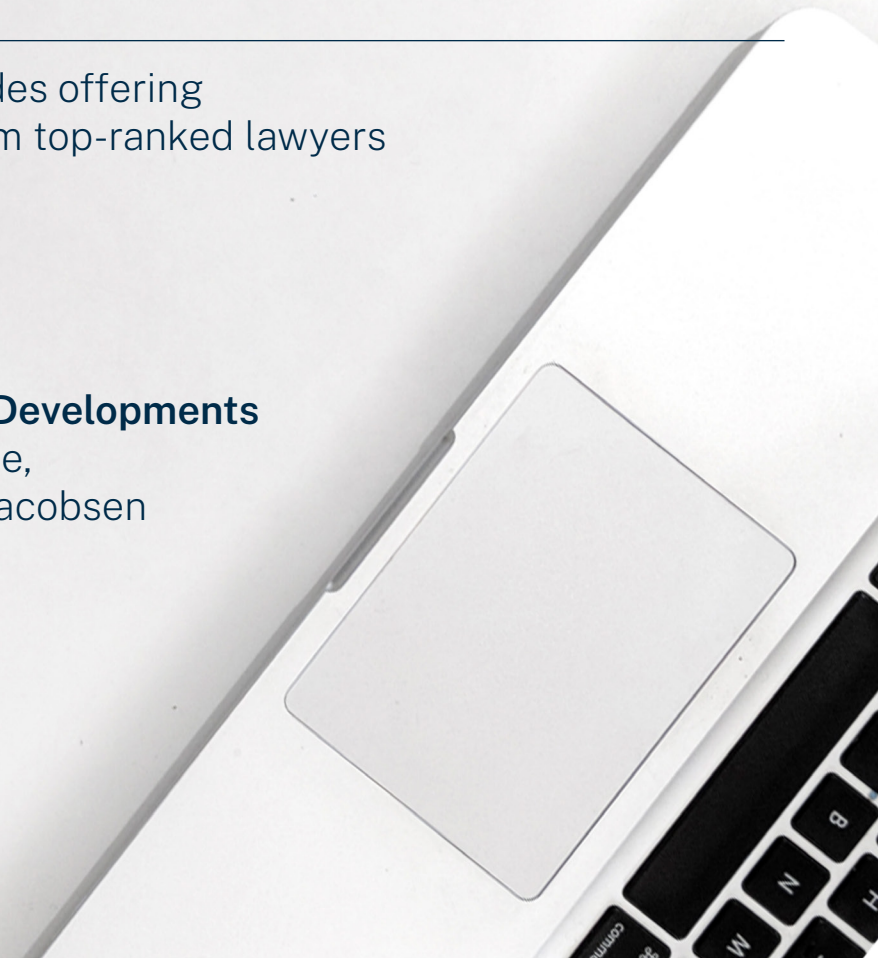
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2025

Definitive global law guides offering comparative analysis from top-ranked lawyers



USA – Illinois: Trends & Developments

Paul Yovanic, Jason Priebe,
Ada Dolph and Michael Jacobsen
Seyfarth Shaw LLP

USA – ILLINOIS

Trends and Developments

Contributed by:
Paul Yovanic, Jason Priebe, Ada Dolph and Michael Jacobsen
Seyfarth Shaw LLP

Seyfarth Shaw LLP has a data law practice comprising an interdisciplinary team of nearly 50 attorneys with expertise in data privacy, cybersecurity, e-discovery, information governance, data science and analytics, records retention, and AI. The firm provides outcome-driven counselling to help clients navigate data regulations, ensuring compliance with both domestic and international standards. Its tailored strategies and practical approach to data governance, privacy policies, and cybersecurity measures empower businesses to protect and leverage their greatest asset – data. In addition to proactive counselling, Seyfarth's data law practice excels in litigation across all areas of data law. The firm's attorneys defend clients against data breach claims, regulatory enforcement actions, and e-discovery disputes. It offers practical, innovative solutions in high-stakes litigation, ensuring clients are prepared for any data-related legal challenges. Whether managing complex e-discovery processes, responding to cybersecurity incidents, or navigating workplace biometrics, the team delivers exceptional legal representation and practical strategic advice.

