
AMNESTY INTERNATIONAL

AMR 51/0211/2025

PALANTIR: RESPONSE FROM PALANTIR TO AMNESTY INTERNATIONAL

As part of its research into the United States' use of artificial intelligence (AI)-powered surveillance tools used to monitor migrants, including international students who are speaking up for Palestinian human rights and protesting the ongoing Genocide in Gaza, Amnesty International wrote to companies Palantir Technologies and Babel Street on 10 July 2025 requesting information on our findings. Babel Street did not respond and Palantir sent a response on 24 July 2025 which is attached below. This is in relation to the press release *USA/Global: Tech made by Palantir and Babel Street pose surveillance threats to pro-Palestine student protestors & migrants*.

Ref: TC AMR 51/2025.6879

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

Dear [REDACTED],

RE: PALANTIR'S LINKS TO THE MONITORING OF ACTIVISTS AND IMMIGRATION ENFORCEMENT IN THE UNITED STATES

I am writing from Amnesty International, an independent global human rights movement of more than ten million people.

Amongst other issues, Amnesty International campaigns to make sure that governments uphold their legal obligation to protect the rights of refugees, asylum-seekers, and migrants. Amnesty International also campaigns for corporations to respect human rights given that companies have a responsibility to respect human rights wherever they operate in the world. As Palantir's own Human Rights Policy acknowledges, the scope and meaning of this responsibility have been articulated in the UN Guiding Principles on Business and Human Rights (UN Guiding Principles). The UN Guiding Principles require all businesses, from small and medium-sized enterprises to large multinational enterprises, to avoid causing or contributing to adverse human rights impacts through their own business activities. Companies should also use their leverage to mitigate and address any such adverse impact that is directly linked to their operations, products or services through their business relationships, including by cooperating in their remediation.¹

In order to meet their corporate responsibility to respect human rights, companies should carry out human rights due diligence to identify, prevent, mitigate and account for how they address their any risks or impacts on human rights. The UN Guiding Principles also underscore the importance of communicating externally about how businesses address human rights impacts, particularly when concerns are raised by or on behalf of affected people. Specifically, Principle 21 of the UN Guiding Principles states: "Business enterprises whose operations or operating contexts pose risks of severe human rights impacts should report formally on how they address them. In all instances, communications should... [p]rovide information that is sufficient to evaluate the adequacy of an enterprise's response to the particular human rights impact involved". The corporate responsibility to respect applies fully and equally to all businesses regardless of their size, and sector, ownership and structure.

¹ United Nations Guiding principles on business and human rights, UN Doc. HR/PUB/11/04, 2011
[ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf](https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf)

Furthermore, this responsibility is independent of a State's own human rights obligations and exists over and above compliance with national laws and regulations protecting human rights.²

Amnesty International has reviewed documentation detailing Palantir's role in supplying the US' Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) with products that have enabled the monitoring of migrants, including student activists, and powered widely disproportionate and human rights violating immigration enforcement in the United States. Of particular concern is the current US administration's "Catch and Revoke" system,³ which combines social media monitoring, visa status tracking, and automated threat assessment, potentially leading to arbitrary deportations and violations of privacy rights. Among the at least 80 ongoing AI projects housed at ICE and CBP as of this time, the surveillance and analytics products supplied by Palantir's Immigration OS match the capabilities described under the 'Catch and Revoke' system.

I am writing today to notify you that on the basis of the review of documentation noted above, Amnesty International will be publishing research on key human rights risks pertaining to Palantir's links to the monitoring of activists and immigration enforcement in the USA and to provide you with an opportunity to respond and provide further information prior to publication. We are making you aware of this research to provide you with an opportunity to respond and provide further information prior to publication, and to ensure that your response is appropriately reflected in the final publication.

In addition to commenting on the conclusions below, please do provide any information on how Palantir has fulfilled its human rights responsibilities on this matter, including any and all human rights due diligence efforts.

Our conclusions in relation to Palantir are detailed below:

THE USE OF PALANTIR PRODUCTS IN CATCH & REVOKE

Recent developments in US surveillance systems present significant human rights concerns, particularly in the context of heightened monitoring of student activists, including Palestinian solidarity protestors, and immigration enforcement. The integration and centralization of previously disparate surveillance tools, coupled with new executive orders and aggressive border and immigration enforcement policies, has created an unprecedented system of monitoring and control. Of particular concern is the "Catch and Revoke" system,⁴ which combines social media monitoring, visa status tracking, and automated threat assessment, potentially leading to arbitrary deportations and violations of privacy rights.⁵

As of 9th April, the U.S. Citizenship and Immigration Services (USCIS) publicly acknowledged to: 'consider social media content that indicates an alien endorsing, espousing, promoting, or supporting antisemitic terrorism, antisemitic terrorist organizations, or other antisemitic activity as a negative factor in any USCIS **discretionary analysis** when adjudicating immigration benefit requests. This guidance is effective immediately.'⁶

² UNGPs, Principle 11 including Commentary.

