

April 19, 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 Advance Notice of Proposed Rulemaking Regarding Access to Americans' Bulk Sensitive Data and Government-Related Data by Countries of Concern

In response to the Federal Register notice issued on March 5, 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 Advance Notice of Proposed Rulemaking (ANPRM) regarding access to Americans' bulk sensitive data and government-related data by countries of concern.

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 \$1.8 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.

¹ Department of Justice, National Security Division, *National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Data and Government-Related Data by Countries of Concern*, 89 FR 15780 (March 5, 2024), available at <https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and>.

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>

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 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 applaud 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 ANPRM, the small business innovators we represent urge DOJ to consider the following recommendations:

- ***Preventing Interference with Internal Activities of Companies with a Distributed Workforce:*** 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. To prevent 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.

- ***Aligning the Definitions of Covered Person and Data Brokerage with Existing Requirements:*** The ANPRM proposes 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.
- ***Preserving the Free Flow of Typical Economic Activity:*** The App Association approves 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. 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.
- ***Ensuring a Harmonized International Trade Environment:*** The App Association is highly supportive of coordination with other regulatory regimes as contemplated in the ANPRM and underlying Executive Order. As the ANPRM notes, 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.

The App Association appreciates the opportunity to submit these comments on the ANPRM. 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,

A handwritten signature in black ink, appearing to read "B. Scarpelli". The signature is fluid and cursive, with a large initial "B" and a stylized "S".

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

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