Consumer Technology Association™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

April 19, 2024

The Honorable Merrick Garland
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530

Re: National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern (89 FR 15780; Docket No. NSD 104)

Dear Attorney General Garland:

The Consumer Technology Association (CTA) appreciates the opportunity to submit written comments on the Department of Justice's (DOJ) advance notice of proposed rulemaking (ANPRM) regarding access to Americans' bulk sensitive personal data and government-related data by countries of concern. The consumer technology industry is predicated on designing and delivering products for use by people, whether in households, businesses, or governments. The protection of sensitive data is therefore of paramount importance. CTA also recognizes the importance of narrowly tailored approaches to addressing discrete national security challenges while ensuring U.S. economic competitiveness. We therefore offer our comments in the spirit of constructive engagement and collaboration to address a shared concern.

CTA represents the more than $505 billion U.S. consumer technology industry, which supports more than 18 million U.S. jobs. Our membership comprises over 1,300 companies from every facet of the consumer technology industry, including manufacturers, distributors, developers, retailers, and integrators, with 80 percent of CTA members being start-ups or small and mid-sized companies. CTA also owns and produces CES®—the most powerful tech event in the world—which showcases and serves as a forum for discussion of international policies concerning existing and new technologies, international technology trade and investment, and global opportunities and challenges facing the consumer technology industry. CES 2025 takes place on January 7-10, 2025, in Las Vegas. We strongly encourage DOJ leaders and staff to participate and engage with industry at this event.

First, CTA's comments outline key principles for consideration by the National Security Division as it considers the shape of any proposed rule. Then, in the attached Annex, we offer answers to certain questions from the ANPRM that are particularly relevant to the consumer technology industry.

1. **U.S. Technology Leadership Is Necessary to Address National Security Challenges AND Negotiate Strong Digital Trade Rules**

CTA appreciates the balance that Executive Order 14,117 (EO) and the ANPRM seek to achieve on national security, civil rights, innovation, and economic competitiveness. As the largest and most innovative economy in the world, the

United States stands to reap the greatest benefits from the international data economy. The choices the United States makes with respect to identifying and addressing perceived security threats relating to data will therefore find significant resonance with other countries. CTA strongly believes that the United States should be a visible leader in global discussions on technology and should proudly promote U.S. values in those discussions. The hallmark of effective global leadership lies in proactively addressing domestic issues while simultaneously seeking better approaches at the international level.

In that regard, the United States must negotiate new international rules regarding Data Free Flow with Trust, building on the essential work on this topic at the G7 under the leadership of Japan. Unfortunately, at present, the Office of the U.S. Trade Representative (USTR) is taking a "pause" on negotiating new rules, as it considers what "policy space" the United States may need domestically on digital trade. CTA firmly disagrees with this approach and believes that it contravenes U.S. national security interests in this space.

In fact, USTR – supported by a whole-of-government effort – should reinvigorate itself as to the objectives it set out for itself at the start of this administration - walk, chew gum, and play chess at the same time when it comes to digital trade. USTR can work closely with U.S. regulators, U.S. law enforcers, and the U.S. national security apparatus and consult with Congress on digital trade, all while negotiating the highest standard rules possible consistent with U.S. law and regulation. These rules should prohibit global restrictions on cross-border data flows, prohibit global requirements to locate computing facilities domestically, and allow for traditional exceptions to address legitimate public policy objectives.

By "pausing" and seeking “policy space", the U.S. government is signaling to foreign governments that existing international rules may be deficient and ceding technology leadership to other countries, many of which are entirely comfortable with restricting the free flow of data across borders and requiring that companies store their data locally.[1] By contrast, binding and enforceable provisions in trade agreements (and other types of bilateral or plurilateral agreements) that promote the free flow of data across borders - with trust - support a more innovative and competitive global economy.

2. U.S. Sensitive Data Will Not Be Secure if Harmful Restrictions on Cross-Border Data Flows and Data Localization Requirements Continue to Proliferate

Every year, USTR publishes the National Trade Estimate (NTE) Report on Foreign Trade Barriers, a "comprehensive review of significant foreign barriers to U.S. exports of goods and services, U.S. foreign direct investment, and U.S. electronic commerce in key export markets for the United States."[2] Prior to 2024, this report had contained many barriers to digital trade. In March, USTR signaled that it would scale back the digital trade barriers identified in the 2024 NTE because other governments should also have "policy space" to determine their own digital trade measures.

The operating assumption of USTR seems to be that governments should control the flow of data and information across borders. A better approach would be to let businesses and the private sector manage their own data flows

[1] For example, Russia enacted Federal Law No. 152-FZ of July 27, 2006 on Personal Data (as amended), which requires personal data to be stored in Russia and limits cross border transfers. Additionally, China passed a series of laws, including the Personal Information Protection Law, which requires personal information to be stored in China.

