November 29, 2024

Submitted via Electronic Mail to www.regulations.gov

U.S. Department of Justice
National Security Division, Foreign Investment Review Section
175 N Street NE, 12th Floor
Washington, District of Columbia 20002

RE: Comments of ACT | The App Association on the Proposed Rule Regarding Access to Americans' Bulk Sensitive Data and Government-Related Data by Countries of Concern

In response to the notice issued on October 9, 2024,[1] ACT | The App Association hereby submits comments to the Department of Justice (DOJ) National Security Division in response to its request for public input on the Proposed Rule implementing Executive Order 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, by prohibiting and restricting certain data transactions with certain countries or persons.

The App Association represents thousands of small business innovators and startups in the software development and high-tech space located around the globe.[2] As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. Today, that digital economy is worth more than ti1.8 trillion annually and provides over 6.1 million American jobs.[3]

While the global digital economy holds great promise for App Association member companies, our members face a diverse array of challenges when entering new markets. Some of these challenges involve restrictions imposed by potential trading partners. These restrictions, commonly referred to as "trade barriers," reflect in the laws, regulations, policies, or practices that protect domestic goods and services from foreign competition, artificially stimulate exports of particular domestic goods and services, or fail

[1] Department of Justice, National Security Division, *Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons*, 28 CFR Part 202 (October 29, 2024), available at https://www.regulations.gov/document/DOJ-NSD-2024-0004-0001.

[2] ACT | The App Association, *About*, *available at* http://actonline.org/about.

[3] ACT | The App Association, *State of the U.S. App Economy: 2023*, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf

to provide adequate and effective protection of intellectual property rights. These barriers take many forms but have the same net effect: impeding U.S. exports and investment.

The App Association also understands the importance of balancing the benefits of international trade and access to foreign markets with the national security concerns that are implicated by certain types of economic activity. Protecting the privacy and security of Americans' user data is a key concern of our members. We appreciate DOJ's efforts to understand and examine the balance between protecting Americans' privacy and protection from national security threats and maintaining an international trade environment where American small businesses can continue to thrive. We commit to working with DOJ and other stakeholders to strike such a balance. With respect to digital trade, the small business innovators we represent prioritize the following:

- ***Enabling Cross-Border Data Flows:*** The seamless flow of data between economies and across political borders is essential to the functioning of the global economy. Small business technology developers must be able to rely on unfettered data flows as they seek access to new markets.

- ***Prohibiting Data Localization Policies:*** American companies looking to expand into new markets often face regulations that force them and other foreign providers to build and/or use local infrastructure in the country. Data localization requirements seriously hinder imports and exports, reduce an economy's international competitiveness, and undermine domestic economic diversification. Our members do not have the resources to build or maintain unique infrastructure in every country in which they do business, and these requirements effectively exclude them from commerce.

- ***Preserving the Ability to Utilize Strong Encryption Techniques to Protect End User Security and Privacy:*** Global digital trade depends on the use of strong encryption techniques to keep users safe from harms like identity theft. However, some governments continue to demand that backdoors be built into encryption keys for the purpose of government access. These policies jeopardize the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. From a privacy and security standpoint, the viability of an app company's product depends on the trust of its end users.

With respect to the specific proposals contemplated in the Proposed Rule, the small business innovators we represent urge DOJ to consider the following recommendations:

- ***Aligning the Definitions of Covered Person and Data Brokerage with Existing Requirements:*** The App Association recommends several changes to proposed definitions, including:

    - "Data Brokerage" – The App Association strongly encourages DOJ to refine the definition of "data brokerage" to ensure its scope is limited to the

sale of data. As it stands, the definition encompasses "the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data from any person ('the provider') to any other person ('the recipient'), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data." The inclusion of "similar commercial transactions" introduces unnecessary ambiguity, which could lead to misinterpretation and unintended consequences. To address this, the Department could consider adopting a clearer standard, such as those outlined in state privacy laws like Virginia's or Connecticut's, which explicitly tie such transactions to the exchange of consideration. This approach provides a more precise framework, reducing uncertainty while ensuring that the definition effectively captures the intended activities.

