ALSTON & BIRD

www.alston.com

Insurance Insights

June 2025

Insurance Insights Spotlight

Google Threat Intelligence announced on June 17 that hacker group Scattered Spider, known for attacking a sector at a time, has renewed attacks against insurers. Google Threat Intelligence has warned insurers to be on the lookout for social engineering schemes targeting call centers. Beyond this imminent threat, the data privacy space has captured our attention this quarter due to a continued flurry of state legislative activity. While insurers are typically exempted from the growing number of states' comprehensive privacy laws (and instead subject to the Gramm–Leach–Bliley Act and states' adoption of insurance-specific regulations), insurers still face evolving and varying obligations across different states. Here, we highlight recent privacy law developments in California, New York, and Illinois. We also invite experts from our Privacy, Cyber & Data Strategy Team to give their thoughts on top considerations for insurers.

Also in this edition, we head to summer school as we cover certain civil procedure developments in class actions and other contexts. While these holdings aren't shocking, they involve procedural rules that frequently impact insurers.

- Tania Kazi (Rice), Andy Tuck, Tiffany Powers, Alex Lorenzo

Eye on Privacy

California: Adding Layers to an Onion?

Privacy laws in California have been convoluted for insurers. The California Financial Information Privacy Act (CFIPA) adds protections beyond the federal Gramm–Leach–Bliley Act (GLBA), including permitting consumers to opt out of affiliate sharing and requiring written consent before sharing information with nonaffiliates. Separately, California's Insurance Information and Privacy Protection Act (IIPA) sets requirements for personal information received in connection with an insurance transaction, including standards for notice, collection, and obtaining written authorization before disclosure.

California's comprehensive privacy law—the 2018 California Consumer Privacy Act (CCPA), as revised in 2020 by the California Privacy Rights Act (CPRA)—contains a more nuanced carve-out for insurers than the one found in many other states' laws. Instead of an entity-level exclusion, it excluded only the data collected by insurers that was already regulated by the GLBA and CFIPA. So while data collected as part of an insurance transaction is subject to the industry-specific laws, insurers could still be subject to the CCPA as to other data.

On November 8, 2024, the California Privacy Protection Agency board proposed new regulations to update the CCPA and clarify how it applies to insurance companies. This would formalize an understanding that insurers must comply with the CCPA for consumer information not collected as part of an insurance transaction. The proposed regulation (as modified on May 9, 2025) provides illustrative examples: the CCPA covers information collected from website visitors who have not applied for an insurance product and information collected from employees and job applicants; it does not cover information submitted as part of a claim for coverage. A public comment period on the proposed regulation closed on June 2, 2025.

A new bill introduced in the California Senate on February 12, 2025, the Insurance Consumer Privacy Protection Act of 2025 (SB 354), aims to strengthen and modernize the privacy framework for insurers and their third-party service providers. Building on (but not entirely replacing) existing protections, SB 354 would include requirements to:

- Exercise due diligence in overseeing third-party service providers that process personal information and include certain provisions in service-provider contracts.
- Limit processing of consumers' personal information only to that reasonably necessary to an insurance transaction, certain marketing and research activities, and specified other purposes.
- Delete personal information no longer necessary to the performance of an insurance transaction or specified other purposes.
- Obtain express consent for use of personal information for any purpose other than the insurance transaction requested; provide clear privacy notices.
- Provide consumers the right to correct or delete inaccuracies in their records.

The California Department of Insurance, which has sponsored the bill, would have enforcement authority to impose penalties for violations. The bill remains under review in the state Senate. ■

Meet our California insurance team:

Bo Phillips

Sam Park

Kathy Huang

Tom Evans

Rachel Lowe

Tania Kazi (Rice)

Gillian Clow

Jonathan Kim

Samantha Burdick

Eye on Privacy

New York: Sharpening Focus on AI and Privacy

The privacy landscape is also evolving in New York, directly impacting insurers:

