How Companies Should Be Thinking About Disclosing AI Usage to Consumers

*Contributed by **Stuart Levi**, **Meredith Slawe**, and **Priya Matadar**, Skadden, Arps, Slate, Meagher & Flom LLP*

April 2024

As artificial intelligence (AI) tools and consumer demand for curated and personalized content continue to proliferate, companies are increasingly considering how they might incorporate AI into their service offerings. This can include using AI to improve customer service, tailor product recommendations, streamline inventory management, empower and inform customer-facing employees, and troubleshoot the user experience. A primary focus of the March 2024 annual Shoptalk conference—which brings together retailers to discuss the future of their industry—was devoted to the varied use cases for AI in consumer-facing activities, with sessions titled "Creating the Next Growth Wave with AI-Powered Commerce," "Pioneering Applications of Generative AI," and "Leveraging AI to Scale Personalization."

As companies explore the use of AI tools to meet consumer expectations and optimize the customer experience, they should consider how to approach related disclosures. A thoughtful disclosure policy will not only help minimize a company's legal risk, but will also bolster consumer trust and transparency with respect to the company's data practices.

Disclosure Required Under New AI Law in Utah

On March 13, 2024, Utah governor Spencer J. Cox signed into law the Utah Artificial Intelligence Policy Act (**SB 149**), making Utah the first state to mandate certain customer disclosure requirements relating to AI. Under the Utah Act, a company that uses AI to interact with a person must "clearly and conspicuously" disclose such use if asked or prompted by that person. In addition, persons who provide services of a regulated occupation—i.e., generally an occupation that requires a license or state certification to practice —must "prominently" disclose when a person is interacting with generative AI in the provision of the regulated service.

There is no private right of action under the Utah Act, and the law acknowledges the need for further exploration of this technology and consultation with businesses and consumer groups through the creation of a state Office of Artificial Intelligence Policy. While the Utah Act is the first state law of this kind, it would not be surprising if other states adopted similar, or stricter, disclosure requirements. For example, a **bill** was introduced in New York earlier this year that would require clear disclosures of data usage in connection with AI systems. Companies outside of Utah may therefore want to consider whether they view the Utah Act as a potential baseline for AI disclosures, at least with respect to how they respond to consumer inquiries as to whether AI is being used in customer interactions.

The FTC Perspective

In recent months, the FTC has made a number of pronouncements regarding the use of AI, and particularly in connection with how companies treat customer data associated with these technologies. As with many areas, the FTC's focus is on ensuring that consumers are not misled or deceived regarding the use of AI tools or the treatment of their personal information. This is consistent with the FTC's approach to promoting the accuracy of consumer-facing disclosures about the use of various technology tools.

The FTC made certain statements on AI even before AI had achieved mainstream adoption. For example, in a 2020 Business Blog, ***Using Artificial Intelligence and Algorithms***, the FTC advised companies using AI tools to "be careful not to mislead consumers about the nature of the interaction" lest they run the risk of an enforcement action. The list of uses that the FTC identified with the potential of deceiving customers included "phony follower, deepfakes, or an AI chatbot." In that same Business Blog, the FTC acknowledged that more data leads to better algorithms, but cautioned that companies need to be transparent —"secretly collecting audio or visual data – or any sensitive data – to feed an algorithm could also give rise to an FTC action."

More recently, in February 2024, in reaction to the growing use of AI tools that can mimic an individual, the FTC sought public comment on a **rule** that would make it unlawful for companies to provide goods or services that they know or have reason to know will be used to harm consumers through impersonation. FTC Chair Lina M. Khan emphasized the urgency of safeguarding the public from impersonation fraud and highlighted the potential of AI tools such as voice cloning to facilitate sophisticated scams. Moreover, the FTC **press release** introducing the proposed rule specifically noted that this rule would apply to "an AI platform that creates images, video, or text, to provide goods or services."

