KPMG Biometric Information Privacy Act (BIPA) services

In February 2023, the Illinois Supreme Court filed its opinion regarding the case of *Latrina Cothron v. White Castle System, Inc.* stating "a separate claim for damages can arise each time a business fails to seek permission to gather biometric data from workers or consumers or fails to disclose retention plans for that information."[1] This case will likely lead to an influx of litigation, and companies must be prepared to respond and mitigate risks surrounding claims.

What is the Biometric Information Privacy Act?

The Biometric Information Privacy Act[2] (BIPA), which was passed in 2008, is an Illinois legislation that aims to "ensure that individuals are in control of their own biometric data." Biometric data includes retina or iris scans, fingerprints, voiceprints, hand scans, facial geometry, DNA, and other unique biological information.

The BIPA created a standard for how companies in Illinois should handle biometric information. It does not allow for a company to sell or profit from the access to employee biometric information. Companies are prohibited from collecting biometric information unless they:

- Inform the person, in writing, of what data is being collected or stored
- Inform the person of the specific purpose and length of time for which the data will be collected, stored, and used
- Obtain the person's written consent.[3]

With a five-year statute of limitations, BIPA states that unintentional violators could be fined $1,000 or actual damages, whichever is greater. Intentional violators could be fined $5,000 or actual damages, whichever is greater.

Impact to companies

Illinois businesses have become entangled in BIPA litigation—leaving them with the option of settling or facing expensive litigation. This new ruling makes it easier for individuals to sue businesses for violating biometric privacy rights. Individuals can sue for each instance of a violation – meaning businesses could face significant financial penalties for even a small oversight in compliance.

KPMG BIPA services

KPMG offers a wide array of BIPA services to help our clients mitigate and respond to BIPA violation claims. KPMG BIPA services are modeled after the industry-recognized Electronic Discovery Reference Model (EDRM) framework. These services are supported by the KPMG global organization of member firms that includes 750 experienced forensic technology professionals who work in the computer forensics, cyber, privacy, and eDiscovery fields.

[1] Source: Bloomberg Law, 2023
[2] Source: Illinois General Assembly, 2008
[3] ACLU of Illinois, 2023

Phase	Example services
Governance	• Map the workflow around the collection, retention, and transmittal of biometric data. • Review consent tracking workflows. • Confirm retention and availability of required records needed to respond to litigation. • Review the opt-out process. • Assess third parties (e.g., data handling, security, profiting/selling of data, etc.).
Identification	• Perform interviews and technical collections to identify systems capturing biometric information, underlying data captured, data and log retention, log export formats, etc. • Perform specialized data mapping for third-party systems storing biometric data. These systems can range from timecard systems, fingerprint or retina scanners, photo or video recording and storage systems, and other technology used for authentication purposes. • Map biometric data transmittal pathways.
Preservation and collection	• Develop defensible preservation and collection protocols for capturing available biometric data logs. • Assist company with developing in-house preservation and collection processes. • Assist with the extraction or export of data from systems using biometric data.
Processing	• Normalize, convert, or process collected artifacts and logs into a format more suitable for review and analysis. • Leverage a dedicated processing team and industry-leading data processing tools. • Capture and report processing statistics and exceptions.
Analysis and review	• Forensically analyze logs and other artifacts to help determine answers to questions including, but not limited to: – Which employees or customers were impacted with alleged BIPA violations? – How many times was an individual's biometric data captured? – How many times was the captured data transmitted to another party? – When did those transmittals take place and to whom?
Reporting and productions	• Provide fact-based affidavits, declarations, and/or courtroom testimony, etc. from a KPMG digital forensic subject matter professional (SMP) outlining the identification, preservation, collection, and analysis methodology and findings. • Create eDiscovery productions, if necessary, to opposing parties using industry-recognized production formats or using agreed-upon production specifications.
Expert witness testimony	• Provide expert witness testimony.

About KPMG Cyber Threat Management

KPMG has over 20 years of experience supporting its clients with litigation, investigations, and regulatory requests, providing a range of eDiscovery services, and implementing large-scale tools for a wide range of matters. We are committed to providing the highest level of support to our clients with a focus on leveraging our eDiscovery and extensive analytics experience to help get to key facts and drive substantive outcomes.

The KPMG digital forensics lab, located in Chicago, is home to more than 30 digital forensic professionals with experience imaging devices and analyzing forensic data using industry-recognized and custom-made forensic tools. KPMG LLP was granted a patent by the United States Patent and Trademark Office for KPMG Digital Responder (KDR), a solution enabling rapid response, forensic collection, and reporting capabilities.

KPMG LLP is the US member firm of KPMG International. KPMG has over 3,200 professionals dedicated to delivering cybersecurity services around the world, with over 25,000 additional risk-focused consultants (with a variety of backgrounds—including IT, regulatory, and forensic) available to support our clients' needs. Our professionals are experienced in identifying, preserving, collecting, and analyzing electronically stored information (ESI) so that it can be presented in court.

Contact us

David Nides
Principal, Cyber Security Services
T: 651-338-3809
E: dnides@kpmg.com

Jonathan Fairtlough
Principal, Cyber Security Services
T: 213-598-4181
E: jfairtlough@kpmg.com

Anthony DeSarro
Director, Cyber Security Services
T: 678-575-7119
E: adesarro@kpmg.com

Dennis Labossiere
Manager, Cyber Security Services
T: 401-465-6593
E: dlabossiere@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia