Palantir

April 7, 2025

To whom it may concern,

Palantir Technologies Inc. (“Palantir”) is a U.S.-based software company that deploys software platforms to enable public, private, and non-governmental organizations to integrate, analyze, collaborate, and make operational decisions with their data, including through the integration of AI capabilities, in a secure and privacy-protective way. At Palantir, we see our work as a duty and privilege: to support the United States of America, its vital national interests, and the civilization of which it is a part. We are proud that this includes making the software upon which many of the world’s most vital institutions, from defense and intelligence agencies to companies in the healthcare, energy, and manufacturing sectors, rely.

We are excited to contribute our thoughts to the House Energy and Commerce Committee’s Privacy Working Group efforts. We applaud the Working Group’s initiative to undertake deliberations regarding the framework and essential details of a federal comprehensive data privacy and security law, and we appreciate the delicate balance that must be struck in this work between maintaining a commitment to America’s democratic process on the one hand, and on the other, the creation of a federal data security and privacy law that will safeguard the privacy rights of all Americans while encouraging innovation. Our response to the Working Group’s Request for Information is based on insights gathered over 20 years of experience building technology to improve institutional mission outcomes while upholding American values in the use of our software products, including AI enablement tools and platforms.

We hope the following recommendations help the Privacy Working Group lay the groundwork for decades of strong, steady U.S. leadership in a world increasingly at risk to forces of instability, crisis, and conflict.

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing a federal comprehensive data privacy and security law and associated documents without attribution

I. Roles and Responsibilities

The digital economy includes a wide range of business models, including entities that collect information directly from consumers, those that process personal information on another business's behalf, and others that collate and sell personal information.

A. **How can a federal comprehensive data privacy and security law account for different roles in the digital economy (e.g., controllers, processors, and third parties) in a way that effectively protects consumers?**

- While the EU General Data Protection Regulation introduces a number of complicating challenges that are worth interrogating to determine the right balance between supporting existing transatlantic obligations for multinational organizations and protecting the interests of American consumers, there are also several features of the GDPR that provide a useful (and now well understood/adopted) operational framework to build upon.
    - Specifically, GDPR's division into two categories of responsibility: Controllers, who actually make the decisions about how to use personal data, and Processors, who act on behalf of the controller and at the controller's direction. Ultimately, Controllers bear the brunt of liability because they are the ones making the decisions about how to process personal data.
    - In general, these definitions have held up and using them would reduce compliance burden for most companies, which have already begun framing their obligations to align with GDPR.
- However, one possible gap to consider with respect to this entity type distinction is the degree to which the definitions (i.e., controller as the entity that "determines the purposes for which and the means by which personal data is processed" whereas the processor "processes personal data only on behalf of the controller") might index too heavily on the notion of "processing" and therefore risk losing sight of the place of data stewardship, i.e., managing long-term oversight over what happens with personal data held by institutions, whether or not it is immediately being used or "processed."

B. **What are appropriate obligations for different regulated entities, and what are the practical and legal limitations associated with each type of entity?**

- Obligations for different regulated entities should be structured to provide graduated practical and legal responsibilities proportionate to the degree of responsibility they carry in directing and determining the purposes and means and handling and processing personal information. For example, assessments of privacy risks, prioritization of vulnerabilities, and documentation mitigation measures and practices in their data handling applications (via Privacy Impact Assessments or similar evaluation tools) may be most appropriately conducted by data controllers, albeit with supporting technical or other inputs from relevant processors.

- Other functions that may be carried out by different regulated entities — to varying degrees of expectation and responsibility for a given application environment — include:

    - Establishing clear policies and procedures for data handling, storage, and processing (primarily a controller responsibility);

    - Define roles and responsibilities for privacy and security management (primarily a controller responsibility, but with some processor obligations);

    - Identify and assess privacy and security risks related to data, systems, and processes primarily a controller responsibility, but with some processor obligations);

    - Implement security controls and develop strategies to mitigate identified risks (both a controller and processor responsibility);

    - Conduct regular audits to assess the effectiveness of privacy and security controls (primarily a controller responsibility, but with some processor obligations);

    - Monitor security events and incidents to detect and respond to threats (both a controller and processor responsibility); and

    - Conform to a common standard or outline that enables both ease of regulatory oversight evaluations and public disclosure legibility/accessibility (both a controller and processor responsibility).

C. **Should a comprehensive data privacy and security law take into consideration an entity's size, and any accompanying protections, exclusions, or obligations?**

- Yes, in order to balance the burden of privacy regulation with innovation.
    - We recommend crafting exemptions for smaller organizations, or tailoring regulations so that they only apply to entities over a certain size. This would ensure smaller businesses are not disproportionately affected by the compliance burden of new regulations.
    - The working group should consider sensible metrics for defining size: e.g., market cap, revenue, employee count, customer base, or a combination of these and other features. Previous comprehensive privacy legislation drafts have attempted to use these types of measures.
- We note that a multitude of exclusions and exceptions runs the risk of overcomplicating compliance and reducing consumer confidence in data protections. The goal should be minimal or very simple exceptions, and greater focus should be placed on making the actual substance of the regulation simple (i.e., simple to understand and simple to implement), rather than having a complex regulation with many elaborate carveouts.
- In addition to exempting smaller organizations, we also recommend the working group consider exemptions for critical business operations and security functions of organizations, such as:
    - Fraud detection / prevention
    - Operations necessary to maintain and provide services, including security incident response and mitigation
    - Responding in good faith to valid legal process requests from law enforcement officials
    - Completing transactions for which personal information has been explicitly collected and consented to be used

II. Personal Information, Transparency, and Consumer Rights

A federal comprehensive data privacy and security law should apply to personally identifiable information and provide consumers with clear disclosures and rights to their personal information.

A. Please describe the appropriate scope of such a law, including definitions of "personal information" and "sensitive personal information."

- Scope:
  - Proposal: "Any organization [modulo exempted organizations] that processes the data of United States citizens or residents" ("U.S. persons").
    - Any organization handling the data of U.S. persons should be subject to laws that protect the data of U.S. persons, no matter where they are based. This is the best way to guard against organizations based offshore that poorly handle sensitive data.
- Definitions
  - We recognize the challenge of defining personal information, especially against a backdrop of existing — and often inconsistent — definitions enshrined in other sectoral (e.g., HIPAA) and jurisdictional (e.g., CPPA/CPRA, GDPR) privacy legislation. As a company that provides configurable privacy enhancing technology capabilities adaptable to heterogeneous definitions of personal and sensitive personal information, we are agnostic to the specific attributes of a chosen definition. We do, however, wish to urge caution on two areas of potential ambiguity that flow from sub-optimal definitions:
    - Definition approaches should consider how they lend themselves to practicable approaches to deidentification (i.e., via anonymization, pseudonymization, or other means). Definitions that, for example, foreground clear concepts such as linkability might allow for cleaner approaches to deidentification. See our white paper 'Beyond Anonymization' for an extended discussion of these and related issues: https://www.palantir.com/assets/xrfr7uokpv1b/5oWSVdic2rPQtBlKnqTw25/a87cbcc9439481cf21cdf693bcd4f575/Beyond_Anonymisation-_A_comprehensive_approach_to_handling_personal_data.pdf)

        - Given the ever-expanding ubiquity of public sources of information (i.e., accessible in varying forms via commercial data brokers, social media websites, public registries, etc.), a definition approach should consider the interplay of reasonable expectations of privacy as it relates to so-called 'publicly available information.'

B. **What disclosures should consumers be provided with regard to the collection, processing, and transfer of their personal information and sensitive personal information?**

- Entities should provide clear, articulate, and reasonably specific documentation of the intended use cases for which data is to be collected, processed, transferred.
    - For instance, "general marketing" is an example of too vague an explanation of legitimate purpose of use. Instead, stating, "marketing of complementary services within X months of collection," would establish a clearer framework for onward use for collected data.

