

Leehee Brauner

Abhijit Sarmah

English 1101

3 October 2025

What are the long-term societal and ethical consequences of relying on private AI-driven surveillance platforms like Palantir in the name of national security?

Before I began this project, I believed that the surveillance technologies, despite imposing on our privacy, overall made our society safer. I knew that the data being collected from our phones, social media, and even traffic cameras put us at risk for hacking, identity theft, or harassment; but that these risks did not outweigh the benefits to national security. I assumed that these surveillance technologies were developed and managed by the Department of Defense and used in improving national security and public safety. My perspective began to shift after attending a talk by the Alexander Hamilton Society, an international affairs club on campus, where I learned how AI was being integrated into surveillance technologies. During a talk on private AI surveillance companies, specifically Palantir, I learned what a huge role Palantir played not just in U.S. national security, but also the local and state police forces. When I realized that these AI surveillance systems were designed and owned by private firms with very little public oversight, it unsettled me. As an international affairs student interested in national and global security, I wondered whether entrusting vital security functions to private companies could put the public at risk. I hypothesized that these AI platforms improved the accuracy of surveillance and decision-making in the short term, but that these short-term security benefits

came at a deeper cost in terms of normalizing pervasive surveillance and the ethics of using surveillance technologies that may ultimately weaken the values and security they were meant to protect..Although at first I believed that AI surveillance platforms like Palantir improved national security by making intelligence more precise, after researching, I realized that their biggest impact is not their ability to process large amounts of data but that they restructured the foundations of the security administration, which came at the expense of democratic oversight.

The US and most Western governments have become dependent on Palantir as their main data analytics platform, blurring the line between national and state security agencies and private corporations. Scholars Ulbricht and refer to this dependence as “infrastructural” in their article, “In Palantir We Trust? Regulation of Data Analysis Platforms in Public Security,” because the whole defense system has grown reliant on these AI-powered tools. AI platforms like Palantir integrate information from millions of separate databases and run it through their own interfaces. These interfaces allow them to choose how the data is presented, meaning they choose what is deemed dangerous and how officials see the data (Ulbricht & Egbert 4). Most data-protection laws, like the European Union’s General Data Protection Regulation (GDPR), were written to regulate discrete data controllers or processors. These laws were not written with “infrastructural intermediaries” like Palantir in mind; therefore, they can't be practically applied to it. A 2021 report by Privacy International, *All Roads Lead to Palantir*, documents how being an infrastructural intermediary allowed Palantir to grow quickly inside the public health and security sectors in the UK. The report shows of the contracts between Palantir and the British government were negotiated under emergency COVID-19 procurement rules, meaning they did not have to abide by the usual parliamentary-oversight procedures , which would have made Palantir compete for the bid and undergo inspection by elected public officials (Privacy

International 9). These quick deals gave Palantir a foot in the door to access to sensitive immigration, policing, and health data without having to deal with democratic consent or debate over privacy laws. This report shows that Palantir's dominance is not only dangerous because it leads to a loss of individual privacy, but also because it undermines public accountability. When the infrastructure of security is privately owned, elected officials and courts can be sidelined. This lack of democratic accountability leads to public mistrust of the government. When there is no trust, there is no consent of the governed, and therefore, the very foundations of democracy are shaken. I realized that my initial expectation that this debate would be over whether individuals were losing privacy was wrong, and that the deeper issue is structural. Embedding these private infrastructures into national-security systems risks governments losing the ability to define priorities and oversee the tools they use. This led me to question whether the promise of more precise and humane targeting in warfare was even trustworthy when the categories and visualizations themselves are defined by private actors.

Through my research, I found that AI surveillance tools do not just raise structural concerns; they bring into light ethical questions about how we define “precision” and how we apply it on a national security level. Helkala, Lucas, Barrett, and Syse argue in “Ethical Challenges in AI-Enhanced Military Operations” that AI technologies are often marketed as reducing civilian casualties and enabling faster, more informed decisions (2). At first, this seems like a clear moral motive for developing AI surveillance tools, because fewer mistakes in targeting should mean fewer lives lost, right? This concept may not be so straightforward. One of the tools offered by Palantir is called the Investigative Case Management (ICM), “the ICM system provides case-management tools that integrate data from external repositories, store case information for sharing and reporting, and link telecommunications data obtained through

subpoenas.” (DHS, 2016) . According to Knight and Gekker’s study, ICM's profiling determines how investigators see and interpret information, shaping what they consider relevant or suspicious. These profiles are based on existing biases, meaning the algorithm categorizes people based on race, income, location, etc. These flagged individuals may be subject to disproportionate scrutiny or inaccurate assumptions (Knight & Gekker, 8). When data is being categorized, visualized, and prioritized by a private company, even if there are fewer operational errors, it embeds systemic biases in decision-making processes. These sources made me realize that we can't measure the ethics of AI surveillance just based on efficiency or casualty reduction; we must take into account who controls the data and definitions, and how these definitions affect real-life outcomes. When these biased systems are used over and over again, it normalizes using private companies' objectives in government decisions, and its consequences extend far beyond the immediate operational gains.

