How 2 Tech Statutes Are Being Applied To Agentic AI

By **Liza Cotter, Taya Bokert and Kristen Pavlounis** (February 2, 2026)

Liza Cotter

Taya Bokert

Kristen Pavlounis

It has often been said that the law is technologically neutral, and, certainly, the application of old laws to new technologies is nothing new. But it is also the case that such applications often lead to unanticipated results.

The use of computer fraud statutes to prohibit data scraping and the application of wiretapping laws to website tracking pixels are some recent examples of legal frameworks tested by — and also testing — technological innovation. The rapid rise of agentic artificial intelligence tools that can perform complex, multistep tasks with minimal human intervention presents the next frontier for these legal challenges.

Amazon's recent lawsuit against Perplexity — Amazon.com Services LLC v. Perplexity AI Inc. — filed in the U.S. District Court for the Northern District of California on Nov. 4 raises novel questions about who may authorize access to an online service when an AI agent acts on a user's behalf, what constitutes access or authentication circumvention in an agentic workflow, and whether AI agents are meaningfully different from scrapers and bots.

Against that backdrop, we examine how two statutes in particular — the Computer Fraud and Abuse Act, or CFAA, and the California Invasion of Privacy Act, or CIPA — are being applied to agentic AI, surveying recent case law and offering practical takeaways for companies developing or deploying these technologies.

The CFAA and Analogous State Computer Access Laws

Enacted in 1986, the CFAA is a federal antihacking law that imposes civil and criminal liability for accessing a protected computer, either "without authorization" or in a manner that "exceeds authorized access." Originally aimed at protecting government and financial institution computers, its reach has expanded to cover nearly any device connected to the internet.

Additionally, most states have analogous computer crime statutes, though not all provide a private right of action. As applied to websites and online services, the CFAA's restrictions have been clarified by key court decisions.

In Van Buren v. U.S., the U.S. Supreme Court held in 2021 that the "exceeds authorized access" prong applies only when a person accesses data from areas of a computer — like files or folders — that are off-limits to that person, and that it does not cover those who access permissible data for an improper purpose.

The U.S. Court of Appeals for the Ninth Circuit's 2022 decision in hiQ Labs Inc. v. LinkedIn Corp. established that scraping publicly accessible websites with no authentication gate does not violate the "without authorization" prong of the CFAA.

By contrast, Ninth Circuit cases finding liability where defendants bypass authentication or technical barriers (e.g., password gates, IP blocks) indicate that scraping or access behind such gates can violate the CFAA. For example, in Facebook Inc. v. Power Ventures Inc., in 2016, the Ninth Circuit found access without authorization where the defendant circumvented IP-blocking barriers. However, the Supreme Court has not definitively interpreted the scope of the CFAA's "without authorization" provision, and courts differ in their analyses of gated websites.

The Amazon case raises some novel considerations under the CFAA and similar state law statutes, and may serve as a case study of how those laws will be applied to agentic AI. In connection with the Amazon store, Amazon customers have unique credentials to access private accounts.

Perplexity's Comet, when provided with the login credentials of the Amazon account holder and prompted by such account holder, autonomously browses the Amazon store and makes purchases on the account holder's behalf. Comet's actions appear to Amazon as ordinary human user behavior.

While the technology is new, the legal claims mirror previous CFAA cases. Amazon alleges that Comet was not authorized to access nonpublic pages, effectively bypassing an authentication gate and triggering CFAA liability. Amazon claims it repeatedly notified Perplexity that automated access was prohibited, implemented technical barriers, and sent a cease-and-desist letter.

Amazon further alleges that Perplexity updated Comet specifically to circumvent the barriers Amazon implemented. Perplexity challenges the basis of the CFAA claims because Comet is acting at the user's direction. This raises the question of whether AI agents, acting on a user's behalf, are legally distinct from unauthorized scrapers and bots.

The outcome of the Amazon case may provide insight into how courts will treat autonomous agentic technologies that act on behalf of users within permissioned systems, particularly where a platform asserts that such delegation exceeds the scope of authorization.

CIPA

CIPA, a California statute enacted in 1967 to prevent private and commercial electronic surveillance, is increasingly applied to modern technologies. CIPA provides for a private right of action and statutory damages of $5,000 per violation.

Other states have similar wiretapping laws to CIPA, such as the Florida Security of Communications Act and the Massachusetts Wiretap Act, and have also experienced a recent surge of wiretapping litigation, as applied to new technologies.

Plaintiffs commonly bring claims under Section 631(a) of CIPA, which criminalizes, in summary, (1) intentionally tapping or making unauthorized connections to telephone or telegraph lines; (2) willfully and without the consent of all parties to the communication, or in any unauthorized manner, reading or attempting to learn the contents of a communication in transit; or (3) using or communicating in any way the information obtained through such conduct.

Section 631(a) of CIPA requires that third parties obtain consent from all parties to the communication, creating a higher risk of liability than state wiretapping statutes where only one party's consent to the communication is required (e.g., New York, Colorado).

Additionally, while historically applied to telephone calls, courts have established that Section 631(a) also applies to internet communications, further illustrating the broad scope of the statute.

California courts generally agree that liability under Section 631(a) only applies to third parties and cannot extend to the parties to the communication themselves, as such parties cannot be said to be listening in on their own communications.[1]

CIPA claims under Section 631(a) have already been litigated in connection with agentic AI technologies like chatbots and voice assistants, with plaintiffs arguing that the AI acts as a third party recording a communication without the consent of all parties.

For example, in a lawsuit filed in 2023 — Ambriz v. Google LLC — in the Northern District of California, the plaintiffs alleged that Google's AI-powered Cloud Contact Center, which provides businesses with a virtual agent to field consumer calls, transfer calls to human agents, and provide support on calls between consumers and human agents (e.g., generating transcripts, proposing "smart replies"), enabled Google to listen in on, record and analyze calls between consumers and businesses without obtaining proper consent from the consumers.

