How AI Enhances Surveillance Against Communities Without Their Knowledge

By: Shaina Kumar and Rishi Chandra

Introduction

As Artificial Intelligence becomes more advanced and spectacular, it is easier to be lured into the "AI Hype" mindset, without critically analyzing the harms these technologies are perpetuating today. One such harm is the AI-enabled rapid advancement and proliferation of global surveillance systems that oppress marginalized communities. AI makes the work of surveillance much more hidden, thus allowing the enhancement of surveillance practices against marginalized communities to become more normalized and acceptable. This blog analyzes the technology behind AI-surveillance before focusing on two case studies (ICE in America and Israel's Occupation of the Gaza Strip) that illustrate how AI is entrenching and advancing these practices across governments and the globe.

How AI Is Revolutionizing Facial Recognition

In order to grasp how vulnerable we are in the presence of AI surveillance, it is important to understand the unique nature of these AI technologies compared with prior surveillance methods. AI surveillance, which relies on a combination of systems such as machine learning, computer vision, vision-language models, and edge computing, enables real-time search and analysis of video feeds ("What is AI Surveillance: Benefits, Applications and Future Potential"). As these technologies advance, analytics become cheaper and more accessible both publicly and privately (Stanley). Giving even more entities the ability to incorporate monitoring into their products makes it harder to identify when the practice occurs and to regulate how the monitoring is conducted and used. Our concern is that these surveillance mechanisms are becoming more pervasive and accessible while simultaneously less visible to those being monitored. The greater risk lies not with malicious actors but with trusted institutions exploiting the scalability of AI surveillance and the sheer number of people and behaviors it can monitor. Facial recognition specifically provides a clear example of how these broader AI capabilities are fundamentally reshaping surveillance. At a technical level, facial recognition systems are no longer static image matching; instead, they are AI-powered systems that can continuously identify and track individuals across contexts and environments in real time. Thus, facial recognition has surpassed targeted investigations, with agencies such as the TSA using it to automate identity verification and speed up airport security screening ("What is AI Surveillance: Benefits, Applications and Future Potential"). This new form of facial-recognition surveillance normalizes the collection of biometric data across spaces, but public understanding of how these systems operate may not be advancing as quickly as the technology itself.

AI and ICE

With the new capabilities AI has provided, facial recognition is no longer a tool for identification, but rather a tool for the monitoring of individuals at an unprecedented level of opacity. The evolution of its application and the extent of public awareness and consent are demonstrated clearly within the United States. Agencies like the U.S. Immigration and Customs Enforcement have expanded the use of facial recognition beyond its original intent, prompting concerns for more targeted regulation and governance. The original functionality primarily supported border enforcement, but it has expanded into forms of domestic monitoring that are discretely embedded in our lives. AI-powered immigration enforcement systems are now used to identify and investigate U.S. citizens through social media monitoring, location-tracking systems, and facial recognition databases, even though their capabilities were meant to track only non-citizens.

We can see evidence of this expansion through major investments in AI surveillance infrastructure.The DHS has awarded contracts, including $30 million for Palantir's ImmigrationOS platform, designed for granular tracking of immigrants and real-time monitoring of self-deportations, along with multimillion-dollar contracts for Clearview AI facial-recognition software and iris-scanning technologies from BI2 Technologies. ICE has also reportedly deployed social media monitoring and location-tracking systems capable of analyzing the movements of large groups of people baselessly, without warrants or individualized suspicion (Hubbard).

These systems are also being integrated into consumer-facing technologies that many individuals may not even recognize as surveillance tools or threats. Facial recognition capabilities integrated into platforms we use for everyday safety and security make it hard to distinguish between private technology and law-enforcement infrastructure. For example, Ring has introduced features marketed as convenient tools for recognizing family members, neighbors, or frequent visitors, called "Familiar Faces." However, this tool has the same underlying facial recognition capabilities that can also support ICE's efforts to locate people for mass deportation. Ring's recent cancellation of its partnership with Flock Safety, an AI-powered surveillance camera company that shares footage with law enforcement agencies, including ICE, further grounds our concern about consumer security products and government surveillance system entanglement (Silberling and Bort).

So far, we have described how facial recognition technologies have expanded beyond immigration enforcement and into the real-time monitoring of citizens who are not suspected of crimes at all with AI. We have also explicitly expressed concerns about privacy invasion and the lack of consent and awareness. However, we note that increased awareness of the presence of AI facial recognition systems alone does little to protect individuals once such surveillance becomes unavoidable. Individuals aware that their identities and behaviors can be continuously monitored

are likely less willing to openly express their beliefs or engage authentically in public and private life, out of fear of being monitored or flagged. This is where the need for stronger government oversight, transparency requirements, independent audits, and biometric privacy protections arises.

Israel's Surveillance In The Gaza Strip

AI-powered surveillance is not isolated to America, but is rather a transnational security phenomenon used to demarcate, oppress, and control individuals across the world. Israel's war (and alleged genocide) in the occupied Gaza Strip has shed light on how Israel uses facial recognition technology and other AI-powered monitoring systems to manage and control Palestinians.

