U.S. Risk, LLC

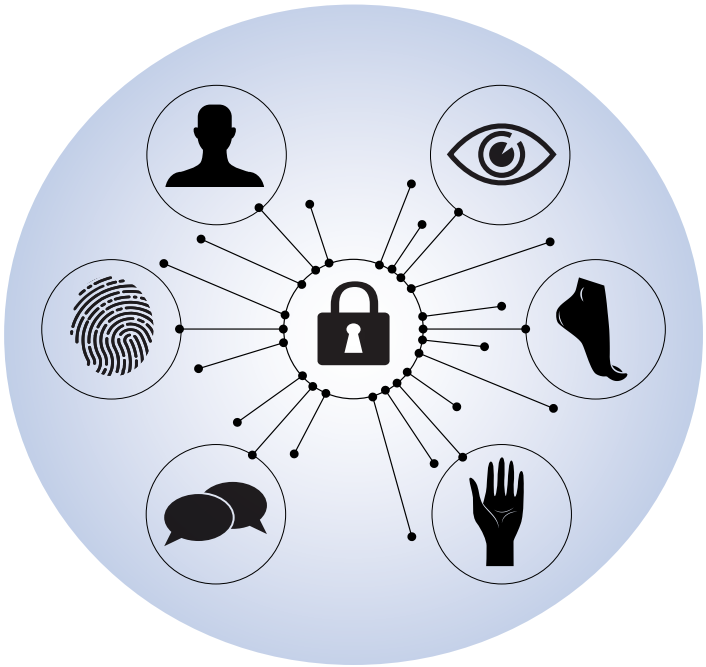
THE NEWEST ISSUE IN PRIVACY: BIOMETRIC LAWS

As the gavel rang down on the first jury verdict in a case involving Illinois' Biometric Privacy Act (BIPA), a flood of legal cases and new biometric laws began. A whirlwind of class action litigation has begun against employers, consumer businesses and technology companies with claims of violating biometric privacy rights. Biometric laws can impact both cyber and employment practices liability (EPL) coverage, so businesses need to be aware of their obligations as non-compliance can create significant exposure.

BIOMETRIC PRIVACY LAWS

The use of biometric data is a complex issue involving security, privacy, and consent that has been, until recently, largely unregulated. Biometric privacy laws generally require businesses to track, inform employees or consumers of, and provide methods for employees or consumers to consent to the collection of biometric information or biometric identifiers. Organizations typically must provide notice, obtain written consent and make certain disclosures before they can collect, use or store biometric data.

In the BNSF Railway case mentioned above, they were charged with requiring biometric identifiers in the form of fingerprints and biometric information. The jury verdict was significant because the railroad was held liable even though they had a vendor actually doing the collection and processing of the personal information.



› Biometric Information

Biometric Information typically relates to data or information related to:

- body measurements
- calculations related to human characteristics
- any other information defined as biometric information under a Federal or state law or statute cited as part of a claim.

Biometric Information includes, but is not limited to, data or information related to fingerprints, iris (eye) scans, voice recognition, facial or other physiological recognition or an individual's DNA. "Soft" biometrics are traits that are physical, behavioral or other identifiable characters but aren't as distinctive or permanent, such as hair color or height.

› Sample Policy Exclusion Endorsement Language

There are numerous fine points that should be carefully considered when applying a policy exclusion:

Sample employment practices exclusion language:

- based upon, arising from or in consequence of involving the actual or alleged violation of any federal, state, or local statutory biometric privacy law or any such similar common law anywhere in the world, that govern or relate to the collection, use, safeguarding, handling, storage, retention, or destruction of biometric information, provided that this exclusion does not apply to any employment claim alleging Retaliation, whether actual or constructive, with respects to a claimants exercise of a right pursuant to any such laws.

Sample cyber, wrongful collection, web tracking language:

- the insurer shall not be liable to defend, pay, indemnify or reimburse an insured with respect to any claim based upon, resulting from arising out of, in consequence of, or in any way connected with or involving, directly or indirectly, the collection or storage of biometric information.
- any claim based upon, resulting from, arising out of, in consequence of, or in any way connected with or involving, directly or indirectly the wrongful collection or wrongful use of protected information by or on behalf of an insured entity that is in violation of a privacy law.
- the actual or alleged use of a web beacon, a tracking pixel or other software tool to collect, track, report or monitor an individual's activity, behavior or other information; however this exclusion will not apply to an otherwise covered loss arising out of the theft or loss by the insured entity of protected information in the care, custody or control of the insured entity.