- As we've reported before, several states have adopted the National Association of Insurance Commissioners' (NAIC) model bulletin on the use of artificial intelligence in insurance. On July 11, 2024, the New York Department of Financial Services (NYDFS) finalized and issued Circular Letter No. 7, Use of Artificial Intelligence Systems and External Consumer Data and Information Sources in Insurance Underwriting and Pricing, which covers many of the same principles as the NAIC model bulletin but differs in some key respects. For example, it focuses only on underwriting and pricing, includes steps for a comprehensive assessment to ensure underwriting and pricing guidelines are not unfairly discriminatory, and includes a detailed notice requirement to potential insureds about the use of AI or external consumer data. Although Circular Letter No. 7 does not amend existing laws or regulations, we anticipate that the NYDFS will announce examination and enforcement plans under this interpretation of existing laws. Click here for a further discussion.
- On October 16, 2024, the NYDFS issued an industry letter containing guidance for assessing and responding to what it considers the most pressing cybersecurity risks in the use of AI. Recommended controls for combatting these risks include risk assessments, incident response and business continuity and disaster recovery plans, multi-factor authentication using forms of authentication that cannot be impersonated by deepfakes, cybersecurity training, and management of third-party service-provider agreements. Click here for a further discussion.
- On January 22, 2025, the New York state legislature passed the Health Information Privacy Act, which is now awaiting the governor's signature. Like Washington's My Health My Data Act of 2023, New York's act would broadly regulate health data not already governed by HIPAA. Unlike Washington's act, the New York Health Information Privacy Act does not exempt information subject to the Gramm–Leach–Bliley Act. Accordingly, insurers (other than health insurers already subject to HIPAA) may be required to comply with the act when processing health information linkable to an individual or device if the insurer or insured are in New York. Many insurers are likely already complying, such as by declining to sell health information to third parties and obtaining authorization before collecting health information beyond that necessary for providing the product requested by the consumer. But insurers should be aware of their obligations under the act, which will take effect one year after it is signed into law. Click here for a further discussion.
- Two recent amendments to New York's data breach notification law should be considered in companies' incident response plans. A December 2024 amendment, effective immediately, imposes a 30-day deadline for notifying affected state residents of a data breach—one of the shortest notification deadlines in the country. A February 2025 amendment clarifies that NYDFS-regulated entities must notify the NYDFS of a breach. Further, effective March 21, 2025, the law's definition of "private information" was expanded to include medical and health insurance information, meaning that breaches involving medical and health insurance information now trigger not only HIPAA notification requirements but also notification obligations under New York law. ■

Meet our New York insurance team:


Patrick Gennardo


Reade Seligmann

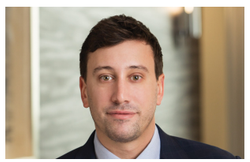

Adam Kaiser


Elizabeth Buckel


Mona Bhalla

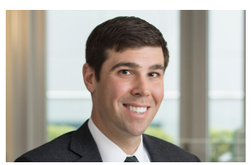

Joanna Schorr


Alex Lorenzo


Matthew Byers


Eric Kuwana


Arianna Clark


Steven Penaro

School's Out, But Civil Procedure Class Is In

Plaintiffs Fail to Crack the (Genetic) Code as Another Court Holds Illinois's GIPA Does Not Apply to Life Insurance Underwriting

Thompson v. Prudential Insurance Co. of America, **No. 3:23-cv-03904 (S.D. Ill. Mar. 31, 2025).**

After seeing success in privacy class actions under Illinois's Biometric Information Privacy Act (BIPA), the plaintiff's bar in recent years has turned its attention to BIPA's sister statute, the Genetic Information Privacy Act (GIPA). Originally passed in 1998, GIPA was intended to bar discrimination on the basis of genetic information. It was amended in 2008 when BIPA was passed, with courts now interpreting the statutes similarly. Like BIPA, GIPA includes a private right of action with statutory damages for each violation. Since 2023, three Illinois federal decisions have relied on BIPA-interpretation cases to hold that an individual only needs to allege a violation of legal rights to bring a private right of action under GIPA. This has spurred class actions alleging that employers or health insurers seeking family medical history violate GIPA's prohibition on the collection of genetic information.

