



State Privacy Laws Poised to Fight Unauthorized Voice Cloning

**This article was [originally published](#) in Bloomberg Law on July 16, 2024.*

Jul 16, 2024

Categories:
[Publications](#)

Authors:
[William S. Morriss](#)

Unauthorized voice cloning using generative artificial intelligence is a growing concern. But state privacy laws have potential to help fight voice cloning.

Illinois' Biometric Information Privacy [Act](#) is a good vehicle to examine this potential. It provides a private right of action that has caused a significant body of relevant case law to be developed. While BIPA case law doesn't explicitly address voice cloning, it illustrates two principles that would be relevant to any attempt to use biometric protection to stop voice cloning.

First, BIPA case law shows that using AI to generate a voice with the same characteristics as the data subjects' is actionable only if those characteristics are specific enough to identify the data subject. This is demonstrated by [Carpenter v. McDonald's Corp.](#), in which the judge found that characteristics extracted from voice recordings using AI weren't a "voiceprint" because they couldn't "be identified uniquely" by those characteristics alone.

Second, BIPA case law shows that the way an AI system processes information will determine if it uses a protected biometric identifier. Whether a particular voice cloning system uses data unique enough to qualify as a protected voiceprint will likely be left for a jury to decide.

This is illustrated by [In re Facebook Biometric Information Privacy Litigation](#) where the main issue was whether Facebook collected and stored scans of face geometry—a type of biometric identifier protected under BIPA. Both sides had access to the source code of the AI system and to a research paper titled "DeepFace" that described its operation.

But the court couldn't resolve the question of whether the AI system collected or stored a "scan of face geometry." It held that "a jury will need to resolve the genuine factual disputes surrounding

facial scanning and the recognition technology.”

Given these principles, a plaintiff likely could make a viable BIPA claim based on unauthorized voice cloning. While the characteristics from the AI system in Carpenter weren’t sufficient to qualify as a voiceprint, the AI in that case was simply used to take orders.

By contrast, voice cloning AI is designed to emulate a person’s voice. The characteristics an AI voice cloning system would use are likely to be more detailed than the high-level characteristics in Carpenter. Determining whether the characteristics used are unique enough to qualify as a voiceprint requires identifying what those characteristics are, and then determining if their collective uniqueness is sufficient to uniquely identify the cloned speaker.

This requires delving into the details of the underlying AI model an inquiry that, as shown in *In re Facebook*, is likely to provide an alleged voice-cloning victim with enough arguments to avoid their claim being tossed before trial. As a result, for the right plaintiff (an Illinois resident), and with the right AI (a system that can uniquely emulate the plaintiff’s voice), BIPA appears likely to provide a remedy for unauthorized voice cloning.

Other States

At least one other state privacy law appears to be suitable for protecting those states’ residents from unauthorized voice cloning. Washington’s My Health My Data [Act](#) explicitly defines consumer health data as including biometric data and prohibits collecting that data without the data subject’s consent, unless doing so is necessary to provide a requested product or service.

This is analogous to BIPA’s prohibition on collecting biometric identifiers without first obtaining a release from the data subject. It implies that My Health My Data could address unauthorized voice cloning according to the principles discussed above in the context of BIPA. Even laws that don’t expressly mention biometrics may apply, as voiceprints that can identify a particular person appear to fall within common definitions of personal data used in multiple states.

However, some state privacy laws include provisions that present obstacles to applying them to voice cloning. The Vermont Data Privacy [Act](#) excludes any data generated from an audio recording “unless such data is generated to identify a specific individual” from its definition of biometric data.

Vermont’s law is recent enough that it’s unclear how this exclusion will be applied or if it can be overcome in the voice cloning context. It’s at least in tension with the general rule under BIPA that a voiceprint is protected if it’s specific enough that it could be used to identify a particular individual, even if it is never actually used for that purpose.

While state privacy laws are potential tools for addressing unauthorized voice cloning, state by state variations are important.

Privacy law also can supplement other state actions, such as Tennessee’s [ELVIS Act](#), which allows recording artists and others to file lawsuits based on unauthorized use of their voice.

The sticking point is that a person’s voice can’t be the subject of a federal copyright. And other state law voice protections aren’t as broad and are applicable only in certain contexts (such as advertising), or only for certain types of people.

Given the limitations of existing voice-specific protections, additional legal tools may be needed to address the risks posed by voice cloning technology. Given the presumed uniqueness of a person’s voice, and the widespread use of voice as a biometric authentication mechanism, privacy law may be able to provide just such a supplement to voice protections, such as the ELVIS Act.

Reproduced with permission. Published 7/16/2024. Copyright 2024 Bloomberg Industry Group 800-372-1033. For further use please visit <https://www.bloombergindustry.com/copyright-and-usage-guidelines-copyright/>

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.