Google argued that it was not a third-party listener of the communications between the consumer and the agent under Section 631(a), but a provider of a tool, akin to a tape recorder, for the use of the business or human agent in its communication with the consumer. In its decision on Feb. 10, 2025, the Ambriz court, drawing on precedent from the Ninth Circuit, used the capability test to assess Google's potential liability under Section 631(a), which focuses on whether the defendant had the ability to use the information gleaned from the communication for its own purposes.[2]

In this case, the Ambriz court found that the plaintiffs adequately alleged that Google had the capability to use data received from customer service calls for its own purposes, because, under the terms of service governing Google Cloud Contact Center AI, Google asserted the right to use customer data for its own purposes where the businesses with which it contracts granted consent. The court found that the terms implied that Google had the technological ability to use the information gleaned from the communications at issue.

The capability test was also applied in Taylor v. ConverseNow Technologies Inc., also filed in the Northern District of California and decided on Aug. 11, 2025. There, the defendant, ConverseNow, provided an AI voice assistant used by businesses like Dominos to process customer orders and collect customer information (e.g., name, address, credit card information), and the plaintiff customer, Taylor, alleged that her information was used by ConverseNow for its own purposes, without the plaintiff's consent.

The court found it was plausible that ConverseNow had the capability to use the data derived from the calls for its own purposes, in part because the ConverseNow website and privacy policy noted that ConverseNow uses the information it processes on calls to improve its "platform, advertisements, products and services."

The ConverseNow and Ambriz cases suggest that providers of AI agents may not trigger Section 631(a) liability if the providers' agents are used solely to provide services to a party to facilitate a communication, and not used internally by the provider.

Uncertainty remains as to which AI agents and circumstances will trigger CIPA liability, as the application of CIPA is highly specific to the technology, which is inherently dynamic and

variable, and provider terms can vary in how they construe a provider's rights to use the information derived from the technology for its own purposes.

Additionally, AI — and, particularly, agentic AI — can blur the role of a technology provider acting as an unauthorized third party subject to CIPA liability as opposed to a provider of a tool that functions merely as an extension of a party to the communication. Unlike more passive, limited technologies — such as voice-to-text transcription tools or tape recorders — AI systems are capable of performing complex analysis and interpretation of communications, which raises the question of whether the provider should be viewed as a third-party participant rather than a neutral provider.

Takeaways

The application of laws like the CFAA and CIPA to agentic AI is still developing. However, recent case law provides some initial guidance. Companies developing or deploying these technologies should consider the following practical takeaways to mitigate legal risks.

User authorization may not be enough to avoid CFAA liability.

As seen in the Amazon case, platforms may argue that only the platform can authorize access to their systems, regardless of user authorization. Companies whose agents access third-party platforms should carefully review those platforms' terms of use for restrictions on automated access and be aware that a user granting access to their account may not be a complete defense under the CFAA.

Circumventing technical barriers is a key indicator of unauthorized access.

Following the hiQ Labs decision, accessing publicly available information behind a gate (e.g., a login or CAPTCHA) can lead to CFAA liability. Designing AI agents to bypass IP blocks, bot-detection tools or other access controls is likely to significantly increase the risk of CFAA claims and liability.

Mind the capability test for CIPA Section 631(a) liability.

As the court in Ambriz highlighted, liability for third-party eavesdropping can hinge on whether the AI provider has the capability, i.e., the technological ability, to use communicated data for its own purposes.

AI vendors should consider whether it is feasible to structure their services and contractual agreements to clarify they are acting solely as a service provider to one of the parties, without the ability to use communicated content for independent purposes like model training or product improvement. This position will be more challenging for companies with a business need to use such data for independent purposes.

Clearly define agentic AI practices in your terms of use.

For companies that deploy AI agents, your terms should explicitly state what the agents do, what data they collect, and how that data is used (and by whom). For companies concerned about access to your platforms by AI agents, your terms should clearly prohibit or restrict automated access if that is your policy. Any ambiguity in terms of use can be portrayed unfavorably in litigation.

Provide clear disclosures and obtain robust user consent.

Whether deploying an AI chatbot on your website or offering an AI agent that acts on a user's behalf, transparency is key. Clearly disclose that the user is interacting with AI, explain what the AI will do with the information provided, and obtain affirmative consent before the interaction or data collection begins. This can help mitigate risks under both CIPA, by establishing consent from a party to the communication, and the CFAA, by strengthening arguments about authorization.

Liza Cotter is a partner, and Taya Bokert and Kristen Pavlounis are associates, at Weil Gotshal & Manges LLP.

Weil partner Olivia Greer contributed to this article.

[1] CIPA claims have also been brought under Section 638.51, which criminalizes the unconsented use of a "pen register," a device or process that records or decodes routing, addressing, or signaling information (such as IP addresses or URLs), but not the contents of a communication. Following precedential cases like Greenley v. Kochava, Inc., plaintiffs have argued that embedding website analytics tools that collect and transmit this type of data to third parties constitutes the use of a pen register in violation of CIPA.

[2] The "capability test" stands in contrast to the "extension test" (applied in certain Ninth Circuit CIPA cases), where liability under 631(a) only attaches if the defendant actually used the content of the communication for its own, independent purposes. The Ambriz court, opting to apply the "capability test" agreed with the Ninth Circuit's holding in Javier v. Assurance IQ, LLC that because the third prong of 631(a) already imposes a "use" requirement (using or communicating in any way the information obtained through conduct described in the first two prongs), it would swallow the third prong of 631(a) to read a use requirement into the other two prongs of 631(a).