Authors

Paul Yovanic is a senior associate in Seyfarth's litigation department. His practice focuses on class actions, including data, privacy, and information security litigation. He has extensive experience defending clients against data breach and state law privacy claims, including the Illinois Biometric Information Privacy Act (BIPA) and the Illinois Genetic Information Privacy Act, often litigating matters of first impression. He has defended more than 50 BIPA class actions, including some of the most high-profile lawsuits in the country. He also counsels and performs risk assessments for clients using or considering biometric-capable technologies. Paul is a member of The Sedona Conference Working Group 11 on Data Security and Privacy Liability.

Jason Priebe is a partner in Seyfarth's data law group and associate general counsel for the firm. He is an authority on data privacy, cybersecurity and e-discovery. He advises clients on compliance, risk management, and litigation, focusing on GDPR, CCPA, cross-border data transfers, and incident response. Jason helps businesses develop defensible data retention policies, mitigate privacy risks in vendor contracts, and navigate regulatory inquiries. He also counsels organisations on litigation holds, investigations, and data breaches. Jason is a recognised authority on domestic and international privacy compliance, and routinely provides advice on the establishment of policies and procedures for electronic information management, controls, security and governance.

Contributed by: Paul Yovanic, Jason Priebe, Ada Dolph and Michael Jacobsen, **Seyfarth Shaw LLP**

Ada Dolph is a partner at Seyfarth with over 20 years' experience at the firm. She is a trusted adviser on biometric privacy, data protection, and workplace privacy laws. She counsels clients on compliance with the Illinois Biometric Information Privacy Act (BIPA), the Illinois Genetic Information Privacy Act and other evolving privacy regulations, helping businesses mitigate litigation risks and navigate complex data protection challenges. Ada defends companies in high-stakes BIPA class actions and other privacy-related disputes, leveraging her deep experience in employment and consumer privacy issues. She was lead counsel in the first BIPA case heard by the US Court of Appeals for the Seventh Circuit, resulting in a complete dismissal of the action.

Michael Jacobsen is a partner in Seyfarth's labour & employment department and leads Seyfarth's Illinois Biometric Information Privacy Act (BIPA) class action team. He helps businesses navigate the complexities of BIPA and other evolving privacy laws, providing strategic guidance on risk mitigation, policy development, and statutory compliance. Michael defends clients in high-stakes BIPA litigation, and counsels them on best practices for biometric data collection and consent requirements. Clients rely on Michael's expertise to reach decisive, favourable resolutions early on in the matters he defends, as well as in the ongoing development of successful, long-term strategies both in and beyond litigation.

Seyfarth Shaw LLP

233 South Wacker Drive
Suite 8000
Chicago
IL 60606
USA

Tel: +1 312 460 5000
Fax: +1 312 460 7000
Email: pyovanic@seyfarth.com
Web: www.seyfarth.com

Illinois Privacy Trends and Developments for 2025

In recent years, Illinois has emerged as a key player in the evolving landscape of privacy law, with several groundbreaking developments shaping the protection of personal data. At the forefront of these efforts is the Illinois Biometric Information Privacy Act (BIPA), which has set a high standard for biometric data protection, sparking significant legal attention. The state's commitment to privacy has expanded to a recent surge in litigation under the Illinois Genetic Information Privacy Act (GIPA), addressing the delicate intersection of genetic data and individual rights. Additionally, Illinois is leading the charge in regulating the use of artificial intelligence (AI) in the workplace, as concerns over employee privacy and algorithmic accountability grow. This article explores these trends, highlighting the legal landscape's shifting focus on safeguarding personal information in an increasingly data-driven world, and includes an analysis of Illinois' recently proposed omnibus privacy bill.

