



The Use of Artificial Intelligence for Government Surveillance

Siddhi Jain

I. EXECUTIVE SUMMARY

When millions of Americans installed Ring doorbells, they thought they were buying a security camera, not building a surveillance network for law enforcement. Yet, Amazon shared Ring footage with police hundreds of times without a warrant or consent of those who owned the doorbell.

The FBI is now openly buying American's location histories from data brokers, and the United States Department of Homeland Security (DHS) received \$165 billion in funding for 2025, much of it directed towards artificial intelligence (AI) surveillance with private companies [1]. This brief examines how the U.S. government has conducted unwarranted monitoring through surveillance utilizing AI while in direct conflict with the Fourth Amendment, and how this issue can be combated through policy measures.

II. OVERVIEW

A. Relevance

Government surveillance is not a new concept; in recent years however, AI has made it cheaper, faster, and harder to detect, aiding substantially in its recent expansion. U.S. Immigration and Customs Enforcement (ICE), a federal agency, has spent \$30 million on Palantir's ImmigrationOS, a system that collects and combines personal information to track people in real-time, along with \$4.6 million on

iris-scanning smartphones, and \$3.75 million on Clearview AI facial recognition. Internal footage shows these technologies being used on teenagers who were not carrying identification, raising concerns about how easily powerful surveillance tools can be deployed on those without sufficient legal safeguards [2]. The expansion of the use of monitoring tools has created concerns about the government crossing private boundaries while providing little transparency. Existing privacy laws were written long before modern AI surveillance tools, leaving loopholes that are increasingly exploited against by federal law enforcement, immigration, intelligence, and local police agencies, while Americans are left with sparse legal protection.

III. HISTORY

A. Current Stances

The surveillance of citizens by the U.S. government did not start with AI. In 2013, former National Security Agency (NSA) contractor Edward Snowden exposed the NSA's PRISM program, revealing how the government had been quietly collecting phone records and internet communications of millions of Americans without their knowledge or consent. The legal justification for this issue was Section 702 of the Foreign Intelligence Surveillance Act (FISA), a law that was written to monitor foreign enemies, but has been repeatedly used to justify surveilling Americans without warrant. The FBI was running criminal queries through this database without judicial approval, and although recent legislation aimed to restrict this practice,

most queries can still be labeled as having foreign intelligence purposes, making reforms largely ineffective [4].

While it is not the origin of privacy issues, AI has allowed the problem to grow exponentially worse. Government contractors are selling the ability to scan millions of social media posts and create generated summaries of what Americans are saying online to agencies like the DHS, sparking concerns about privacy, free expression, and the potential for mass surveillance of everyday online activity without individual's consent or knowledge [3]. Congress has attempted to respond to this infringement on personal autonomy with legislation such as the 2026 Government Surveillance Reform Act—requiring warrants before accessing private communication—but it has yet to progress through the legislature. The Office of Management and Budget enforced AI guidelines that appeared strict until it was revealed that companies could opt out whenever they found the rules to be a personal inconvenience [4]. There has been some previous effort at legislative reform, however, all attempts have effectively failed as unrecognized loop-holes continue to work in the favor of private companies, rendering existing legislation obsolete

IV. POLICY PROBLEM

A. Stakeholders

The primary stakeholders in this issue are everyday Americans, specifically, those in communities that are commonly targeted by AI surveillance systems. Immigrant communities are particularly scrutinized, as tools such as facial recognition, biometric scanning, and social media monitoring, which were once used for identifying non-citizens, are now being used

within U.S. communities as well. Now, in neighborhoods residents—regardless of their legal status—live under the kind of monitoring that was previously reserved for foreign enemies [5].

Facial recognition systems utilized in the United States are often trained on disproportionately white datasets, leading to consistently higher false positive rates when applied to other racial minorities—including Black, Native American, Asian American, and Pacific Islander populations. This in turn directly leads to wrongful arrests, and cannot be attributed to technical flaws [6]. The American Civil Liberties Union (ACLU) has now documented more than a dozen wrongful arrests that were due to police reliance on facial recognition, with the technology showing higher false match rates when used on people of color, women, elderly, and youth populations. Every one of those wrongful arrests represents an upended family, a job at risk, and a damaged trust in public institutions [7].

Law enforcement agencies are also stakeholders as they are the primary operators of these surveillance systems and benefit from the efficiency AI promises. However, they also bear the significant legal liability when these tools fail and community relationships get damaged because of surveillance expansion without consent.

Private technology contractors like Clearview AI and PenLink are also some of the most powerful stakeholders, as they profit from government contracts while facing little accountability for the outcomes.