[2] https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/march/ustr-releases-2023-national-trade-estimate-report-foreign-trade-barriers

through contractual relationships under existing laws or through interoperable mechanisms negotiated among governments, such as the APEC Cross-Border Privacy Rules System[3] or the EU-U.S. Data Privacy Framework Program.[4]

However, the ultimate reason that USTR is scaling back these barriers to digital trade is that it and other U.S. agencies, including the Federal Trade Commission (FTC), are proactively encouraging other governments to impose onerous and discriminatory new digital measures on U.S. technology companies. This coordination with other governments, such as the European Union, is part of a misguided approach to competition policy at USTR, in dereliction of its responsibility over trade policy. Instead of breaking down restrictions on cross-border data flows and data localization requirements, USTR is now urging other governments to undertake such measures based on a deeply flawed notion that doing so will somehow benefit competition in the United States. Recent statements by FTC Chair Lina Khan confirm that she supports USTR's collaboration with other governments.

This does not bode well for the security of the sensitive data of Americans. While a final rule may prohibit and restrict access to sensitive data of Americans by countries of concern, there is no reason to suggest that doing so makes that data more secure, given that where data transits and is stored is generally irrelevant to its security so long as security measures taken to protect data while in transit and at rest are appropriate to any relevant risks. However, in adopting such a rule, the United States misdirects its focus, and should instead re-commit to addressing the broader trend of restrictions on cross-border data flows and data localization requirements by numerous other countries, including U.S. allies and key trading partners. The Organization for Economic Cooperation and Development (OECD), of which the United States is a member, has extensively catalogued such measures over the course of many years.[5]

We urge DOJ to convey to USTR how its decision to ignore these harmful measures is, at best short-sighted, but at worst antithetical, to serious U.S. efforts to protect Americans' sensitive data. For example, restricting cross-border data flows may limit many American companies from operating in those jurisdictions altogether, and may drive companies that are still able to operate in those jurisdictions to create original data repositories in many different countries rather than having a single data set in the cloud that is accessible from those countries. Having these multiple touch points on sensitive data of Americans will ultimately increase cybersecurity risk. The more the United States stands back, the more these adverse measures will proliferate and endanger U.S. economic interests, undermine free speech and human rights across the world, and ultimately harm broader U.S. national security interests. [6]

3. Working with Allies to Address Shared Concerns on Data Security is the Best Approach for the United States

As we have witnessed in the recent past, when the United States acts alone to address security and economic issues, its allies and key trading partners may not go along willingly or at all. In this way, unilateral U.S. actions like the Section 232 national security tariffs on steel and aluminum and the Section 301 tariffs on products of China, lead to unintended consequences that cause harm to U.S. businesses, workers, and consumers. If DOJ and its interagency partners do not coordinate a possible final rule with U.S. allies and work with them to address their concerns, their businesses and citizens may also be harmed. This is particularly the case given what appear to be extraterritorial aspects of the envisaged rule. For example, the ANPRM prohibits "U.S. persons" from "knowingly directing any

[3] APEC Cross-Border Privacy Rules (CBPR) System, https://cbprs.org/

[4] EU-U.S. Dasta Privacy Framework, https://www.dataprivacyframework.gov/s/ (note such framework also includes extensions for the UK and Switzerland).

[5] https://www.oecd.org/publications/the-nature-evolution-and-potential-implications-of-data-localisation-measures-179f718a-en.htm

[6] https://freedomhouse.org/article/coalition-letter-urging-biden-administration-protect-free-and-open-internet

covered data transactions that would be prohibited…. if engaged in by a U.S. person."[7] Thus, if a "U.S. person" is in any senior level position at a multinational or foreign company, this rule could cause entities in other countries to be restricted from certain transfers.[8]

CTA strongly encourages DOJ to coordinate with U.S. allies and key trading partners to the greatest extent possible to identify the core national security challenges regarding data security in countries of concern and explore collective actions to address those challenges. DOJ should consider working with the Department of State and the Department of Commerce to engage our allies and key trading partners through existing or new bilateral fora, bilateral and regional trade agreements, and effective international fora (e.g., the G7 and the OECD). Collaborative institutions and agreements would enable collective action in addressing national security challenges may provide greater certainty to U.S. businesses over time while conveying to countries of concern that they cannot divide and conquer the free and democratic world.

4. A Final Rule on Data Security Must Contain a Transparent and Effective Process that Includes Public Comment and Consultation with Congress On Designating Additional Countries as Countries of Concern

CTA is mindful that the authorities created by the executive branch can be stretched, circumvented or negated by a subsequent Administrations. We do not dispute that there may be real national security challenges with respect to countries that DOJ may identify as countries of concern for the purpose of a final rule on data security. However, a future administration may decide to designate additional countries in the name of national security to address other considerations that it deems relevant, but in ways that do not meet the thresholds established by this EO. Establishing a process to consult the public and Congress on any additions to the list of countries of concern will ensure a balanced and thorough vetting of the proposed country(ices) and the potential impact on national security, including the potential economic and commercial impacts for the United States.