U.S. Risk, LLC

THE NEWEST ISSUE IN PRIVACY: BIOMETRIC LAWS

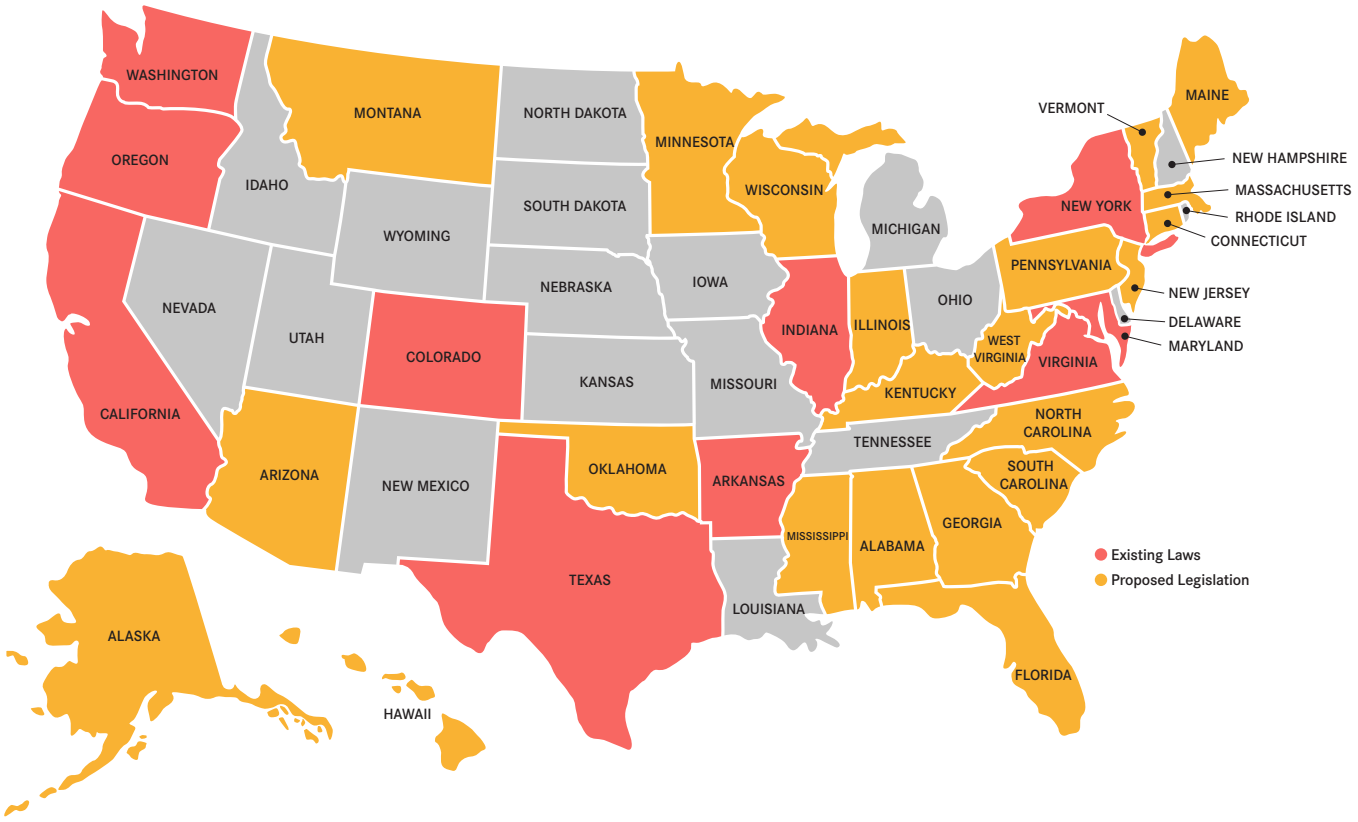
THE FUTURE OF LITIGATION

Predictions are that policies will become much more specific as far as exclusions for biometric-related privacy information is concerned with facial recognition a popular target for class action suits.

