Cindy Cohn
Executive Director
Electronic Frontier Foundation

6 March 2026

Dear Ms. Cohn,

We appreciate your time and continued engagement on these matters. As we stated in our earlier response to your report on Palantir's work in US immigration and as we explained during our 2 February 2026 discussion with you on these matters, we have a longstanding respect for the role that EFF has played in the online civil liberties space over the years. As we explained, Palantir holds an abiding concern not only for the continued competent functioning of essential government institutions and their critical mandates, but also for how and where our products are used, and their proximity to potential violations of human rights.

We appreciate this continued dialogue and the opportunity to correct misunderstandings and misperceptions of our work. We have attempted to address your questions as best as we can below, in a format that, as you requested, is appropriate for public release and additional transparency. As you know, we have restrictions in the specificity that we can provide because of contracting requirements, especially for customers operating in secure government spaces and in line with the "legitimate requirements of commercial confidentiality," as recognized by the UN Guiding Principles on Business and Human Rights. We appreciate your understanding of these legal and operational restrictions, and that our need to abide by them does not detract from our serious commitments to respecting fundamental rights concerns.

Palantir's Approach to Human Rights Centers on the Need to Engage

We appreciate your awareness of Palantir's stated commitment to our human rights policy,

and your acknowledgement of other similar rights-affirming commitments from company statements and documents, and the ways in which we operationalize our longstanding mission of empowering the institutions who often directly oversee the realization, and protection of fundamental rights.

As we indicate in our human rights policy, Palantir's founding mission focused on protecting the US from terrorism ***without*** compromising on privacy and civil liberties in the way intelligence and security agencies carried out their work. This is explicitly called out in our human rights policy, in our focus on the fundamental rights to security (UDHR Article 3) and privacy (UDHR Article 12). We note those principles not only because they were and are the most relevant human rights risks to our business via customer use of our products, but also because they represent the inherent tension that often exists between fundamental rights themselves. At the time of Palantir's founding, the common consensus was that security can be achieved, but it must come at the expense of privacy. We rejected that zero-sum formulation then and we continue to reject it now, but we surface it here again as it is crucial to understanding how we continue to conceptualize fundamental rights considerations in the various contexts, including our work with the US government.

As your letter acknowledges, and in line with international standards on preventing and addressing the risk of adverse impacts on human rights, Palantir has a framework for assessing and mitigating the risk of these rights being violated, where we:

> *"examine multiple dimensions of privacy risks, such as compliance with current legal standards, protecting the fundamental rights of impacted communities, respect for rule of law and political and social stability, promoting fairness and equity, preventing discrimination, and adhering to societal norms and ethical standards."*

As we've detailed before, we believe this layered approach to navigating fundamental rights risks is essential. This occurs in multiple contexts: onboarding potential customers, designing individual use cases or workflows with existing customers, and in relation to a myriad of big and small product decisions. We also regularly turn down work that we feel does not align with our values.

Finally, we often articulate our belief that our legal responsibilities are the floor for our broader risk assessments. This is best demonstrated in our approach to product philosophy across disciplines. We were, for example, building for the central data

protection principles and provisions of GDPR well before the regulation was formalized - because we hold and adhere to the conviction that our software platforms needed the strongest privacy and data governance technical controls irrespective of formal legal requirements. Several years ago, we began working on directly incorporating International Humanitarian Law (IHL) principles into our defense platform, not in response to an explicit legal or policy mandate from our (prospective) government customers, but because we proactively identified a need to demonstrate — in direct, applied actions — how thoughtful engineering choices could buttress IHL priorities in this emerging space. Leveraging our values to proactively build the next frontier of rights-affirming technology defines Palantir, as does our belief that the public sector needs technology developers who are willing to grapple with the challenges encountered by bedrock institutions dealing with complex and imperfect outcomes with regard to fundamental rights considerations.

