Biometric Privacy

Why the floodgates are opening on biometric privacy claims.

DECEMBER 2023

Gallagher

Insights

1. **There are many reasons why organizations collect the biometric data of their staff and consumers**, including fingerprints and face scans. Thanks to modern technology, it's quick, convenient, and completely unique to the individual.

2. **However, a growing number of lawsuits are being filed against companies for poor management around the use of biometric data.** There are calls for more clarity and standardized procedures around collecting, storing, and using sensitive, personally identifiable physical and biological data sources.

3. Although it was enacted in 2008, the Biometric Information Privacy Act (BIPA) is gaining more attention due to the number of class actions it has unleashed in recent years. **Firms have fallen foul of the biometric data protection rules** by failing to obtain necessary permissions from individuals, and for transmitting their information to third parties without consent.

4. **Recent court decisions highlight the potential billion-dollar exposure that companies may face for negligent and reckless biometric data practices.** The widespread adoption of biometric technologies contributes to the heightened risk of litigation.

5. Inevitably, the rise in BIPA-related lawsuits has resulted in the introduction of new wordings within general liability, employment practices liability, D&O, and cyber insurance policies. **Carriers have a reduced appetite for risks with suspected BIPA exposures** and are actively introducing exclusions to protect against an increased frequency and severity of claims.

Why the floodgates are opening on biometric privacy claims

A decade ago, certain social media platforms were embracing the latest facial recognition technology for tagging photos and tracking users, largely without consent.

Then came the lawsuits. Today, most tech firms have dumped the technology, with Facebook owner Meta announcing it would be shutting down its facial recognition system in November 2021.[1]

There are many reasons why organizations collect the biometric data of their staff and consumers. Thanks to modern technology, it's quick, convenient, and completely unique to the individual.

From clocking in and clocking out to unlocking smartphones, accessing bank accounts, and passing through airports, fingerprints, eye retina, and face scans improve security and offer a seamless customer experience.

While this innovation provides a range of benefits and efficiencies, it also presents a raft of risk exposures for companies to grapple with. Key amongst these are laws dictating how biometric data should be collected, stored, used, and secured.

A number of US states are in the process of adopting the Biometric Information Privacy Act (BIPA), with the anticipation that we will see a steady rise in BIPA breach lawsuits. But even in parts of the world where the regulation is playing catch-up, there are important considerations to be made and best practices to follow.

2023: A year of landmark rulings

In December 2018, a plaintiff filed a class action lawsuit against her former employer. She claimed the fast-food franchise had collected and misused her biometric information without consent, by disclosing her fingerprint scans to a third-party vendor.

In February 2023, the Illinois Supreme Court imposed penalties, potentially amounting to $17 billion in damages, for violating Illinois' Biometric Information Privacy Act (BIPA).[2] According to this latest ruling, under the Act, each and every scan or transmission of the plaintiff's fingerprint data amounted to a separate violation.

The case followed fast on the heels on another Illinois Supreme Court ruling which determined that a five-year statute of limitations applies to all BIPA actions.[3]

The size of the most recent settlements and the move by a number of other US states to adopt BIPA legislation have significant implications for all businesses that collect and utilize biometric data. From big tech to healthcare, retail, and transportation, the net has been cast wide where potential BIPA infringements are concerned.

Although it was enacted in 2008, BIPA is gaining more attention due to the number of class actions it has unleashed in recent years and as more businesses deploy biometric security technology to obtain personally identifiable information. Firms have fallen foul of the biometric data protection rules by failing to obtain necessary permissions from individuals, and for transmitting their information to third parties without consent.

The emergence of a suite of biometric data protection laws can be attributed to the desire of regulators to protect individuals against potential misuse of their biometric data, especially considering advancements in technology that have made the collection and use of biometric data more prevalent. "The regulations aim to establish clear guidelines for the collection, storage, use, and sharing of biometric data," explains Haytham Zohny, Senior Vice President of US Casualty, Gallagher.