This agency action follows the FTC's recent finalization of its **rule** prohibiting the fraudulent impersonation of governments, businesses, and their officials or agents in interstate commerce, and is part of the FTC's stated efforts to promote consumer protection and fair competition in the digital landscape. If implemented, this rule could have significant implications for a wide range of businesses, especially for those that offer AI tools for product development or customer interaction. The public comment period is currently open, and **submissions** can be made through the Federal Register's website until April 30, 2024.

Consumer Class Action Activity

The use of consumer-facing AI tools has drawn the attention of the plaintiffs' class action bar which has already brought claims alleging that certain purported uses of AI tools violate the California Invasion of Privacy Act (**CIPA**), which is California's wiretapping statute. For example, on February 14, 2024, plaintiff Christopher Barulich filed a putative class action **complaint** in the U.S. District Court for the Central District of California against Home Depot and Google, alleging that these companies violated Section 631 of the **CIPA** through their alleged use of an AI-enabled customer service tool. That section prohibits, in pertinent part, any person from reading, attempting to read, or learning the contents or meaning of any message or communication willfully and without the consent of all parties to the communication, and permits private rights of action. This case reflects one of many attempts to stretch a state criminal wiretapping statute.

Many lawyers in California have tested the limits of **CIPA** in a variety of class contexts, in large part driven by the availability of uncapped aggregate statutory damages. There is typically a window where many businesses feel compelled to settle claims while the courts consider—and ultimately reject—the theory of liability. Once that happens, a group of serial litigants and their counsel pivot to a new theory and start the cycle again.

The plaintiff alleges that Home Depot used Google's Cloud Contact Center AI (CCAI), a technology through which customers first speak to an automated agent that "listens" to the customer service call, transcribes and analyzes the call in real time, and then suggests possible replies to a live Home Depot agent to whom the customer is then transferred. The plaintiff asserts that by enabling this process, Home Depot allowed Google "to access, record, read and learn the contents of [customers'] calls" without their prior consent. He alleges that he was unaware that he was ever speaking to an automated agent or that the content of his calls was passed to a third party—here, Google—for analysis.

The plaintiff also alleges that Home Depot and Google have "the capability to use the contents of the communications it intercepts for purposes beyond the scope of individual customer service calls," for example, "us[ing] information and data gleaned from customer service calls" to further train or develop its AI models. The complaint alleges that the foregoing activity allowed Google to "eavesdrop or wiretap into live conversations between callers and Home Depot," in violation of Section 631 of **CIPA**, and that Home Depot violates that section of **CIPA** by "knowingly and willingly enabl[ing]" Google to learn the contents of those communications in real time. This complaint is the latest in a series of efforts by the plaintiffs' bar to shoehorn technology into a statutory scheme that was not intended to apply in this context.

The class action plaintiffs' bar is prolific and creative. In addition, many professional litigants cycle through websites and mobile apps with the goal of identifying perceived gaps in disclosures. As a result, as companies incorporate new technologies, they should ensure that they make corresponding updates, as needed, to their privacy policies and other disclosures.

Best Practices for AI Disclosures

Apart from the Utah AI Policy Act referenced above, it is important to note that there are no federal or state laws mandating AI-specific disclosures.

However, it is becoming a best practice for companies to disclose their AI-usage in customer-facing applications and services either within their privacy policies or through other channels. Indeed, many businesses operating chat features (whether or not AI driven) now choose to include disclosures as part of the user interaction flow. This comes on the heels of a wave of threatened and filed putative class litigation challenging the absence of such disclosures under **CIPA**. While such disclosures are not strictly required—and these **CIPA** claims were rejected by many courts (see, e.g., *Licea v. Cinmar* **659 F. Supp. 3**d 1096 (C.D. Cal. 2023))—they are a good practice for mitigating risk and setting consumer expectations.

A thoughtful disclosure practice can mitigate or even eliminate a company's risk of enforcement actions or litigation alleging that the company misled customers about its use of AI or how the customer data is being used in connection with AI tools. When evaluating whether and how to disclose their AI use in their privacy policies or otherwise, companies should also be mindful of the increased attention that AI is receiving from consumers, regulators, and plaintiffs' class action lawyers.