In this case, the plaintiff unsuccessfully tried to expand GIPA's reach to life insurers. The plaintiff argued that life insurance medical exams "created" genetic information through family medical history questionnaires and blood-sample testing and that GIPA barred life insurers from using this information to make underwriting decisions. The life insurers argued that GIPA's text, framework, and legislative history all make clear that GIPA's bar on insurers' use of genetic information only applies to health insurers.

In a complete defense win, the district court agreed with the life insurers, relying heavily on an analogous opinion issued just months earlier. The court also rejected the plaintiff's attempt to distinguish her case by arguing that the defendants were covered by the statute because they also offered separate health insurance products, and thus were health insurers. The court found that applying GIPA in this manner would create an "anomalous regulatory scheme" whereby the same conduct (using genetic information for life insurance underwriting) would not be regulated when the insurer offers only life insurance products, but would be when the insurer also offers health insurance products. ■

The Lying Down Unnamed Class Member

Laboratory Corp. of America Holdings v. Davis, **No. 24-304 (U.S. June 5, 2025).**

The Supreme Court heard oral argument on April 29, 2025 in a case that might have settled an important question for insurers that face class actions: whether a federal court may certify a Rule 23(b)(3) class that includes uninjured class members who lack standing. That case involved an Americans with Disabilities Act challenge to a self-service kiosk option that was inaccessible to blind patients, but the putative class included people who would have chosen to check in at the front desk instead of through the kiosk option anyway. However, the district court narrowed the operative class definition while the interlocutory appeal was pending, and on June 5, the Supreme Court dismissed the writ of certiorari as improvidently granted.

The following patchwork of approaches by district and appellate courts therefore remains intact: (1) Article III bars certification of a damages class that includes any members without standing; (2) a damages class can be certified if there is only a de minimis number of class members without standing; (3) a damages class can be certified unless a large number of members lack standing; or (4) a class may be certified regardless of unnamed class members' standing unless there are other Rule 23 problems (e.g., the standing issues would result in a predominance of individualized issues).

We predict that the Court will resolve this question in a forthcoming term. At oral argument, Justices Jackson, Sotomayor, Kagan, and Gorsuch raised questions about the practicalities of determining whether there are any uninjured class members at the time of class certification. On the other hand, Justice Kavanaugh dissented from the Court's procedural dismissal, making his merits position clear: "Federal courts may not certify a damages class under Rule 23 when, as here, the proposed class includes both injured and uninjured class members." He noted that overinflated classes can "coerce businesses into costly settlements that they sometimes must reluctantly swallow rather than betting the company on the uncertainties of trial." He relied on Rule 23 instead of Article III, finding that common questions would not predominate when the class consists of both injured and uninjured class members. Defendants may find his comments useful in jurisdictions where this question is unsettled or even when courts find no Article III issue with certifying a class. ■

School's Out, But Civil Procedure Class Is In

A Tale of a Tenacious Class Action Defendant

***Ford v. Progressive Specialty Insurance Co.,* No. 2:21-cv-04147 (E.D. Pa. Mar. 5, 2025).**

It is no surprise that the court denied class certification in this case. After a collision with an underinsured vehicle, the plaintiff sought to stack underinsured motorist coverage between his motorcycle policy and another policy that covered two additional automobiles. However, the plaintiff had signed a statutorily mandated stacking waiver that, pursuant to Pennsylvania Supreme Court holdings, was only enforceable in certain circumstances. The plaintiff sought certification of a class of policyholders who were denied uninsured or underinsured motorist coverage due to the stacking waiver or household/regular-use exclusion.

The parties conducted extensive class-certification-related discovery, but the plaintiff could only identify 98 potential class members. In opposition to class certification, the insurer submitted an employee declaration assessing the claim files and circumstances of each of those denials. The insurer was able to whittle the putative class down to only eight potential class members. Nonetheless, the court conducted a thorough analysis of each Rule 23 element. It found that the plaintiff had not established numerosity, commonality, typicality, or adequacy. Individual issues would predominate because there were several individual issues related to assessing each claim denial, including who was at fault for the underlying accident, whether denial of coverage was appropriate under the stacking waiver under Pennsylvania law, and whether there was another valid basis for denial.