- "Personal Health Data" – The App Association recommends that DOJ revise the definition of "personal health data" to focus on information that "identifies" (rather than merely "relates to") a physical or mental health condition. Privacy concerns are unquestionably significant when data can directly identify an individual's health status; however, DOJ should avoid unnecessarily restricting information flows that are merely associated with health matters but do not identify a specific health condition. Such overly broad restrictions could impede access to goods and services, disrupt commerce, and stifle innovation without providing meaningful privacy protections.

- "Sensitive Data" – DOJ's proposed definition of sensitive data diverges significantly from established interpretations of personal and sensitive personal data under existing privacy laws. While we acknowledge DOJ's prior consideration of this issue, we emphasize that this inconsistency will impose substantial compliance challenges, particularly for multinational companies navigating diverse privacy and data protection regulations across multiple jurisdictions. The definition introduces confusion by blending traditional elements of sensitive data with "covered personal identifiers," which are more commonly categorized as personal data. This conflation expands the scope of sensitive data unnecessarily, making it unclear whether companies should treat DOJ's definition as a novel concept or as a reimagining of the term under existing legal frameworks. Additionally, the definition includes typical elements of sensitive data—such as precise geolocation, health data, and financial data—but extends to all online identifiers when used to identify an individual. This broad interpretation lowers the threshold for what qualifies as sensitive data, potentially encompassing far more information than necessary.

  To address these concerns, the NPRM should better align with existing privacy laws. For example, the definition of precise geolocation could be narrowed to match the California Consumer Privacy Act of 2018. Similarly,

the scope of biometric identifiers should be refined to reflect the narrower definitions found in most state privacy laws. Such adjustments would enhance clarity, reduce unnecessary compliance burdens, and ensure consistency with established legal standards.

We also renew our request that DOJ exclude encrypted data from the definition of bulk sensitive data. In the NPRM, DOJ declined to do this because it believes that countries of concern could accumulate encrypted data for future decryption using quantum technology, which is are speculative and insufficient as a bases for this decision. Encryption is a vital and effective tool used widely today, and we believe that applying this rule to encrypted data is misaligned with the Federal government's approach to national security and encryption widely.

- "Covered Personal Identifiers" – The App Association requests that DOJ provide greater clarity regarding the exclusions from the definition of "covered personal identifiers." While the NPRM notes that "demographic or contact data that is linked only to other demographic or contact data" is excluded, it does not define "demographic or contact data" beyond offering a non-exhaustive list of examples, creating ambiguity. We recommend clearly defining "demographic or contact data" and explicitly outlining the scope of exclusions, which should encompass data that has been anonymized, de-identified, pseudonymized, aggregated, or classified as publicly available under applicable privacy laws. Doing so would align with existing laws, regulations, and industry best practices, ensuring consistency and reducing compliance uncertainty.

  Additionally, the proposed definition of "covered personal identifiers" should be revised to exclude scenarios where identifiers are combined with other low-risk identifiers, such as IP addresses or contact data. While DOJ's rules are intended to regulate the sharing of sensitive personal data, it is unclear how these specific identifiers pose a meaningful risk of revealing sensitive information. Narrowing the scope of covered personal identifiers in this way would maintain the focus of DOJ's rules while avoiding unnecessary regulatory burdens for low-risk data use.

- "Covered Person" – DOJ's Proposed Rule establishes that the term "covered person" include a company that is at least 50 percent owned, directly or indirectly, by a country of concern. Even when not publicly traded themselves, small businesses and startups may be invested in by larger entities with ownership percentages that may change with market conditions. We recommend that DOJ consider the knowledge-based standard currently employed in the Bureau of Industry and Security's (BIS) export control rules. Similarly, the concept of data brokers is included in the text of numerous state and federal laws. In defining "data brokerage" here, DOJ should look to those definitions to ensure that this new

rulemaking does not result in an overbroad category that unduly includes service providers and other non-data broker entities and activities.