We urge DOJ to include in a proposed rule effective guardrails for designating additional countries of concern and work with the Congress on codifying these guardrails into law. Such guardrails could include notice and comment processes for proposed designations, obligations to obtain the sense of the Congress on designation (e.g., through a resolution of approval), or obligations to pursue negotiations with possible additional countries of concern first prior to designation. Without effective guardrails, CTA is concerned that a future administration could abuse the powerful authority that a final rule would provide.

5. A New Program and Final Rule on Data Security is Not a Substitute for Federal Privacy Law

CTA has long advocated for a comprehensive federal privacy law in the United States and continues to urge the Congress to pass such a law. We believe that a federal privacy law would ensure consistency and clarity for consumers and innovators when it comes to protecting consumers' personal information. CTA also shared more detailed views on this topic in comments to the FTC in the Commercial Surveillance and Data Security Rulemaking, where we argue that it is important to recognize the benefits of responsible data use rather than focus exclusively on consumer data misuse. CTA urges the DOJ exercise the same level of caution in developing data security rules here.

---

[7] ANPRM, Section III (G), https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[8] Note that such potential reach is also made clear by the examples in Section III (G). *See e.g.* Example 42 (A *U.S. person* is an officer, senior manager, or equivalent senior-level employee at a foreign company that is not a *covered person,* and the foreign company undertakes a *covered data transaction* at that *U.S. person'* s direction or with that *U.S. person'* s approval when the *covered data transaction* would be prohibited if performed by a *U.S. person*).

We welcome the statement in the Federal Register Notice that a possible final rule on data security would exempt domestic transactions regarding sales of bulk sensitive personal data within the United States and by U.S. persons. We recommend to the Department that a proposed rule contains specific, ironclad language to make good on this statement to give assurances to stakeholders that the data security program and final rule would not in any way be a substitute for a federal privacy law.

More, any data flow restrictions need to be limited by specific company certification or accountability demonstration mechanisms (e.g., Global/APEC Cross-Border Privacy Rules, Binding Corporate Rules, and Standard Contractual Clauses) to allow for maximum flexibility for companies.

Regarding the recently introduced American Privacy Rights Act, CTA appreciates this bipartisan, bicameral effort to pass a federal data privacy law to protect consumers' personal information. CTA has long advocated that a uniform federal privacy law is needed for innovation to thrive and American leadership in emerging technologies like artificial intelligence. We support a national privacy standard that preempts state laws, providing legal clarity for companies to operate and consistent protections across state borders for consumers. We look forward to working on this effort with the Senate Commerce and House Energy & Commerce committees.[9]

6. A Final Rule Should Clearly Define Terminology Included in the ANPRM

In our review of the ANPRM, CTA has identified several terms that require clear definitions. These terms must reflect existing definitions in U.S. law and regulation, to avoid differences and the creation of unintended consequences. Unclear or inconsistent definitions could lead to impacts on related and/or unrelated areas of U.S. law and regulation. These terms include:

- Prohibited transactions
- Restricted transactions
- Data broker[10]
- Sensitive personal data
- Vendor agreements
- Employment agreements
- Investment agreements
- U.S. individual
- Country of concern[11]

[9] https://www.cta.tech/Resources/Newsroom/Media-Releases/2024/April/CTA-Statement-on-American-Privacy-Rights-Act

[10] This should be refined to be consistent with other interpretations – i.e., California's DELETE Act (Cal. Civ. Code. 1798.99.80) which says "Data broker" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.

[11] The ANPRM contemplates a definition from the EO. Yet, we have a definition of foreign adversary that is found in CFR Title 15(A)(7)(A) Section 7.2 Foreign adversary means any foreign government or foreign non-government person determined by the Secretary to have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons. We also have a definition of "covered nation" that is used in HR 7520 that is found in statute: 10 US Code Section 4872(d)(2) that includes North Korea, China, Russian Federation and Iran. There is a benefit to referring to a statutory definition in that it limits the potential for arbitrary executive changes as the result of administration changes.

7. DOJ Should Revise the Definition of "Covered Data Transaction" and Provide a Limited Definition of "Sale"

In drafting a proposed rule, CTA recommends that DOJ revise the scope of "covered data transaction" to exclude intragroup data transactions, where the recipient collects or processes sensitive personal data in the normal course of business. The recipient in a corporate group is bound by the same rules and requirements for data processing as the entity providing the sensitive personal data ("provider"). This includes the transfer to service providers who process the personal data on behalf of the provider. In addition, employees (including individual contractors) are subjected to a duty of confidentiality during his or her employment.

Additionally, we believe that "sale" should be a defined term and should not include the following data transactions: (i) the disclosure of personal data to a service provider that processes the personal data on behalf of a U.S. company; (ii) the disclosure of personal data to a third party for purposes of providing a product or service requested by an U.S. person; (iii) the disclosure or transfer to a subsidiary or affiliate of an a U.S. company.[12]

8. DOJ Should Avoid Including Certain Legitimate Business Practices in the Scope of Transactions

Consumer technology firms engage in a vast array of legitimate business practices in the United States and all over the world. Advertising is one of these practices and can involve the use of bulk personal sensitive data. According to CTA's 2022 Research Report on U.S. Consumer Privacy Sentiments[13], a majority of U.S. adults are not extremely concerned with how personal information will be used for marketing/advertising purposes. CTA recommends that DOJ exclude advertising transactions from possible prohibited or restricted transactions. By including advertising in the scope, DOJ may inadvertently curtail the ability of U.S. companies from advertising their products and services to U.S. customers.

As DOJ is considering with the provisions of certain financial services, it should exempt data exchanged incidental to the provision of telecommunications and broadband services to consumers, enterprises, and government. These services include the signaling and data necessary for the provisioning and functioning of roaming and/or mobile services, and the signaling and data necessary for the provisioning and functioning of internet connectivity (ISP service). Such services will include the processing of any data provided by the consumer, enterprise, or government while using those services and the interconnection arrangements with global telecommunications network providers necessary to realize global communications. Further, telecommunications and broadband service providers shall be able to use, disclose, or permit access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents to initiate, render, bill, and collect for telecommunications services.

9. Sensible Exemptions are Critical to U.S. Businesses and Should Avoid Ambiguity

CTA welcomes the exemption for intracompany transfers of bulk sensitive personal data from the United States to countries of concern. This is a sensible exemption that acknowledges that such transfers likely do not pose a national security risk given the multitude of compliance obligations that U.S. businesses must protect the personal data of Americans. It also recognizes that businesses must frequently move data within and among their corporate entities during normal business operations.

---

[12] CTA also recommends that DOJ consider including a provision in a final rule that allows for otherwise covered data transactions to be made, when the transactions are accompanied by specific contractual terms around the security and protection of data as well as notice requirements, audit rights and downstream protection requirements.

[13] https://shop.cta.tech/products/data-privacy-u-s-consumer-attitudes-and-behaviors

While the ANPRM recognizes this reality by proposing an exemption for intra-entity transactions, the effectiveness and clarity of the proposed exemption is severely compromised by the inclusion of language indicating that the underlying transaction must be "incident to business operations" and part of "ancillary business operations." This both creates significant uncertainty as to the scope of the exemption, but also appears to turn the logic for restricting transactions on its head – instead of permitting all transactions that do not entail transfers of the kind intended to be prevented in the EO, the proposed exemption would only permit a narrow slice of vaguely defined transactions. As such, we propose that the exemption be reframed to provide that data transactions between a U.S. person and its subsidiary or affiliate that are part of ordinary business operations will not be subject to prohibition or restriction, provided that the sale or transfer of data for commercial gain is not itself the primary purpose of the transaction.

10. Transfers of Public Government-Related Data Can Be Legitimate

The United States government makes a massive amount of data available to the public for free. Often U.S. firms use this data internally to inform their business practices. They may also transfer that free, public data to potential partners in other countries, including in countries of concern. If there is no sale of the government-related data, which is already free for U.S. and international persons to consume and share, then it would make sense for transfers of such data to be excluded from the scope of a proposed rule.

11. DOJ Should Consult with Other U.S. National Security and Economic Agencies to Inform the Buildout of the Data Security Program

CTA applauds DOJ for its close coordination with other U.S. government agencies in its work to date on the data security ANPRM. Creating a new program that will impact U.S. private sector activity will require attention to detail, thoughtfulness, and flexibility. We encourage DOJ to consult with other U.S. government agencies in its development of the data security program, especially those agencies who have stood up new programs on technology, data, and national security in recent years. These agencies include the Bureau of Industry and Security and the International Trade Administration within the Department of Commerce, as well as the Departments of State and the Treasury.

12. A Final Rule Should Include Mechanisms for Entities in Countries of Concern to Demonstrate that They Can Be Trusted with U.S. Bulk Sensitive Personal Information

CTA understands that the Executive Order and ANPRM contemplate the prohibition of sales of certain types of U.S. bulk sensitive personal information to entities in countries of concern. It may be the case that this prohibition, additional possible restrictions in a final rule, and other U.S. government policies change actions by, and the perception of, countries of concern for the better. Should overall bilateral relations improve as a result, DOJ could consider creating a mechanism for entities in (or subject to the jurisdiction of) countries of concern to demonstrate that they can be trusted with U.S. bulk sensitive personal information.

Such a mechanism could include negotiations between DOJ and entities in countries of concern that wish to demonstrate the robustness of their data governance practices. Such negotiations could also be valuable sources of information on relevant practices, laws, and regulation in countries of concern. Whether as a part of a proposed rule or through a parallel process, DOJ should consider possible pathways for entities in countries of concern to demonstrate trust.

