POLICY TIP SHEET

AI Transcription and Facial Recognition:

Why States Need Clear Guardrails

By Levi Mikula

November 2025

THE PROBLEMS

- **Rapid advances in artificial intelligence are outpacing existing privacy and surveillance laws.**
- **AI transcription and facial-recognition systems have already produced false accusations and wrongful arrests.**
- **Worn or handheld AI devices can now record and transcribe private conversations without notice or consent.**
- **Outdated consent and wiretapping laws leave major gaps in protection for everyday citizens.**
- **Without clear guardrails, unverified AI outputs risk being treated as reliable evidence in law enforcement or legal proceedings.**

THE SOLUTIONS

- **Update federal and state privacy laws to reflect how AI tools collect, analyze, and store personal data.**
- **Require warrants or judicial oversight for any AI-assisted surveillance or transcription of private communications.**
- **Clarify that AI systems are tools—not "parties" to a conversation—and cannot consent on their own.**
- **Encourage states to coordinate consent standards and ensure stricter laws apply when conversations cross borders.**
- **Establish transparency and accountability requirements for facial recognition and other AI systems used by government agencies.**
- **Promote responsible innovation by developing clear, consistent guidelines for how AI may be used in public safety and law enforcement.**

Artificial intelligence holds great promise for improving public services and efficiency, but its rapid, unregulated expansion also raises serious privacy and constitutional concerns. Without clear safeguards, AI tools capable of recording, transcribing, and analyzing human communication could erode Americans' Fourth Amendment protections against unreasonable searches and surveillance. These systems can enable the capture of private conversations, online interactions, or behavioral data without consent or judicial oversight.

Early uses of AI transcription and facial-recognition technologies have already produced serious errors, leading to false accusations and even wrongful arrests. Policymakers must act now to establish guardrails that encourage innovation while protecting fundamental rights.

THE DANGERS OF AI TRANSCRIPTION AND SURVEILLANCE

AI-driven tools are increasingly being used in law enforcement, journalism, and legal proceedings—often without adequate validation or human oversight. When flawed or "hallucinated" outputs are treated as factual evidence, they can compromise investigations and endanger innocent people.

PFLN PRO-FAMILY LEGISLATIVE NETWORK BY WALLBUILDERS

OUR REPUBLIC

For instance, in King County, Washington, the chief deputy prosecutor prohibited AI-generated police narratives after an officer filed a report for a crime scene he had never visited.[1] The case highlighted how generative tools can fabricate details that appear credible but are entirely false.[2]

Similar issues have surfaced in the courts. In early 2025, Stanford professor Jeffrey Hancock saw his legal challenge to Minnesota's deepfake law dismissed after his filing—drafted partly with ChatGPT—cited nonexistent cases.[3]

Independent studies have shown that AI transcription tools, including Whisper, frequently insert fictional or inflammatory content such as allusions to violence, sexual innuendo, and demographic stereotypes.[4] Researchers documented transcripts that added words such as "blood-soaked stroller" and "terror knife" to benign audio recordings, or turned filler words into complete sentences.[5]

These same reliability issues extend to other AI-powered surveillance technologies. In one instance, a man was arrested for murder based largely on a "gunshot" detected by ShotSpotter, a program designed to identify firearm sounds from video feeds. The charge was later dropped after investigators found no corroborating evidence, and experts noted that the software can misclassify noises or adjust reported data after the fact.[6]

Facial recognition systems have produced comparable harms. Christopher Gatlin, a 29-year-old father of four, was arrested and detained for more than two years before charges were dropped; he was one of several Americans misidentified by AI-based matches. A *Washington Post* investigation found that 15 of 23 police departments across 12 states had made arrests primarily on facial recognition results, often without additional supporting evidence.[7]

Together, these incidents demonstrate that AI transcription, acoustic detection, and facial-recognition systems—when used without human verification or clear legal safeguards—can transform technical errors into life-altering consequences. Policymakers must ensure that evidence generated or interpreted by AI is subject to rigorous validation before it affects any person's rights.

POLICY RECOMMENDATIONS

As of mid-2025, at least four states—Colorado, Connecticut, California, and Vermont—have enacted broad AI governance laws, while many others have pending bills. Nearly half of all states have yet to introduce any AI-specific legislation, leaving significant gaps in privacy and evidentiary protections.[8]

To address these gaps and ensure that artificial intelligence strengthens rather than undermines civil liberties, policymakers at every level should act proactively to clarify how existing privacy and surveillance laws apply to AI and to establish guardrails for its responsible use.