Illinois Biometric Information Privacy Act (BIPA, 740 ILCS 14/ et seq.)

Enacted in 2008, BIPA regulates the collection, use, and handling of biometric identifiers and information by private entities. After a relatively quiet period spanning nearly a decade, the statute experienced a significant surge in activity following the 2019 landmark decision by the Supreme Court of Illinois in Rosenbach v Six Flags Entertainment Corporation. In Rosenbach, the Court held that a plaintiff need not plead actual harm or injury resulting from an alleged BIPA violation to seek relief under the Act. Subsequently, more than 1,500 BIPA lawsuits have been filed in Illinois.

While BIPA had been largely untested before Rosenbach, the bevy of lawsuits that followed gave rise to a series of critical threshold matters for courts of review in Illinois to resolve. Here are the latest BIPA issues that are taking centre stage in 2025.

Healthcare exemption for time clocks

The definition of "biometric identifier" under BIPA excludes "information captured from a patient in a healthcare setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996 [HIPAA]." In late 2023, the Illinois Supreme Court held in Mosby v Ingalls Memorial Hospital that alleged biometric information collected by a healthcare provider from its employees – in addition to that collected from patients – could fall within the scope of this "healthcare exemption" when the information is used for purposes related to "health care", "treatment", "payment", or "operations", as those terms are defined by HIPAA. However, Mosby specifically concerned nurses using a medication dispensing system and its finger-scan device to provide patient care.

The case did not concern the more common fact-pattern in which healthcare workers allege violations of BIPA when they are using a timekeeping system with a finger- or hand-scanning device. Since Mosby, Illinois trial courts have been split on whether the Illinois Supreme Court's ruling extends to this latter context. One view, for instance, has been that the exemption does not apply because HIPAA does not define "health care operations" to extend to a human resource department managing employee payroll or processing vacation time or sick days, while another has been that the exemption does apply because the provider is collecting and using the alleged biometric data to track employee time so that it can conduct health care operations and receive

payment for healthcare in compliance with federal, state, and local regulations. As a result, the split is all but certain to lead to further guidance by Illinois reviewing courts on the breadth and limits of the BIPA healthcare exemption.

State contractor exemption

BIPA also provides that "[n]othing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government." To date, only one Illinois appellate court has addressed this exemption. In Enriquez v Navy Pier, Inc., the defendant was a not-for-profit corporation that operated exclusively for the purpose of "supporting, sustaining, investing its funds in and for, and lessening the burdens of government related to the operation of Navy Pier" in Chicago. In affirming the dismissal of the plaintiff's complaint based on the state contractor exemption, the First District Illinois Appellate Court articulated the following test.

An entity falls within the exemption if it:

- is a contractor;
- is of a unit of government; and
- was working for that unit of government at the time it collected or disseminated the alleged biometric information.

The court reasoned that the defendant fell under this exemption because it was a "contractor" under the ordinary meaning set forth in Black's Law Dictionary and it "worked for" the government entity that owned Navy Pier because it performed services for it under their contract.

Despite this broad interpretation of the state contractor exemption in Enriquez, Illinois trial courts have been inconsistent in their application of the exemption. For example, the Circuit Court of Cook County in Miranda v Pexco, LLC ruled that "when working for" means during the same period of time that the plaintiff was working for the defendant rather than while the defendant was actively working on fulfilling the government contract or while the plaintiff was working on the contract. The Court framed the issue as a "temporal question" that asks simply whether the plaintiff was working for the defendant during the same time that the defendant had a government contract and was a state contractor or subcontractor, and such question could be decided on a motion to dismiss. On the other hand, other Illinois trial courts have ruled that discovery and an inquiry into the type of contract at issue or the amount of revenue that the entity derives from the contract may be necessary to determine the applicability of the BIPA state contractor exemption – such that any ruling on the exemption would have to be reserved for summary judgment.