Conclusion

CTA recognizes the importance of calibrating any new program on data security and alignment it with existing U.S. policy, law, and regulation. As DOJ works with its interagency partners to review comments in response to the

ANPRM, CTA stands ready to serve as a helpful resource. We look forward to reviewing a proposed rule at the appropriate time and providing further constructive feedback.

/s/ Ed Brzytwa
Ed Brzytwa
Vice President of International Trade
Consumer Technology Association

/s/ Rachel Nemeth
Rachel Nemeth
Senior Director of Regulatory Affairs
Consumer Technology Association

Annex - CTA Responses to Specific Questions in the ANPRM

- **What additional information or clarifications are you seeking from DOJ on the following terms related to covered data transactions? Are there any additional factors that DOJ should consider on these terms?**

    - Vendor agreements: We seek clarification that vendor agreements are only covered when it involves a "bulk" amount of sensitive personal data, consistent with the examples 19-22, and make clear that data that doesn't meet this threshold is out of scope.

    - Exempt transactions: As noted above, we believe that an exemption for intra-entity transactions should be clearly defined and crafted such that the rule's prohibition on covered data transactions only addresses those narrow categories of transactions that create potential national security risk. However, should DOJ elect to maintain its current approach, we would ask for further clarity on what constitutes "ordinarily incident to and part of ancillary business operations." For example, it would be of business interest in some cases for global companies to allow certain foreign persons with professional expertise to access U.S. data (pending definitions) to perform a specific job function even though they are based in countries of concern. We seek clarification on whether this is exempted, if not, we welcome ways, such as adding security controls and standards, to ensure flexibility.

- **What are some business scenarios in which the applicability of the ANPRM/EO remains unclear?**

  We seek clarity on what applies more specifically on Government-related data. The ANPRM proposes expanding the definition of "Government-related data to include "any precise geolocation data, regardless of volume, for any location within any area enumerated on a list of specific geofenced areas associated with military, other government, or other sensitive facilities or locations (the Government-Related Location Data List)." This is an extremely broad category of data. The ANPRM should clearly articulate that if companies are not engaging in the sale of such Government-related data, it would not be in scope, consistent with the examples 10 & 11.

Question 1. *In what ways, if any, should the Department of Justice elaborate or amend the definition of bulk U.S. sensitive personal data? If the definition should be elaborated or amended, why?*

CTA Response: DOJ should align the definition of sensitive data with existing state level comprehensive privacy laws. As discussed below, DOJ should also exclude de-identified, pseudonymized, encrypted, and publicly available information in alignment with existing US state-level comprehensive privacy and data breach notification laws, and information encrypted using industry-standard encryption (e.g., in accordance with a standard to be developed by NIST).

Question 2. *Should the Department of Justice treat data that is anonymized, pseudonymized, de-identified, or encrypted differently? If so, why?*

CTA Response: DOJ should explicitly exempt from the scope of "sensitive personal data" and "government-related data" any personal data that has been encrypted, or anonymized or de-identified in such a way as to render it no longer personal data under state-level comprehensive privacy data breach notification laws in the United States. In doing so, we would encourage DOJ to be clear about how it is using the terms listed in this question. The terms "anonymized," "pseudonymized," and "de-identified" can be confusing because there is little agreement—among either technical and policy experts, legal practitioners, or regulatory authorities —about how they should be used. Some actors, often technical ones, use the terms to refer to particular methods of reducing the risk of identifiability

of data. For example, “anonymization” and “de-identification” may be used to refer to the removal of direct and indirect identifiers, such as names, from a dataset, while “pseudonymization” may be used to refer to the replacement of identifiers with pseudonyms or tokens.

Other actors, often legal ones, use those terms to refer not to particular technical methods, but to the level of risk reduction those methods achieve and the legal protections that apply as a result. In particular, the terms “de-identified” and “anonymized” may, depending on the jurisdiction, refer to data that has been treated in such a way as to no longer be “personal data” - to no longer be subject to most of the obligations comprehensive data privacy laws apply. In the United States, “de-identified” tends to be used in state-level laws, while other jurisdictions tend to use “anonymized.” “Pseudonymized” is sometimes used to refer to data whose risk of re-identifiability has been reduced, but to a level that falls short of “anonymized” or “de-identified,” rendering individuals identifiable only with the use of additional, separate information. In some jurisdictions, pseudonymized data is considered personal data under comprehensive privacy laws, but is not subject to certain requirements, such as data subject rights.

Unlike “anonymization,” “de-identification,” and “pseudonymization,” there is general agreement across U.S. state-level comprehensive privacy laws that “publicly available” data should generally include data made lawfully available to the public either by the individual or through government record or widely distributed media. There is also agreement that “publicly available” data is not personal data.