These fines can be massive, if it's calculated on a per-occurrence basis, in which case it really adds up. And that's why so many carriers are moving to exclude biometric liability in their policy wordings. There are a few different ways you could be covered for fines and lawsuits. In theory, you could be insured for a breach of biometric privacy under your cyber policy.

If a company breaches the privacy of its own employees by mishandling their biometric data, it could potentially lead to employment practices liability. And the company may even be held responsible for any privacy-related damages under its liability policies, where there is a privacy component, personal advertising injury, which could potentially be triggered.

—***Jessica Cullen,*** *Managing Director, US Casualty, Gallagher*

Notable biometric data protection lawsuits

- In 2018, Burlington Northern and Santa Fe Railway (BNSF) Railway, a major freight railroad network in the United States, was sued by a group of its truck drivers for collecting, storing, and using their fingerprint data without due consent. The transportation giant eventually settled in September 2023, after an initial jury award of $228M was overturned. Terms of the settlement were not disclosed.[4]
- It followed a record $650M settlement of a privacy lawsuit against Meta's Facebook in February 2021, under the Act, whereby the company was accused of using photo face-tagging and other biometric data without consent. In July, Meta reached another settlement for BIPA violations, this time via a class action lawsuit brought against Instagram. Other tech firms to reach settlements for alleged breaches under Illinois' BIPA regime include TikTok ($92M) and Google ($100M).[5]
- Most recently, in July 2023, a class action lawsuit was filed against the parent company of Twitter, X Corp., for alleged violations of BIPA, involving facial recognition on photographs uploaded onto the social media platform. Plaintiffs in the case are seeking damages of up to $5,000 per violation of BIPA, in addition to court costs and legal fees.[6]
- Lawsuits are not just being brought in Illinois. In 2022, Texas Attorney General Paxton activated a long-dormant state privacy law and filed lawsuits against Meta and Google, accusing the firms of collecting and misusing the facial and voice recognition data of millions of Texans over a period of several years.[7] The Texas law provides fines up to $25,000 per violation.

Spotlight

Biometric data: What is it?

Biometric data is difficult to mimic and manipulate, making it more accurate, reliable, and secure.[9] There are numerous advantages associated with biometric data. However, the threat of rapid cyber attacks,[10] data manipulation, and poor data management practices are prompting greater privacy concerns.

Physiological and behavioral information are the two main categories of biometric data.[8] Physiological data involves different body parts to identify and authenticate an individual, including:

- Fingerprint
- Face
- Iris
- Retina
- Voice
- Hand geometry
- Vein pattern

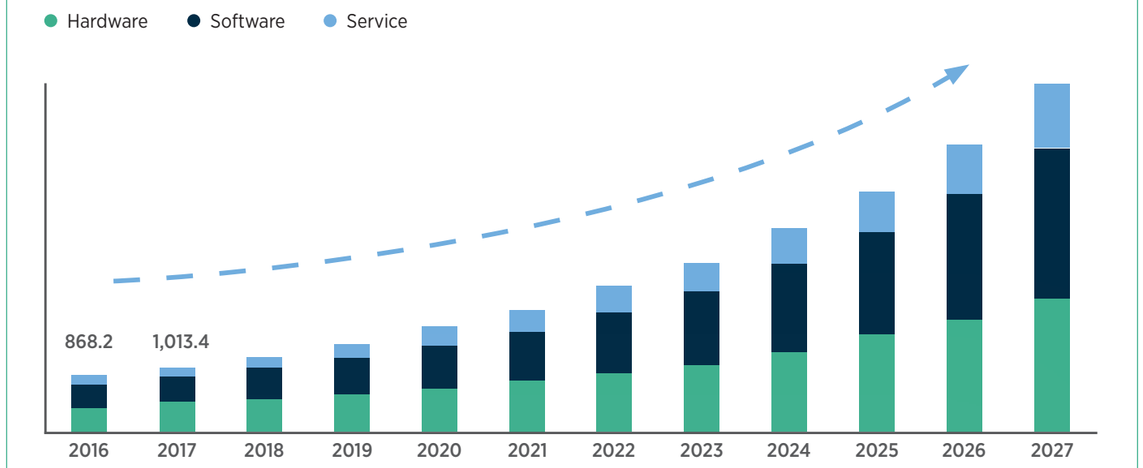
In terms of behavioral data, an individual's digital, physical, and cognitive behavior is used for identification and authentication. Examples of behavioral data include:

- Voice recognition
- Gait analysis
- Signature dynamics
- Mouse dynamics
- Keystroke dynamics

Exponential growth and adoption

Biometric data is unique. This fact alone, along with its ease of use, has led to widespread adoption. In 2022, the market for digital identity solutions, which includes biometric technology, was valued at $28 billion, and it is projected to surpass $70 billion by 2027.[11]

US contactless biometric technology market size, by component, 2016–2027[12]



Biometric data use cases

Identification and authentication are the two most common use cases for biometric data.

Employee verification
Clocking-in machines are one of the most popular and early-adoption use cases for biometric technology. They are being widely used for employee identification and verification within the financial services sector, government entities, universities, retail, and technology enterprises.

Customer recognition
Biometric data is useful for customer recognition because it provides a seamless and secure way to identify and authenticate customers. By using biometrics for customer recognition, businesses can ensure that only authorized individuals can access their services, reducing the risk of identity theft or fraud.

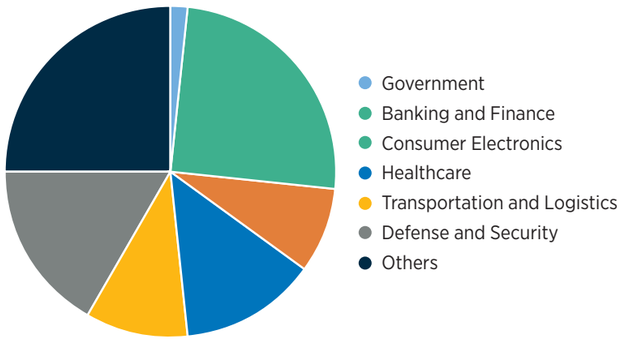
For example, the car-sharing service Drivy uses facial biometrics to verify drivers digitally.[13] Amazon is enabling contactless retail payments in supermarkets like Whole Foods, where the customers no longer need their wallets or even a phone to pay. They can hover their palm over an Amazon One device to make the payment.[14]

Smart device access
Accessing smart devices with fingerprints, face, iris, and voice commands has become commonplace, with use as part of multi-factor authentication. Biometrics are able to unlock devices faster than passwords for frequent operations.[15]

Criminal identification in law enforcement
Correctional facilities employ biometrics to identify and verify criminals. These methods help authorities enroll and confirm the identity of individuals within the penitentiary system. Correctional systems around Atlanta are in the process of biometric-driven in-prison surveillance system to track inmates by tracking their heartbeat and determining their location to precise levels.[16]

Government projects
Managing identification is a massive concern for governments.[17] Incorporating biometric data into national identity cards and digital passports brings citizens onto one platform and enables common services. It also helps to minimize fraudulent activities, but at the same time contains the sensitive data of millions of people. Countries have also issued biometric passports[18] to protect against identity theft and stop illegal entry into other countries.[19]

Industries with the biggest share of the global biometric technology market[20]