C. **Please identify consumer protections that should be included in a comprehensive data privacy and security law. What considerations are relevant to how consumers enforce these protections and how businesses comply with related requirements?**

- We believe the following consumer protections should be included in any comprehensive data privacy and security law:
    - Right to Delete / Right of Erasure
        - Deletion is one of the most important remedies for violations of privacy, and all Americans should have a right to ask entities covered by this regulation to delete their personal information. Right to erasure is already common across existing regulatory frameworks.
    - Right to Know / Right to Access
        - Americans should be able to know when and how their personal information is being processed, so that they can make informed decisions about how their data is and should be used. This kind of access request right is also common across existing privacy regulations.
    - Compliance with Rights of Access and Erasure
        - Organizations will need to be able to identify personal data within their systems to comply with these rights.

        - While opponents of strong privacy legislation might say that requiring organizations to identify (and potentially delete) personal data upon request is unduly difficult to comply with, we cannot stress enough the importance of holding organizations that process Americans' most sensitive information to at least this bar.

        - We have seen with first-hand experience how the foundational data governance that would enable these privacy rights is both readily practicable through competent technology tools and also fundamentally complementary with business goals and business practices that align with consumer confidence and trustworthiness. Data quality, governance, and protection is not a burden, and in fact allows organizations to more efficiently organize to deliver on their business priorities – including leveraging more advanced technologies, like AI, on their data.

        - There should be no zero-sum tradeoff between supporting basic privacy rights and achieving business objectives. With the right technology, you can do both.

    - Right of Redress

        - For consequential decisions or consumer outcomes impacting individuals' livelihoods, health, and well-being, they should have a right to request redress for adverse decisions that lead to curtailment, rejection, limitation, denial, etc. of services when such decisions may be based on potentially errant information and/or decision-making processes (including both manual and algorithmic or automated decision-making).

- The above outlined consumer protections offer important measures for reaffirming the rights of American consumers. Their full implementation, however, may implicate organizational, procedural, and technical burdens that are onerous to smaller ventures. It may therefore be prudent to consider a tiered or graduated framework for operationalizing these protections, with escalating requirements as organizations grow in both their risk profile and capacity to support such measures.

D. **What heightened protections should attach to the collection, processing, and transfer of sensitive personal information?**

- Regardless of a party's standing as controller or processor, we view the following as core privacy and security protective principles for the collection, processing, and transfer of all personally information, whether or not it rises to defined level of sensitivity:

  - **Purpose/Use Limitation** - Organizations should be required to justify why they need to access or use sensitive data
  - **Data Minimization** - Sensitive data should by default be minimized to the greatest extent possible
  - **Storage Limitation / Scheduled Deletion** - Sensitive data should be deleted when it is no longer needed, reducing the risk of unintended leaks or exposure
  - **Security Controls** - Consumer data should be protected through hardware and software tools which prevent unauthorized access, use, disclosure, or modification.
  - **Incident Response** - Organizations handling consumer data should have a clear incident response plan to address security breaches and data privacy violations.
  - **Oversight & Governance** - Organizations handling consumer data should institute a framework for oversight and data governance to ensure that consumer data is handled responsibly and securely

- The above principles are well established within existing privacy protective frameworks, including various formulation of the of the Fair Information Principles (FIPs) and Fair Information Practice Principles (FIPPs). See, for example the Department of Homeland Security's articulation of the Fair Information Practice Principles (FIPPS): https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf

- These articulated principles should be reinforced through a mix of both organizational practices and technical controls. While prescriptive approaches to institutional practices tend to be more difficult and less effective to impose (given the multitude of creative business approaches taken by America's entrepreneurs and business leaders), more discrete specifications of the supporting technical controls can be articulated and provided as examples.

  - Organizations processing and storing consumer data should have technical controls which include access controls, data encryption, identity and access management, and regulator audits, all working together to protect sensitive data.
  - Palantir has first-hand experience building and configuring tools for these kinds of capabilities, we know it's feasible with the right technology investments, and we have long advocated for this in our prior policy submissions:
    - 2022 FTC RFI (See Page 10, Page 16: https://downloads.regulations.gov/FTC-2022-0053-0702/attachment_1.pdf)
    - 2022 NTIA RFI (See Page 13: https://downloads.regulations.gov/NTIA-2023-0001-0020/attachment_1.pdf)

III. Existing Privacy Frameworks & Protections

Since 2016, U.S. trading partners and a growing number of states have enacted comprehensive data privacy and security laws to govern the collection, processing, and transfer of personal information.