As federal lawmakers have not yet enacted nationwide, uniform privacy regulatory guidelines, new waves of state and municipal level biometric privacy laws are growing. Companies should expect more local laws, and a continuation of lawmakers transitioning away from administrative enforcement and towards private rights of action as the main enforcement for new biometrics laws, exposing businesses to significant class action litigation risks. There will also be an increase in policing of facial biometrics by the FTC as they have made it clear this is one of their top priorities.

BIOMETRIC LAWS AND BILL BY STATE

Laws regarding biometrics have been handled for the most part on a state by state basis. Ten states currently have biometrics laws in place, with the majority of the remaining states with legislation proposed and/or under consideration.



THE BOTTOM LINE

Biometrics litigation and liability exposure will continue to increase and even the most diligent organization can be susceptible to a claim. A trusted expert highly experienced in EPL and cyber policy wording and how to customize policy terms needs to be brought into the process as early as possible to help clients assess their exposure in this fast-changing arena and ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.

U.S. Risk, LLC

THE NEWEST ISSUE IN PRIVACY: BIOMETRIC LAWS

While many states already have or are considering a wide range of privacy laws, biometrics have sharply come into focus. The following is a general overview to many of the laws several states have already put into place that affect businesses as well as proposals under review.

STATE	STATUTE/PROPOSED LAW	OVERVIEW
Alabama	*Consumer Privacy Act*	*Would require certain disclosures about the information it collects and has collected and the purposes for which that information is used.*
Arkansas	**Personal Information Protection Act**	**Requires reasonable steps be taken to destroy or arrange to have destroyed a customer's records containing personal information as well as implementation and maintenance of reasonable security practices and procedures.**
Alaska	*Consumer Data Privacy Act*	*Would require consumers be notified before having their personal information collected.*
	Personal Information Use and Privacy Act	*Would require consumers be notified before having their personal information collected. Would also give consumers the right to request this information be deleted.*
Arizona	*AZ H.B. 2729*	*Would amend a current law prohibiting the collection of personally identifiable data by changing the definition of sensitive information to include biometric information.*
	AZ H.B. 2865	*Would allow consumers to opt out of their personal data being sold to a third party.*
California	**California Consumer Privacy Act**	**Comprehensive data privacy statute that obligates the business to make disclosures regarding collection of biometric data.**
Colorado	**Consumer Protection Act**	**If personal identifying information including biometrics is maintained, owned or licensed, a written plan for disposal must be developed, and reasonable security protocols and practices must be implemented.**
	Colorado Privacy Act	**Gives consumers the right to request disclosure of the information a business collects, request deletion and opt out of the sale of the information.**
	CO H.B. 1244	*Would require an organization that collects, stores, or uses biometric identifiers of a Colorado consumer to provide the consumer with information about the identifiers collected, obtain consent, and have the ability to revoke consent.*
Connecticut	*CT S.B. 134*	*Would give consumers the right to request disclosure and deletion of information that a business collects and opt out of the sale of such information.*
	Connecticut Consumer Privacy Act	*Would establish a framework for controlling and processing personal data, responsibilities and privacy protection standards for data controllers and processors. It also would grant consumers the right to access, correct, delete and obtain a copy of their data and opt out of the processing of personal data for the purposes of targeted advertising.*
Florida	*Privacy Protection Act*	*Would allow consumers to opt out of their personal data being sold to a third party.*
	Consumer Data Privacy Act	*Would require certain business to maintain an online privacy policy that provides information regarding the personal information being collected. Would also grant consumers the right to access, correct, delete, and obtain a copy of personal data.*
Georgia	*Georgia Computer Data Privacy Act*	*Would require certain businesses to disclose information regarding personal information collected about a consumer and give consumers the right to request deletion of personal information.*
Hawaii	*H.B. 2572*	*Would amend the requirements for handling consumer personal information for the purposes of security.*
	S.B. 2797/H.B. 2428	*Would establish a framework for controlling and processing personal data, responsibilities and privacy protection standards for data controllers and processors. It also would grant consumers the right to access, correct, delete and obtain a copy of their data and opt out of the processing of personal data for the purposes of targeted advertising.*

Items in bold are laws in place at the time of this writing and are subject to change.

