Take a Defensive Posture

Avoid becoming a target for AI privacy lawsuits

by: Greg Goldberg, BTA General Counsel

The rapid growth of artificial intelligence (AI) technology has spawned a broad range of new products and use cases designed to run offices more smoothly and efficiently. Although the upside of these advancements may seem limitless, the reality is more nuanced.

In the absence of meaningful federal AI laws and a patchwork of inconsistent rules across individual states, in many cases the task of regulating AI falls to the courts. And lurking behind every corner are plaintiffs' class action attorneys seeking to monetize uncertainty in the regulatory landscape to generate bankable lawsuits. Last October, Legal Perspective highlighted a series of privacy lawsuits filed in California seeking to apply a Cold War-era trap-and-trace law written during the telephone age to application programming interfaces (APIs) and software development kits (SDKs) embedded in websites that gather data from website visitors.

This month, Legal Perspective considers Lisota v. Heartland Dental LLC, a lawsuit accusing companies using AI phone systems of illegally eavesdropping. Lisota arises from the healthcare industry, but the legal issues are relevant to any company deploying AI-assisted call handling technologies, such as automated service desks or AI receptionists.

According to the plaintiffs' complaint, defendant Heartland Dental provides administrative and call-center services to dental clinics. In turn, Heartland Dental relies on cloud-based phone systems provided by co-defendant, RingCentral, to handle overflow call volumes. RingCentral's phone systems allegedly incorporate AI tools that capture and transcribe real-time call details provided by patients. RingCentral's AI tools then analyze the call details to assist call-center staff members with identifying a caller's needs, prioritizing responses and spotting opportunities to schedule appointments. In other words, plaintiffs allege RingCentral's AI technology does not simply route calls; they allege it actively listens to conversations, processes them and converts them into data.

Accordingly, plaintiffs claim the AI systems unlawfully eavesdrop on phone calls in violation of the Federal Wiretap Act, a statute that prohibits the interception of telephonic communications without consent. In its initial ruling, the court found that the alleged unauthorized recording of plaintiffs' phone calls raises a legitimate privacy concern that may be redressed in court, but ultimately ruled in favor of the defendants.

The court reasoned that because RingCentral's AI recording tools are a core component of its phone service, those tools fall within an exception to the wiretap law. Because RingCentral was forthright about its AI data collection practices, and because those practices were a key selling point of its software, RingCentral was not eavesdropping on callers surreptitiously in violation of the Wiretap Act.

Following the initial dismissal of the case, the plaintiffs filed an amended complaint raising new allegations, including one potential bombshell. Plaintiffs expanded the scope of the allegations to accuse RingCentral of using recorded call data to train its own AI models. This new claim raises an important question: When an AI-enabled product collects customer information and feeds it into a large language model, who is entitled to benefit from that information and what safeguards can be implemented to protect customers' privacy? Based on this new legal theory, many analysts believe the plaintiffs' amended complaint is likely to survive the defendants' next motion to dismiss.

In light of the proliferation of AI-based privacy lawsuits and the prohibitive expense of defending against class actions, BTA members should consider adopting a defensive posture in order to avoid becoming litigation targets. First, consider disclosing at the top of calls that AI tools may be in use. This way, customers are placed on notice. Second, give customers the option to speak with a human representative. Although AI systems can handle routine requests efficiently, callers with privacy concerns may prefer human interaction. Third, carefully review contracts with AI vendors to understand how call data is used, including whether conversations are stored, whether recordings are used for training models and what measures exist to protect customer information. Finally, internal policies should define when AI tools are appropriate and when sensitive calls should be routed directly to human staff members.

Although the chances of being dragged into a class action lawsuit may seem remote, dealers cannot be too careful. One reason, of course, is that plaintiffs' attorneys are just as likely to be using AI tools to identify who they are going to sue next. In summary: Climbing out on a limb may be unavoidable. Handing a lawyer a saw, on the other hand, rarely is. ■

Greg Goldberg, partner at Barta | Goldberg, is general counsel for the Business Technology Association. He can be reached at ggoldberg@bartagoldberg.com or (847) 922-0945.