³ United States Department of State, '100 Days of an America First State Department', April 2025, <https://www.state.gov/releases/2025/04/100-days-of-an-america-first-state-department/>

⁴ United States Department of State, '100 Days of an America First State Department', April 2025, <https://www.state.gov/releases/2025/04/100-days-of-an-america-first-state-department/>

⁵ US Citizenship and Immigration Services (USCIS), 'DHS to Begin Screening Aliens' Social Media Activity for Antisemitism', 9 April 2025, <https://www.uscis.gov/newsroom/news-releases/dhs-to-begin-screening-aliens-social-media-activity-for-antisemitism>

⁶ US Citizenship and Immigration Services (USCIS), 'DHS to Begin Screening Aliens' Social Media Activity for Antisemitism', 9 April 2025, <https://www.uscis.gov/newsroom/news-releases/dhs-to-begin-screening-aliens-social-media-activity-for-antisemitism>

Review of documentation by Amnesty International has found that Palantir's ImmigrationOS possesses automated open-source intelligence (OSINT) capabilities that enable constant monitoring, surveillance, and assessments. These include real-time monitoring of social media posts across multiple platforms, pattern recognition and sentiment analysis, data aggregation from various public and private sources multiple government databases, automated threat assessment, potentially leading to arbitrary deportations and violations of privacy rights. These capabilities match those described in the Catch and Revoke system.

The application of AI surveillance tools in the current context supercharges intimidation efforts by the US authorities against migrants, with heightened risks to peaceful student protestors across campuses for showcasing solidarity against an ongoing genocide in Gaza.

The human rights implications risks and impacts of your product being used in this context are of grave concern. These systems risk contributing to human rights violations, namely the rights to privacy, freedom of expression and access to information, freedom of movement equality and non-discrimination, and the right to liberty and protest.

The Catch and Revoke system draws upon products that the US State Department holds private contracts for; the department acknowledges that it currently hosts at least 80 AI projects/use cases on their own website.⁷ A number of different products are listed for social media and open-source intelligence "on travelers who may be subject to further screening for potential violation of laws that CBP is authorized to enforce or administer."⁸ Amnesty International was also able to identify a completed contract between ICE's Enforcement and Removals Operations and Palantir Technologies, detailing the wide-ranging features provided by the company.⁹

Amnesty reviewed documentation detailing how Palantir was awarded a \$30M contract by ICE to track self-deportations and identify priority deportation cases, particularly visa overstays. According to media reports, leaked slack [message](#) by Akash Jain, Chief Technology Officer of Palantir Technologies and President of Palantir USG,¹⁰ have stated: "Over the last few weeks we prototyped a new set of data integrations and workflows with ICE" and added: "The new administration's focus on leveraging data to drive enforcement operations has accelerated those efforts."

The system, referred to as Immigration Lifecycle Operating System (Immigration OS), was contracted for on April 11, 2025, by the current administration, the date for which it was required to be operational as well. Immigration OS serves as an upgrade to Palantir's Investigative Case Management system, already used by ICE since 2014,¹¹ according to procurement documents reviewed by Amnesty International.¹²

⁷ US Department of Homeland Security, 'United States Customs and Border Protection – AI Use Cases', <https://www.dhs.gov/ai/use-case-inventory/cbp>

⁸ US Department of Homeland Security, 'United States Customs and Border Protection – AI Use Cases', <https://www.dhs.gov/ai/use-case-inventory/cbp>

⁹ System for Award Management (SAM.gov), 'Investigative Case Management - Additional Capabilities', 11 April 2025, <https://sam.gov/opp/f71acee6010c423db4902446a59a690c/view>

¹⁰ 404 Media, 'Leaked: Palantir's Plan to Help ICE Deport People', 17 April 2025, <https://www.404media.co/leaked-palantirs-plan-to-help-ice-deport-people/>; US Department of Homeland Security, 'United States Customs and Border Protection – AI Use Cases', <https://www.dhs.gov/ai/use-case-inventory/cbp>

¹¹ System for Award Management (SAM.gov), 'ICE Investigative Case Management System', 26 September 2014, <https://sam.gov/opp/36fb3b697a2ccb4ec7084b4e0ec6cdb9/view>

¹² System for Award Management (SAM.gov), 'Investigative Case Management - Additional Capabilities', 11 April 2025, <https://sam.gov/opp/f71acee6010c423db4902446a59a690c/view>

ICE's Enforcement and Removals Operations (ERO)'s technical needs for the completed contract have been described in their own words below, as listed on the U.S. General Services Administration Federal Government's System for Award Management (SAM) site:

"ICE Enforcement and Removals Operations (ERO) urgently requires the following system capabilities and outcomes, hereby referred to as ICE's Immigration Lifecycle Operating System (ImmigrationOS), in support of Presidential Executive Orders including EO 14159 - Protecting the American People Against Invasion and Executive Order 13773 - Enforcing Federal Law With Respect to Transnational Criminal Organizations and Preventing International Trafficking:

Targeting and Enforcement Prioritization, which includes streamlining selection and apprehension operations of illegal aliens based on ICE enforcement priorities—especially affiliates of known transnational criminal organizations (TCOs), violent criminals, and visa overstays.