Illinois	**Biometric Information Privacy Act**	**If a private entity possesses, captures, collects, obtains or discloses biometric information or identifiers, they may be required to provide a written policy, establish a retention schedule and create guidelines for destroying biometric identifiers and biometric information. They must establish protection standard and inform subjects of the specific purposes and length of term for which biometric information is being collected, stored, or used. There must also be a written release to proceed with the collection or disclosure of the biometric information.**
	Biometric Specific BIPA Amendments	*H.B. 3414 would eliminate the "for each violation" language relating to recoverable damages.* *H.B. 3304/S.B. 2039 would repeal the BIPA in its entirety.* *H.B. 3112 would exclude timekeeping systems used by employers, making the BIPA solely enforceable by Illinois Attorney General, requiring a plaintiff show actual harm; allow for recovery of damages only for initial violation; and reduce the amount of liquidated damages recoverable.* *S.B. 300/HS.B. 559 would exclude from the definition of "biometric information" any "information that cannot be used to recreate original identifier," eliminating the public policy requirement, allowing for a cure period, and allowing only for recovery of actual damages.* *H.B. 1764 would give the Illinois Attorney General sole power to enforce BIPA in instances of actual harm and exempt employers.* *H.B. 560 would eliminate the "right of action" section and replace it with Department of Labor enforcement.* *S.B. 602 would exclude "information captured and converted to a mathematical representation" from the BIPA's definition of "biometric identifiers" and exclude "biometric time clocks" and "biometric locks" from the BIPA's responsibility.* *S.B. 1607/S.B. 3782 would exempt from the BIPA's oversight employers who collect, capture, obtain, or otherwise use biometric information for recording employee work hours, security purposes, facility access, or human resources purposes.* *H.B. 4569/S.B. 3413 would remove from the BIPA's purview health care employers.* *H.B. 4692/S.B. 3874 would exclude "information captured and converted to a mathematical representation" from the BIPA's definition of "biometric identifiers" and excluding "biometric time clocks" and "biometric locks.". It would also state that notice and consent is only required during an initial collection of biometric identifiers or information.* *H.B. 5396 would provide that entitlement to relief in actions brought by employees are as provided in the Illinois Workers' Compensation Act.*
	Consumer Privacy Act	*Would require a business to inform a consumer the categories of personal information to be collected and the purposes for which the personal information would be used.*
Indiana	*Consumer Privacy Act*	*Would require businesses to disclose information regarding personal information collected about a consumer and would give consumers the right to request deletion of personal information.*
Kentucky	*S.B. 278/S.B. 280/H.B. 32*	*Would require a private entity in possession of biometric identifiers or information develop a written policy, retention schedule and guidelines for permanently destroying biometric identifiers and information. Would also require informed written consent prior to collection.*
	S.B. 15	*Would establish a framework for controlling and processing personal data, responsibilities and privacy protection standards for data controllers and processors. It would grant consumers the right to access, correct, delete and obtain a copy of personal data and opt out of the processing of personal data for the purposes of targeted advertising.*

Items in bold are laws in place at the time of this writing and are subject to change.

