PUBLICATION

AI and Privacy on a Legal Collision Course: Steps Businesses Should Take Now

Authors: Matthew George White, David J. Oberly
August 28, 2025

The continued, rapid advancement of Artificial intelligence (AI) technologies comes with increasing risks for businesses, demanding that they navigate such issues more carefully than ever. Considering recent privacy class action trends detailed in this alert, companies that utilize AI in their business operations should immediately review and modify their compliance programs as necessary to mitigate legal risk and liability exposure.

Imagine this scenario: Your company just launched a new AI-powered customer support tool. It's fast, responsive, and delights users – exactly the kind of digital experience your leadership has been pushing for. Months later, and seemingly out of nowhere, you are served with a class action complaint. The lawsuit alleges that your AI tool records customer conversations and uses those recordings to improve and enhance the tool's capabilities and functionality, without first obtaining customer consent. As a result, your platform violates numerous wiretapping, biometrics, and consumer protection laws, entitling your customers to statutory damages ranging between $5,000 and $20,000 for *each* violation of *each* separate statute – even though they suffered no actual injury or harm of any kind.

Far-fetched? Not really – this scenario represents the latest privacy class action trend, which has generated a tremendous number of bet-the-company litigation with no sign of slowing down for the foreseeable future.

A Closer Look: The Rise of Privacy Class Action Litigation Targeting AI Data Use

The above scenario mirrors a growing number of real-world cases in which AI-enabled innovation is colliding with privacy expectations – and landing companies in court. Let's take a closer look at some other real-world examples:

When Data Training Looks Like Data Misuse

In one closely watched case, a facial recognition technology firm was alleged to have scraped billions of publicly available photos from social media platforms and image-sharing websites for use in training its AI. The catch? It allegedly did so without user consent, purportedly triggering liability under state biometrics laws that require clear notice and affirmative consent before collecting face geometry scans and other types of biometric data.

The company argued that these activities did not give rise to liability because the data that had been collected was publicly available and used for legitimate purposes, such as identifying suspects for its law enforcement customers. These arguments failed to persuade the court, and the dispute was later settled for $92 *million*. From a broader perspective, the action portends how courts may evaluate "public" data used to train private AI models in future class actions.

"Always Listening": Virtual Assistants Under Fire

A leading technology company was hit with a putative class action lawsuit alleging that its voice-activated AI assistant recorded user and non-user conversations without their consent – even when the wake word hadn't

been spoken. The plaintiffs alleged the system captured background conversations, stored them, and in some cases, used them to improve AI performance – again, all without users' knowledge or consent.

The company countered that such recordings were incidental, anonymized, and used solely to improve functionality, meaning that its activities did not give rise to liability. The court rejected these arguments, reasoning that the plaintiffs' allegations that the recordings were accessible to third-party contractors and could contain sensitive personally identifiable information (PII) plausibly stated a potential claim for relief. Ultimately, the case settled for nearly nine figures, underscoring how privacy missteps – even unintentional ones – can carry massive risk.

AI-Driven Call Monitoring and the Two-Party Consent Trap

Another lawsuit targeted a customer service transcription platform that integrates with popular video conferencing tools. In that case, the plaintiffs alleged the company's AI service recorded and transcribed business meetings, webinars, and client calls without informing all participants, purportedly in violation of two-party consent laws in certain jurisdictions that make it illegal to record a conversation without the express consent of *everyone* involved.

The company argued the two-party consent claims necessarily failed because its data processing activities were disclosed in its privacy notice at the time of the alleged violations, and because the hosting user supplied valid consent on behalf of all participants. The court disagreed, finding the absence of any *explicit* disclosures to guests or third-party participants was enough for the claims to survive dismissal at the pleading stage.

"Therapist" Bots and Misleading Advice to Minors

State privacy regulators are currently in the midst of an ongoing investigation into chatbot platforms that purport to offer mental and emotional health support to children and teens, but which fail to disclose to users that they are communicating with AI on the other end of the chat, as opposed to an actual healthcare professional.

The regulators at the helm of the investigation have taken issue with these platforms, in particular, because of how they blur the line between technology and therapy, raising concerns that users are being deceived into relying on unvetted, non-human advice. The matter has also generated a much broader public debate about where to draw the line in terms of AI's role in providing sensitive services, including whether and to what extent disclosures may be necessary to adequately safeguard individuals who interact with this advanced AI, oftentimes during periods of extreme vulnerability.

How These Trends Impact Your Business

The legal risks and liability exposure associated with this AI data use privacy class action trend are significant in scope, extending to all organizations – regardless of size or sector – that develop, supply, or use AI tools.

In addition – as indicated above – many of the statutes implicated in this wave of class action filings permit the recovery of high, per-violation statutory damages awards for mere technical non-compliance, and where no actual injury or harm has occurred. This low bar for establishing liability, combined with high damages awards, has supercharged the enormous volume of class action filings that continues apace today.

With that said, class action litigation is not the only threat that companies face, as federal and state privacy regulators are also bringing enforcement actions against companies that fail to use personally identifiable information (PII) generated through AI in a compliant, responsible manner.