Self-Deportation Tracking, which includes near real-time visibility into instances of self-deportation and integration with enforcement prioritization systems to inform policy, ensure efficient appropriate resource allocation, and accurately report metrics of alien departures from the United States.

Immigration Lifecycle Process, which includes streamlined end to end immigration lifecycle from identification to removal, with increased efficiency in deportation logistics, minimizing time and resource expenditure.

ICE requires software licenses, configuration services, engineering services, and hosting services in order to obtain a prototype of ImmigrationOS prior to September 25, 2025. ICE proposes to modify the existing Investigative Case Management (ICM) System Task Order 70CTD022FR0000170 in order to procure these services."

The use of AI-enabled tools like Palantir's ImmigrationOS, combined with abusive and discriminatory administrative powers in visa revocation,¹³ warrantless raids, detention, and deportations, is of high risk of creating a chilling effect on human rights, particularly affecting individuals in vulnerable situations. The fact that the system is couched in a political context that asymmetrically targets specific ethnic and religious groups, and has seen further degradation since the start of 2025—in particular through the execution of the Catch and Revoke initiative—furthermore, raises serious concerns about discrimination and profiling.

The overarching context of repression,¹⁴ and discriminatory surveillance and immigration enforcement practices,¹⁵ in particular against international students,¹⁶ demonstrates the clear risk of contributions to human rights violations posed to any actor or technology that aids the administration in these endeavours. The use of

¹³ Amnesty International, 'Stop revoking visas of foreign students', 21 April 2025, <https://www.amnesty.org/en/documents/amr51/9290/2025/en/>

¹⁴ Amnesty International, 'People seeking safety at risk in the USA', 21 January 2025, <https://www.amnesty.org/en/documents/amr51/8933/2025/en/>; Amnesty International, 'Unlawful Expulsions to El Salvador Endanger Lives Amid Ongoing State of Emergency', 25 March 2025, <https://www.amnesty.org/en/latest/news/2025/03/unlawful-expulsions-to-el-salvador-endanger-lives-amid-ongoing-state-of-emergency/>

¹⁵ Amnesty International, 'Urgent Action: Stop Revoking Visas of Foreign Students', 22 April 2025, <https://www.amnesty.org/en/wp-content/uploads/2025/04/AMR5192902025ENGLISH.pdf>

¹⁶ Amnesty International USA, 'Amnesty International USA and ACLU Work with College and University Students to Help Protect their Campuses from President Trump's Attack on Human Rights', 16 April 2025, <https://www.amnestyusa.org/press-releases/amnesty-international-usa-and-aclu-work-with-college-and-university-students-to-help-protect-their-campus-from-president-trumps-attack-on-human-rights/>

ImmigrationOS within the Catch & Revoke framework risks creating an unprecedented surveillance apparatus that enables mass monitoring and automated decision-making affecting individuals' human rights.

FAILURE TO PROACTIVELY PREVENT OR ADEQUATELY MITIGATE ABUSES OF THE HUMAN RIGHTS OF TARGETED MIGRANT COMMUNITIES

The reported supply of products to the current US administration would indicate that Palantir Technologies are operating against its own stated human rights concerns about work with ERO and CBP under the Trump administration. Knowledge of possible human rights harms, and a failure to take appropriate action to prevent and mitigate such harms, suggests a major failure of human rights due diligence by the company. Palantir could and should have known about the possible human rights violations committed by ICE and could and should have refrained from entering a further contractual relationship for ImmigrationOS. The fact that Palantir itself has historically raised concerns around this demonstrates that the company has the capacity to analyse and understand the human rights but chose to enter a contractual relationship with ICE irrespective of these risks. Palantir's conduct with the current administration has raised serious human rights concerns, including violations of:

- **The right to privacy:** Through extensive data collection and processing without knowledge and consent, Palantir products could be used to subject individuals residing in the USA to routine violations of their rights to privacy, by treating them as suspicious by default, without suspicion or documentation of criminal wrongdoing. By extending the dragnet of surveillance and residency consequences on the basis of political speech—and specifically, speech that is calling for the rights of another population to be observed under international law—Palantir Technologies is empowering the current administration in its illegitimate, disproportionate, and unnecessary abuses of this technology.
- **The right to freedom of expression and peaceful assembly:** Through mass surveillance and potential targeting of political speech, Palantir products can be used to target people directly for arrest and deportation, on the basis of their protected expression. Students, and any resident in the USA, could be subjected to unwarranted flagging, identification, detention and deportation, on the basis of expression and protest, as has been documented extensively over the last 6 months. Palantir products can furthermore be used to impart a chilling effect on individuals, and in particular students, engaged in their constitutional and international human right to protest.
- **Right to equality and non-discrimination:** Palantir's continued support, and its addition of further automated surveillance capabilities to the US government's discriminatory and arbitrary immigration policies, risks contributing to ongoing human rights violations. The current administration's repressive tactics and summary revocation of people's immigration status demonstrate a lack of respect for human rights to freedom of expression and peaceful assembly. It represents an overt violation of the right to equality and non-discrimination, with visa-holders, and asylees explicitly targeted by the AI-driven systems. Through the use of automated tools that prioritise 'deportation efficiency', in a context in which abusive government practices in relation to immigration, and international students in particular, Palantir risks further exacerbating discriminatory outcomes faced by targeted individuals.

CONCLUSION

In the past, Palantir itself has acknowledged that its contracts with CBP were controversial, demonstrating its awareness of the risks.¹⁷ In 2019, in its S-1 filing, Palantir identified a reputational risk to its business, acknowledging, “Our relationships with government customers and customers that are engaged in certain sensitive industries, including organizations whose products or activities are or are perceived to be harmful, has resulted in public criticism, including from political and social activists, and unfavorable coverage in the media. Activists have also engaged in public protests at our properties.”¹⁸ In fact, Palantir’s own employees have protested its contracts with DHS facilitating abusive immigration enforcement.¹⁹

In a letter addressed to Amnesty International on 19 October 2020, during the 1st Trump administration, Palantir acknowledged that it had *‘[...] purposefully declined to take on contracts with ERO and CBP under the current Administration because we share your organization’s concern with the potential serious human rights violations against migrants, refugees, and asylum seekers at the U.S. – Mexico border and risks of disproportionate immigration enforcement inside the U.S.’*²⁰

In June 2025, ten Senators and Representatives further expressed concern and demanded transparency from Palantir on its contracts with the federal government.²¹

Based on Amnesty International’s assessment of available documentation, Palantir Technologies has failed to fulfill its human rights responsibilities due to the lack of adequate human rights due diligence, by not taking appropriate measures to prevent and mitigate their products being used by the US Administration to systematically impart human rights abuses on migrant communities within the United States, including students. In so doing, Palantir are risking contributing to serious human rights violations, the risks of which it should and could have known about. Palantir must immediately cease their work with the US administration related to immigration enforcement, and they must conduct and publish the full findings of human rights due diligence processes

Amnesty International intends to publish a public statement about our concerns and may include part or all of your response in the statement. To enable us to consider incorporating this into our public statement, please respond by email to [REDACTED] copied in, by the close of business on 24 July 2025.

¹⁷ See, e.g., www.washingtonpost.com/business/2019/08/22/war-inside-palantir-data-mining-firms-ties-ice-under-attack-by-employees/.

¹⁸ United States Securities and Exchange Commission, FORM S-1REGISTRATION STATEMENT UNDER THE SECURITIES ACT OF 1933, Palantir Technologies Inc., 25 August 2020, available at <http://edgar.secdatabase.com/2567/119312520239121/filing-main.htm>

¹⁹ The Washington Post, ‘The war inside Palantir: Data-mining firm’s ties to ICE under attack by employees’, 22 August 2019, <http://www.washingtonpost.com/business/2019/08/22/war-inside-palantir-data-mining-firms-ties-ice-under-attack-by-employees>.

²⁰ Business and Human Rights Resource Centre, ‘RE: Amnesty International Letter dated 10 September 2020’, 18 September 2020, https://media.business-humanrights.org/media/documents/Palantir-Technologies-Response-to-Amnesty-International-Letter_VYQb6ID.pdf

²¹ The New York Times, ‘Lawmakers Demand Palantir Provide Information About U.S. Contracts’, 17 June 2025, <https://www.nytimes.com/2025/06/17/technology/palantir-government-contracts-democrats-letter.html?smid=nytcore-ios-share&referringSource=articleShare>

Sincerely,



Amnesty Tech,
Amnesty International



[REDACTED]

Dear [REDACTED] and [REDACTED],

We appreciate the opportunity for Palantir Technologies (“Palantir”) to respond to your letter (ref TC AMR 51/2025.6879) and to provide a direct response to allegations raised prior to the release of your planned report on Palantir’s alleged ties to purported human rights violations taking place in the US around immigration enforcement. As with previous inquiries from Amnesty International, we welcome sincere, good faith engagement to provide more detail about our work. We also want to correct the record about where and how our products are being used, especially in domains with the potential to impact fundamental rights. As you note in your letter, Palantir’s human rights policy includes a stated commitment to respect human rights in our work; that policy has its roots in the founding thesis of our company and more than 20 years of work enabling public, private, and non-profit sector institutions to address the world’s most challenging problems, from defense, to healthcare, to disaster response.