A. **Please provide any insights learned from existing comprehensive data privacy and security laws that may be relevant to the working group's efforts, including these frameworks' efficacy at protecting consumers and impacts on both data-driven innovation and small businesses.**

- The comprehensive privacy legislation enacted by the State of California is a notable example of how robust standards from a single jurisdiction can influence the legislative measures adopted by other states. It has also set a benchmark for the contractual, organizational, and technical measures that businesses across the United States must implement when processing consumer data. This has led to a relatively uniform standard of behavior regarding consumer data protection, as California is one of the largest US states by population, economy, and concentration of technology firms. Consequently, businesses that may process the data of California residents, are compelled to adopt these measures, inadvertently benefiting non-California residents as well due to the necessity to uniformly scale business operations.

- Similarly, the EU and UK GDPR frameworks require companies processing the personal data of EU or UK citizens and residents to comply with their standards, and have driven a global shift in data protection practices.

- Given the size, population, and economy of the United States, a comprehensive US Federal Privacy legislation could have a similar impact, enhancing consumer data protections and fostering innovation in this field.

- Regarding the impact on small businesses, many state laws, including California's, exempt smaller businesses from compliance, applying requirements only to for-profit entities with a certain gross annual revenue or number of employees. Additionally, many state privacy laws include specific exemptions for non-profit organizations, research entities, state and government agencies, and healthcare organizations (which must adhere to comprehensive HIPAA requirements). This approach helps avoid conflicts of interest where implementing certain measures might be impractical or already addressed by other specific legislation.

B. **Please describe the degree to which U.S. privacy protections are fragmented at the state-level and the costs associated with fragmentation, including uneven rights for consumers and costs to businesses and innovators.**

- While many states have implemented or are in the process of enacting comprehensive privacy legislation, these laws are not consistent. They differ in terms of rights related to accessing, correcting, and deleting personal data, as well as whether consumers can object to certain types of data processing. States also vary in the types of protections they offer for different processing methods. In today's mobile economy, this results in an uneven field of rights for US persons, particularly for those who frequently travel or change their state of residence due to work. A single US person who has traveled through or lived in multiple states and used services from various businesses in those states will find that they do not have the same rights to protection and objection regarding their personal data across these states.

C. **Given the proliferation of state requirements, what is the appropriate degree of preemption that a federal comprehensive data privacy and security law should adopt?**

- A traditional framework of preemption could make sense with regard to a comprehensive federal privacy legislation. This approach is especially worth considering to the extent it adopts existing effective and generally understood concepts of data protection to create a baseline and empowers states to adopt their own stricter regulations if they so see fit.

D. **How should a federal comprehensive privacy law account for existing federal and state sectoral laws (e.g., HIPAA, FCRA, GLBA, COPPA)?**

- A federal data privacy and security law should act as a baseline that improves consumer confidence, not as an overarching regulatory scheme that broadly invalidates existing laws.

IV. Data Security

A foundational goal for any federal comprehensive privacy law should be increased security of Americans' personal information.

A. **How can such a law improve data security for consumers? What are appropriate requirements to place on regulated entities?**

- We recommend a previous answer we submitted: **Answer to Question 47** in our 2022 FTC RFI Response (https://downloads.regulations.gov/FTC-2022-0053-0702/attachment_1.pdf, page 16).

V. Artificial Intelligence

Most state comprehensive data privacy and security laws regulate AI through "automated decision-making" requirements. A growing number of states are also enacting—or are seeking to enact—additional AI-specific laws. These developments raise questions about the role of privacy and consumer protection standards in AI regulation and the impact on U.S. AI leadership.