Core to our approach to fundamental rights is that we prioritize engagement on missions closest to the fundamental rights themselves, often with the institutions directly charged with overseeing the administering and enjoyment of common goods. As articulated in our human rights policy:

> *At Palantir, we believe that working to protect fundamental human rights requires engagement, including engagement with the institutions whose vital tasks exist in tension with certain human rights.* ***Just as we best protect privacy and civil liberties by responsibly enabling the essential missions of security, defense, and intelligence, we believe we best uphold our commitment to secure human rights by enabling and supporting properly functioning global institutions.*** *We believe that as a responsible corporate citizen, we must not only assess our work for any potential negative human rights impact, but also work to promote the positive role that our software can play in protecting vulnerable populations and in promoting the functioning of legitimate institutions around the world.*

As a result of making it our mission to move towards (not away from) some of the most complex and rights-oriented work in the world, we recognize that these issues are complex, as are the solutions, and we do not agree that there is always a clear-cut choice that leads to the maximization and protection of fundamental rights. Try as we might, or any other entity operating in rights-impacting spaces will attest, we must operate in a world filled with institutions making decisions every day around human rights principles that are inherently in tension with one another. This is another theme we spell out both in our human rights policy, but also in other writings on these themes:

Additionally, we recognize the complexity of human rights and the potential for certain rights to exist in tension with each other in the spaces where Palantir more regularly operates. We recognize the nuance involved in certain areas we work in where core human rights tenets such as security and privacy have the potential to conflict with each other. By embracing this nuance we ensure that these type of tensions do not become mutually exclusive, and we allow for institutions to further their difficult but important missions. Even in doing so, we will continue to incorporate privacy and civil liberties as fundamental components of our products and approach.

Our work doesn't just have incidental impact on fundamental rights. That is why Palantir takes such a robust approach to analyzing risks and operationalizing our respect for human rights through the ways we build our products and work with our customers. Palantir believes, at our founding and today, that the answer is not to flee from complex problems when things get difficult; our world needs - perhaps now more than ever - those willing to move towards the hardest problems.

Palantir's Work in Immigration

As we have previously explained, many of the concerns that you raised blur the line between government agencies (specifically CBP and ICE) and imply that any behavior or decisions undertaken by these agencies, regardless of the timeline, were directly facilitated by Palantir's software. As we have said before, this is incorrect. We therefore appreciate the opportunity to (yet) again correct the record.

Specifically, and at the outset: ***Customs and Border Protection (CBP) is not a customer of Palantir.*** Any concerns that you have related to current or past actions by CBP are unrelated to the scope of work of any Palantir contract. Simply put, as we do not have any contracts with CBP, we provide no services to CBP. This is something we have repeatedly clarified externally. To be clear – it is not that Palantir has chosen to never work with CBP. To the contrary, there are many places where we believe our software could usefully contribute to CBP's critical mission set. If and when faced with future opportunities to work with CBP, we will evaluate those potential opportunities, as we do all other opportunities, with an eye to their holistic impact on the world, inclusive of fundamental human rights risks. But again: we do not have a contract with CBP, and the concerns that you raise with respect to presumed or alleged work with CBP are off the mark.

Another core theme in your letter and specifically referred to in your questions is the implication that Palantir is not only facilitating unfettered data sharing and illegal access between government departments, but that we are also building a purported database to track protesters and label them "domestic terrorists." Your letter even asks us to clarify that we are not involved, to which again we can say: we are not involved, even should such an effort exist (and we have no awareness of such an effort existing).

Finally, in regard to Palantir's specific body of work with ICE, including the ELITE tool, this is again a space where Palantir has previously laid out, transparently and with considerable detail given the sensitivity and confidentiality requirements surrounding our work, how our products are used. As we have previously explained in our response to your initial report, in our discussions with you, and in other public statements:

- ***Palantir is not working on any master database project to unify databases across federal departments. Palantir has not proposed the US Government build a "master list" for the surveillance of citizens, nor have we been asked to consider building such a system for any customer. Such a hypothetical project is fundamentally at odds with Palantir's values and our commitment to work in support of liberal democracies.***
- Such an effort would not only run afoul of any number of legislative, policy, and procedural restrictions on the federal government, but it would also be at odds with Palantir's long-established and entrenched regard for the protection of privacy and civil liberties. Further, any such project would represent a massive breach of trust and be an existential threat to our business.
- Palantir has worked with the federal government for almost 20 years. Separate contracts with various government departments simply do not represent evidence of some broader effort to build a "mega-database." The suggestion misperceives the structure of our customer licenses and product infrastructure.
- Palantir is not facilitating widespread and unfettered data sharing across our government customers, as each customer instance of our software is legally, technically, and operationally distinct. Government data sharing across departments is subject to, and governed by, data sharing agreements and government oversight. Any data sharing facilitated by Palantir across departments is done according to legal and technical requirements, including those of the Privacy Act of 1974.