- ***Ensuring the Appropriate Distribution of Risk and Liability:*** We urge DOJ to provide clearer guidance regarding liability under the rules for key actors in impacted value chains. While the NPRM attempts to address CSP liability through a "know or reasonably should have known" standard, the definition of "knowingly" is overly broad and risks being applied retrospectively. This is particularly concerning for parties that do not directly access client data but instead process, store, or facilitate data movement at the client's direction. We recommend limiting the definition of "knowingly" to instances of actual knowledge, rather than a subjective "should have known" standard that invites hindsight bias. The standard DOJ proposes creates uncertainty and leaves good faith parties vulnerable to retroactive evaluations of their actions, potentially penalizing them for outcomes they could not reasonably predict. DOJ's proposed treatment of emerging technologies compounds this uncertainty. As a prime example, DOJ's NPRM describes a scenario involving a U.S. subsidiary of a foreign company developing an AI system trained on bulk sensitive data. The assumption that the AI system—or its chatbot—will inevitably reproduce sensitive data is overly simplistic and problematic. Following this logic, any technology with potential vulnerabilities or misuse risks could be classified as a "covered transaction."

  This approach, coupled with the expansive definition of "knowingly," creates an ambiguous regulatory environment that discourages innovation and the adoption of new technologies. Furthermore, it stretches the concept of data brokerage to encompass not only intentional actions but also unforeseen outcomes and malicious acts, exacerbating compliance challenges. To address these concerns, we strongly recommend that the final rule clarify two key points:

  - **Liability Assignment:** The responsibility for compliance should rest with the data owner, not the CSP, which acts merely as a service provider without control over the data's use.

  - **Narrower Definition of "Knowingly":** The term should be defined to require actual knowledge of specific issues, avoiding the ambiguity of the "should have known" standard.

  The changes the App Association recommends would provide much-needed clarity, foster an environment conducive to innovation, and align regulatory expectations with practical realities in data management and technology development.

- ***Preserving the Free Flow of Typical Economic Activity:*** The App Association supports of DOJ's proposal to exempt data transfers executed in the ordinary course of conducting financial services-, payment processing-, and regulatory

compliance-related transactions from new requirements under the proposed rule. Such data transfers would not be of a kind that implicates the national security concerns raised by DOJ, but additional restrictions on such transfers could have costly impacts on otherwise beneficial international transactions. The App Association therefore recommends that DOJ exclude from the rule any sharing of information that is essential for providing, maintaining, or offering products or services within an online marketplace. Similarly, DOJ should consider exemptions for data transfers that are merely incidental to the use of communications services, as well as transfers of encrypted data, which is secured against unauthorized access.

Further specific recommendations for changes to DOJ's exemptions include:

- *Financial services exemption:* To improve Example 10, we recommend clarifying that requests from regulatory authorities in countries of concern should be exempt as "ordinarily incident to the provision of financial services" if the request is lawful under the country's legal framework and it pertains to financial activities covered by the Financial Services Exemption. Prohibiting compliance with such requests would create legal comity issues. Clear guidance will ensure businesses can operate effectively while adhering to local and international requirements.

  We also recommend adding an example to complement Example 11 clarifying that data transfers may be necessary both in response to government requests and as part of routine reporting requirements. DOJ should provide for companies' providing reports or information mandated by the laws, regulations, or official guidance of the country of concern.

  We further support adding an example to clarify that cyber services can be viewed as ancillary to processing payments and funds transfers, serving as a means of risk mitigation and prevention.

