CARLTON FIELDS

Racing Ahead: Privacy, Cybersecurity, and AI Heats for the Life Insurance Industry

May 09, 2024

Drivers, start your engines. It has been months of high speed for privacy, cybersecurity, and artificial intelligence. **On the privacy circuit:**

- **Heat 1:** The NAIC's New Privacy Model Stalls
  It might be a false start for the National Association of Insurance Commissioners' new privacy model, Insurance Consumer Privacy Protection Model Law #674. After years of effort, the team is regrouping its efforts. Whether it'll be a rain delay or a full rainout remains to be seen.

- **Heat 2:** GIPA Plaintiffs Search for Traction
  A series of putative class actions has been filed against life insurance companies by plaintiffs eager to expand the track for Illinois' Genetic Information Privacy Act (GIPA). *See* "Lawsuits Alleging Violations of Illinois' GIPA Are Piling Into Court Like Clowns Out of a Circus Car," *Expect Focus – Life, Annuity, and Retirement Solutions* (January 2024). In a recent filing, GIPA plaintiffs amended their complaint allegations to specifically plead family history as "protected health information that is genetic information" and add allegations highlighting the involvement of HIPAA-covered entities. The plaintiffs, however, have yet to address one of the largest speed bumps in their case: extensive legislative history reflecting Congress' intent to limit GIPA's application and exclude life insurers' underwriting practices from the race. Here's hoping this contest turns into a demolition derby of the plaintiffs' claims on the next lap.

On the cybersecurity circuit:

- **Heat 1:** The Change Healthcare Attack
  In late February 2024, health care technology provider Change Healthcare was struck with a devastating ransomware attack. The attack hit the brakes on the largest health care payment system in the United States, and the blowout has reverberated throughout the U.S. health care system for more than a month. A second attack was reported in April 2024. Even outside the health care industry, these attacks serve as a reminder of the importance of cyber readiness, vendor due diligence, auditing, and good contracting regarding obligations in case of a data incident.

- **Heat 2:** The NAIC's CERP
  The NAIC Cybersecurity Working Group's Cybersecurity Event Response Plan (CERP) finished its first lap and was adopted at the 2024 Spring National Meeting. The CERP builds on the NAIC's Insurance Data Security Model Law (#668) and, although it is intended to help insurance departments respond to cybersecurity event reports, it also serves as a yellow flag for insurers regarding departments' likely inquiries and approaches to investigating cybersecurity events. The CERP, however, is far from its finish line. As explained by the NAIC, the CERP is intended to be a living document, subject to changes as cybersecurity events and technology develop. With that in mind, the CERP is a valuable resource, but the pit crew is already planning adjustments.

On the artificial intelligence circuit, it's a burnout to regulate AI.

- **Heat 1:** Lawmakers and Regulators Off to the Races

    - **Lane 1:** State law and regulations concerning AI have continued their breakneck pace. From Utah's Artificial Intelligence Policy Act to California's Privacy Protection Agency releasing new draft AI regulations to the EU passing the EU AI Act, more and more jurisdictions are passing AI-specific legislation. Not to be outdone, the number of states adopting the NAIC's model bulletin on the use of AI systems by insurers, or otherwise issuing AI bulletins, has continued accelerating. *See* "Current Standings of AI Guidance and Requirements by States." Objects in the mirror may be closer than they appear.

    - **Lane 2:** The SEC put the pedal to the metal on its earlier warnings and settled its first two "AI washing" enforcement actions. In March 2024, the SEC announced settlements with two different investment advisers for allegedly misrepresenting that they "were using AI in certain ways when, in fact, they were not." *See* "Cinch Up! AI Enforcement Starts With Washing Charges."

    - **Lane 3:** The Federal Communications Commission announced its position that AI-generated voices are "artificial" for purposes of the Telephone Consumer Protection Act, and therefore require prior express written consent. Users of such AI-generated voices may want to consider updating their TCPA consents to specifically gather consent for the use of such voices.

- **Heat 2:** Eyes Up for Accelerating Litigation
  As companies implement AI in more use cases, AI adopters need to keep their eyes up for litigation that may litter the track. From insurers partnering with AI providers to streamline their review of medical records for underwriting purposes, or considering tools to assist agents, the potential use cases for AI are seemingly limitless. There are, however, certain "rules of the road" and risks to consider. The *Carlton Fields 2024 Class Action Survey* found that privacy litigation is the greatest area of anticipated risk arising from the use of generative AI, and this litigation has already begun. Either based on the alleged collection and processing of personal information without proper notice and consent or linked to particular use cases, plaintiffs have already begun burning rubber. Four significant litigation examples:

  - **Lane 1:** CIPA Claims
    A recently filed putative class action alleged violations of the California Invasion of Privacy Act (CIPA) based on a company's use of AI to transcribe, monitor, and analyze customer service calls in real time and suggest potential responses to the agent speaking with the customer. The plaintiff alleges that callers were not told that their phone calls would be recorded or disclosed to service providers and that the tool was effectively an intentional wiretap, entitling him and all similarly situated class members to statutory damages of $5,000 per violation. CIPA allegations have been a recent favorite of plaintiffs' firms, and there are many laps left to run.

  - **Lane 2:** Data Scraping
    A recent decision found that scraping data from social media websites for use in training large language models (LLM) was not a violation of the platforms' terms when not logged into such sites. This could trigger social media platforms to shift more of their data behind account login screens or modify their terms to clarify the scope of their application; but until then, entities looking for datasets to train their LLMs may have a closing window to pass the competition.

  - **Lane 3:** Illegal Passing
    Litigation has also arisen regarding the sharing of driving information with large data brokers, such as LexisNexis. A recent lawsuit alleged that LexisNexis received information on drivers' driving behaviors from their cars and shared such information with car insurers evaluating such drivers' risks. The case could have significant reverberations for those in the industry who rely on LexisNexis risk scores.

- **Lane 4:** AI as a Nonstarter
  A putative class action lawsuit alleges that an insurer using a software tool to facilitate claims processing was impermissibly using AI to violate individuals' rights. The parties do not appear to agree even upon what race they are in, strongly disagreeing on whether the tool involved is AI at all (versus simple automation) and whether individuals were harmed by its use or simply received the same result they would have received without the tool's use.

Unfortunately, the racers show no signs of throttling down, so buckle up and prepare for the long race ahead. Ready, set, go!

Authored By

Ann Young Black

Patricia M. Carreiro

Related Practices

Life, Annuity, and Retirement Solutions
Cybersecurity and Privacy
Digital and E-Commerce Engagement and Innovation
Financial Services Regulatory

Related Industries

Life, Annuity, and Retirement Solutions