Maine	*Consumer Privacy Act*	*Would require consumers be informed on the personal information being collected and give a consumer the rights to request that the business disclose the categories of personal information collected, request deletion and to opt out of their personal data being sold to a third party.*
Maryland	**Personal Information Protection Act**	**Requires a business to take reasonable steps to protect against unauthorized access to or use of personal information including requiring in contracts with that certain service providers will implement and maintain reasonable security procedures and practices.**
	Biometric Identifiers Privacy Act	*Would require a private entity in possession of biometric identifiers to develop a written policy and establish a retention schedule and guidelines for permanently destroying biometric identifiers.*
	Online Consumer Protection Act	*Would require businesses collecting a consumer's personal information to clearly and conspicuously provide notice to the consumer regarding the collection, use, and disclosure of the information collected. Consumers would have the right to request a copy or deletion of his/her personal information and to opt out of their personal data being sold to a third party.*
Massachusetts	*Information Privacy Act*	*Would require certain businesses to share an individual's personal information only with third-party entities that will agree to provide the same duties of care, loyalty, and confidentiality imposed by this Act.*
	Biometric Information Privacy Act	*Would require a private entity in possession of biometric identifiers or information develop a written policy, retention schedule and guidelines for permanently destroying biometric identifiers and information. Would also require informed written consent prior to collection.*
Minnesota	*Consumer Data Privacy Act*	*Would establish a framework for controlling and processing personal data, responsibilities and privacy protection standards for data controllers and processors. Consumers would have the right to access, correct, delete and obtain a copy of personal data and opt out of the processing of personal data for the purposes of targeted advertising.*
Mississippi	*Consumer Data Privacy Act*	*Would require a business that collects personal information about a consumer to disclose certain information and provide a consumer the right to request deletion, and opt out of sale, of personal information.*
Montana	*Online Personal Information Protection Act*	*Would require any business that owns a website or an online service that collects and maintains biometric information to post a privacy policy on its website.*
New Jersey	*N.J. A.B. 3625*	*Would require a private entity in possession of biometric identifiers or biometric information to develop a written policy and establish a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information. Would also require informed written consent prior to collection of biometric identifiers or biometric information.*
	Disclosure and Accountability Transparency Act	*Would establish a framework for controlling and processing personally identifiable information.*
New York	**Stop Hacks and Improve Electronic Data Security Act**	**Comprehensive data security statute that applies to biometric information.**
	NY LAB Law	**Prohibits employers from requiring a fingerprint from employees as a condition of securing employment or of continuing employment, unless as provided by other laws.**
	Biometric Privacy Act	*Would require a private entity in possession of biometric identifiers or biometric information develop a written policy, establish a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information and require informed written consent prior to collection of biometric identifiers or biometric information.*
	Privacy Act	*Would prohibit the use, processing, or transfer of personal data of consumers unless the consumer process express and documented consent. Companies would also need to disclose their methods of de-identifying personal data, place special safeguards around data sharing, and allow consumers to obtain the names of any with whom their information is shared. Creates a special account to fund a new office of privacy and data protection.*

Items in bold are laws in place at the time of this writing and are subject to change.

New York	*NY A.B. 488*	*Would prohibit biometric data from being used for marketing purposes.*
	NY S.B. 567/A.B. 3709	*Would provide consumers the right to request info about biometric data collected. Consumers would be allowed to opt out of their personal data being sold to a third party. It prohibits discrimination against individuals who direct that their personal information not be sold. Requires that there be a clear and conspicuous link on the business's website titled "Do Not Sell My Biometric Information."*
	It's Your Data Act	*Would classify as a misdemeanor the failure to obtain written consent before collecting, storing, or using biometric data and would provide for recovery of actual damages. Would also require a business that collects a consumer's personal information disclose certain information in an online privacy policy.*
	Digital Fairness Act	*Would require a covered entity in possession of biometric information to develop a written policy, establish a retention schedule and guidelines for permanently destroying biometric information. Would also require informed written consent prior to the collection, capture, purchase, or receipt through trade of an individual's biometric information.*
	NY S.B. 5879	*Would prohibit the use of biometric identifiers or biometric information for any advertising, marketing, promotion, or other activity that is intended to be used to influence business volume, sales, or market share or to evaluate the effectiveness of marketing practices or personnel.*
North Carolina	*Consumer Privacy Act*	*Would establish a framework for controlling and processing personal data, responsibilities and privacy protection standards for data controllers and processors, and grant consumers the right to access, correct, delete and obtain a copy of personal data and opt out of the processing of personal data for the purposes of targeted advertising.*
Oklahoma	*Computer Data Privacy Act*	*Would require informed written consent before data collection and would allow consumers to opt out of their personal data being sold to a third party. Also prohibits discrimination against individuals who choose to have their information deleted.*
	OK H.B. 1130	*Would require any business or website that operates an online business or website that collects a consumer's personal digital information or data to conspicuously post on its website homepage information regarding the information to be collected or disclosed.*
	Voice Recognition Privacy Act	*Would prohibit a person or entity from using a voice recognition feature without prominently informing the user about certain information relating to the voice recognition feature.*
	Computer Data Privacy Act of 2022	*Would require businesses to disclose to consumers certain information in the company's privacy policies and would allow consumers to opt out of their personal data being sold to a third party, request deletion of personal information, and prohibit discrimination against individuals who exercise rights under the statute.*
Oregon	**Portland City Code**	**Prohibits the use of facial recognition technologies in places of public accommodation by private entities within the boundaries of the City of Portland.**
Pennsylvania	*Consumer Data Privacy Act*	*Would provide consumers the right to request info about biometric information collected. They would be able to opt out of their personal data being sold to a third party and discrimination would be prohibited against individuals who exercise rights under the statute. Requires that there be a clear and conspicuous link on the business's website titled "Do Not Sell My Biometric Information."*
	Consumer Data Protection Act	*Would establish a framework for controlling and processing personal data, responsibilities and privacy protection standards for data controllers and processors, and grant consumers the right to access, correct, delete and obtain a copy of personal data plus opt out of the processing of personal data for the purposes of targeted advertising.*
South Carolina	*Biometric Data Privacy Act*	*Would require a business inform the consumer about the information being collected and used. Would also grant consumers the right to access, delete and obtain a copy of personal data. Requires that there be a clear and conspicuous notice with a reasonably full and complete description of the business's practice governing the processing of personally identifying information.*

