Biometric Data: Privacy, Cybersecurity & Insurance Considerations

October 2020

LOCKTON®

AUTHORS

Maryam Rad
VP, Insurance & Claims Counsel
mrad@lockton.com
213.689.0504

Tim Smit
CIPP/US, CISSP
Global Privacy &
Cyber Risk Consulting Leader
timothy.smit@lockton.com
303.414 .6011

Riley Brant
Account Manager
riley.brant@lockton.com
312.669.6887

Mary Smigielski
Co-Chair of Illinois Biometric
Information Privacy Act Group
Lewis Brisbois
Mary.Smigielski@lewisbrisbois.com
312.463.3377

Data is often considered the most valuable asset in the world.

As the world becomes more digitally connected and as technology advances, gathering, using and storing biometric data will continue to present unique privacy and cybersecurity challenges.

Some of these include:

01 Understanding the distinctive risks associated with collecting, utilizing and retaining such information

02 Legal compliance obligations under biometric information and privacy protection laws and regulations

03 Loss control and prevention measures necessary to protect the information

04 Implementing appropriate insurance risk transfer mechanisms

Understanding the risk

There are a variety of definitions for biometric information, but essentially it is the unique biological and/or behavioral characteristics that can identify an individual. In other words, "a measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity including facial images, fingerprints, and iris scan samples."[1]

Many organizations utilize biometric data for authentication purposes, e.g., fingerprint to record working hours, facial recognition to enter secure premises, and voice recognition for phone banking. Accuracy and reliability of the technology present one set of risk considerations for organizations. In December 2019, the National Institute of Standards and Technology (NIST) published the third part to its Face Recognition Vendor Test and found "empirical evidence for the existence of demographic differentials in the majority of contemporary face recognition algorithms ..."[2] Additionally, there can also be issues related to discrimination if error rates significantly vary across demographics (e.g., race, national origin, age and gender). It is clear that further research and development are necessary regarding the various biometric modalities.[3] Organizations that employ biometric authentication technologies should be mindful of the associated dependability and accuracy risks.

Potential liability from compromised biometric data and regulatory enforcement related to the use, collection and storage of biometric data are significant concerns for organizations utilizing these technologies. Back in 2015, the Office of Personnel Management issued a statement that up to 5.6 million individuals' fingerprints may have been compromised by a breach.[4] That incident resulted in litigation, which still continues, being filed by those affected by the breach.[5] In May 2020, the American Civil Liberties Union filed suit against a technology company offering facial recognition software for use by organizations, including private companies and law enforcement. The lawsuit "seeks to remedy an extraordinary and unprecedented violation of Illinois residents' privacy rights..."[6]

Given the various potential risk sources associated with biometric data, it is important to understand the extent to which an organization collects, uses and/or stores that data and what technologies are being used in connection with the data to properly assess potential exposures and compliance obligations.

Regulatory & compliance considerations

Illinois Biometric Information Privacy Act (BIPA)

IN 2008, ILLINOIS BECAME THE FIRST STATE TO ENACT A LAW SPECIFICALLY PROTECTING BIOMETRIC DATA. BIPA is considered the most stringent and litigated biometric privacy law in the United States and is the only one that creates a private right of action. To that end, over 400 BIPA class action lawsuits have been filed in the past five years. Most BIPA lawsuits arise in the employment context through time clocks, building security, corporate computer access, duo authentication, safes and lockboxes, and facial temperature scans. Other BIPA lawsuits are based on point-of-sale systems, schoolchildren paying for lunch, or social media scanning of users' pictures, such as Facebook's Tag Suggestions tool.

BIPA was enacted after a company offering a biometric authentication application that was tested in Illinois and allowed consumers to pay by touching a finger to a reader at a convenience store or other business went into bankruptcy. The biometric data collected by the company was considered an asset in the bankruptcy, prompting the Illinois legislature to take note. There were significant concerns about what would ultimately happen to the biometric data. In passing the statute, the legislature stated, "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, Social Security numbers, when compromised, can be changed."[7] BIPA regulates the collection and use of "Biometric Identifiers" and "Biometric Information." BIPA protects biometric identifiers, which is limited to a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, and specifies many things that are not biometric identifiers and thus not covered by BIPA, including writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color and more. Biometric information, defined 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, is also protected by BIPA. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

BIPA requires private entities doing business in Illinois to comply with several requirements pertaining to the collection and storage of biometric information, including obtaining prior written consent for the collection, use and storage of biometric data; securely storing such data; and having a public written policy regarding the retention and destruction of biometric data. The law imposes hefty penalties for each violation: $1,000 for each negligent violation and $5,000 for each reckless or intentional violation plus attorney's fees.

BIPA went largely unnoticed when it was passed, and many companies were unaware of BIPA's requirements. Others were aware of BIPA's requirements but determined that the technology they used did not collect biometric identifiers under the statute and thus did not obtain consent.