Retroactivity of statutory damages amendment

In the seminal case of Cothron v White Castle System, Inc. in 2023, the Illinois Supreme Court ruled that a BIPA claim accrues each time that biometric identifiers or information are collected or disseminated, and not only on the first scan and first transmission. While the defendant and others cautioned that this interpretation of the statute could potentially result in "annihilative liability" – ie, to the extent it was read as endorsing a separate damages award for each scan or dissemination of biometric information – the Illinois Supreme Court emphasised that there is no language in the Act suggesting a legislative intent to authorise an award that would result in the financial destruction of a business. Nonetheless, in light of these policy concerns, the Illinois Supreme Court urged the Illinois legislature to clarify its intent regarding the assess-

ment of damages. The legislature heeded this call in an effort that culminated in August 2024, when Governor Pritzker signed into law Senate Bill 2979, which amended the BIPA damages provision to limit an aggrieved individual's damages to a single recovery for the same method of collection.

In light of some plaintiffs' attorneys who saw Cothron as a green light to pursue a "per-scan" damages theory, defendants sought rulings retroactively applying the amendment to cases that were filed before it was enacted. Similar to the healthcare and state contractor exemptions, however, courts have been divided on this retroactivity issue, as well.

For instance, in Gregg v Central Transport LLC, a court in the Northern District of Illinois ruled that the revision applied retroactively from BIPA's original enactment. As the court explained, in Illinois, there is a presumption that statutory amendments are intended to change existing law, and under this presumption courts must determine whether the change applies retroactively or only prospectively. However, this presumption does not apply when the circumstances indicate that the legislature intended to only interpret or clarify the original act. Because the Illinois Supreme Court in Cothron had expressly invited the legislature to clarify its intent, the court in Gregg found that the revision was merely a clarification rather than a substantive change. As a result, the Gregg court treated the amendment as if it had "been in place all along".

In contrast, in Schwartz v Supply Network, Inc., another court in the Northern District of Illinois found that the amendment constituted a change, not a clarification, and could not be applied retroactively. While acknowledging that the legislature can explicitly indicate its intent to merely clarify the law in the statutory text, the court concluded that "nothing in the text of the amendment indicates that it is merely clarifying" BIPA.

Illinois Genetic Information Privacy Act (GIPA, 410 ILCS 513/ et seq.)

The Illinois Genetic Information Privacy Act (GIPA), enacted a decade before BIPA, remained a seldom-cited law until 2023. Since then, over 100 class action lawsuits have been filed under GIPA.

GIPA was designed to protect individuals who are hesitant to seek genetic testing due to concerns that the results could be disclosed without consent or used discriminatorily. Following the passage of the Genetic Information Nondiscrimination Act (GINA) in 2008, Illinois amended GIPA to align with federal law, ensuring that covered entities treat genetic information in accordance with GINA's requirements. GIPA's definition of "genetic information" was also revised to align with the meaning set out in HIPAA, as specified in 45 C.F.R. 160.103. This federal regulation defines genetic information as data related to:

- an individual's genetic tests;
- genetic tests of the individual's family members;
- the manifestation of disease or disorder in the individual's family members; or
- any request for, or receipt of, genetic services, or participation in genetic-related clinical research by the individual or their family members.

GIPA places various restrictions on employers, such as prohibiting:

- the request for genetic information as a condition of employment;

- employment decisions influenced by an individual's genetic information; and
- retaliation against employees who assert violations of the Act.

Like BIPA, GIPA includes a private right of action and a tiered statutory penalty damages model: USD2,500 per negligent violation and USD15,000 per intentional or reckless violation. Given the similarities of the language in the damages provisions of BIPA and GIPA, it is likely that an Illinois court would find that the damages under GIPA are also discretionary, as held in the context of BIPA in Cothron.

