Generative Artificial Intelligence and Biometric Data Collection Risks

By: Gamelah Palagonia, FIP, CIPM, CIPT, CIPP/E, CIPP/US, CIPP/G, ARM, RPLU+, CPLP

In the rapidly evolving landscape of artificial intelligence (AI), new tools such as virtual personal assistants, voice assistants, chatbots, and large language models are transforming the way humans interact with technology. Although revolutionary, these tools also bring significant risks, especially in biometric data collection and privacy. This article delves into these challenges, the evolving legal landscape, and the necessary measures for ethical and lawful AI use.

Consent Issues with Generative AI

Certain AI tools that record and transcribe meetings, such as Zoom AI, notify attendees that the meeting is being recorded – the problem is that if an attendee doesn't agree to be recorded, they are not allowed into the meeting. This method doesn't solve the issue of consent as attendees may feel coerced into consenting to being recorded as they must attend the meeting for business purposes. Similar AI tools are being deployed with no option for consent. Attendees only find out they have been recorded after the meeting ends and they receive the transcript and recording.

Generative AI technologies can pose significant data privacy challenges. Any personal data fed to AIs can become part of the tool's training data, and the organization may be unable to control how it is used. Additionally, if organizations fail to gain consumers' consent to run their personal data through generative AI, this could constitute a privacy violation under current and developing laws.

Data Collection Legislation

Currently, there is no Federal law governing the use of AI technologies. However, there are other laws that cover the data collected. For example, voiceprints, machine-generated patterns of curved lines and whorls that identify a person's voice, are considered biometric data and there are laws governing these in certain states, such as the infamous Illinois Biometric Protection Act (BIPA) and the Texas Capture and Use of Biometric Identifier ACT (CUBI). BIPA provides for statutory damages of $1,000 for each negligent violation and up to $5,000 for reckless or intentional violations. CUBI provides for a civil penalty of no more than $25,000 for each violation, enforceable by the Texas Attorney General. There are also biometric laws in Colorado, Maryland, Oregon, New York, and Washington. Many other states have proposed similar legislation.

Consumer Protection Issues & Progress at the State Level

At a federal level, the Federal Trade Commission (FTC) has been analyzing consumer protection issues related to biometric information for over a decade. Under Section 5 of the FTC Act, the FTC can bring actions against businesses for unfair and deceptive trade practices related to the collection and use of consumers' biometric information and the marketing and use of biometric information technologies.

In 2024, there was some progress at the state level. On May 17, 2024, Colorado became the first state to enact comprehensive AI legislation. Senate Bill 24-205, "Concerning Consumer Protections in Interactions with Artificial Intelligence Systems," (the "Colorado AI Act") will become effective February 1, 2026.

The Colorado AI Act was passed to remedy a concern over the possibility of "algorithmic discrimination." This is defined as unlawful differential treatment or impact that disfavors an individual or group of individuals based on their actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, veteran status or other classification protected under the laws of Colorado or federal law. The burdens of the Colorado AI Act fall on developers and deployers of these decision-making systems.

On September 19, 2024, California took the lead on data privacy again with the passage of the landmark California Artificial Intelligence Transparency Act SB 942 (CAITA) which protects consumers by giving them the ability to determine if content has been generated by AI. Violators of this law are subject to a civil penalty of $5,000 per violation. CAITA becomes effective January 1, 2026.

On September 28, 2024, California also enacted SB 1120, which regulates the use of artificial intelligence (AI), an algorithm, or "other software tool" in utilization review and utilization management (UR/UM) functions by healthcare service plans (HCSPs) or disability insurers and their contractors.

A few other states have passed AI legislation for particular functions or processes, including New York's AI Local Law 144, the Illinois Artificial Intelligence Video Act, and the Illinois Limit Predictive Analysis Use Bill HB3773, which apply to automated employment decisions. Maryland's HB1202 for facial recognition and Utah's SB149 for algorithmic bias also apply.

Looking Ahead: Proper Data Collection and Risk Mitigation

The absence of federal regulation and well-defined guidelines for AI systems creates significant uncertainty for businesses and consumers. Proper data collection and protection policies, coupled with risk mitigation controls, can help organizations adopt AI tools and other new technologies without violating laws, losing consumer trust or accidentally leaking personal data.

One way companies can mitigate risk is by deploying the new NIST AI Risk Management Framework (RMF). This NIST AI RMF offers a path to minimize potential impacts of AI systems, such as threats to civil liberties and rights, while also providing opportunities to maximize positive impacts. Addressing, documenting, and managing AI risks and potential negative impacts effectively can lead to more trustworthy AI systems. By proactively implementing these measures, organizations can navigate the complexities of AI adoption while safeguarding privacy and building consumer confidence.