The Federal Trade Commission (FTC) – the nation's *de facto* federal privacy regulator – has aggressively pursued enforcement actions targeting the use of AI data. Moreover, in its recent blog post, the FTC explicitly warns companies that it has brought, and will continue to bring, enforcement actions for insufficient disclosures that fail to fully inform users how their PII generated from AI is being collected and used. In the same guidance, the agency also notes that companies open themselves up to FTC enforcement actions if they fail to uphold their privacy commitments, such as by retaining or using PII generated through AI for additional, non-disclosed purposes without providing clear and conspicuous notice and obtaining affirmative express consent.

State privacy regulators have stepped up their enforcement efforts as well. Of note, the Texas attorney general (AG) recently pursued two separate enforcement actions, both involving major technology companies. In each action, the AG alleged non-compliance with the state's unfair, deceptive, and abusive acts and practices (UDAAP) and consumer privacy laws in connection with the internal use of PII to improve and enhance their AI solutions. To resolve the civil matters, the companies ultimately agreed to pay civil penalties of $1.4 and $1.375 *billion*, respectively.

Looking ahead, the volume of class action litigation targeting missteps when using PII from AI tools will continue its upward trajectory for the foreseeable future. Privacy regulators will also remain active in their efforts to combat these same issues. Consequently, companies are well advised to consider implementing modifications and enhancements to their compliance programs to address and manage these outsized risks, including several strategic measures discussed in detail below.

What You Can Do Now

Courts and regulators have moved beyond the question of *whether* privacy laws apply to the use of PII generated through AI tools in the first instance and are now focused on *how* and to *what extent* they apply in the context of AI.

Here are six steps every company using AI technology should take now:

1. Understand What Data AI Tools Are Collecting – and Why

Audit AI-driven systems to identify what data they ingest, store, and use to learn. Evaluate whether that data includes PII or sensitive data, as well as any processing activities that could trigger wiretapping, biometrics, or consumer protection laws.

2. Update Privacy Notices

Ensure privacy notices and similar external-facing disclosures are easily accessible and available to users. Include detailed language explaining the types of PII that may be collected by the tool, and how that data may be used and/or shared, as applicable. In particular, ensure notices clearly explain if and how PII is used to train models or for other internal purposes.

Consider dynamic disclosures that adapt to new AI features and use cases, as well as any disclosures that may be necessary where third-party software providers or other vendors are implicated. Clear and conspicuous disclosures in privacy notices is key for both legal compliance and strengthening trust and loyalty with end users.

3. Validate Consent Mechanisms

Relying on general terms of service is risky – especially in jurisdictions requiring explicit and informed consent. Thus, where possible, avoid relying on passive or blanket consent. Instead, implement granular opt-ins where

feasible, and in all instances where legally required (*e.g.*, for biometric data or voice recordings). Design consents so they are readily accessible and easy to understand, so that users can make informed decisions about how their PII may be used.

Clickwrap mechanisms – which require users to take an affirmative action signifying their consent – should also be used whenever possible and tested prior to real-time deployment to confirm no PII is collected until consent is affirmatively manifested by the user.

4. Limit Access and Retention Through Privacy-By-Design

Use privacy-by-design principles to minimize data retention and restrict internal access. Configure AI tool settings to limit the collection, use, and retention of PII to what is necessary. Collect PII only for specific, explicit, and legitimate purposes. Refrain from using or processing PII generated by AI tools in a manner that is incompatible with the purposes disclosed to users at the initial time of collection. Systems that utilize user-generated content to train or improve AI should be segregated and governed by strict access controls.

5. Vendor Technology Agreements

Ensure contracts are executed with all third-party AI solution providers and other third parties that may otherwise have access to PII by way of an AI tool. Contracts should include provisions that: (1) require the vendor to maintain strict compliance with applicable law governing the use of AI tools and associated PII; (2) limit the use of PII by the vendor to only that which is necessary for the vendor to perform its obligations under the contract; (3) bar the vendor from using or disclosing any PII for its own benefit or that of any third party; and (4) obligate the vendor to fully indemnify the company for any claims, losses, expenses, or fees (including attorney's fees) arising from a breach of the contract by the vendor or any actual *or alleged* non-compliance with applicable law. Thereafter, regularly review and audit vendor practices, data flows, and configurations to confirm continued compliance with legal and contractual obligations.

6. Work with Experienced Counsel Early – Not After the Lawsuit

Pre-deployment legal review can surface issues that will be hard (and expensive) to fix later. Have a litigation response plan if your AI tool is challenged in court or through a regulatory inquiry. Involving counsel early in the process can pay dividends in limiting future issues.

The Final Word: Innovate Responsibly, Litigate Strategically

The rise of AI doesn't mean the end of privacy. Just the opposite, it demands companies navigate these issues more carefully than ever. What might seem like harmless model training or platform optimization can easily be perceived – or alleged – to be a privacy violation if users feel misled or surveilled.

At Baker Donelson, our dedicated and experienced AI Team helps companies at every stage of the AI journey – from product design and risk analysis to defending lawsuits and regulatory enforcement actions. Whether you're developing or deploying an AI tool or facing claims over one that's already live, our team can help you protect your business, your customers, and your reputation. If you have any questions on these issues, please reach out to the authors, Matt White and David Oberly, or any member of Baker Donelson's AI Team.