Most GIPA lawsuits involve claims related to employment applications or post-offer medical exams requesting genetic information in violation of the law. However, over the past year, plaintiffs have sought to expand GIPA's scope by targeting technology companies that use tracking tools for marketing purposes, arguing that GIPA also prohibits disclosing genetic test results or identifying information in a way that reveals the subject's identity. Courts, so far, have generally been hesitant to rule on challenges related to the definition of genetic information at the motion to dismiss stage, or have rejected arguments that the information purportedly solicited was not genetic information given the broad allegations of the complaint. Notably, however, one court has ruled on a motion to dismiss that a plaintiff's claim regarding the use of genetic information in a company wellness programme was pre-empted by the Employment Retirement Income Security Act (ERISA).

Currently, GIPA lawsuits are far fewer in number than BIPA cases filed in the first two years following the Rosenbach decision. The slower pace is likely due to GIPA's inherent complexities, including determining what qualifies as genetic information and whether the information was solicited as a condition of employment or for another legitimate purpose, such as non-privacy regulations, like those imposed by the Occupational Safety and Health Administration (OSHA). It is anticipated that some of the cases filed in 2023 will be due for class certification briefing this year, and even summary judgment, which will provide clarity on whether plaintiffs can maintain the claims alleged, or whether the defences and justifications for the alleged conduct can defeat the claims.

AI in the workplace

Illinois has had AI employment restrictions in place since 2019 – long before AI went mainstream. The Illinois Artificial Intelligence Video Interview Act (AIVIA, 820 ILCS 42/ et seq.) governs employers' use of AI analysis in video interviews. Similar to the requirements under BIPA, AIVIA requires employers using "an artificial intelligence analysis" of job applicants' video interviews to provide various notices, obtain certain consents, and have specific-data management practices.

In 2024, Illinois expanded its focus on AI in the workplace when the legislature passed and Governor Pritzker signed into law Illinois House Bill 3773, which requires employers to provide notice to applicants and employees that the employer is using AI for various employment decisions, prohibits the use of zip codes, and contains an explicit statement that employers may not use AI in a way that subjects employees to discrimination.

The reach of the new law's disclosure obligation is expansive, covering an employer's use of AI in "recruitment, hiring, promotion, renewal of employment, selection for training or apprenticeship, discharge, discipline, tenure, or the

terms, privileges, or conditions of employment." The statutory language appears to encompass any "use" of AI for these purposes, not just fully automated decision-making. The new law does not go into effect until 1 January 2026, so the exact details of the required disclosures under the new law have yet to be fleshed out. That said, the Illinois Department of Human Rights (IDHR) is authorised to establish rules for its implementation. This could include specifying when and how notice must be given, though it remains to be seen whether the IDHR will follow the approaches seen in other states such as Colorado. In any event, the law's broad wording appears to extend the disclosure requirement to a wide range of AI applications in the employment context.

In addition, the new AI law prohibits AI-driven discrimination against protected classes under the Illinois Human Rights Act. However, the provisions of the new law do not introduce new obligations for employers, as discriminatory practices have already been prohibited under existing law. Instead, the law merely reiterates that AI decisions must comply with existing non-discrimination principles, emphasising the importance of fairness in AI-assisted employment processes. Further, the law specifically forbids using zip codes as proxies for protected classes, such as race or national origin, in AI tools. This aims to prevent biased decision-making based on indirect correlations between zip codes and protected characteristics. However, the law does not restrict the use of zip codes altogether or extend to other forms of location data, so employers can still use other geographic data in AI systems.

Illinois Privacy Rights Act (proposed, Senate Bill 0052)

Illinois first attempted to pass a statewide consumer privacy law in 2021 with the Illinois Privacy Rights Act (IPRA). Unlike most other state privacy laws, the IPRA included a proposed "purpose limitation" requirement. In the context of personal information processing, a "purpose limitation" is intended to prohibit businesses from retaining personal information beyond the originally disclosed or mutually understood purpose without subsequent notice and permission from the consumer. This would have, at the time, distinguished Illinois from other states' privacy laws, as it sought to prevent the indefinite retention of consumer data. However, the bill never made it to a vote, largely due to competing legislative priorities stemming from the COVID-19 pandemic.