B. Risks of Indifference

The risks of failing to regulate AI surveillance extend far beyond privacy. License plate reader databases have already been shared with federal immigration agencies to monitor immigrant

communities, and Customs and Border Protection has recently been granted access to over 80,000 Flock cameras (stationary AI powered license plate readers) as part of an abortion investigation in 2025. Yes, you heard that right – Customs and Border Protection was involved in an abortion investigation using AI surveillance. Tools once used for one stated purpose are now being repurposed for other more malicious ones [8].

What began as AI-powered immigration enforcement at the southern border has quietly expanded into everyday life, something experts are calling “mission creep.” Constitutionally protected behavior, whether that is attending a protest, seeking medical care, or simply moving through public space, will be at risk. Communities that are already facing an increase in surveillance and law enforcement targeting will have the greatest burden; granted, all will be affected by this Fourth Amendment erosion [2].

C. Nonpartisan Reasoning

The opposition to unchecked AI surveillance is one of the few things Americans across all parties actually agree on. In Texas, the ACLU and the conservative Texas Public Policy Foundation have both come out against warrantless surveillance, warning that unchecked police technology violates constitutional protections. Protecting citizens from warrantless government intrusion has never been a partisan issue, but instead a founding principle of the United States [10]. The benefits of non partisan intervention include but are not limited to the following:

- 1) Civil liberties across all parties: The Fourth Amendment protects everyone regardless of their background. Conservative and

liberal lawmakers have both shown concern for government agencies using AI tracking systems because it conflicts with the foundational American principle of limited government power.

- 2) Economic costs are shared: Every wrongful arrest from a faulty facial recognition match costs cities money in lawsuits; money that comes from taxpayers. Better oversight would reduce those costs and rebuild community trust.
- 3) Community stability depends on it: When people cannot move through their own neighborhoods without being tracked, they pull back from schools, health clinics, and local institutions. That has consequences for entire families and communities, not just the individuals being surveilled.

V. TRIED POLICY

Efforts to regulate AI surveillance have produced more paperwork than protection. The Government Surveillance Reform Act, introduced in 2026, would require warrants before accessing private communications but has not been passed. The Office of Management and Budget issued AI guidelines that sounded promising until companies were able to opt out whenever the rules became inconvenient, rendering it futile [4].

At the state level, Texas shows how reform can

look promising on paper and still change very little. In June 2025, Governor Abbott signed the Texas Responsible Artificial Intelligence Act (TRAIGA), making Texas the only state after Colorado to pass broad AI regulation. TRAIGA prohibits AI from being used to violate constitutional rights and requires consent before collecting biometric data. However, TRAIGA is enforced by the Texas Attorney General; individuals who are harmed cannot sue, and companies can avoid liability overall if they discover and fix their own violations. No party has to report violations and there is no system in place to check whether the compliance is valid [11].

The most concrete proof that TRIAGA's intentions failed is that Department of Public Safety (DPS) practices have remained unchanged even after it passed. Texas already had laws restricting biometric data collection without consent, yet the state kept its contract with Clearview AI, a company that scrapes billions of images without consent. The state created exceptions for its own agencies and TRAIGA did not address that issue [10].

VI. POLICY OPTIONS

Mandatory warrant requirements for AI-derived data

One of the more straightforward ways to fix the Fourth Amendment gap is to require law enforcement to obtain a judicial warrant before buying or accessing location data, social media profiles, or biometric matches, no matter where the data comes from. The Supreme Court established in *Carpenter v. United States* (2018) that warrants are required for cell phone location data

from carriers. Legal experts argue that buying the same data from a broker should be no different.

The obvious pushback from law enforcement is that warrants slow things down in time-sensitive situations. However, this is addressable by wiretap which already allows for after-the-fact judicial review in actual emergencies, and that same structure could apply here.

Audit requirements for AI surveillance contracts

Law enforcement agencies using AI surveillance tools should be required to undergo independent third-party audits, with results made public. Right now, how tools like Tangles, a law enforcement data aggregating and analysis tool, are actually being used is largely unknown because DPS withholds records and refuses to answer questions about the software. Communities cannot push back against surveillance they lack information about.

At a local level, city and county laws could require agencies operating within city limits to disclose its AI tools, vendors, costs, and audit results to a civilian oversight board. The main resistance will come from agencies whose tool inventory is sensitive information, but that consequence is something that has to be weighed against the public's right to know how they are being monitored.

