Proskauer

Litigation Breeding Ground: Illinois' Biometric Information Privacy Act

Privacy Law Blog on **March 18, 2021**

Illinois' Biometric Information Privacy Act ("BIPA") is alive and well as a potential breeding ground for litigation for tech companies. In the last month, two settlements have been announced in class actions where the plaintiffs alleged violations of BIPA in the U.S. District Court for the Northern District of Illinois. These settlements show that companies collecting biometrics should take care to ensure that their practices do not run afoul of BIPA's requirements.

What is BIPA?

A biometric identifier is a retina or iris scan, fingerprint, voiceprint or scan of the hand or face geometry. Biometric information is any information based on an individual's biometric identifier used to identify an individual. Notably, BIPA expressly excludes, among other things, photographs and information captured from a patient in a health care setting from its definition of a biometric identifier.

Under BIPA, a private entity cannot collect, capture, purchase, receive through trade or otherwise obtain a person's biometric identifier or biometric information without: (a) informing the subject in writing that a biometric identifier or biometric information is being collected or stored; (b) informing the subject in writing of the specific purpose and duration for which it is being collected, stored and used; and (c) receiving the subject's written consent. BIPA also requires that private entities that possess biometric identifiers or biometric information:

1. Develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers or biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied, or within three years of the individual's last interaction with the private entity, whichever occurs first;
2. Store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry and in a manner that is the same as or more protective than the manner

in which the private entity stores, transmits, and protects other confidential and sensitive information;

3. Not sell, lease, trade or otherwise profit from such identifiers or information; and
4. Not disclose or otherwise disseminate such information unless the subject of the identifier or information consents, the disclosure or redisclosure completes a financial transaction requested or authorized by the subject or the disclosure or redisclosure is required by law, valid warrant or subpoena.

Perhaps the most significant aspect of BIPA is that it provides a private right of action for individuals harmed by BIPA violations and statutory damages up to $1,000 for each negligent violation and up to $5,000 for each intentional or reckless violation. The statute itself does not contain a statute of limitations. In 2019, the Illinois Supreme Court ruled in *Rosenbach v. Six Flags*, that actual harm is not required to establish standing to sue under BIPA – a procedural violation is sufficient to support a private right of action.

Recent BIPA Cases

As noted, BIPA remains a fertile ground for litigation, in particular due to its private right of action. On February 18, 2021, the plaintiffs in a putative class action announced that they reached an undisclosed settlement-in-principle to resolve their claims against Shutterfly, Inc. ("Shutterfly") in the U.S. District Court for the Northern District of Illinois. The plaintiffs alleged Shutterfly stored their biometric data from its facial recognition technology without their consent, thereby violating BIPA. According to the plaintiffs, Shutterfly's technology scans people's faces in uploaded pictures, regardless of whether that person is a registered user of Shutterfly, and either suggests a user tag a previously identified individual or asks whether the user would like to name an unrecognized individual.

The following week, in the same district court, the popular video-sharing app TikTok reached a proposed $92 million settlement in a multi-district class action litigation in which the plaintiffs had alleged TikTok collected, captured, obtained, stored and disclosed users' facial geometric scans without users' consent. The settlement will provide compensation for TikTok users and ensure it respects users' privacy.

Implications

In determining whether BIPA applies to its operations, a company should consider whether it actively targets consumers for collection of biometric data, or merely provides the technology for the collection of such data to another party. In Corey Heard v. Becton, Dickinson & Co., for instance, the court held that BIPA did not apply to the defendant, a manufacturer of an automated medication dispensing system, because it did not directly collect biometric information. If BIPA does apply, the company should immediately comply with the statute's five requirements described above, which includes providing notice, obtaining written consent and following BIPA's security requirements.

Remember – suits under BIPA have been filed in many jurisdictions outside of Illinois, as was the case in H.K. et al. v. Google LLC. Moreover, a company whose principal place of business is not in Illinois may still be subject to BIPA if it has sufficient contacts with the state to establish personal jurisdiction.

Due to the COVID-19 pandemic, many employers and schools have turned to remote work and learning, and some use facial recognition or other forms of biometric information as a contactless way to track employees' time or ensure secure access to information or buildings. Companies using this technology in particular may want to consider their possible obligations under BIPA.

Watch this space for further developments on BIPA litigation.

View Original

Related Professionals

- **Julia D. Alonzo**
  Litigation Legal Director and Head of Women's Initiatives
- **Brooke G. Gottlieb**
  Associate