Using technology from the Israeli company Corsight, Israel's military intelligence unit initially used a facial recognition program to search for captured Israelis who were taken hostage by Hamas during the October 7, 2023, attacks (Frenkel). However, as Israel adopted a more bellicose agenda, the technology's purpose switched to identifying and targeting Hamas terrorists or anyone tied to Hamas and other militant groups. Crucially, the technology is known to be faulty at identifying targets, despite Corsight claiming it needs less than 50% of a face for accurate identification (Frenkel).

Furthermore, Israeli intelligence uses Google Photos in conjunction with Corsight's technology. They upload photos of known people to Google Photos, creating a database that can be exploited, as Google Photos is known for its superior face-matching and identification capabilities, even with minimal visual information. Thus, cameras equipped with this tech are spread throughout the strip, unbeknownst to Palestinians. AI-powered facial recognition systems contribute to and exacerbate tensions (Frenkel). As mentioned previously, this facial recognition technology is not incredibly accurate and can easily lead to false accusations and racial profiling. For example, the poet Abu Tohah unknowingly walked into an area littered with facial-recognition embedded cameras, which accused him of being on an Israeli list of wanted people. These technologies have real-life consequences: Abu Toha was allegedly beaten and interrogated in a detention center for two days before being returned to the Gaza Strip (Frenkel).

In addition, Israel uses a series of different AI-powered tools to monitor the Gaza Strip, including "Lavender," "The Gospel," and "Where's Daddy?". "Lavender" is a machine learning tool that assigns Palestinians in Gaza a numerical score representing the suspected likelihood that they are involved with an armed group (Human Rights Watch). Analysts at Human Rights Watch believe Lavender (or another surveillance tool) uses a semi-supervised machine-learning technique called "positive unlabeled learning." According to Human Rights Watch, positive unlabeled learning "trains an algorithm from a dataset containing both labeled (positive) and unlabeled (negative) data." (Human Rights Watch). The algorithm combs through data on people suspected of affiliating with militant groups, then uses the characteristics it notes to identify additional suspects in the general population. "Lavender" and other predictive policing tools utilize biased, inaccurate data as well as broad definitions of "terrorism," thus leading to potential human rights violations. The issues with these algorithmic tools stem from their

black-box nature (in which AI systems are designed to hide their inner workings and are therefore much harder to hold accountable), biased data, and automation bias (in which people trust these tools because they believe they are more neutral than humans) (Human Rights Watch).

Conclusion

As AI technology becomes more advanced, it is crucial that we understand how these systems are being used to perpetuate harm against marginalized communities. The United States and Israel are just two examples of a broader trend of nation-states using AI to advance surveillance while normalizing it. AI-powered immigration tracking and the numerous multimillion-dollar contracts between the DHS and private AI contractors represent the increasing entrenchment of the US military-industrial complex. Likewise, Israel's use of biased tools like "Lavender" expands the power of the Israeli state while normalizing violence against Palestinians. Ultimately, a healthy democracy thrives when we discuss and analyze how the inventions of our time are being used to erode human rights and civil liberties.

Works Cited

Frenkel, Sheera. “Israel Deploys Expansive Facial Recognition Program in Gaza.” *The New York Times* [Tel Aviv], 27 Mar. 2024, Israel Deploys Expansive Facial Recognition Program in Gaza.

Hubbard, Steven. “ICE Uses a Growing Web of AI Services to Power Its Immigration Enforcement and Surveillance.” *American Immigration Council*, American Immigration Council, 18 December 2025, https://www.americanimmigrationcouncil.org/blog/ice-uses-ai-immigration-enforcement-surveillance/. Accessed 1 May 2026.

Hubbard, Steven. “Mission Creep: AI Surveillance at DHS Crosses Dangerous Line Into Tracking Americans.” *American Immigration Council*, American Immigration Council, 06 February 2026, https://www.americanimmigrationcouncil.org/blog/ice-ai-surveillance-tracking-americans/. Accessed 1 May 2026.

Silberling, Amanda, and Julie Bort. “Amazon's Ring cancels partnership with Flock, a network of AI cameras used by ICE, feds, and police.” *TechCrunch*, 13 February 2026, https://techcrunch.com/2026/02/13/amazons-ring-cancels-partnership-with-flock-a-network-of-ai-cameras-used-by-ice-feds-and-police/. Accessed 1 May 2026.

Stanley, Jay. “Machine Surveillance is Being Super-Charged by Large AI Models.” *ACLU*, American Civil Liberties Union, 21 March 2025, https://www.aclu.org/news/privacy-technology/machine-surveillance-is-being-super-charged-by-large-ai-models. Accessed 1 May 2026.

Questions and Answers: Israeli Military's Use of Digital Tools in Gaza | Human Rights Watch. 10 Sept. 2024, https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-of-digital-tools-in-gaza.

"What is AI Surveillance: Benefits, Applications and Future Potential." *Omnilert*, 7 April 2026, https://www.omnilert.com/blog/ai-surveillance-benefits-applications-and-future-potential. Accessed 1 May 2026.