Despite the plaintiff's failing on every requirement, the court still reached analysis of whether it could partially certify a class under Rule 23(c)(4)—a seldom-used rule that allows courts to maintain a class as to "particular issues." As described by the court, it could potentially "manufacture predominance through the nimble use of such carving." It declined to do so due to the number

of legal and factual variables between insureds. But this case serves as a reminder of the potential usefulness of extensive class discovery and the importance of diligence in opposing the Rule 23 considerations even when the outcome seems clear. ■

The Unbearable Lightness of Declaratory Relief

***Siino v. Foresters Life Insurance & Annuity Co.,* No. 23-16176 (9th Cir. Apr. 1, 2025).**

We've previously covered the trends in class actions brought under California's no-lapse statutes, which set forth certain notice requirements before a life insurance policy issued in California may lapse. In December, the Ninth Circuit held that to recover damages related to the lapse, the lack of a statutorily compliant notice must have caused the lapse and alleged harm.

In April, the Ninth Circuit clarified whether policyholders could use a tailored declaratory relief claim to circumvent the causation requirement. In addition to a breach of contract claim, the plaintiff sought a declaration that the insurer failed to comply with the no-lapse statutes and that her policy remained valid without the need to pay back overdue premiums. The plaintiff held onto the first part of her claim—a declaration that the insurer violated the statutory notice requirements—through some weaving.

The Ninth Circuit first addressed whether the district court abused its discretion in considering the declaratory relief claim at all. The Ninth Circuit decided that the declaratory relief claim did not duplicate the breach of contract claim because it did not require evidence of damages and could serve a useful purpose by addressing the additional idea of whether the plaintiff was required to pay back overdue premiums.

Next, the Ninth Circuit addressed the declaratory relief claim in two parts. It upheld a declaration that the insurer violated the no-lapse statutes because that declaration could not be used as an offensive "sword" allowing the plaintiff to collect damages. Instead, it would merely serve as a "shield" in case the insurer sought payment of overdue premiums. The Ninth Circuit reversed a declaration that the policy remained valid because the plaintiff had not shown that her injury was caused by the lack of notice.

We could see district courts reaching a different outcome when exercising discretion about the usefulness of a mere declaration of a statutory violation. But regardless, the holding left the plaintiff with a seemingly hollow remedy.

In other lapse litigation news, we note that the California Supreme Court has agreed to review whether the no-lapse statutes apply to policies that originated in other states. ■

Counting Amount in Controversy Chickens

***Farmers Direct Property & Casualty Insurance Co. v. Perez,* No. 23-3320 (9th Cir. Mar. 6, 2025).**

In many instances, we recommend that insurers choose to litigate in California federal courts over state courts when possible. Particularly for defendant insurers, considerations include the slightly more defendant-friendly "plausibility" pleading standard in federal court, the necessity of conducting a Rule 26(f) conference before starting discovery, and more robust procedures for expert disclosures. So we welcome this Ninth Circuit ruling, which clarifies the "amount in controversy" requirement for federal diversity jurisdiction in declaratory judgment actions. In this action disputing coverage obligations related to an underlying lawsuit, the court held that the amount in controversy was not capped at the $25,000 policy limit but instead included anticipated underlying future defense fees and costs that there was "at least an arguable basis" the insurer would incur. The court adopted a rule that the party seeking diversity jurisdiction must establish, by a preponderance of the evidence, a "legal possibility" of the controversy exceeding $75,000. This aligns with similar holdings in other circuits that have addressed this issue (including the Third, Fourth, Fifth, Sixth, Eighth, and Tenth Circuits). ■

Tort Reform

As Tort Reform Takes Hold in Georgia, Will Other States Follow?

Signed into law in April 2025 and effective immediately, Georgia Senate Bill 68 makes significant changes to Georgia's civil litigation procedures. The reform carries a stated goal of stabilizing insurance costs for businesses and consumers.