- There is a genuine need and indeed legislated requirements (e.g., The Modernizing Government Technology Act, The Federal Information Security Modernization Act (FISMA)) to update IT systems and digital infrastructure in the federal government in order to improve operational efficiencies and prevent unnecessary waste. Such efforts can and should be pursued responsibly.
- Palantir has worked with Immigration and Customs Enforcement (ICE) since the first Obama administration, notably by providing software that supports investigations into transnational criminal organizations engaged in major criminal activity with a nexus to the border, such as human smuggling and drug trafficking. Our recent pilot contract with ICE, the negotiation of which began under the Biden administration, reflects a continued commitment by Palantir to support the US government in its most central missions.
- As part of that pilot project, the ELITE tool is used for prioritized enforcement to surface the likely addresses of specific individuals, such as those with final orders of removal or with high severity criminal charges. The purpose of this tool is identifying the location of known foreign nationals who meet criteria for removal, not for mass prioritization of "locations where lots of people it might detain could be based."
- Palantir's role in this tooling centers on data integration, enabling ICE to incorporate data sources to which it has access (including DHS data and limited data shared by other departments under a data sharing agreement permitting it to be used for immigration enforcement purposes). This data includes information needed by ICE officers and agents to accurately assess whether an individual can be removed, whether an individual has a court-ordered stay on their removal, or whether they have status that precludes their removal.
- While there may be instances of limited information sharing between select component agencies of HHS and ICE pursuant to lawful authority, these instances are governed by the same requirements that apply to other components of government under the Privacy Act and other applicable laws and policies.
- Palantir's platforms are built with an indelible audit log — all platform interactions, from data ingest onwards, are subject to detailed logging. Palantir's platforms are designed with privacy, security, and auditability at their core.
- With Palantir software, as with any other software, product, or tool in government or in private hands, there is always the risk of misuse. The reality that "technology is not ethically neutral, and can be used for good or harm," is noted in Palantir's code

of conduct, to which all Palantir employees are accountable. Because we are mindful of such risks, we build our software to help support accountability functions that can be used to audit and investigate instances of misuse or abuse of sensitive data.

- Palantir takes a rigorous approach to respecting human rights, from the development to customer use of our products. We also actively support humanitarian missions around the world, from fighting human trafficking, to disaster relief, to the defense of sovereign nations.

The applicability of human rights due diligence in Palantir's work must be predicated on both the facts of what our software does and the realities of the operational contexts where our software is deployed. Many of the specific questions raised in your letter seek to connect Palantir's software to allegations of "grievous human rights abuses." The bases for drawing those speculative connections, however, seem to be either fundamental misunderstandings of the nature of our product capabilities and the scope of our contractual relationships with customers or the repetition of inaccurate claims that we've previously rebutted and again clarified directly above. Nevertheless, Palantir will continue to abide by our stated commitments, even if we are unable to publicly report on the specifics.

We recognize the complexity that our work with the US government presents, especially during such polarizing times. Palantir has worked with the US government for two decades and across multiple administrations of both parties, and we see it as our enduring mission to support those who work tirelessly to help our institutions function, even when that work is controversial. Our team regularly meets with institutional investors, human rights advocacy organizations, customers, media, and other interested parties (including yourselves) who have questions around our work. In 2026 alone, we've held over 15 long form discussions with stakeholders across the human rights spectrum. It is our strong belief that discussion on complex topics merits this level of engagement, where open dialogue is prioritized over cursory reporting that is incapable of carrying the needed nuance.

For our part, we will continue to run towards the institutions and challenges that most directly correlate to the realization of fundamental rights, even as they implicate messy and often intractable practical challenges. As we note in our human rights policy, this is where we believe our products can do the most good: through an enduring support of the institutions that collectively uphold imperfect but still functioning democracies, rather than

pledging support conditioned on political orientation.

Sincerely,

Courtney Bowman
Global Director of Privacy & Civil Liberties Engineering
Palantir Technologies Inc.