Towards multimodal authentication

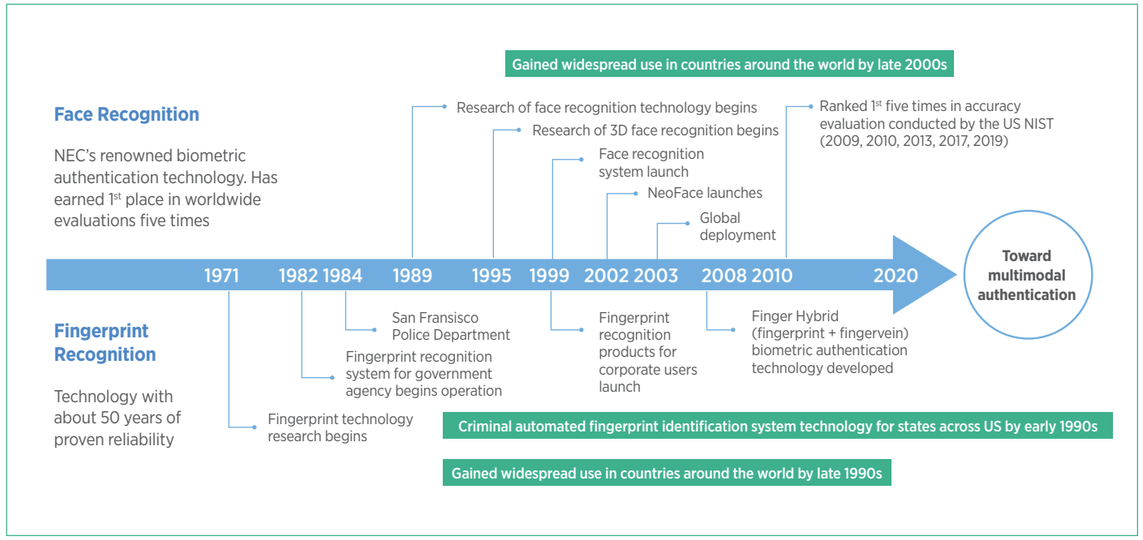
Biometric authentication has been introduced in an attempt to combat data manipulation and provide a convenient and secure digital identity. However, malicious practices have posed a challenge to the use of the technology.

Biometric data is lucrative to hackers who can exploit biometric datasets to plan more sophisticated attacks. Cybercriminals use a variety of attack methods, including spoofing and deepfake attacks to overcome biometric systems.

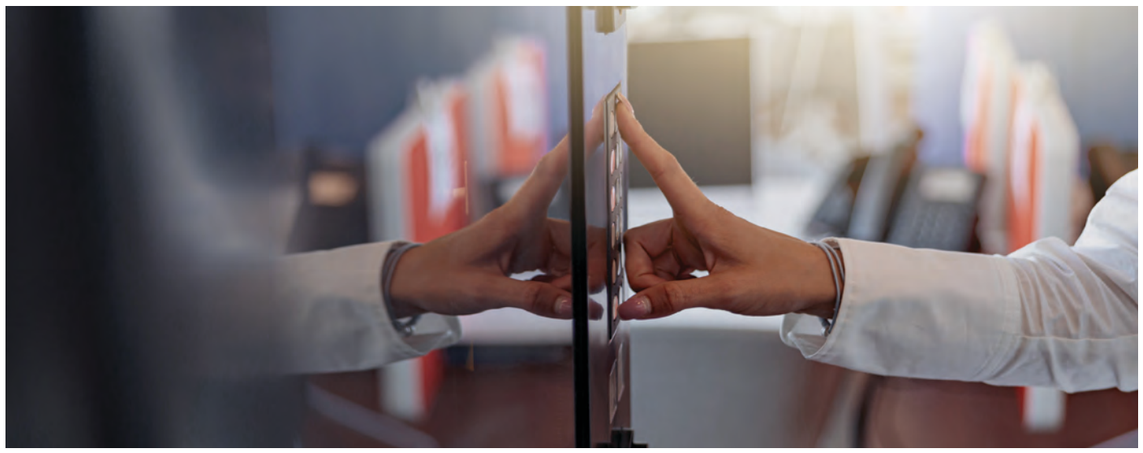
In 2015, hackers gained access to the systems of the US Office of Personnel Management (OPM), compromising the personal information, including fingerprints, of over 21 million individuals.[21]

As cyber risk grows, biometric technology is heading towards a multimodal approach whereby companies use multiple biometric traits for identification or authentication purposes.[22] In some of the latest advancements, biometric researchers are using brain and heart signals to increase the strength and security of their recognition systems.[23]

Past, present, and the future of biometric technology



Source: The history of biometrics, RecFaces.



