expressly disclaim any responsibility for or knowledge of relevant restrictions or requirements. This is eerily similar to the environment that existed at the time retailers were pitched by mobile marketing vendors to roll out the earliest text message marketing programs, which led to a flurry of class action activity that challenged compliance and the sufficiency of consent under the Telephone Consumer Protection Act (TCPA). There has been a recent uptick in biometrics-based litigation—with a particular focus in the employment context—against companies such as United Airlines, Intercontinental Hotels, Facebook, Hyatt, Bob Evans Restaurants, and dozens of others. Plaintiffs' attorneys have publicly shared their expectation that this litigation wave will continue as companies continue to integrate technology involving retina and iris scans, facial recognition, and fingerprinting, in connection with their employees and customers.

As retailers consider employing facial recognition technology tools to track customers, collect data about consumer demographics, assess moods and other behaviors, and improve loss-protection efforts, as well as fingerprinting technology for employee verification and customer authentication at the POS, it is important that they understand the state laws that may apply and the robust consent and privacy-based requirements under them.

While only three states (Illinois, Texas, and Washington) have enacted legislation comprehensively regulating the retention, protection, and disclosure of biometric data, many others have considered it, and many more are likely to do so as the collection of such information becomes more mainstream. At present, only the Illinois statute—the Biometric Information Privacy Act (BIPA), 740 ILCS 14—provides for a private right of action and statutory damages provision ($1,000 up to $5,000 per violation, with no express cap on aggregate damages). Consequently, the BIPA has garnered attention from plaintiffs' class action lawyers, who are currently prosecuting cases in Illinois federal and state courts, as well as in California (under the BIPA, subject to an Illinois choice-of-law provision in consumer-facing terms and conditions). While retailers should be acquainted with the requirements of the BIPA, they should also be mindful of ongoing efforts in other states to regulate the collection, retention, and disclosure of biometric data. Notably, some industry groups/coalitions representing technology companies and retailers have engaged in successful lobbying efforts designed to demonstrate to state lawmakers how beneficial facial recognition technology can be not only for marketing, but also for security, in an effort to shut down potential legislation. For example, a coalition that lobbied against passage of the Montana Biometric Information Privacy Act wrote that it carries with it "a huge risk of costly class action[s]," and "imposes highly specific notice and consent requirements that would make it unworkable to obtain consent for positive users of biometric data."

Is There a Federal Biometrics Law?

Currently, there is no federal law in place that comprehensively regulates the collection and retention of biometric data. But with the heightened focus on privacy and data security, that may change. Unlike credit/debit card and social security numbers, a person's likeness and fingerprint cannot be readily changed upon a breach or misappropriation of data. In November 2017, Senator Patrick Leahy (D-VT), with six cosponsors, introduced the Consumer Privacy Protection Act, which addresses the privacy and security of personal information, including biometric data. In this proposed legislation, there is no private right of action, but it expressly authorizes the FTC, the federal AG, and state AGs to bring enforcement actions. Senator Leahy's press release stated, "The Consumer Privacy Protection Act requires that corporations meet certain baseline privacy and data security standards to keep information they store about consumers safe, and it requires that these firms provide notice and protection to consumers in the event of a breach. This legislation protects broad categories of data, including:

(1) social security numbers and other government-issued identification numbers; (2) financial account information, including credit card numbers and bank accounts; (3) online usernames and passwords, including email names and passwords; (4) unique biometric data, including fingerprints and faceprints; (5) information about a person's physical and mental health; (6) information about geolocation; and (7) access to private digital photographs and videos." As of February 14, 2018, this bill had been referred to several committees and subcommittees.

What are Biometrics?

There is no universal definition of biometrics. In the most general terms, biometrics usually refers either to measurable human biological and behavioral characteristics that can be used for identification or to the automated means of recognizing individuals based upon those characteristics.

The BIPA governs "biometric identifiers" and "biometric information" (which are collectively referred to as "biometric data"). The former is defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." The latter, in turn, is defined as "any information . . . based on an individual's biometric identifier used to identify an individual."

What are the BIPA's Requirements?

Although the BIPA was enacted in 2008, it was not on the radar of the plaintiffs' bar until 2015, when several test cases were filed. This pattern mirrors the TCPA insofar as that statute was enacted in 1992, and the litigation explosion occurred many years later. The BIPA imposes strict notice-and-consent requirements on businesses before they may "collect, capture, purchase, receive through trade, or otherwise obtain" biometric data. Specifically, an individual must be given written notice of, and provide written consent to, the initial collection and storage of his or her biometric data as well as the purpose and length of time that data will be stored and used. Any business that collects or obtains such biometric data must (1) develop a written data-retention policy that is available to the public and that meets statutory requirements; (2) obtain a written release from the person from whom the data is being collected that explains that biometric data is being collected and explains the specific purpose of the collection; (3) restrict the transfer or disclosure of biometric data to very limited circumstances; and (4) protect and store that data to, at least, the same degree that it protects other confidential or sensitive information.

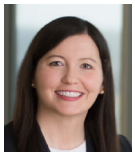
As noted above, the BIPA creates a private right of action for an "aggrieved person," and provides for statutory damages of $1,000 for each negligent violation and $5,000 for each intentional or reckless violation. This private right of action is unique under the BIPA; in the other states with laws governing biometrics, enforcement is vested strictly with the state AGs.

What Should Retailers Do?

As retailers explore new ways to implement technology, it is important to be mindful of the fact that consumer privacy laws are constantly evolving. Retailers are disproportionately targeted in class action litigation, given their visibility and the ease with which plaintiffs' lawyers can follow their practices. Indeed, attorneys are actively monitoring retailers' privacy policies and consumer-facing terms and conditions, and are deploying "investigators" or serial plaintiff clients to visit brick-and-mortar stores and to scour websites in an effort to manufacture claims. Unfortunately, even innocent transgressions can expose businesses to potentially crushing damages.

The latest technology innovations are undoubtedly exciting and transformative—but in some cases, they may come with a host of compliance requirements that retailers should not expect to learn about from their vendors. In weighing the value these tools may bring to the business, retailers should carefully consider how they can effectively roll them out while mitigating litigation risk. With respect to biometric data in particular, retailers should examine and document how they will obtain the requisite consent and how they will capture, retain, protect, and destroy data. Additionally, retailers should implement safeguards in the event of an attempted breach. When this data is accessible to or stored by vendors, retailers should have written agreements with those vendors that include robust requirements on the part of the vendors, favorable indemnification provisions, and insurance requirements.

Primary Contacts



Kathryn E. Deal
Partner
Philadelphia
(215) 988-3386
kathryn.deal@dbr.com

Justin O. Kay
Partner
Chicago
(312) 569-1381
justin.kay@dbr.com

Matthew J. Fedor
Partner
Florham Park
(973) 529-7329
matthew.fedor@dbr.com

Meredith C. Slawe
Partner
Philadelphia
(215) 988-3347
meredith.slawe@dbr.com

Drinker Biddle

www.drinkerbiddle.com

CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY | NEW YORK | PENNSYLVANIA | TEXAS | WASHINGTON DC | LONDON