We encourage DOJ to look to state comprehensive privacy laws when crafting “de-identified data” and “publicly available data” exemptions. For example, the VCDPA defines “de-identified data” as “data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person,” and “publicly available information” as “information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.” VCDPA exempts “de-identified data” and “publicly available data” from the scope of personal data. DOJ should explicitly exempt such data from the scope of “sensitive personal data” and “government-related data”. Not only would this ensure alignment with existing laws, but it would also ensure that the final rules are properly targeted to realistic risks. “De-identified data” that cannot reasonably be linked to an identifiable United States individual cannot be exploited by countries of concern.

Similarly, the terms “government-related data” and “bulk sensitive personal data” should explicitly exclude data encrypted using industry-standard encryption, such as those which comply with cryptographic standards for data at rest and data in motion promulgated by the National Institute of Standards and Technology (NIST). Encryption is commonly accepted as one of the most effective measures available to prevent third-parties from accessing data without permission, and undergirds the security of data for individuals, companies and governments around the world.

DOJ’s definition of “access” appears to acknowledge that the ability to decrypt may be fundamental to a third party’s ability to access content. As such, encrypted data, where persons or countries of concern do not possess the key required to decrypt it, does not present the kinds of risks the Executive Order and this Rulemaking seek to address.

As with all technology, innovation presents new challenges and demands the development of new solutions. While work is ongoing to develop quantum computing capabilities that can decipher encrypted data, these efforts are far from a stage where they can be operationalized, let alone at the scale that would be required to decrypt the kinds of

bulk data at issue in this rulemaking. Moreover, simultaneous work is underway to develop quantum resistant cryptographic algorithms, of which NIST has approved several.[14]

Given the significant work already being undertaken in this space, most encryption experts and researchers from academia, private and public sectors, and the open-source community expect that modern encryption schemes will continue to advance ahead of increases in scalable computational technology (including the availability of quantum computing at scale).

Including encrypted data in the scope of this rulemaking by defining it as sensitive personal data would set a concerning precedent about the treatment and security presumptions of encrypted data while failing to further the stated purpose of the EO, and it would run counter to the EO's instruction that the Attorney General "carefully calibrate[] actions to minimize the risks associated with access to Americans' bulk sensitive personal data and government-related data by countries of concern and persons that are "owned by, controlled by, or subject to the jurisdiction or direction of" countries of concern, while minimizing disruption to commercial activity."

Question 3. *Should the Department of Justice consider amending the definitions applicable to any of the six categories of sensitive personal data? If the definition should be elaborated or amended, why?*

CTA Response: We appreciate DOJ's efforts to specify categories that are narrowly tailored to the most exploitable kinds and uses of data. For example, with regard to "biometric identifiers," DOJ is right to recognize that data about persons' physical characteristics poses risks when used to recognize or verify their identities. We also appreciate DOJ's grounding of "personal health data" in Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009, together with their implementing regulations codified at 45 C.F.R. Parts 160 to 164 ("HIPAA") and its implementing regulations, which helps to facilitate compliance.

That said, DOJ should consider clarifying the definition of "covered personal identifiers." We appreciate DOJ's recognition that, as described in the Order, there are two important limitations on the scope of this category. First, under the Order, covered personal identifiers must be "personally identifiable data." Second, they must, perhaps when combined with other data, be made "exploitable by a country of concern."

However, as currently defined, "covered personal identifiers" could encompass some combinations of listed identifiers that are neither personally identifiable data nor exploitable by a country of concern. To address this inconsistency, we would suggest that DOJ, when drafting proposed final rules, take three steps.

First, DOJ should make its intent to narrow the types of data that is and is not subject to the rule clear and explicitly exempt de-identified data. Specifically, if DOJ adopts our previous recommendation to exempt de-identified data from the scope of sensitive personal data, DOJ could point to that exemption—and the language used in the VCDPA. Doing so would align with DOJ's stated intention in the ANPRM that "covered personal identifiers" be "much narrower than the categories of material typically covered by laws and policies aimed generally at protecting personal privacy."

Second, DOJ should, when drafting proposed final rules, further refine what particular risks must arise for "covered personal identifiers" to be "exploitable by a country of concern." We understand that DOJ intends to do so. The ANPRM states that "the Department does not intend to impose an obligation on transacting parties to independently determine whether particular combinations of data would be 'exploitable by a country of concern'; rather, the

[14] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Department intends to identify specific classes of data that, when combined, would satisfy this standard." We would encourage DOJ to develop a full record on this issue in the proposed final rules, which will allow for more thorough comments at that point.

Third, DOJ should add two explicit exemptions from the scope of "covered personal identifiers." First, it should exempt any combination of the following three kinds of listed identifiers, unless such combination renders a U.S. individual identifiable to the receiving transacting party: (i) a device- or hardware-based identifier; (ii) an advertising identifier; and (iii) a network-based identifier. Such combinations may be processed by covered persons on behalf of U.S. entities to provide products or services requested by U.S. individuals, and often may not make those individuals personally identifiable. This would prevent "covered personal identifiers" from capturing massive quantities of non-sensitive data by better aligning the definition of "covered personal identifiers" with the broader definition of "sensitive personal data" under existing privacy laws.