The more I researched, the more I realized that normalizing the use of private AI surveillance by the government did not just impact individual privacy rights or even those of local authorities, it changed the whole sphere of international security practices and had long-term repercussions on societies. We saw through Ulbricht and Egbert's report how Palantir has become a permanent infrastructural actor in several European security agencies. This dependence leaves states reliant on corporate definitions of what is a risk versus what is secure , rather than operating like a democracy, where decisions are based on deliberation and votes. Privacy International’s report "All Roads Lead to Palantir" (2021) demonstrates how quickly such platforms can expand through shady, opaque procurement processes. Globally, this normalization does not just suggest that private companies are making public decisions, it also carries some serious threats to national security. For instance Palantir can export its tools to rival

nations with no loyalty to U.S. interests. The societal implications for the average person are just as terrifying. Perpetual monitoring, where everyday activities, relationships, and even the use of social media are inputted into algorithmic profiles, generates suspicion, the silencing of free speech, and discourages people from participating in politics. The marginalized communities are the most severely affected as they are the ones that suffer the most from the increased scrutiny and punishment of the kind. AI surveillance does not stop at questions of effectiveness or short-term operational wins; it alters social norms, changes the nature of the relationship between citizens and their governments, and has a hand in the geopolitical distribution of power.

In my research question, I asked about the long-term societal and ethical consequences of surveillance platforms like Palantir. I originally assumed that AI surveillance tools' benefits to national security outweighed their flaws. However, after researching, I found that benefits such as improved data integration, faster intelligence processing, and more precise operational decisions remove nearly all democratic oversight, embed corporate logic into state decision-making, and normalize surveillance in ways that are difficult, if not impossible, to reverse. As an international affairs student, this research made me reconsider the trade-offs between protecting our current needs, such as protecting our citizens' rights now, versus preserving democratic accountability for future generations. These AI surveillance tools are more efficient and make fewer errors, but they also raise questions about who controls the lens through which governments interpret threats and how that power shapes our societies both domestically and abroad. In the end, I think surveillance isn't inherently good or bad, but how we use the information it gives us can be tricky. It can be difficult to figure out how to not overstep on core values such as freedom, privacy, and accountability, all of which security is meant to defend. In the end, the long-term societal and ethical consequences of these technologies depend on the

government's ability to balance security needs while preserving democratic principles, so the tools meant to protect us don't end up controlling us.

Work Cited

Helkala, Kirsi M., George Lucas, Edward Barrett, and Henrik Syse, editors. "Editorial: Ethical Challenges in AI-Enhanced Military Operations." *Frontiers in Big Data*, vol. 6, 2023, article 1229252.

Iliadis, Alexandros, and Lauren Acker. *The Seer and the Seen: Innovation, Vision, and Surveillance in the Data-Driven City*. MIT Press, 2022.

Knight, Will, and Rafi Gekker. "Palantir's Investigative Case Management (ICM) Platform and Its Ethical Implications." *Journal of Surveillance Studies*, vol. 8, no. 1, 2023, pp. 5–18.

Privacy International, and NoTechForTyrants. All Roads Lead to Palantir: A Review of How the Data Analytics Company Has Embedded Itself Throughout the UK. Privacy International, 2021. PDF.

Ulbricht, Daniel, and Lauren Egbert. “In Palantir We Trust? Regulation of Data Analysis Platforms in Public Security.” *Surveillance & Society*, vol. 22, no. 3, 2024, pp. 1–14.

United States, Department of Homeland Security. Privacy Impact Assessment for the Investigative Case Management (ICM) System. 7 July 2016, www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-july2016.pdf

National Institute of Standards and Technology (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce, Jan. 2023, <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

.

Office of Science and Technology Policy (OSTP). Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. The White House, Oct. 2022, <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>

.

Brundage, Miles, et al. “Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims.” *Journal of AI Policy*, vol. 1, no. 2, 2020, pp. 1–25, <https://arxiv.org/abs/2004.07213>

.

Defense Advanced Research Projects Agency (DARPA). AI Next Campaign. U.S. Department of Defense, 2018, <https://www.darpa.mil/work-with-us/ai-next-campaign>