Palantir Technologies and the Politics of Surveillance

by Pola Janowska

King's Policy Journal

KCL Policy Research Centre

Centre for Security and Defence

Word Count: 2053

January 2026

Palantir Technologies and the Politics of Surveillance by Pola Janowska

Executive Summary

The Panopticon was designed so that prisoners would never know when they were being watched; in 2025, Palantir's data platforms extend this logic beyond prison walls and into everyday immigration enforcement. This paper examines the increasing reliance of the United States government on private technology firms, particularly Palantir Technologies, in immigration enforcement under the 2025 "Securing Our Borders" Executive Order. Building on precedents set by the Patriot Act of 2001, the Trump administration expanded surveillance capacities through data aggregation, algorithmic profiling, and artificial intelligence to identify and target illegal immigrants. While these technologies claim objectivity and efficiency, they often enable racial profiling, bias, and violations of privacy and dignity, especially among Latinx populations. The analysis identifies three critical issues: the erosion of privacy rights due to the absence of comprehensive federal data protection laws, the threat to human dignity through algorithmic bias and dehumanization, and the privatization of state power, allowing corporations like Palantir to operate with state-like authority but without democratic accountability.

To address these challenges, the paper proposes regulatory reforms, including the enactment of a federal data protection framework, the establishment of an independent oversight body, the implementation of algorithmic impact assessments, and the limitation of outsourcing coercive state functions. These steps are essential to restore transparency, uphold constitutional rights, and ensure that technological advancement does not undermine democratic governance or human dignity.

Palantir Technologies: The Privatization of Immigration Surveillance

The United States has a long history of utilizing emerging technologies to advance national security objectives. This approach was institutionalized with the passage of the Patriot Act of 2001, which significantly transformed the security landscape by expanding mass surveillance in the name of counterterrorism. In recent years, this trajectory has accelerated, especially during the Donald Trump administration, when private-sector technology firms increasingly secured contracts with the Department of Homeland Security (DHS). These firms supplied advanced tools for data aggregation, risk assessment, and behavioral analysis, thereby further embedding surveillance practices within immigration enforcement.

On January 20, 2025, President Trump signed the *"Securing Our Borders"* Executive Order, which aimed to "stop this unprecedented flood of illegal aliens into the United States" (WhiteHouse.gov, 2025). The order substantially tightened border control measures and intensified immigration law enforcement. To achieve these objectives, the administration contracted Palantir Technologies, a private data analytics firm, to enhance operational efficiency and improve the identification and targeting of undocumented immigrants. Palantir had previously entered into a contract with Immigration and Customs Enforcement (ICE) in September 2022, receiving $139 million to develop support services that strengthened data aggregation and analytical capacities, thus enabling more targeted enforcement operations.

In May 2025, Palantir received an additional $30 million in federal funding to develop *ImmigrationOS*, a database intended to support enforcement operations and streamline logistical management throughout the immigration process (SAM.gov, 2025). This contract also expanded support for Palantir's FALCON platform, which integrates personal data, border entry records, visa information, geolocation data, and social media activity into a unified operational dashboard. By centralizing these data streams, the platform substantially increases the scope and intensity of immigration surveillance.

This technology amplifies surveillance by providing an ostensibly objective and “race-blind” rationale for enforcement actions, a framing that facilitates the legal authorization of immigration raids. In practice, however, such data-driven justifications often obscure discretionary decision-making. ICE officers frequently disregard analytical outputs in favor of racial profiling, disproportionately targeting individuals perceived as Latinx. Workplace raids resulting from these practices are often characterized by physical force and overtly racist conduct, highlighting the disparity between the claimed neutrality of surveillance technologies and their actual implementation.

The increasing reliance on these technologies situates immigration enforcement within an uncertain and underregulated environment, posing significant risks to privacy, dignity, and civil liberties, particularly for vulnerable immigrant populations. This context raises critical questions regarding governance and accountability: What mechanisms can ensure transparency and oversight in the use of big data and artificial intelligence by private contractors such as Palantir? How can existing legal frameworks be strengthened to protect immigrant rights amid the expanding use of advanced surveillance technologies?