Growing privacy concerns

Biometric systems collect huge amounts of user data to verify and authenticate identity. Biometric information is the most personal and sensitive data available. Since its inception, companies have had unrestricted access to the collection and use of biometric data, often without sharing sufficient information about their collection process and usage techniques.

But this is changing. In recent years, activists[24] and former employees have filed a number of lawsuits against companies for poor management around the use of biometric data. There are calls for more clarity and standardized procedures around collecting, storing, and using sensitive, personally identifiable physical and biological data sources.

Unlike passwords or personal identification numbers (PINs), biometric data is unique to the individual and cannot be replaced or modified. Once compromised, cyber attackers can exploit the data to impersonate biometric identifiers, such as fingerprints and facial characteristics, giving access to network and financial systems.

Cyber attackers use this technique to beat biometric authentication methods and gain access to valuable data. In March 2021, for instance, a criminal gang was able to dupe a Chinese government facial recognition system using manipulated personal information and high-definition photos bought on the Dark Web to fake tax invoices worth $76.2 million.[25]

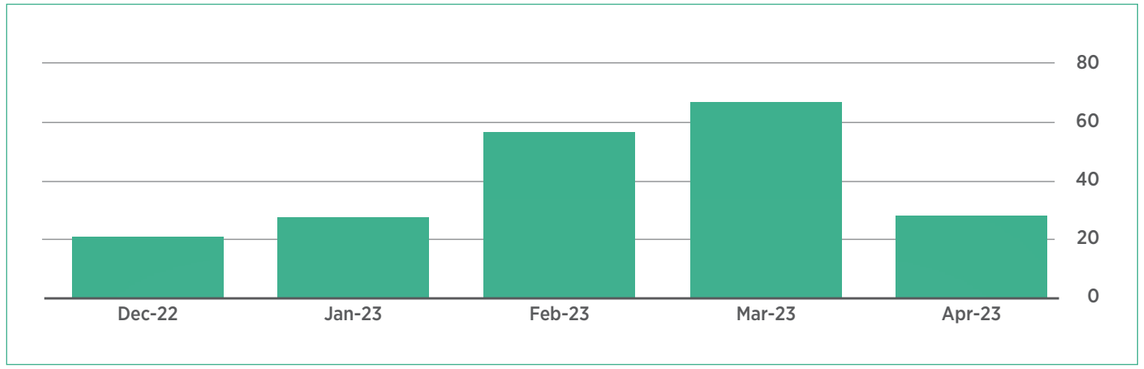
The ability to compromise personally identifiable information is one reason behind consumers' growing mistrust in sharing their biometric data with companies and authorities. According to a survey by Paysafe, 45% of consumers are not comfortable granting access to this information.[26] Among their concerns are that companies will sell the data for monetary gains, transfer it to third parties, or misuse it for tracking and profiling.

Using biometric data to carry out surveillance on citizens has emerged as one of the largest ongoing privacy concerns. In its latest policy statement, the Federal Trade Commission (FTC) warned businesses against the unfair and deceptive use of biometric data;[27] in particular, there is concern about using data to track consumers at specific locations and obtain sensitive personal information about their whereabouts and buying activities.

> In recent years, biometric surveillance has grown more sophisticated and pervasive, posing new threats to privacy and civil rights.
>
> — ***Samuel Levine,*** *Director of the FTC's Bureau of Consumer Protection*[28]

In the face of growing biometric use, increasing lawsuits, and hefty penalties, privacy is now the top priority for legislators and businesses. Illinois, Texas, and Washington have enacted the most comprehensive biometric laws to date. BIPA has emerged as the most stringent amongst these.