Second, DOJ should exempt any data that is processed by a covered person on behalf of a U.S. person if: (i) the purpose of the processing is product research, development, or improvement; (ii) the U.S. person directs and controls the manner of processing the data; and (iii) the covered person is contractually bound by the U.S. person to maintain the privacy and security of the data. Failure to include this exemption would stifle large swaths of innovation by precluding multinational companies from relying on talent and manufacturing pipelines in other countries.

Question 10. *At what level should the Department of Justice set the precision (i.e., numbers of meters/feet) in defining precise geolocation data? What are common commercial applications of geolocation data, and what level of precision is required to support those applications? When geolocation data is "fuzzed" in some commercial applications to reduce potential privacy impacts, what are common techniques for "fuzzing" the data, what is the resulting reduction in the level of precision, and how effective are those techniques in reducing the sensitivity of the data? To what extent should the definition be informed by the level of precision for geolocation data used in certain state data-privacy laws, such as a radius of 1,850 feet (see, e.g., Cal. Civ. Code section 1798.140(w)) or a radius of 1,750 feet (see, e.g., Utah Civ. Code section 13-61-101(33(a)))?*

CTA Response: DOJ should define precise geolocation data such that it is aligned with the California Consumer Privacy Act as amended by the California Privacy Rights Act, which generally define precise geolocation data as: "any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet".

Question 11. *Should the Department of Justice consider changing any of the categorical exclusions to the definition of sensitive personal data? How should the program define the exclusion for data that is lawfully a matter of public record, particularly in light of data that is scraped from the internet or data points that are themselves public but whose linkage to the same individual is not public? What types of data are generally available to the public through open-access repositories?*

When considering the exclusions to the definition of "sensitive personal data," the DOJ should consider how common R&D data annotations of otherwise non-sensitive data could become subject to the final rule, and the chilling effect this could have on the open research community and the sharing of useful datasets that fuel innovation and increase trust and fairness, particularly in the fields of artificial intelligence and machine learning.

It remains unclear how the categorical exclusions to the definition of "sensitive personal data" would apply for specific categories information included in the definition of sensitive personal data, including for biometric identifiers. This lack of clarity risks unintentionally capturing otherwise useful or innocuous data created and used by the research community that do not pose national security risks. Specifically, although the ANPRM considers certain

categorical exclusions, such as for certain lawfully shared public data records and federally funded research, without a more explicit exclusion, the final rule could still capture the majority of applicable research data made available through open-access repositories.

For example, research data subject to the rule could include computer-vision datasets made available by universities and industry for useful tasks, such as improving pedestrian detection for self-driving cars or evaluating bias in facial recognition technologies. Common annotation techniques, such as tagging facial landmarks like eyes, noses, or lips in a photo, may be considered biometric data covered by the rule, despite no additional sensitive personal information being disclosed beyond what was already apparent from the photo itself. The same could be applied to vocal datasets used to improve speech recognition and text-to-speech technologies, where the open sharing of lesser available datasets, such as speech patterns of those with disabilities or impediments, is crucial to ensuring the technology can work well for all people. By virtue of being accessible over the internet, including in countries of concern, such datasets could fall under this national security policy. It should not be the case that innocuous labeling of apparent features (e.g., the location of an eye or a mouth, patterns in a voice recording) in otherwise non-sensitive data should convert such data into a national security threat.

Such large-scale datasets involving biometric annotations are typically made available to the public through dataset-sharing libraries, like Hugging Face, usually by and for the research community to enable the training and evaluation of artificial intelligence and machine learning technologies. Promoting access to and disclosure of data in this way is a community norm and expectation for publication at many research conferences, which enables peer review and reproducibility so the research can be vetted and advanced. To prohibit the sharing of annotations that can be derived from non-sensitive data without the use of any additional identifying information would only mean that anyone accessing the data would need to repeat the annotation exercise at their own expense; perhaps a mild annoyance for true national security threats, but a potentially significant barrier for academic institutions and independent/SME research labs.

In finalizing the rule, DOJ should not impose overly broad restrictions on bulk sensitive personal data such that it restricts the sharing of biometric annotations that are available from the otherwise non-sensitive data. This would have a needless and disproportionate impact on the research community – for whom sharing these datasets provides utility and is sometimes necessary to uphold ethical standards in publication – with little to no effect on US national-security risks.

In defining the exclusion for data that is "lawfully a matter of public record," DOJ should consider clarifying the exclusion in two ways. First, we would encourage DOJ to clearly establish that "publicly available" information is exempt and rely on the definition of "publicly available information" from state comprehensive privacy laws. For example, the VCDPA defines "publicly available information" as "information that is lawfully made available through federal, state, or local government records, or information that [the disclosing transacting party] has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by [the identifiable U.S. individual to whom the information relates], or by a person to whom [the identifiable U.S. individual] has disclosed the information, unless [the identifiable U.S. individual] has restricted the information to a specific audience."