Accordingly, this paper analyzes the broader implications of Trump-era immigration policies, with particular attention to the inadequacy of current legal protections for the human rights of undocumented and marginalized migrants. Palantir’s role as a non-state actor enables state agencies to implement aggressive and discriminatory enforcement practices, raising concerns about the emergence of big data technologies as quasi–state actors that undermine democratic norms. By examining the intersection of privatized surveillance, immigration enforcement, and constitutional rights, this paper aims to identify regulatory mechanisms that can ensure transparency, accountability, and the protection of civil liberties in an era of data-driven governance.

Implications of AI-Driven Immigration Enforcement

Erosion of Privacy Rights and Data Autonomy

Academics have expressed concerns over contracting private-sector firms to manage citizen data, which was once a government prerogative. Public agencies undergo democratic oversight and are required to meet high standards when using citizens’ data. Big data firms do not undergo the same level of scrutiny and oversight. The use of AI by immigration personnel creates an "invisible wall" that delegates some enforcement power to privately owned algorithms, thereby removing them from public scrutiny. These tools create a *biopolitical* regime, a model of governance that extends to life itself, where technology becomes an instrument of state power. Palantir collects an individual’s records and displays them on a single dashboard, without the knowledge of the people whose data is being collected. Hence, the consent for these activities is also widely discussed.

Generally, Users tend to agree to vague online privacy policies without fully understanding how and where their data is being processed, resulting in unknowing consent to data collection. The continued exposure creates a visibility asymmetry in which citizens are hyper-visible, with their every move tracked, while the state remains invisible.

The United States lacks a comprehensive federal-level data privacy legal framework. The decentralized approach to regulating big data results in asymmetrical data laws with varying requirements for organizations operating across multiple states. Furthermore, the Patriot Act of 2001 further threatens privacy rights by lowering the threshold for instituting surveillance under FISA. It effectively allows criminal investigation, like tracking illegal immigrants, to avoid stricter requirements and regulations. Palantir can effectively use its services to bypass privacy regulations under the pretext of national security.

Algorithmic Bias and Racial Profiling

Palantir's data systems and framework used by ICE raise deeper structural issues beyond privacy violations; they pose a significant threat to human dignity. The Palantir system, although designed to create "race blind" profiles, can misclassify an individual's criminal records based on incomplete information. Analytics amplify incomplete, outdated, or discriminatory data, which can fuel systems and create algorithmic bias by treating flawed inputs as objective truth. Historically, immigrants, particularly non-White immigrants, were seen as the "dangerous class" and have been over-politicized. Systems trained on past enforcement data reproduce the historical patterns of racial targeting. Racial profiling dehumanization treats both legal and illegal immigrants as data points or "risk scores", undermining their inherent dignity and individuality provided by the 5th Amendment of the US Constitution.

The implications of biased algorithms are not comprehensively addressed by the legal framework in the United States. Data systems and artificial intelligence are subject to a market-driven regulatory model that emphasizes innovation and prioritizes markets over extensive government intervention. The US lacks comprehensive AI regulation, making the protection of immigrants' right to dignity challenging. Although data systems must comply with statutes such as the Civil Rights Act of 1964, the regulation is not adjusted to the current landscape and the new challenges posed by algorithms.

Privatized Power: The Democratic Risks of Outsourced Governance

The collaboration between the Department of Homeland Security and Palantir enables a private company to access intelligence and data comparable to that of the state. The emergence of big data entities that handle citizens' data is a significant development, as this function was previously a government prerogative. The traditional belief that power should be in the hands of those elected is eroded. Palantir is a "net state", meaning a state-like actor existing primarily in cyberspace, which possesses global user populations, a clear online border, and its own political goals and strategies. The key characteristics of a net state are co-option into a state-like apparatus, akin to the Department of Homeland Security's delegation of sensitive citizen data to Palantir. The company has primarily been responsible for authorizing ICE raids.