- *Intra-company exemption:* As we have previously noted for DOJ, many App Association members develop their products utilizing a distributed workforce that may be partially located outside of the United States. Such a practice is common and may be necessary to keep costs down in developing certain parts of a software product or service. Preventing access to company customer or user data by employees, contractors, interns, etc., within a company could drastically drive up costs and significantly slow the product development process, all without a tangible benefit to U.S. national security interests. Similarly, our members may employ foreign nationals in the United States for the purpose of product development and restricting data access for those individuals would be extremely burdensome. The App Association, therefore, requests that DOJ provide an exemption for intra-company data access and transfers. Such transfers may be in the context of billing systems, internal

communications such as email, internal operations management programs, and other uses that are part of the ordinary course of business for many companies.

In response to DOJ's proposals in the NPRM, the App Association supports broadening the intra-company group exemption past data sharing incidental to specific administrative or ancillary business functions by granting a full exemption for all instances in which a part of the company located in a country of concern receives data from its U.S. counterpart, rather than just scenarios where a U.S.-based component shares information with a counterpart in a country of concern. Furthermore, we recommend that the DOJ consider implementing an encryption requirement, such that the exemption would apply to all data transfers from a U.S.-based part of a company to a counterpart in a country of concern, provided that encryption is utilized.

- *Telecommunications services exemption:* We suggest that the DOJ enhance the definition to more clearly encompass other forms of communication, including data delivery, internet access, and messaging.

- ***Protection of Intellectual Property:*** The App Association strongly recommends that DOJ include language to safeguard confidential and proprietary information, as well as trade secrets contained in the reports and audits, from public disclosure or use as evidence.

- ***Ensuring a Harmonized International Trade Environment:*** The App Association is highly supportive of coordination with other regulatory regimes as contemplated in the Proposed Rule and underlying Executive Order. As DOJ has already acknowledged, companies involved in international trade are already subject to national security-related requirements overseen by the Committee on Foreign Investment in the United States (CFIUS), the Office of Foreign Assets Control (OFAC), BIS, and other entities. If new rules promulgated by DOJ create additional requirements that conflict with existing regulations, the international trade environment will become more difficult for startups and small businesses to navigate. Efforts to harmonize the various applicable regimes will be greatly beneficial to the companies seeking to comply.

- ***Easing Compliance Burdens:*** The App Association is concerned about the high burdens of compliance for the small business community, and raises the following to reduce these burdens while supporting DOJ's goals and mission:

  - Because App Association members widely take robust steps to address data privacy and export control requirements which can and should be applied to compliance with DOJ's new compliance program. Relatedly, proposed CISA security requirements impose overly stringent due diligence and audit expectations, and that CISA should consider aligning

its requirements with established cybersecurity standards.

- Section 202.302 unnecessarily expands the rule to cover not only transactions with designated covered persons but also all foreign entities. The requirement to contractually obligate foreign parties to avoid engaging in subsequent covered data transactions with covered persons is overly rigid. DOJ should take an approach focused on flagged concerns, similar to export control laws, rather than imposing contractual requirements on all foreign parties. Additionally, DOJ should clarify that this regulation will not apply to agreements made before the effective date (if the DOJ intends for the regulation to apply to prior agreements, the App Association requests that an effective date be established that allows U.S. companies sufficient time to adjust their existing contracts).

- DOJ's proposed requirement for an external auditor is unwarranted, and the App Association encourages DOJ to instead permit the use of an independent internal auditor. Should an audit conducted for other purposes to be used, provided it meets the requirements of this program.

- Overall, the implementation of DOJ's new rules will require small companies to modify their systems and contracts to effectively track data in ways they did not previously. Because it is vital to ensure that companies have adequate time to comply with these changes, we suggest that the NPRM should become effective one year after the final rules are published.

The App Association appreciates the opportunity to submit these comments on the Proposed Rule. We stand ready to work with DOJ and other stakeholders to protect the privacy and security of all of Americans while maintaining a competitive environment for U.S. businesses and innovators.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005