Second, regarding DOJ concern about data in the public record that is scraped from the internet or other data points and is then linked to an individual's non-public data, we would encourage DOJ to anchor its analysis in the foreseeability of this linkage by the disclosing transacting party. Specifically, DOJ should clarify that for such data that would otherwise fall into one of the six categories of sensitive personal data to be considered "sensitive personal data," the linkage must be reasonably foreseeable by the disclosing transacting party. Without this clarification, nearly any public data points could be said to be "sensitive personal data," because it is at least theoretically possible

that any receiving transacting party could find some way of linking any public data point to an individual using any theoretical non-public data points.

Question 16. *How should the Department define information or informational materials? What factors should the Department take into account in its definition? What relevant precedents from other IEEPA-based programs should the Department take into account when defining the term?*

CTA Response: DOJ should clarify that the rules are not intended to regulate any Internet traffic – content or metadata – transiting to end-users in countries of concern where that data is created or transmitted by or on internet-based platforms or services that are designed to create or exchange any content that is expressive in nature. U.S. companies or persons constantly send information (including covered information) on Internet platforms that is intended for further distribution to other users of the Internet – including to individuals and companies in countries of concern. This interpretation would align with Congress' intent when it enacted and updated the IEEPA Berman Amendment to "facilitat[e] transactions and activities incident to the flow of informational materials…to ensure the robust exchange of informational materials." U.S. v. Amirnazmi, 645 F.3d 564, 586, 587 (3d Cir. 2011). Such data is necessarily personal communications, information, or informational materials excluded from the Executive's authority under 50 U.S.C. 1702(b)(1) & (3).

Question 17. *In what ways, if any, should the Department of Justice elaborate or amend the definition of government-related data, including with respect to "recent former" employees or contractors, and "former senior officials"?*

CTA Response: DOJ should provide clear, bright line rules clarifying what when an individual constitutes a "recent former" employee or contractor as well as "former senior official" to ensure these requirements are consistently interpreted and operationalized across industry.

Question 22. *What modifications to enhance clarity, if any, should be made to the definitions under consideration for data brokerage, vendor agreements, employment agreements, and investment agreements?*

CTA Response: DOJ should include a defined term for "data broker" in alignment with existing state laws, such as California Civ. Code 1798.99.80, whereby a data broker is defined as followed:

- "Data broker" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. "Data broker" does not include any of the following:
- An entity to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).
- An entity to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.
- An entity to the extent that it is covered by the Insurance Information and Privacy Protection Act (Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code)."

DOJ has not adequately defined the circumstances under which a vendor or employment agreement "involves" covered data. While the ANPRM lays out a handful of specific examples, no definition of "involves" is provided and the examples given are not sufficient for U.S. companies to identify covered agreements. To resolve this problem, DOJ should (i) define what it means to "involve" covered data or (ii) specify that only vendor or employment agreements where access to data is contemplated as part of the vendor's or employee's responsibilities/duties "involve" covered data and are subject to the new rules.

DOJ should exempt from the scope of vendor agreements those in which: (i) the vendor is providing product research, development, or improvement services for a U.S. person; (ii) any sensitive personal data is processed by the

vendor only in ways ordinarily incident to and part of that product research, development, or improvement; (iii) the U.S. person directs and controls the manner of processing the data; and (iv) the vendor is contractually bound by the U.S. person to maintain the privacy and security of the data.

Many U.S. companies rely on suppliers and manufacturers in other countries to produce and assemble products. When such physical products involve data processing, providing those suppliers and manufacturers with data is often necessary to enable product development, testing, and quality control. Assuming that the U.S. companies carefully control their vendors' processing of this data, such arrangements should not fall within the scope of vendor agreements.

DOJ should also exempt agreements (including interconnection and peering arrangements) pertaining to the exchange of telecommunications and Internet traffic over subsea cables or terrestrial telecommunication facilities from any rulemaking pertaining to "vendor agreements" because such agreements do not implicate significant privacy/security concerns and will be separately addressed by the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector.

Question 39. *How feasible is it to contract with prospective customers to prevent pass-through sales, re-sale, or onward transfers of bulk U.S. sensitive personal data or government-related data to countries of concern or covered persons? Do technical means exist to prevent such onward sales or transfers? If yes, what are such technical means?*

CTA Response: DOJ should exempt agreements governing the exchange of telecommunications and Internet traffic with foreign carriers from rulemaking related to "vendor agreements," including rulemaking intended to prevent pass-through sales, re-sale, or onward transfers. Existing rules affecting common carriers, such as existing and likely forthcoming net neutrality/open Internet rules from the FCC charge common carriers with carrying traffic over the Internet indiscriminately and refraining from blocking, throttling, or otherwise interfering with customer traffic. As a result, any rules intended to prevent "pass-through sales, re-sale, or onward transfers" of bulk U.S. sensitive data or government-related data to countries of concern or covered persons should not apply to agreements governing the exchange of telecommunications and Internet traffic.