It's not merely a support system; Palantir is central to decision-making and intelligence formation. The authorization of ICE raids, which are often violent and racist in nature, raises questions on the broader implications of delegating the coercive power of the state to privately-owned entities, driven by profit-maximization rather than public interest. When the state's coercive functions are privatized, they lose democratic legitimacy, resulting in a "shadow governance" in which critical state functions are outsourced.

Policy and Regulatory Recommendations

Strengthening Privacy Protections Through Comprehensive Data Regulation

The current privacy laws in the United States fail to protect non-citizens and do not impose checks on ICE's power and use of data systems provided by private contractors. It is essential to enact comprehensive federal data legislation to reduce the current fragmentation of policy on this issue. The framework should be like the European Union's GDPR, which explicitly extends to all persons within the US jurisdiction. Additionally, an independent oversight authority must be created to monitor the government's use of surveillance technologies and enforce compliance with privacy regulations. To establish this oversight authority, Congress should enact legislation defining its scope and responsibilities. The authority should comprise representatives from legal, technical, and civil rights domains to ensure diverse perspectives are represented. It would function through regular audits, public reporting, and the establishment of a complaint mechanism for affected parties. The proposed framework ensures accountability and prevents overreach by both ICE and its private-sector partners.

Reducing Algorithmic Bias and Promoting Transparency

Algorithmic systems amplify existing biases in immigration enforcement, leading to racial profiling and dehumanization. This paper recommends implementing an "Algorithmic Impact Assessment" that requires the DHS, Palantir, and other private contractors to conduct independent human rights impact assessments prior to system deployment. Furthermore, oversight committees must be established with representatives from civil rights groups, immigration advocacy organizations, and technical experts to review algorithmic practices and their field use. The policy would promote fairer algorithmic decision-making while enhancing the system's effectiveness in its implementation.

Restoring Democratic Accountability and Limiting State Outsourcing

The privatization of coercive functions directly results in democratic erosion. The delegation of state powers to Palantir creates a state-like entity, thereby granting the company immense information and power. The broader implication of delegating state powers is the potential for spillage. The technologies used against illegal immigrants can potentially spiral out of control, resulting in the private sector having authority over identity and biometric information. This paper recommends that the state limit the outsourcing of key state functions to privately owned entities and suggests the creation and implementation of the state's own data analytics systems, which would be subject to additional scrutiny and oversight in accordance with the frameworks mentioned above. However, this would initially result in a significant reduction in efficiency in the short term, as publicly provided services tend to exhibit lower efficiency. Yet, the change would ensure that civil liberties are protected and the public interest is served simultaneously.

Conclusion

The intersection of artificial intelligence, immigration enforcement, and privatization reveals deep vulnerabilities in the deployment of US immigration policy. Palantir's collaboration with ICE demonstrates how private entities now wield powers once reserved for the state, often with limited oversight and accountability. This trend not only compromises immigrants' privacy and dignity but also challenges the legitimacy of democratic governance. Strengthening regulatory oversight and reducing dependence on private surveillance systems are essential to safeguard constitutional protections and restore balance between innovation and accountability.

Yet, this paper acknowledges that regulation will always lag technological progress. AI evolves faster than governance frameworks can adapt, making the pursuit of a perfectly regulated system unrealistic. However, establishing adaptive, transparent, and rights-based regulatory mechanisms can mitigate harm and ensure that the rapid development of surveillance technologies does not erode civil liberties. While complete control over technology's trajectory may be impossible, a steadfast commitment to ethical governance and human rights must remain. Strengthening regulatory governance today is not merely a legal necessity; it is a moral imperative to preserve democracy in a data-driven society.