Number of BIPA lawsuits filed in Illinois circuit courts[32]



From December 17, 2022 to April 17, 2023
Source: Bloomberg Law analysis

What is the BIPA Act?

On October 3, 2008, the State of Illinois passed the Biometric Information Privacy Act (BIPA) to regulate the collection, use, and handling of information and safeguard citizens from risky practices.[29] The BIPA Act requires businesses operating in Illinois to comply with several requirements pertaining to collecting and storing biometric data.

It requires businesses that store biometric information to inform the subject in writing that the data is being collected or stored and the purpose and duration for which it is being collected. And it expects businesses to seek the subject's written consent.

Violations of BIPA incur penalties of $1,000 per violation for a negligent act and $5,000 if the violation is deemed to be intentional or reckless. BIPA is currently considered to be one of the US's most stringent privacy regulations, spawning several class action lawsuits for alleged infringements.[30] According to Reuters, 180 BIPA lawsuits were filed in Illinois during the first four months of 2023.[31]

Other biometric data protection laws in the US

Texas

In 2009, Texas enacted the Capture or Use of Biometric Identifier Act (CUBI)[33] to bar companies from capturing biometric identifiers for commercial purposes without prior notice or consent. According to the CUBI, selling or disclosing biometric identifiers is a penalized crime. Businesses in Texas are required to protect collected biometric data and delete it within a reasonable time frame.

Washington

In 2017, Washington enacted a biometric privacy law, H.B. 1493,[34] to safeguard its citizens from collecting biometric information without their consent. The law also prevents the use of biometric data for commercial purposes but does not include facial recognition data as a biometric identifier.

Growing commercial risk exposures

Recent court decisions highlight the potential billion-dollar exposure that companies may face for negligent and reckless biometric data practices. The widespread adoption of biometric technologies contributes to the heightened risk of litigation.

Employers should be particularly aware of their responsibilities. More than half of the 182 BIPA lawsuits to date involve the violation of BIPA regulations in the workplace, primarily around the collection and use of employees' fingerprints for timekeeping purposes.[35]

Meanwhile, consumer-facing companies, financial services, healthcare institutions, transport authorities, and high-tech companies are among the most frequent biometric data collectors. From virtual try-ons in fashion to financial transactions and identification verification, all transactions involving the capture of biometric information could become the focus of data privacy concerns.

Biometric lawsuits in the US are no longer limited to Illinois. In 2022, California, Kentucky, Maryland, and New York proposed standalone biometric laws with broad similarities to BIPA.[36] Several states, such as Virginia, Colorado, and Utah, have already passed new laws that have or will take effect in 2023,[37] and more are expected to follow this year. Businesses need to carefully plan their biometric data protection strategies considering the growing awareness of privacy infringements and the emergence of more stringent regulatory frameworks.

Understand the law
Businesses need proactive measures to understand the existing and emerging laws' definitions, requirements, and penalties.

Risk assessment
With the emergence of new biometric laws, businesses need to assess the risks associated with biometric data usage. In addition to that, compliance audits can ensure adherence to biometric data privacy laws.

Establish biometric policies
Having written policies documenting the collection, storage, and use of biometric data and gathering consent before collecting biometric information will help businesses avoid future legal challenges.

Establish security requirements
Under the BIPA Act and other biometric protection laws, businesses operating in specific states need to implement and maintain data security safeguards to protect biometric data from improper access, disclosure, or acquisition.

Train employees
Every data security initiative is a shared responsibility. Businesses must educate their employees on the importance of biometric information protection and provide training on data handling, security protocols, and privacy practices.

Companies' response to strengthening data protections should encompass a broader view of their business priorities and strategies. Businesses need to review their biometric data protection and privacy policies against the broader context of emerging regulations.

Adhering to biometric laws like the BIPA Act is not strictly a tech company problem; it spans all industries and business classes where they collect any identifiable information.