Before addressing the specific claims of your letter, we note our deep concern with and objections to its framing, which includes incorrect claims about Palantir’s work. We welcome an open dialogue about the important issues raised by your letter, but it is critical that those discussions are grounded in truth. Given Palantir’s role in providing essential services to the US government across multiple administrations, we strive to be as transparent as possible about how our software products work. We have published extensive information about our products in the public domain to address common misperceptions about Palantir’s work, which includes allegations in your letter.

In order to provide as much clarity as possible, we’re delineating our response to your report into the following parts: 1) addressing the underlying claims within your letter, including correcting certain key facts about Palantir’s contracts with the US federal government; 2) responding to the specific allegation that Palantir is providing a technology platform to enact the recent “Catch and Revoke” policy; 3) explaining how Palantir views the need for institutional engagement on key public challenges over withdrawal; and 4) addressing the charge that Palantir needs to provide more transparency about our work.

Section 1: Addressing the underlying claims within the letter, especially with regard to the conflation of key facts around existing Palantir contracts with the federal government (which agencies do what, where Palantir has contracts) including correcting certain key facts about Palantir’s contracts with the federal government.

As with all of Palantir’s work, we welcome transparency wherever permissible with respect to the specific character of our products and customer engagements. To be explicit on our actual scope of contractual work: Though we will continue to explore work across government

agencies for which we think our software can positively impact critical mission outcomes, Palantir has no current contracts with CBP. In fact, our last contractual relationship with CBP ended in 2013. Palantir has no current or past contracts with USCIS. Palantir has worked with ICE's Homeland Security Investigations (HSI) division since the first Obama administration (2011) in support of HSI's primary mandate to investigate and defend the United States against transnational criminal threats (including combating [terrorism](#), [opioid trafficking](#), [transnational gangs](#), [child exploitation](#), and [human smuggling](#)). Palantir does have contracts with the Department of State, but they are unrelated to the concerns raised in your letter (see, for example, public reporting on the Department of State's selection of Palantir software to [modernize data management for the Bureau of Medical Services](#) and [enable administrative efficiencies](#)). More recently, Palantir's contract for the Investigative Case Management (ICM) solution for ICE-HSI has been expanded to support a six-month prototyping period focused on three additional mission areas: (a) Enforcement Operations Prioritization and Targeting, (b) Self-Deportation Tracking and (c) Immigration Lifecycle Operations.

Your letter states:

"The Catch and Revoke system draws upon products that the US State Department holds private contracts for; the department acknowledges that it currently hosts at least 80 AI projects/use cases on their own website.⁷ A number of different products are listed for social media and open-source intelligence "on travelers who may be subject to further screening for potential violation of laws that CBP is authorized to enforce or administer."⁸ Amnesty International was also able to identify a completed contract between ICE's Enforcement and Removals Operations and Palantir Technologies, detailing the wide-ranging features provided by the company."

To be clear: Palantir is not providing the operating system for the "catch and revoke" effort.

The completed contract Amnesty International cites does not relate to, and preceded, the "catch and revoke" system. Amnesty International's letter also alleges that the "catch and revoke" policy is being carried out by multiple agencies, including ICE. In fact, the "catch and revoke" policy effort is being led by the State Department; Palantir's recent pilot expansion with ICE, signed in April, is not related to that effort.

Further, you state that:

"Amnesty International has reviewed documentation detailing Palantir's role in supplying the US' Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) with products that have enabled the monitoring of migrants, including student activists, and powered widely disproportionate and human rights violating immigration enforcement in the United States."

As stated above, Palantir has no contracts with CBP, and our work with ICE, as detailed above, does not "[enable] the monitoring of... student activists" Any reporting to the contrary is incorrect. The further suggestion that work to which our products are not connected is "[powering] widely disproportionate and human rights violating immigration enforcement in the United States" is similarly misleading and incorrect.

Section 2: Addressing the specific allegation that Palantir is the platform provider for the "catch and revoke" policy recently unveiled by the Trump administration.

A central claim in your letter is that Palantir is the operating platform for the Trump Administration's "'Catch and Revoke' system, (3) which combines social media monitoring, visa status tracking, and automated threat assessment, potentially leading to arbitrary deportations and violations of privacy rights. Among the at least 80 ongoing AI projects house[d] at ICE and

CBP as of this time, the surveillance and analytics products supplied by Palantir's Immigration OS match the capabilities described under the 'Catch and Revoke' system."