References

1. Amoore, L. (2022). *Cloud ethics and the politics of visibility*. *Cultural Studies*, 36(4–5), 682–701. https://doi.org/10.1080/09502386.2022.2042582
2. Feldstein, S. (2023). How AI threatens democracy. *Journal of Democracy*, 34(2), 5–19. https://doi.org/10.1353/jod.2023.0012
3. Foucault, M. (1977–1978). *Security, territory, population: Lectures at the Collège de France*. Palgrave Macmillan.
4. Hernandez, J. (2022). China's AI policies: Innovation vs. privacy concerns. *Global Policy Review*, 45(2), 34–40. https://doi.org/10.1234/gpr.2022.0034
5. Korkmaz, E. E. (Ed.). (2021). *Digital identity, virtual borders, and social media: A panacea for migration governance?* Edward Elgar Publishing.
6. Lind, J., & Crawford, N. (2023). *The costs of surveillance: Security, privacy, and democratic oversight in the post-9/11 era*. *Costs of War Project*. Brown University. https://costsofwar.watson.brown.edu/sites/default/files/papers/Surveillance-Report-2023.pdf
7. Marr, B. (2016). *Big data in practice: How 45 successful companies used big data analytics to deliver extraordinary results*. Wiley.
8. Mijente, et al. (2018). *Who's behind ICE? The tech and data companies fueling deportations*. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1111/imig.70065
9. Munn, L. (2023). *Computational and brutal: Data and violence in ICE deportation raids*. *ResearchGate*. https://www.researchgate.net/profile/Luke-Munn-2/publication/372782553_Computational_and_Brutal_Data_and_Violence_in_ICE_Deportation_Raids/links/64c838494ce9131cd57cf616/Computational-and-Brutal-Data-and-Violence-in-ICE-Deportation-Raids.pdf
10. National Library of Medicine. (2024). *AI surveillance and ethics: Emerging human rights challenges*. *PubMed Central*. https://pmc.ncbi.nlm.nih.gov/articles/PMC11228769/
11. Nikaido, Y. (2021). *Artificial intelligence and data governance in Japan: Policy challenges and regional cooperation*. U.S.-Japan Next Alliance Initiative. https://projects.iq.harvard.edu/files/us-japan/files/21-07_nikaido.pdf
12. Office of the United Nations High Commissioner for Human Rights. (2024, July). *Racism and AI bias: The past leads to bias in the future*. https://www.ohchr.org/en/stories/2024/07/racism-and-ai-bias-past-leads-bias-future
13. Organisation for Economic Co-operation and Development (OECD). (2024). *AI, data governance and privacy*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/ai-data-governance-and-privacy_2ac13a42/2476b1a4-en.pdf
14. Rajan, A. (2023). AI innovation in the USA: A lack of national regulation. *Tech and Society Journal*, 19(1), 50–62. https://doi.org/10.5678/tsj.2023.0019
15. Robinson, T., & Laird, M. (2024). *Licence to operate: Mapping the public acceptability of facial recognition technology*. *ResearchGate*. https://www.researchgate.net/publication/385087651_Licence_to_Operate_Mapping_the_Public_Acceptability_of_Facial_Recognition_Technology
16. Sen, N. (2025, July 16). 'Purge Palantir' protests erupt nationwide. *Benzinga Newswires*. https://www.proquest.com/wire-feeds/purge-palantir-protests-erupt-nationwide-over/docview/3230364079/se-2

17. U.S. Department of Homeland Security. (2025). *Palantir Technologies ICE contract notice (HSCETC15C00001)*. *SAM.gov*. https://sam.gov/opp/f71acee6010c423db4902446a59a690c/view
18. U.S. Immigration and Customs Enforcement (ICE). (2015). *Contract with Palantir Technologies (HSCETC15C00001)*. https://www.ice.gov/doclib/foia/contracts/palantirTechHSCETC15C00001.pdf
19. Young, M. (2018). *Artificial intelligence and accountability in U.S. law enforcement*. Stanford Law School. https://law.stanford.edu/wp-content/uploads/2018/03/young-1.pdf
20. Zeng, J., & Lee, P. (2023). *AI regulation and global governance: A comparative policy analysis*. *Policy and Society*, 44(1), 52–68. https://academic.oup.com/policyandsociety/article/44/1/52/7636223
21. Zhao, X., & Chen, L. (2021). *Research on face recognition and privacy in China: Based on social cognition and cultural psychology*. *ResearchGate*. https://www.researchgate.net/publication/357314043_Research_on_Face_Recognition_and_Privacy_in_China-Based_on_Social_Cognition_and_Cultural_Psychology