There are many concerns for organizations required to comply with BIPA, including:

- BIPA does not provide for a statute of limitations. However, most courts have been applying a five-year statute of limitations.
- The courts have not decided what counts as a violation. Some contend that anytime someone touched a biometric machine, it counts as a violation (e.g., if a biometric time clock was used, an employee would typically use a clock four times per day [clock in for work, out for lunch, in after lunch, out at the end of the day]). If this theory were accepted and reckless/intentional violations were found, penalties could amount to $20,000 per day per employee.
- There are open questions regarding BIPA's application outside of Illinois.

Although the business community has lobbied for change to BIPA due to the impact on Illinois businesses, proposed amendments to BIPA in 2016, 2018, 2019 and 2020 did not gain traction, and organizations to which the law applies should be mindful and cognizant of their compliance obligations.

Other jurisdictions with biometric privacy regulations

MANY OTHER JURISDICTIONS HAVE ENACTED SPECIFIC BIOMETRIC DATA PROTECTION LAWS.

Each jurisdiction's laws are nuanced, but their objective remains the same: protecting individual's rights to their own unique biological and/or behavioral characteristics. States with specific biometric data protections regulations include Arkansas, Arizona, California, Louisiana, New York, Oregon, Texas and Washington. While other states may not have specific biometric information protection laws, biometric information may still be protected by other privacy regulations or common law. Several states have considered or have pending legislation to regulate biometrics, including laws that would create a private right of action.

There is no U.S. federal biometric data protection law; however, in August 2020, the National Biometric Information Privacy Act was introduced in the United States Senate. It contains three key elements: (1) Consent is required prior to collecting or disclosing biometric identifiers and information; (2) A private right of action against covered entities that violate the law and which allow aggrieved individuals to recovery, among other relief, the greater of $1,000 liquidated damages or actual damages; and (3) An obligation to safeguard biometric identifiers or information similar to how the organization safeguards other confidential and sensitive information such as Social Security numbers.[8]

Under the European Union's General Data Protection Regulation, biometric information is considered protected information and subject to the data privacy law. The data protection authorities enforcing GDPR take violations of biometric data protections very seriously. For example, a school in Sweden was fined approximately $23,000 (200,000 kr) for using facial recognition technology to monitor attendance of 22 secondary school students during a three-week period.[9]

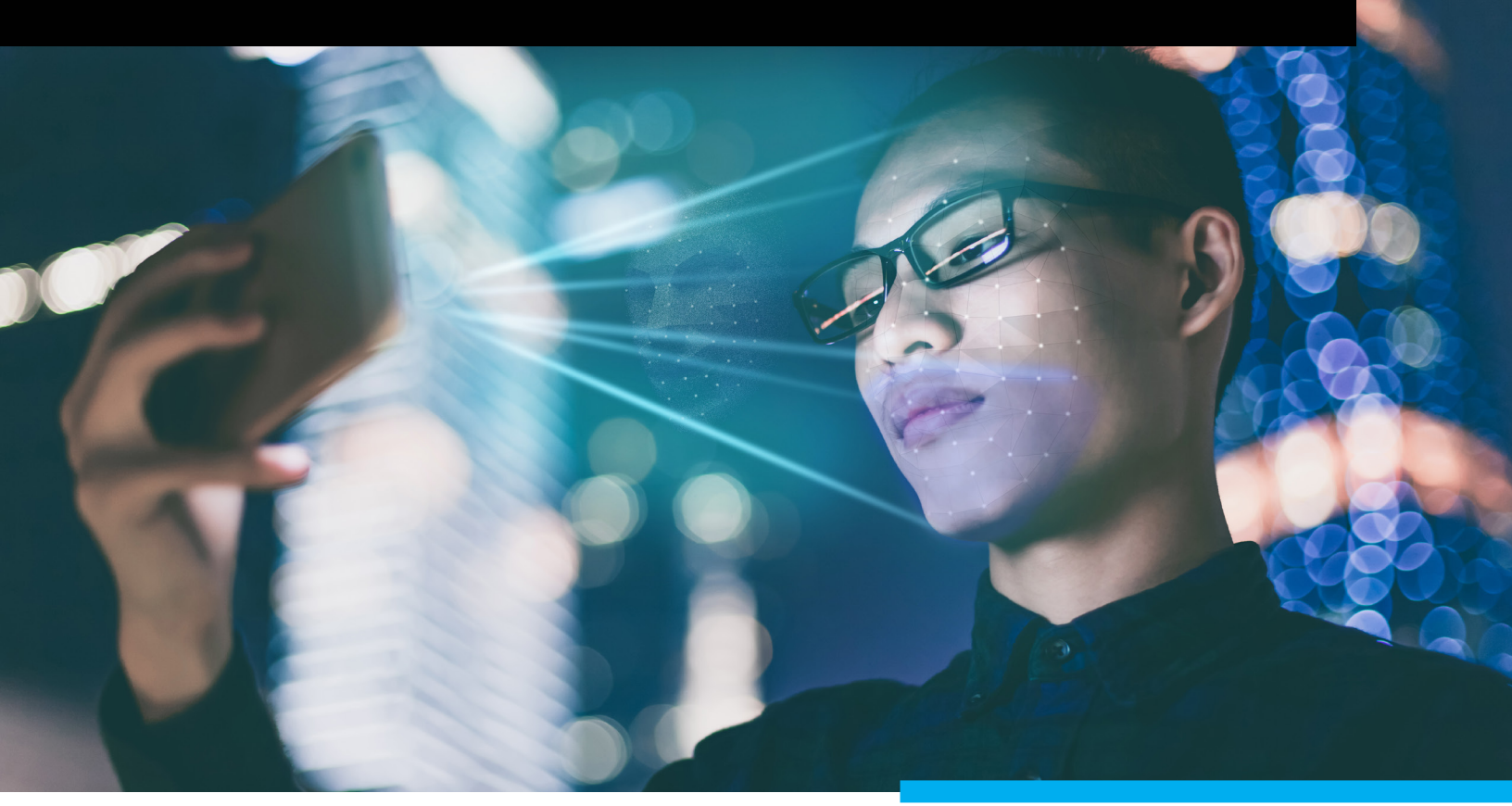
Given the multiple layers of potential compliance obligations, organizations must fully assess their legal compliance obligations at the local, state, federal and international levels.

