retail TouchPoints

MINIMIZING LEGAL RISKS FOR RETAILERS THAT USE **BIOMETRIC DATA**

Written by Gregory W. Knopp and Geoffrey J. Derrick
Akin Gump Strauss Hauer & Feld LLP

Artificial intelligence (AI) tools offer retailers large chunks of data that are helpful in creating robust customer profiles, as well as curated and frictionless customer experiences. Many retailers are aware of the benefits offered by the subset of AI tools that involve biometric data. Facial recognition technology is automating and improving the customer experience in both the online (mobile try-on features) and brick-and-mortar (cashierless stores) sales environments. Some retailers use it as an asset protection measure (to identify known shoplifters). Fingerprinting employees is likewise automating retail timekeeping and jumpstarting wellness programs. Third-party vendors are out in the marketplace aggressively pitching retailers on the exciting benefits of cutting-edge technology tools.

Yet retailers' use of biometric data in certain jurisdictions presents legal and compliance challenges distinct from other types of data. Select state privacy statutes and the European Union's General Data Protection Regulation (GDPR) impose additional requirements on businesses that collect or utilize biometric data from either customers or employees. While no federal law preempts those state statutes, the Federal Trade Commission has issued **guidance on facial recognition technology** that cites its authority under Section 5 of the FTC Act to police unfair or deceptive biometric data practices.

As a result, retailers contemplating the use of technology that involves fingerprinting, facial recognition, voice prints and eye scans, for example, must be mindful of the landscape and the patchwork of state laws that govern biometric data privacy.

Akin Gump
STRAUSS HAUER & FELD LLP

I. The Legal Landscape

Illinois currently has the most robust law governing biometric data, in large part because it contains a private right of action allowing anyone "aggrieved" to sue for specified statutory damages. In 2008, the Illinois General Assembly passed the Biometric Information Privacy Act (BIPA) in response to the Pay By Touch bankruptcy, which approved the sale of the sensitive biometric data that entity had maintained. BIPA provides the most comprehensive set of restrictions on biometric data for any retailer with consumers or employees in Illinois.

BIPA applies to any "private entity" that possesses "biometric identifiers" and/or "biometric information." It defines "biometric identifiers" to include "a retina or iris scan, fingerprint, voiceprint, or scan of hand and face geometry." It defines "biometric information" as "any information, regardless of how it is captured, converted, stored or shared, based on an individual's biometric identifier used to identify an individual." It applies to companies in possession of this data and those that collect, capture, purchase, receive through trade or otherwise obtain biometric data about Illinois residents.

The requirements under the statute include: (1) developing a written "schedule and guidelines" for the retention and destruction of the data; (2) informing the subject "in writing" of the collection, the purpose, and the duration of storage, and obtaining a "written release"; (3) refraining from "sell[ing], leas[ing], trad[ing] or otherwise profit[ing]" from the data; (4) refraining from "disclos[ing]" or "disseminat[ing]" data without consent; and (5) taking reasonable measures to protect the data from disclosure.

Significantly, the private right of action under BIPA — with its accompanying damages calculus of $1000 up to $5000 per violation with no cap on aggregate damages — has sparked a wave of class action lawsuits in the Illinois courts. Many such lawsuits allege purely technical BIPA violations (i.e., no concrete harm such as leaked biometric data). The Illinois Supreme Court recently blessed such violations as sufficient to make a person "aggrieved" and therefore able to sue under BIPA in Rosenbach v. Six Flags Entm't Corp.(Ill. Jan. 25, 2019). As a result of the significant litigation risk for companies that run afoul of BIPA, and the ease with which a plaintiff can pursue a claim following Rosenbach, the Illinois law should be top of mind for any retailer using or considering technology implicating biometric data.

Yet it is not only retailers with consumers or employees in Illinois that need to be mindful of biometric data. Europe's GDPR and biometrics laws in Texas and Washington State, for example, impose similar requirements to BIPA, though there is no threat of class action exposure under these laws. Proposals and amendments also have been percolating through the legislatures in Arkansas, Delaware, New York and New Jersey, and Congress is considering comprehensive privacy legislation involving biometric information. Also, the California Consumer Privacy Act ("CCPA"), which will be effective in January 2020 and includes a limited private right of action, expressly includes biometric information. Other states may soon seek to replicate the CCPA, which reflects a significant shift in the privacy landscape in the U.S.

II. Practical Steps

The retail industry is experiencing a transformation in large part because of unprecedented access to rich data and exciting technology tools. When deploying tools implicating biometric information, it is important for businesses to be aware of the legal landscape and to ensure compliance with the relevant state laws. Some practical tips for retailers to consider include:

- Conducting a privacy assessment or audit in a privileged manner;
- Educating internal clients on the general issues so that pertinent contracts are flagged for the legal department;
- Conducting substantial diligence with respect to third-party vendors;
- Drafting favorable contracts with third-party vendors, including robust indemnification provisions;
- Requiring third-party vendors to obtain insurance coverage that includes BIPA claims and names the retailer as a secondary insured;
- Documenting written consent;
- Developing, implementing and maintaining clear policies;
- Implementing a compliant and publicly available written retention schedule;
- Addressing biometric data in written incident response plans for data breaches;
- Drafting a privacy policy that accurately reflects the retailer's practices;
- Interposing arbitration agreements with class action waivers in the consumer and/or employment context;
- Collecting only what the retailer actually requires;
- Carving out Illinois of biometric technology programs;
- Saving data only for so long as it is needed; and
- Ensuring data is adequately protected.