In 2024, the Illinois legislature revived its efforts with another proposed bill that aligned more closely with existing state privacy frameworks, like California's Consumer Privacy Act (CCPA) and Virginia's Consumer Data Privacy Act (VCDPA). However, controversy arose over the inclusion of individual workers and job applicants in the definition of "consumer" where other state laws typically exclude employment-related information. Strong opposition from industry groups and business interests ultimately contributed to the 2024 bill's failure.

In January 2025, Illinois lawmakers made another effort with the introduction of Senate Bill 0052, now titled the Privacy Rights Act (PRA). The PRA, like the 2024 proposal, includes individual workers and job applicants in its definition of an Illinois "consumer". If enacted, Illinois would be only the second state to provide consumer privacy rights to workers for data collected in the employment context. This inclusion is still a

significant point of contention among industry and privacy interest groups.

Another distinguishing feature of the proposed PRA is its creation of a dedicated enforcement agency, the Privacy Protection Agency (PPA). The PPA would have broad investigative and enforcement authority, including issuing fines and conducting compliance reviews. This centralised enforcement mechanism also sets Illinois apart from most other states, where Attorneys General typically oversee privacy law enforcement. While supporters argue that a dedicated agency would strengthen consumer protections, critics warn it could lead to aggressive regulatory oversight and additional costs for businesses.

The PRA establishes a threshold for compliance based on business size and data practices. It applies to businesses meeting at least one of the following criteria.

- Generating annual gross revenues exceeding USD25 million in the preceding year.
- Buying, selling, or sharing the personal information of 100,000 or more Illinois consumers or households annually.
- Deriving 50% or more of annual revenues from selling or sharing consumers' personal information.

Beyond eligibility criteria, the PRA would require businesses to implement a number of key privacy measures, including the following.

- Providing clear, upfront notice at the point of data collection about the types of personal data collected, the purposes for processing, and retention periods. This would include job applicant- and worker-specific notices.
- Limiting data collection and processing to what is reasonably necessary and proportionate for the disclosed purposes.
- Implementing reasonable security measures to safeguard personal information.
- Entering into contracts with third-party data recipients intended to ensure that compliance obligations extend beyond direct data controllers to the entire data ecosystem.

The PRA also grants Illinois consumers a core set of privacy rights, including access, correction, deletion, and the ability to opt out of data sales and certain data uses. These rights align with those seen in other state privacy laws. The PRA's requirements, when combined with the proposed expansive consumer definition, could create one of the most restrictive regulatory environments for businesses in the country.

The PRA would also allow consumers to sue businesses directly if their personal data is compromised due to inadequate security measures. Consumers could seek statutory damages ranging from USD100 to USD750 per incident. This provision, in combination with the lack of an employment exemption, is expected to fuel heightened compliance efforts and industry pushback – and a potential new bonanza for plaintiff law firms similar to what we have seen in recent years with BIPA lawsuits.

In addition to the individual cause of action, governmental enforcement responsibility under the PRA would be shared between the newly established Privacy Protection Agency (PPA) and the Illinois Attorney General. The PPA would have broad investigative powers, including issuing cease-and-desist orders and imposing fines of up to 2,500 per violation – or USD7,500 for intentional violations or those involving minors' data.

Contributed by: Paul Yovanic, Jason Priebe, Ada Dolph and Michael Jacobsen, **Seyfarth Shaw LLP**

Despite the comprehensive nature of Senate Bill 0052, its path to enactment remains uncertain. Illinois would need to allocate significant financial and administrative resources to make the proposed PPA enforcement agency functional.

Given its repeated efforts over the past several years, Illinois is unlikely to abandon the push for a generalised consumer privacy law in some form or another. Whether through Senate Bill 0052 or a future iteration, lawmakers seem determined to pass an omnibus privacy law. Businesses and consumers alike should expect Illinois to remain active in the national privacy conversation.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com