Information security considerations to reduce risks

Those organizations that presently gather, use and/or store biometric information (and those that may be considering doing so) should continually evaluate their privacy protection programs and compliance obligations given a growing landscape of laws across the United States and globally.

In this regard, organizations should consider as part of their information security practices, implementing the following:

- Data mapping exercise(s)
- Information classification policies and protocols
- Information life cycle review (internally and externally)
- Overlaying information security controls based on information classification
- Developing a regulatory map and conducting gap analysis annually
- Identifying breach/privacy counsel
- Creating an Incident Response Program
- Conducting table-top exercise(s)
- A Security Education, Awareness, and Training (SEAT) program for all workforce members
- Data retention and destruction policies
- Onboarding to cyber insurer's cyber portal for more proactive risk tools (if purchased/available)



Insurance implications

A GOOD CYBER POLICY WILL PROVIDE COVERAGE FOR BIOMETRIC DATA PRIVACY VIOLATIONS. These policies are designed to provide first-party and liability coverages. In a breach of biometric information, a robust cyber policy will cover an organization's expenses related to the investigation, remediation and mitigation of the data breach as well as various expenses and damages arising from liability claims brought against an organization under BIPA and other laws. Additionally, biometric privacy protection regulations in other jurisdictions confer enforcement power on regulators, granting them the authority to impose fines and penalties for privacy violations. A properly structured cyber insurance program should account for risks and potential exposures in the courts as well as through regulators.

Liability claims by employees alleging privacy violation claims in connection with biometric data may trigger an employment practices liability policy depending on the policy's definition of "employment practices wrongful act." Some policies may only extend coverage if the alleged biometric data violations are linked to a traditionally covered "employment practices wrongful act," e.g., discrimination, retaliation, wrongful termination. Given the magnitude of these claims, some employment practices liability insurers are now including specific BIPA and/or privacy violation exclusions on their policies.

Depending on how the claims against the organization are framed, they may also implicate the management liability policy. Coverage depends on whether allegations are made concerning improper management decisions related to the collection, use and storage of biometric data. However, management liability policies often contain bodily injury and/or invasion of privacy exclusion, which may preclude coverage for such a lawsuit.

Finally, it is possible that some general liability insurance policies could also apply to a BIPA and/or other biometric privacy violation liability claims. General liability policies typically provide coverage for "personal injury" offenses, including the oral or written publication of material that violates a person's right of privacy. If there is an allegation that biometric information has been shared with third parties, i.e., published, a general liability policy potentially could afford coverage. However, general liability insurers increasingly are adding exclusions for loss resulting from cyber events. Even in the absence of such exclusions, general liability insurers strenuously resist covering cyber losses.

Considering the multiple insurance implications, it is critical to ensure insurance programs are designed specifically to address the unique and individual risks of the organization's collection, use and storage of biometric data.

While this paper discusses legal and regulatory issues and developments, it is not, and is not intended to be, legal advice.

SOURCES

[1] https://csrc.nist.gov/glossary/term/Biometrics

[2] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[3] https://www.nist.gov/news-events/news/2019/12/nist-releases-data-help-measure-accuracy-biometric-identification

[4] https://www.opm.gov/news/releases/2015/09/cyber-statement-923/

[5] See, *In Re: U.S. Office of Personnel Management Data Security Breach Litigation,* United States District Court, D.C. Case No. 15-1394 (ABJ), MDL Docket No. 2664

[6] https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint

[7] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004

[8] https://www.merkley.senate.gov/news/press-releases/merkley-sanders-introduce-legislation-to-put-strict-limits-on-corporate-use-of-facial-recognition-2020

[9] https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf

UNCOMMONLY INDEPENDENT