Unlike passwords, credit card numbers, or social security numbers, biometric identifiers, such as fingerprints, iris patterns, and voiceprints, are unique to each individual and cannot be altered or changed.

Cyber attacks can use these characteristics to commit fraud, impersonate identity, and carry out more severe attacks. And that's the primary concern surrounding the biometric information and implementation of the BIPA Act.

— ***Haytham Zohny,*** *Senior Vice President, US Casualty, Gallagher*

BIPA: The role of insurance

Inevitably, the rise in BIPA-related lawsuits has resulted in the introduction of new wordings within general liability, employment practices liability, D&O, and cyber insurance policies. Carriers have a reduced appetite for risks with suspected BIPA exposures and are actively introducing exclusions to protect against an increased frequency and severity of claims.

As part of the tripartite relationship, insurance brokers and carriers are there to assist businesses in understanding the evolving challenges and exposures associated with BIPA and other incoming biometric data protection regulations. In particular, they can advise clients on how to improve their policies and procedures around the collection, storage, and use of biometric data.

By adopting best practices and demonstrating compliance with BIPA and other data protection regulations, including GDPR, insurance buyers will both mitigate their exposures and better position themselves ahead of renewal discussions.

The BIPA Act is attracting attention due to large settlements resulting from violations of biometric privacy. This is where companies are found to have used face scans and fingerprints without the consent of employees and/or consumers.

To date, there have been a number of high-profile class action rulings, including settlements with users over the collection and storage of facial scans. Carriers are introducing wordings to protect them against the potential for privacy violation actions, by explicitly excluding BIPA actions or including cyber incident exclusions.

As we approach renewals, clients need to be prepared to answer tough and new underwriting questions relating to these emerging issues, and/or accept the introduction of mandatory exemptions.

— ***Jessica Cullen,*** *Managing Director, US Casualty, Gallagher*

Spotlight

Future trends in biometric data protection

More states enacting privacy legislation around the collection and handling of biometric information, and individuals are becoming more aware of their data protection rights. As a result, the number of BIPA lawsuits is expected to increase. These legal developments have implications for insurance policies and wordings, necessitating a careful evaluation and adjustment of coverage strategies.

Biometric technology has significant potential to deliver a convenient and secure customer experience. Businesses should seek to get ahead of the curve by committing to safe biometric data practices and a thorough understanding of the evolving risk landscape.

As industries continue to embrace new technologies, it is crucial for adopters to be mindful of both the risks and opportunities that the future of biometric technology offers. Risk and insurance managers should discuss potential exposures with their broker and insurer partners, take steps to mitigate these risks and stress test how their insurance policies might respond.

As our reliance on biometric technology grows, and as malicious actors find new and novel ways of compromising our unique biological markers for their own nefarious gains, the protections around this data must become more robust. The trust and reputation of brands depends on this.

Citations

1 https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/

2 Witley Skye, Daphne Zhang. White Castle Ruling Shakes Up Biometric Litigation, *Insurance, Bloomberg Law*. (22 February 2023).

3 Provance D. Matthew, Archis A. Parasharami, John Nadolenco et al. Illinois Supreme Court's Most Recent BIPA Decision Exponentially Increases Potential Exposure for Businesses, *Mayer Brown*. (23 February 2023).

4 Scarcella Mike. BNSF Railway Will Settle Biometric Privacy Case, After $228 mln Verdict Wiped Out, *Reuters*. (19 September 2023).

5 Bellamy D. Fredric and Ashley N. Fernandez. Illinois Court Decisions Acknowledge Biometric Privacy Act's Damages a Potential Business Killer, *Reuters*. (17 April 2023).

6 Wiessner Daniel. Twitter Owes Ex-Employees $500 Million In Severance, Lawsuit Claims, *Reuters*. (13 July 2023).

7 Cabello Marcos. Texas Sues Google for Allegedly Collecting, Using Biometric Data Without Explicit Consent, (CNET, 20 October 2022).