Given the complexity of AI systems and the fact that many companies are exploring AI usage for the first time, an important step in establishing any AI disclosure regime is for a company to fully understand how AI is being used on its platform, including how outputs are generated or decisions are "made" by the AI system, and the risks and shortcomings of such systems. Such knowledge will help protect a company against making good faith, but erroneous, disclosures about the functionality of its systems, including "over-promising" what the system can do. This will also help companies ensure that any marketing statements and policies align with actual practices.

Companies should avoid using "template" AI disclosures or copying what they might see other companies disclosing on their own platforms. While uses by other companies may seem similar, there can be meaningful differences in how they are actually using AI "behind the wall," how they collect and process data, and how they share data with third parties. Drafting tailored disclosure statements can help ensure that policies accurately reflect their own operations, thereby lowering a company's risk of inadvertent misrepresentation.

Most companies today rely on third-party vendors to provide their AI-driven tools and services. This can add a layer of complexity to disclosure practices since a company will need to be aware of how such vendors' tools operate, including how such vendors will use, maintain and protect the company's customer data, and whether the vendor will use any of such data to train its own models. Companies should consider disclosing that the AI tool they are using is being provided by a third party, particularly if they are disclosing a customer's personal data to that vendor. Misuse by a vendor of personal data, or a failure by the vendor to comply with privacy laws, could pose liability risks for the company that retained them.

A company will likely not be able to defend itself against a claim by a regulator or in a private lawsuit by arguing that it was unaware of how a vendor was using data it collected through an AI tool. Further, given that some vendors are themselves reliant on other third-party AI models, it is important for companies to understand, and trace, any uses of their customers' data beyond the vendor and make sure contractual relationships are clearly defined (i.e., where the vendor is clearly identified as a service provider for the company).

While AI disclosures provide important benefits, companies will want to keep their customer-facing policies user friendly and understandable. Therefore, detailed disclosures about the AI technology used, and how it operates, will not benefit the company or its customers, and in many cases, will be difficult for a company to even pull together if it is reliant on a vendor's services. Companies will want to consider providing sufficient disclosure so that its customers have a general understanding that AI is being used and what is happening with their data, as well as including any appropriate disclaimers.

Companies should also consider disclosing how they are using personal data to train their own AI tools. For example, a company may be using customer demographic information, purchase history or online behavior to train or enhance a product recommendation engine. Companies may ultimately conclude that any such usage would be covered by a general disclosure that the company uses personal data to "improve" or "enhance" their own service or to develop new services.

Additional Steps Companies Can Take

In addition to being mindful of the AI disclosures they are making to consumers, companies should stay current on the evolving landscape of AI laws, including privacy laws that while perhaps not AI-specific, implicate AI usage, such as laws regarding automated decision-making. For example, the California Privacy Protection Agency recently issued **proposed regulations** that would give consumers the right to opt out of automated decision-making technologies being applied to their personal data as well as the right to access more information about how the company is using that technology. Similarly, in a recent speech, FTC Chair Lina Khan **stated** that the FTC is crafting clear rules on AI input, including that "some data—particularly peoples' sensitive health data, geolocation data and browsing data—is simply off limits for model training." By surveying proposed regulations, companies will gain a sense of the direction in which the law is breaking on AI disclosures and usage and can take proactive steps in product design to be compliant.

As companies weigh the benefits and risks of AI disclosures, they should also take into account the agreements they have with the vendor providing the AI tool. Companies should make sure that their vendor agreements clearly define the vendor's rights and obligations, particularly with respect to data usage. Companies should also pay close attention to indemnification, limitation of liability caps and any carve-outs to those caps to determine their level of protection and risk.

Ultimately, a robust AI disclosure practice will cultivate trust and confidence among consumers. By aligning AI practices and disclosures with consumer expectations and legal requirements, companies can differentiate themselves in a crowded marketplace, build strong customer relationships and navigate the evolving AI landscape with confidence.