Review before deployment

Before any AI surveillance system gets deployed in a community, residents should have a real opportunity to review it, something that is currently not the case. An algorithmic impact assessment would require agencies to show, before deployment, how accurate the tool actually is and whether it shows no racial bias.

A large majority of wrongful arrests that are dependent on facial recognition software in the

United States involve a Black person. These are not random mistakes but a pattern the technology produces because of how it was trained. Requiring public accuracy data before deployment does not ban anything, but instead ensures that what is being used is honest and will not harm real people in real communities.

VII. CONCLUSIONS

In this paper, I have explored a plethora of topics underlying AI used for surveillance. The legal frameworks meant to protect Americans from government surveillance were written before agencies could find a large amount of personal data online and through cameras. The technology has expanded faster than the laws, and agencies have consistently exploited that expanding gap.

Warrant requirements, independent audits, and pre-deployment assessments do not get rid of the gap entirely, but they encompass some of the minimum required steps it would take to close it. None of these proposals limit law enforcement capabilities, but instead establish transparency between law enforcement and their community that currently does not exist.

In Texas, the consequences of inaction have already taken place. Surveillance data was used in an abortion investigation. License plate databases were shared with immigration authorities. AI cameras were used to monitor protests. People in their community often do not know they are being monitored and therefore have no way to change it. Legislation that allows companies to opt out will not change this issue, however, these barriers can be overcome if we allow for more

transparency.

ACKNOWLEDGMENT

The Institute for Youth in Policy wishes to acknowledge Taylor Beljon-Regen, Patrick Pickren, Tiffany Li, Asher Cohen, Paul Kramer, and other contributors for developing and maintaining the Fellowship Program within the Institute.

REFERENCES

- [1] "US Government Ramps Up Mass Surveillance with Help of AI Tech, Data Brokers – and Your Apps and Devices." *The Conversation*, 23 Apr. 2026, <https://theconversation.com/us-government-ramps-up-mass-surveillance-with-help-of-ai-tech-data-brokers-and-your-apps-and-devices-277440>
- [2] "Mission Creep: AI Surveillance at DHS Crosses Dangerous Line Into Tracking Americans." *American Immigration Council*, 6 Feb. 2026, www.americanimmigrationcouncil.org/blog/ice-ai-surveillance-tracking-americans/.
- [3] "AI is Making it Very Easy for the Government to Spy on You. Some Lawmakers Are Worried." *NBC News*, 27 Apr. 2026, www.nbcnews.com/tech/security/ai-making-easy-government-spy-lawmakers-are-worried-rcna341499.
- [4] "How Loopholes and Opt-Outs Can Tear Apart AI Policy in the United States." *Brennan Center for Justice*, www.brennancenter.org/our-work/analysis-opinion/how-loopholes-and-opt-outs-can-tear-apart-ai-policy-in-the-united-states

- [ar-apart-ai-policy-united-states](#). Accessed 29 Apr. 2026.
- [5] "How DHS Is Expanding Immigration Enforcement Through AI Surveillance." *Jeelani Law Firm*, 24 Feb. 2026, www.jeelani-law.com/dhs-is-expanding-immigration-enforcement-through-ai-surveillance/.
- [6] "Equity, Privacy, Civil Liberties, Human Rights, and Governance." *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*. National Academies of Sciences, Engineering, and Medicine, 2024, www.nationalacademies.org/read/27397/chapter/6.
- [7] "More than a Dozen Wrongful Arrests Due to Police Reliance on Facial Recognition Technology." *American Civil Liberties Union*, 14 Apr. 2026, www.aclu.org/news/privacy-technology/more-than-a-dozen-wrongful-arrests-due-to-police-reliance-on-facial-recognition-technology.
- [8] "Cameras Have Quietly Appeared in Thousands of US Cities – Now, Their Integration with AI Is Sounding Alarms." *The Conversation*, 27 Mar. 2026, <https://theconversation.com/cameras-have-quietly-appeared-in-thousands-of-us-cities-now-their-integration-with-ai-is-sounding-alarms-276928>.
- [9] "Texas' AI-Powered Surveillance Arsenal Has Ballooned. Proposed Laws Provide Few Guardrails." *The Texas Observer*, 31 Mar. 2025, www.texasobserver.org/texas-dps-surveillance-arsenal-artificial-intelligence-legislation/.
- [10] "Groundbreaking Texas AI Law Also Brings Needed Clarity on Use of Biometric Technologies for Security." *Security Industry Association*, 24 Jun. 2025, www.securityindustry.org/2025/06/24/groundbreaking-texas-ai-law-also-brings-needed-clarity-on-use-of-biometric-technologies-for-security/.