Items in bold are laws in place at the time of this writing and are subject to change.

Texas	**Texas Business & Commercial Code**	**Requires that individuals be informed and consent before the capture of a biometric identifier and requires protecting the data from disclosure. Biometric identifiers must be destroyed within a reasonable time. Also prohibits a person in possession of a biometric identifier of an individual from selling, leasing, or otherwise disclosing the biometric identifier unless in certain circumstances.**
	TX H.B. 3741	*Would require businesses provide consumers the right to request info about biometric information collected, allows them to opt out of their personal data being sold to a third party and prohibits discrimination against individuals who exercise rights under the statute. Requires that there be a clear and conspicuous link on the business's website titled "Do Not Sell My Biometric Information."*
	TX S.B. 1952	*Would require a person who captures an individual's biometric identifier for a commercial purpose provide the individual with information on the type of technology used, the purpose or method for capturing or collecting the identifier, and the method for storing data related to the captured identifier.*
	TX H.B. 4164	*Would require certain businesses provide consumers the right to request info about or delete biometric information collected.*
Vermont	*VT H.B. 75*	*Would prohibit use of facial or voice recognition technology unless a consumer opts in. Would also require use of facial recognition technology to be disclosed on a clear, conspicuous, physical sign at the entrance of a building.*
Virginia	**Consumer Data Protection Act**	**Comprehensive data privacy statute that includes obligation to obtain consent prior to collection or use of biometric data.**
Washington	**Washington Rev. Code**	**Provides that a person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose.**
	WA S.B. 5104	*Would prohibit the operation, installation, or commissioning the operating of facial recognition technology in any place of public resort, accommodation, assemblage, or amusement.*
	WA H.B. 1433	*Would require a long-form and short-form privacy policy "persistently and conspicuously" available that provides notice regarding the personal information being processed, captured, used, or disclosed. Would also grant consumers the right to access, correct, delete, and obtain a copy of personal data.*
	Washington Privacy Act	*Would prohibit the processing of "sensitive data" concerning a consumer without consent.*
West Virginia	*Biometric Information Privacy Act*	*Would require a written policy,retention schedule and guidelines for permanently destroying biometric identifiers and biometric information. Would also require informed written consent prior to collection of biometric identifiers or biometric information.*
Wisconsin	*WI A.B. 957*	*Would establish a framework for controlling and processing personally identifiable information.*

Items in bold are laws in place at the time of this writing and are subject to change.

PROPOSED FEDERAL LEGISLATION

Information Transparency & Personal Data Control Act	*Would require the Federal Trade Commission to disseminate regulations requiring that data controllers and processors make available to the public certain information regarding the collection, transmission, storage, processing, selling or sharing of sensitive personal information and obtain consent.*
Online Privacy Act of 2021	*Would require a reasonable mechanism by which an individual can access the categories of personal information and contents of communications about the individual and obtain information about the purpose for collecting, processing, or disclosing of personal information. Would establish a framework for controlling and processing personal data. Would also establish the Digital Privacy Agency.*
Consumer Online Privacy Rights Act	*Would grant consumers the right to access, correct, delete and obtain a copy of covered data and would impose requirements for data security practices on covered entities. Also includes provisions regarding civil rights and whistleblower protection.*

THE BOTTOM LINE

Biometrics litigation and liability exposure will continue to increase and even the most diligent organization can be susceptible to a claim. A trusted expert highly experienced in EPL and cyber policy wording and how to customize policy terms needs to be brought into the process as early as possible to help clients assess their exposure in this fast-changing arena and ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.