Again, Palantir is not providing an operating platform for the "Catch and Revoke" system.

Further, the letter's assertion that Palantir is the operating platform for this system is not supported by concrete evidence, only the suggestion that our systems have similarities to the system used by the State Department.

The letter also states that "review of documentation by Amnesty International has found that Palantir's ImmigrationOS possesses automated open-source intelligence (OSINT) capabilities that enable constant monitoring, surveillance, and assessments. These include real-time monitoring of social media posts across multiple platforms, pattern recognition and sentiment analysis, data aggregation from various public and private sources multiple government databases, automated threat assessment, potentially leading to arbitrary deportations and violations of privacy rights. These capabilities match those described in the Catch and Revoke system."

As stated above, we are not providing an operating platform for the "Catch and Revoke" system. We are not aware of the "documentation" you reference, or of any documentation that would support Amnesty International's implication that our software is supporting the "catch and revoke" system through "automated open-source (OSINT) capabilities" or any other capabilities for that matter.

Finally, you note that *"the application of AI surveillance tools in the current context supercharges intimidation efforts by the US authorities against migrants, with heightened risks to peaceful student protestors across campuses for showcasing solidarity against an ongoing genocide in Gaza."*

Again, Palantir has no part in creating or running a platform to carry out the "Catch and Revoke" system, nor in applying AI-equipped surveillance tools to student protestors, as the statement alleges.

Given the important role that Amnesty International plays in the public discourse, and the potential for unfounded statements like these to inflame discussions about immigration policy, federal contracting, the adoption of technology, and public-private partnerships, we are disappointed that Amnesty International has not applied higher research and reporting standards for verifying facts that underpin these serious allegations.

Section 3: We are committed to fact-based dialogue about our products and systems, but unfounded politicization of Palantir's work undermines the US institutions we have served for decades.

At a higher level, it is critical to understand that Palantir's core mission is to support agencies and institutions - not administrations or particular political projects, and it is in this context that our willingness to engage in difficult and seemingly intractable problems across our government and commercial work is most critical. This framing is articulated in our human rights policy, which you cite in your letter. Upholding fundamental human and civil rights was central to the founding mission of Palantir, and our commitment to those ideals continues today. Effective institutions of government that adhere to due process and the rule of law are critical to the protection of both individuals and democracy as a whole, and we believe that technology has a critical role to play in enabling effective, lawful, and trustworthy government institutions.

At times, work with governments can carry risks for human rights, privacy, and civil liberties.

Palantir takes those risks seriously. We engineer privacy enhancing technology across our product suite and think critically about the workflows our products might enable and our customers' use of our tools. But at the same time, Palantir believes that we — as contractors to the federal government — should not be in a position to set policy on behalf of the US Government. Palantir is not an oversight authority entrusted with scrutinizing or questioning executive branch actors.

Instead, our role is to serve as responsible, law-abiding federal contractors. We take our role seriously – to enable the federal government to serve the people more efficiently, to enable accountability and transparency, and to uphold the requirements of the law. We take on new customers and mission sets in every administration, and we will always be willing to engage in good faith conversations with government counterparts about whether Palantir is a good fit for their mission needs. And fundamentally, we do not believe that disengaging from difficult or contentious mission sets leads to better outcomes on either the mission or the human rights side.

In previous administrations, our work was limited to work with Homeland Security Investigations (HSI). Our recent expansion does include work that directly serves ERO's mission, but as we have made clear it does not include any elements of the "catch and release" program or policy.

We invite a more extensive conversation about the broader role of technology systems and companies in the public sector, and the need for common, interoperable infrastructure to allow for the effective delivery of public services. We believe that dialogue between the private sector, government, and civil society, grounded in complete and accurate information, has the potential to achieve more positive outcomes around critical areas of mutual concern, including the intersection of technology and human rights.

Section 4: Palantir needs to provide greater transparency around our work

Finally, we want to address the general claims throughout your letter that Palantir is not transparent about our work, as well as our broader approach to mitigating risks of adverse human rights outcomes where we operate.

It is important to us to refute those allegations because they run counter to Palantir's founding principles. Palantir is unique in our longstanding commitment to democratic values, dedication to supporting government institutions in addressing their most complex challenges, and working to apply our values and technical expertise to develop products designed to make critical government programs operate with more accountability and efficiency. We have always believed that engaging on hard problems through technology should not come at the price of sacrificing privacy and civil liberties. In well-designed systems, security and privacy should reinforce each other, a principle that guides Palantir in its work.

