CYBERSECURITY AND DATA PRIVACY
INFORMATION MEMO
DECEMBER 9, 2022

Illinois Appellate Court Imposes Strict Timeline for Retention and Destruction of Biometric Data

In *Mora v. J&M Plating, Inc.*, No. 2-21-0692, 2022 IL App (2d) 210692 (Ill. App. Ct. 2d Dist. Nov. 30, 2022), the Illinois Second District Court of Appeals held that Illinois' Biometric Information Privacy Act (BIPA or Act) requires private entities to publish written data retention and destruction policies simultaneously or prior to collecting biometric data. These policies must be made publicly available and can be added directly to an entity's webpage or existing privacy policy. This decision is significant because it establishes a timeline for when these policies must be in place and sends a clear warning that retroactive adoption of retention and destruction schedules violates BIPA. Enacted in 2008, BIPA has been enforced against private entities incorporated outside of Illinois, indicating that this decision may have a national impact on businesses that collect, capture or receive biometric data belonging to Illinois residents—regardless of whether residents are located within the state at the time of collection.

In 2014, defendant, J&M Plating, began collecting and retaining employee fingerprints for time-keeping purposes, including the fingerprints of plaintiff, Trinidad Mora. Nearly four years later, J&M Plating developed and published written retention and destruction policies for the fingerprint data pursuant to BIPA requirements. Mora's employment was later terminated in 2021 and his biometric data was destroyed in accordance with the 2018 policies.

Mora commenced a putative class action against his former employer alleging that J&M Plating violated BIPA by collecting his fingerprints prior to developing retention and destruction policies. J&M Plating moved for summary judgment, arguing that BIPA did not contain any language mandating specific timing requirements for adopting these policies. Further, J&M Plating asserted that Mora was unharmed by this delay, as Mora's data was properly destroyed two weeks following his termination. The trial court granted J&M Plating's motion, but the appellate court reversed the decision. The Second District Appellate Court reasoned that publishing policies post-collection is inconsistent with the Act's "preventative and deterrent purposes."

Retroactive policy creation prevents individuals from learning what will happen to their data before deciding whether to consent to biometric data collection, which defeats the Act's notification function. Notably, the Appellate Court's decision effectively introduces a strict liability standard to BIPA litigation, allowing a litigant to bring a claim without a showing of actual harm. While this is a welcome development for plaintiffs, private entities must now exercise caution when collecting biometric data and ensure that compliant policies are in place before collection.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters, including the development of internal data use policies. If you have any questions about BIPA compliance or data destruction schedules, please contact Jessica Copeland, CIPP/US, Mario Ayoub or any attorney in Bond's cybersecurity and data privacy practice.

BOND SCHOENECK & KING ATTORNEYS