The reforms aimed at limiting excessive damages and frivolous litigation include:

- **Ban on Anchoring**. Precludes argument, testimony, or other references to a specific value or range of values of noneconomic harm, such as pain and suffering. The sole exception is statements made in closing arguments, if those statements have some connection to the facts proved by evidence. This measure applies to all civil cases, including pending cases, that seek damages for bodily injury or wrongful death.
- **Ban on Phantom Damages.** Abolishes the collateral source rule, allowing juries to consider amounts billed by insurance providers and discounts offered by or negotiated for insurers. This measure applies to causes of action that accrue after April 22, 2025.
- **Bifurcation and Trifurcation.** Defendants in cases to recover damages for bodily harm and wrongful death may now elect whether to bifurcate liability and compensatory damages proceedings within a trial. A third phase can be held for a determination of punitive damages. A court may strike this election in limited circumstances.

Other procedural changes, applicable immediately in all civil cases, include:

- **Motion to Dismiss Stays Merit Discovery.** Merits discovery is stayed until the resolution of a motion to dismiss.
- **Voluntary Dismissal.** Precludes the voluntary dismissal of claims without prejudice after the 60th day following the filing of an answer. Among other impacts, this new rule will limit plaintiffs' ability to cherry-pick bellwether cases in mass tort litigation by dismissing less favorable cases.

We are optimistic that these reforms will dampen nuclear verdicts and create less uncertainty for insurers (click here for more discussion). Eyes are now on other states for potential tort reforms. In Texas, Senate Bill 30—which includes codification of common-law limitations on noneconomic damages and additional disclosure requirements for the provision of and payment for medical services—could pass this legislative session. Oklahoma's Senate Bill 1065 looks to cap noneconomic damages awards at $500,000. With success in Georgia and other bills rapidly moving through legislatures across the country, we may see a meaningful reduction to legal exposure in tort cases in the coming months and years. ■

Top 5 Cybersecurity and Privacy Updates for the Insurance Industry

By: Kate Hanniford, Lance Taubin, and Kristen Bartolotta

The global cybersecurity and privacy landscape continues to shift in response to rapid advancements in technology and expanded utility of personal data. Our Privacy, Cyber & Data Strategy Team outlines several trends and changes across jurisdictions that are particularly relevant to insurers.

1. **Regulator Expectations.** In recent years, U.S. state and federal regulators have increasingly emphasized, both through guidance and enforcement actions, more prescriptive and rigorous cybersecurity controls to account for the evolving cyber-threat landscape and technological advancements. Some of the new prescriptive cybersecurity requirements from regulators include implementing phishing-resistant multi-factor authentication (MFA); developing and maintaining a comprehensive, up-to-date asset and software inventory (including tracking any end-of-life (EOL) products); mandatory encryption (in transit and/or at rest) of personal information; and enhanced logging and monitoring measures.

   MFA, for example, is top of mind for regulators. The New York Department of Financial Services has consistently identified MFA as a critical control for all financial services companies, and in its recent industry letter reminded covered entities that MFA must be in place for "all Authorized Users attempting to access Covered Entities' Information Systems or NPI, including customers, employees, contractors, and [third-party service providers]." This means that MFA is required for customers and agents accessing the covered entity's information systems or nonpublic information, and not just for employees and contractors. This requirement will take effect in November 2025. At the federal level, the Federal Trade Commission's

Office of Technology and Division of Privacy and Identity Protection highlighted and encouraged the adoption of phishing-resistant MFA. According to FTC staff, "requiring phishing-resistant multifactor authentication for employees, such as security keys instead of numeric codes or push notifications" can mitigate security risks.

2. **Artificial Intelligence.** Using artificial intelligence (AI) models and platforms enables the insurance industry to make faster and more informed decisions across business sectors, including fraud detection, claims processing, and underwriting. However, AI can introduce additional risks. In addition to the privacy risks associated with typical AI use, like any components of a system, AI systems must be safe and secured from cyberattacks. AI systems can present risks that are not otherwise present in traditional systems.