8 Miller Sterling. The Basics, Usage, and Privacy Concerns of Biometric Data, *Thomson Reuters*. (20 July 2022).

9 Privacy-preserving Biometric Authentication, *IBM*.

10 Brooks Chuck. Cybersecurity Trends & Statistics For 2023; What You Need To Know, *Forbes*. (5 March 2023).

11 Biometric Technologies — Statistics & Facts, *Statista*, (7 July 2023).

12 The History of Biometrics, *RecFaces*.

13 Stowell Therese. How Biometrics Are Transforming the Customer Experience, *Harvard Business Review*. (29 March 2023).

14 Sanjay Dash. Amazon One Palm Payment Technology is Coming to all 500+ Whole Foods Market Stores in the U.S. Amazon News, (20 July 2023).

15 About Touch ID Advanced Security Technology, *Apple*.

16 Matt Burgess. This Surveillance System Tracks Inmates Down to Their Heart Rate, *Wired*. (11 June 2023).

17 Domeyer Axel, Mike McCarthy, Simon Pfeiffer, and Gundbert Scherf. How Governments Can Deliver on the Promise of Digital Id, *McKinsey & Company*. (31 August 2020).

18 Biometric Passport, *Wikipedia*.

19 Biometric Passport: Security, Data Protection & How They Work., (9 October 2023).

20 Biometric Technology Market Size, Share & Trends Analysis Report By Component, By Offering, By Authentication Type, By Application, By End-use, By Region, And Segment Forecasts, 2023–2030.

21 Zetter Kim. The Massive OPM Hack Actually Hit 21 Million People, *Wired*. (9 July 2015).

22 Rajasekar Vani, Bratislav Predić, Muzafer Saracevic. Enhanced Multimodal Biometric Recognition Approach for Smart Cities Based on an Optimized Fuzzy Genetic Algorithm, *Nature*.

23 Rees Megan. The Future Of User Authentication: A Guide To Behavioral Biometrics, *Expert Insights*. (28 March 2023).

24 Mhlungu Gugulethu. How Artificial Intelligence Is Affecting Human Rights and Freedoms, *Global Citizen*, (4 January 2023).

25 Borak Masha. Chinese Government-Run Facial Recognition System Hacked by Tax Fraudsters: Report, (31 March 2021).

26 Aston Roy. Growing consumer trust in biometric authentication, *Paysafe*. (13 February 2020).

27 FTC Warns About Misuses of Biometric Information and Harm to Consumers, *Federal Trade Commission*, (18 March 2023).

28 FTC Warns About Misuses of Biometric Information and Harm to Consumers, *Federal Trade Commission*, (18 March 2023).

29 Biometric Information Privacy Act (BIPA), *ACLU Illinois*.

30 BIPA Litigation Tracker — S.T.O.P. — The Surveillance Technology Oversight Project (stopspying.org).

31 Goldberg P. Howard. BIPA Decisions Illustrate Challenges Facing Companies And Insurance Providers, *Reuters*. (5 September 2023).

32 Joyce Stephen, Skye Witley. Illinois Biometric Privacy Cases Jump 65% After Seminal Ruling, *Bloomberg Law*. (2 May 2023).

33 Huffman Bart, Haylie D. Treas. Texas Enforcement of Biometric Law Focuses on Artificial Intelligence, *Holland & Knight*.

34 Burns Lili, Jonathan Newmark. Washington's Biometric Data Regime Advances Privacy Regulation, *Bloomberg Law*, (16 May 2023).

35 BIPA Litigation Tracker — S.T.O.P. — The Surveillance Technology Oversight Project (stopspying.org).

36 Trifon L. Tara, Brian I. Hays and Brianna Dally. Are You Ready for the BIPA Tsunami? The New Wave of Biometric Statutes, *Locke Lord*. (July 2022).

37 Start Preparing for New State Privacy Laws That Take Effect in 2023, *Gunderson Dettmer*. (21 December 2022).

AJG.com **The Gallagher Way.** Since 1927.