Palantir has always worked to be as transparent as possible. Particularly over the last several years, Palantir has published a variety of pieces that detail [our approach to human rights](#), [how we navigate our defense work while respecting human rights](#), [our privacy-first engineering philosophy](#), and [how we define and operationalize ethical and responsible AI](#). We encourage Amnesty International to review those resources, as well as [our public responses to inquiries from Congress](#) and corrections issued in [response to a misleading and false New York Times article](#) related to many of the same issues.

Conclusion

We welcome the difficult conversations balancing the need to advance technological systems while respecting human rights. It has never been more important for companies like Palantir and

organizations like Amnesty International to engage with each other on the pressing questions of our time. We will continue to encourage rigorous discourse about the best path forward, ever mindful that we share common goals of good government and the safeguarding of fundamental rights.

Sincerely,

[REDACTED]

[REDACTED]

Palantir Technologies

Reference: TC AMR 51/2025.6915

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

8 August 2025

Dear [REDACTED]

RE. PALANTIR'S LINKS TO IMMIGRATION ENFORCEMENT IN THE UNITED STATES

Thank you for your response dated 24 July 2025 and for providing certain clarifications. Amnesty International would also like to provide Palantir with clarity regarding the research we have conducted to date and the human rights concerns that have been raised.

Please note that in our upcoming publication we do not claim that Palantir Technologies has current contracts with Customs and Border Patrol (CBP), United States Citizenship and Immigration Services (USCIS), both of which are under the Department of Homeland Security (DHS), or contracts with the State Department that are relevant to the topic of our research. We base our research and concerns on Palantir's contracts with Immigration and Customs Enforcement (ICE), which is under the Department of Homeland Security, and which we are concerned are being supplied with AI products for use in targeted and discriminatory removal operations. This concerns Palantir's supply of products to ICE Homeland Security Investigations (HSI) and ICE Enforcement Removal Operations (ERO), the two main law enforcement units of ICE.

Additionally, Amnesty has not claimed in the letter, nor in the final output, that Palantir directly provides an "operating platform" for the "Catch and Revoke" system. However, as ICE's Enforcement Removal Operations (ERO) manages all aspects of immigration enforcement processes, including 'the identification, arrest, detention and removal of aliens',¹ we know that ICE is the operational arm tasked with implementing the decisions made by all US agencies concerned with migration management including the State Department. In other words, ICE plays a key role in enforcing the Catch and Revoke policy by way of aggressive tracking and detention tactics, even if the policy as a whole is being implemented by the State Department. AI products supplied to the ICE, including the ERO and HSI are, in other words, implicated in Catch and Revoke.

¹ U.S. Immigration Customs Enforcement, 'Enforcement and Removal Operations', <https://www.ice.gov/about-ice/ero>

Testimonies by federal agents, in respect to immigration enforcement operations affecting students in the state of Massachusetts, also point to the recent role played by Homeland Security Investigations (HSI) in meeting Catch & Revoke objectives, and provide context on how arrests of international students were made on the premise that their presence undermined US foreign policy interests. HSI agents claimed that the involvement of HSI was a development with no precedence prior to the Trump administration.² One federal agent, Brian Cunningham, supervising the arrest of Tufts University student, Rümeyşa Öztürk, reportedly contacted the Homeland Security lawyer to confirm whether the arrest was in fact legal. In a POLITICO article from July 2025, Cunningham was quoted saying: 'I can't recall a time that it's come top-down like this with a visa revocation, under my purview anyway [...] I did contact our legal counsel to make sure that we're on solid legal ground....The operation kind of developed pretty quickly.'³

Furthermore, in the same trial, agents testified that they were unclear and concerned about both the legal basis of the arrests, as well as the involvement of Homeland Security Investigations. They reportedly carried out arrests to the revocation of visas or green cards, or due to '[...] Rubio's determination that their presence was at odds with U.S. foreign policy.' This demonstrates how departments concerned with transnational crimes and even foreign policy in the US administration are interacting with ICE's deportation operations.

In its letter dated 24 July 2025, Palantir itself recognizes that its "work with governments can carry risks for human rights, privacy, and civil liberties. Palantir takes those risks seriously. We engineer privacy enhancing technology across our product suite and think critically about the workflows our products might enable and our customers' use of our tools. But at the same time, Palantir believes that we — as contractors to the federal government — should not be in a position to set policy on behalf of the US Government. Palantir is not an oversight authority entrusted with scrutinizing or questioning executive branch actors." While Amnesty International agrees that it is not Palantir's role to set government policy, the company should ensure that its products are not linked or contributing to human rights abuse. This is a clear requirement of the UN Guiding Principles on Business and Human Rights (UNGPs), which the company itself claims to draw upon for its own human rights, policies and practices. Palantir also emphasized in its letter that it does "not believe that disengaging from difficult or contentious mission sets leads to better outcomes on either the mission or the human rights side". Given this commitment, Palantir should show all efforts it has made to ensure that its products are not being used in a way that would be contrary to human rights and that choosing not to disengage has led to rights-compliant outcomes.