Modernize Privacy and Surveillance Law

Federal and state privacy laws were written long before artificial intelligence became a tool for data analysis or surveillance. Lawmakers should make sure that AI systems follow the same standards of reliability and accountability as any other form of evidence. This could mean:

- Reviewing how AI is used in police reports and investigations to ensure that people, not algorithms, remain responsible for final decisions.
- Making sure that any use of AI to monitor private communications still follows basic warrant requirements.
- Exploring a broader framework that sets guidelines for how AI can be used in public safety.

Clarify Consent and AI Transcription Rules

Many state "wiretapping" or recording-consent laws were written decades ago, long before people could wear devices that automatically capture and transcribe everything around them. Today, AI-enabled recorders built into phones, watches, and even necklaces can store conversations from public or semi-private spaces without anyone realizing it.[9]

Across the country, recording laws vary widely. Most states follow a "one-party consent" standard—allowing a conversation to be recorded if at least one participant agrees—while others require all parties to consent, or apply different rules depending on the type of communication. Under federal law, only one party's consent is generally required.[10] Because of this patchwork, people may violate another state's law without realizing it.

Lawmakers should revisit these rules to decide how they apply when artificial intelligence is doing the recording or transcription. Possible steps include:

- Making clear that AI systems are tools, not "parties," and cannot give consent on their own.
- Considering whether AI-generated recordings or live transcriptions should always require notice to everyone being recorded.
- Encouraging states to update public-recording exceptions so that bystanders in cafés, classrooms, or sidewalks aren't unknowingly captured by always-on devices.
- Promoting cooperation between states so that the stricter consent standard applies when conversations cross state lines.

Establish Accountability and Transparency Standards

Beyond consent, policymakers should make sure AI systems used by law enforcement or government agencies are transparent and open to review. Steps could include:

- Requiring independent checks of AI accuracy before agencies rely on it.
- Notifying defendants when AI tools are used in investigations or prosecutions.
- Setting reasonable limits on how long automatically generated transcripts or recordings can be stored.
- Publicly reporting major errors or wrongful arrests linked to AI systems.

Taking these steps would help modernize outdated laws, build public trust, and ensure that AI supports justice instead of weakening it.

Endnotes

1 Jeremy Harris, “AI-assisted police reports not welcome in King County due to potential errors,” KOMO News, Updated September 28, 2024, https://komonews.com/news/local/king-county-prosecutor-tells-police-not-to-use-ai-artificial-intelligence-for-official-reports-for-now-errors-concerns-law-enforcement-perjury-criminal-justice

2 Matthew Guariglia, “Prosecutors in Washington State Warn Police: Don’t Use Gen AI to Write Reports,” Electronic Frontier Foundation, October 17, 2024, https://www.eff.org/deeplinks/2024/10/prosecutors-washington-state-warn-police-dont-use-gen-ai-write-reports

3 Lars Daniel, “The Irony—AI Expert’s Testimony Collapses Over Fake AI Citations.” Forbes, January 29, 2025, www.forbes.com/sites/larsdaniel/2025/01/29/the-irony-ai-experts-testimony--collapses-over-fake-ai-citations/

4 Garance Burke and Hilke Schellmann, “Researchers say an AI-powered transcription tool used in hospitals invents things no one ever said,” Associated Press, October 26, 2024, https://apnews.com/article/ai-artificial-intelligence-health-business-90020cdf5fa16c79ca2e5b6c4c9bbb14

5 Science.org, “AI transcription tools ‘hallucinate,’ too,” April 26, 2024, https://www.science.org/content/article/ai-transcription-tools-hallucinate-too

6 Garance Burke et al., “How AI-powered tech landed man in jail with scant evidence,” Associated Press, March 5, 2022, https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220

7 Douglas MacMillan et al., “Arrested by AI: Police ignore standards after facial recognition matches,” The Washington Post, January 13, 2025, https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/

8 Iapp.org, “US State AI Governance Legislation Tracker,” last updated October 6, 2025 https://iapp.org/resources/article/us-state-ai-governance-legislation-tracker/#state-ai-governance-law-chart

9 Julian Chokkattu, “Your Next AI Wearable Will Listen to Everything All the Time,” Wired, January 8, 2025, https://www.wired.com/story/bee-ai-omi-always-listening-ai-wearables/

10 Reporters Committee for Freedom of the Press, Introduction to the Reporter’s Recording Guide, accessed October 22, 2025, https://www.rcfp.org/introduction-to-reporters-recording-guide/