   According to a report by the National Institute of Standards and Technology (NIST), there is "potential for adversarial manipulation of training data, adversarial exploitation of model vulnerabilities to adversely affect the performance of the AI system, and even malicious manipulations, modifications or mere interaction with models to exfiltrate sensitive information about people represented in the data, about the model itself, or proprietary enterprise data." As a result, AI systems are uniquely vulnerable to a variety of attacks, including poisoning, evasion, privacy, and abuse. AI systems' unique vulnerabilities to attacks demand strong security measures at each stage of the AI life cycle, including strong cybersecurity architecture

during the design, training, development, and post-deployment stages. Security measures include using cybersecurity policies, procedures, and tooling to prevent the circumvention of security controls, along with ongoing monitoring of the AI models to ensure the validity of outputs and that the model does not decay over time as input data changes.

3. **Cyber-Threat Landscape and AI.** The cybersecurity landscape is constantly evolving with risks across industries and attack vectors, but recently there has been increased risk of threat-actor use of AI and incidents involving third parties. The impact of AI on cybersecurity is likely in its infancy, but threat actors are in fact using AI, specifically generative AI, to create automated, tailored cyberattacks and monitor and model user behavior to inform the threat actors' tactics, techniques, and procedures (TTPs). The offensive use of AI by threat actors was one of the five most dangerous cyber threats in 2023 and 2024, according to the SANS Institute. Threat-actor use of AI has resulted in the increased speed and scale of phishing attacks (because AI can reduce the cost of these attacks by more than 95%) and the creation of deepfakes to threaten a company's brand or impersonate leaders. The current landscape reflects not only advancements in technology but the effect of increasingly interconnected software supply chains. This year's Verizon data breach report noted a rise in third-party risks to companies, with 30% of breaches in 2024 linked to third-party involvement.

4. **Latin America.** We are seeing a significant shift in the cybersecurity and privacy regulatory environment across the region. Although many countries are updating current standards and introducing new laws, we want to highlight two: Chile and Colombia. In January 2025, the Chilean Cybersecurity Framework Law came into force. The law establishes a legal framework for cybersecurity and increases required protections for critical information systems. Under the law, covered entities will have obligations to report and resolve cybersecurity incidents, including implementing controls required by the framework. Chile also updated its comprehensive privacy law to more closely align its standards with the European GDPR, increasing protections afforded to consumers. The Colombia Superintendence of Finance issued a regulation in 2024 that includes requirements for banks, financial institutions, and certain third parties to ensure secure processing of data and sets standards for banks and financial institutions to enter third-party agreements. This is a significant change from the country's previous voluntary model, and part of the Financial Superintendency's push toward open finance.

5. **Notice and Consent.** In January 2025, the Texas attorney general announced a first-of-its-kind lawsuit against an insurance company to enforce the Texas comprehensive data privacy law. The lawsuit related to the company's alleged collection, use, and sale of geolocation data of Texan drivers. The complaint alleged failures in the company's notice and consent structure, including for example (1) failure to provide a reasonably clear and accessible privacy notice; (2) failure to obtain clear, affirmative, freely given, and informed consent from consumers before processing their sensitive data; and (3) failure to disclose the use of consumer personal data for targeted advertising and the way a consumer may exercise their right to opt out. While many of the headlines on state privacy law enforcement are dedicated to California and the CCPA, other state attorneys general are showing increased interest in enforcing their comprehensive data privacy laws.

Although staying ahead of risks and trends in cybersecurity and privacy has become increasingly more complex, it remains critical for companies to stay abreast of the key areas of focus of insurance regulators, address cyber risks at an enterprise level (not in silos), and enhance cyber controls and practices, as appropriate. ■

Contributors

Emma Braden

Arianna Clark

Gillian Clow

Peter Cornick

Calvin Hart

Jonathan Kim

Jyoti Kottamasu

Tejas Patel

Melissa Quintana

Andrew Roberts

Jason Sigalos

Laura Simmons

Blake Simon