While Amnesty International recognises the importance of dialogue and exercising leverage where possible, it is of utmost importance that companies not cause, contribute, or be directly linked to human rights violations. If a company is unable or unwilling to do so, companies should consider responsibly ending the business relationship, as per the UNGPs and the OECD Guidelines for Responsible Business. Assuming Palantir has conducted adequate human rights due diligence on an ongoing basis as per its responsibilities and very own human rights policy, the company knows that it now is operating in an environment that is prone to heightened human rights risks by contracting with federal government agencies that have publicly acknowledged their lack of interest in providing any human rights safeguards in any of its immigration enforcement efforts. This consistent pattern is widely evident not least given Palantir's supply of products that directly implicates it in the operations of ICE's ERO and HSI. At this time, it appears that Palantir is unable or unwilling to exercise leverage, and should therefore immediately disengage.

Finally, Amnesty International has removed references to Palantir's ImmigrationOS tool possessing open-source capabilities.

Upon reading your response, we have the following questions that we are seeking your clarification on:

1. What process has Palantir followed in the past, or plans to follow in the future, to ensure it is meeting its responsibility to respect international human rights law and standards?

² POLITICO, 'Federal agents describe unusual run-up to arrests of Pro-Palestinian academics', 15 July 2025, <https://www.politico.com/news/2025/07/15/pro-palestinian-academics-deportations-trial-00454324>

³ POLITICO, 15 July 2025.

2. To your knowledge, what does ICE's ERO and HSI do, respectively, as enforcement agencies in respect of Catch and Revoke? Please provide Amnesty with any and all assessments that the company has conducted to determine the level of risk that it could be taking on in entering and/or renewing contracts with ICE.
3. Given the operational overlap between the State Department and ICE's ERO operations, how has Palantir ensured that ICE does not use any of its technology for the Catch & Revoke effort, including against international students? What contractual guardrails and ongoing human rights due diligence efforts does Palantir conduct to ensure that there is no risk that its technology is not contributing or directly linked in any way to human rights abuses under international human rights law and standards? Please provide us with any risk assessments you have conducted, given the heightened inherent risks of providing services to government agencies involved in such efforts.
4. Palantir's ImmigrationOS provides (a) Enforcement Operations Prioritization and Targeting, (b) Self- Deportation Tracking and (c) Immigration Lifecycle Operations capabilities, as per Palantir's own description. However, Palantir claims that this does not enable the monitoring of student activists. Given this, can Palantir provide details on what human rights due diligence, impact assessment methods and/or contractual guardrails it has in place to ensure that these features are not linked or contribute to human rights abuses? How can Palantir ensure that specific groups of people, such as migrant students who are exercising their right to free expression, and their data is not processed by ImmigrationOS?
5. What are Palantir's decision-making protocols for responsible disengagement, including contract termination, even where you have long-term government contracts in place (potentially spanning multiple administrations), given that at any point in time during such long-term contracts you may be put on notice of circumstances in which your systems are deployed at risk to human rights?
6. In your response to questions raised by Congress (Senator Wyden and Representative Ocasio-Cortez) published as recently as 18 June (embedded in your response to our previous letter),² you mention that:

"All of our government contracts and the corresponding deployments of software instances are unique to the contracting agency, with legal, procedural, and technical guardrails in place to protect each agency's data"

Please could you expand on the nature of such legal, procedural and technical guardrails in respect of ImmigrationOS, and any manner in which you contribute to legal enforcement of such guardrails?

7. In the same response, you mention that:

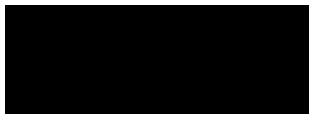
"Palantir is well aware of its obligations to uphold federal law, including relevant privacy regulations. The strength of our software platform is built upon decades of operating in highly secure, sensitive environments, where we help our customers meet the highest standards of security, privacy, data governance, and auditability. To contravene those laws with a federal customer would be entirely unacceptable"

Please could you expand on the due diligence steps taken to ensure that there is no unlawful and unacceptable contravention of privacy regulations, adversely impacting the public in relation to ImmigrationOS? Moreover, can Palantir please explain how it factors in its commitment to international human rights law and standards to these due diligence step?

8. Is Palantir aware of any past or current employees who been seconded or hosted by any government agencies to administer or oversee or assist with deployment and use of ImmigrationOS? If so, can you please provide details on the role of these people in both the Palantir and government side?

Please note that we may reflect any information we receive from you, in whole or in part, in published materials as appropriate. We look forward to receiving your response by close of business on 20 August 2025, by e-mail to [REDACTED]

Sincerely,



Amnesty Tech

Amnesty International