○ **How should a federal comprehensive data privacy and security law account for state-level AI frameworks, including requirements related to automated decision-making?**

- Well-designed privacy and data protection requirements need not be at odds with AI innovation. See **Answer to Question 48** in our 2022 FTC RFI Response (https://downloads.regulations.gov/FTC-2022-0053-0702/attachment_1.pdf)
    - It is our position that sensible data minimization, purpose limitation, and — more generally — strong data governance practices need not be treated as fundamentally at odds with developments and innovations in the domain of algorithmic decision-making or other algorithmic learning-based processes or techniques (often referred to as artificial intelligence (AI) and machine learning (ML)). On the contrary, we observe that these principles are often critical for grounding AI/ML processes and techniques in real-world conditions and for providing clear rails for researchers, engineers, and entrepreneurs to focus their efforts.

- We have repeatedly held that a lack of federal privacy legislation is a barrier to AI innovation. See, for example our response to the 2023 NTIA RFI on AI Accountability Policy (https://downloads.regulations.gov/NTIA-2023-0005-1360/attachment_1.pdf):

- Moreover, the absence of a general federal data protection or AI law may lead to suboptimal developments in relation to AI regulation, such as: (a) companies relying too heavily on the legal frameworks of foreign countries that have already adopted AI-specific regulations; and (b) the emergence of private standards and policies imposed by large digital platforms and other commercial technology giants. Such a patchwork of foreign, state, and local regulations, as well as privately imposed standards, can create confusion and inconsistency in the development and deployment of AI technology. Specifically, it could make it more challenging to ensure that AI systems are developed and used in a responsible and ethical manner and to establish accountability of those responsible for the AI development and its use.

- Consumer rights entitlements are also important considerations. E.g., Right to redress and/or right to challenge automated decision-making outcomes for consequential effects on peoples' livelihoods provides a balance for enabling institutions to achieve efficiency/scale gains with automated/AI tooling while also providing human-in/on-the-loop oversight for addressing instances in which automated processing fails. Redress facilitation is also ultimately good for commercial institutions in ensuring consumer trustworthiness and long-term competitiveness (against less consumer-friendly competitors), as well in availing additional market expansion opportunities to international jurisdictions where such rights entitlements are or will be mandatory.

VI. Accountability & Enforcement

Accountability and enforcement are cornerstones of a data privacy and security regime that protects consumers, promotes compliance, and enables data-driven innovation.

A. **Please identify the benefits and costs of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law.**

- The potential benefits of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law flow from the deep subject matter expertise, knowledge, and experience expert agency personnel have with industry, best practices, and trending issues. This knowledge and experience could translate into efficient identification, investigation, and enforcement of applicable standards. Furthermore, given that some of the most critical data privacy and security issues increasingly turn on the use of advanced digital technologies (such as AI) for which operational context is essential for both identifying and addressing opportunities and risks, it is increasingly important to secure a place for expert knowledge in informing enforcement efforts.

- The potential costs of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law are potentially inconsistent interpretation of sections of the law across agencies, and inconsistent identification, investigation and enforcement, based on varying degrees of agency personnel subject matter expertise and operational speed.

B. **What expertise, legal authorities, and resources are available—or should be made available—to the Federal Trade Commission and state Attorneys General for enforcing such a law?**

- Industry experts and their real-time current subject matter expertise are and should always be available to the FTC, state AGs, and any government body that requires deep knowledge of the privacy and security industry in order to thoughtfully implement and enforce applicable laws. Such industry expertise is especially critical to factor into the knowledge base of enforcement authorities because it often stands as a critical complement to the equities and experiences of other contributors, such as academics, civil society representatives, and researchers. Industry experts notably will have had some of the most direct and current experiences operationally fielding digital technologies and subsequently encountering their most urgent and pragmatically grounded privacy and security risks and challenges.

C. **How could a safe harbor be beneficial or harmful in promoting compliance with obligations related to data privacy and security?**

- As we noted in a 2022 submission to an OSTP Request for Information on Advancing Privacy-Enhancing Technologies (PETS, full text of response here: https://www.nitrd.gov/rfi/2022/87-fr-35250/Palantir-PET-RFI-Response-2022.pdf):
    - The adoption of PETs by entities liable for inappropriate information disclosure and/or use should be incentivized through the expansion of existing safe harbor regulations (such as HIPAA Safe Harbor) and the establishment of new safe harbor regulations to cover the use of PETs.

VII. Additional Information

We welcome any additional information that may be relevant to the working group as it develops a comprehensive data privacy and security law.