November 27, 2024

Office of Public Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington DC 20530

Re: Docket No. NSD 104 – Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons

The Computer & Communications Industry Association (CCIA)[1] is pleased to respond to the Department of Justice's Notice of Proposed Rulemaking on the implementation of Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." CCIA appreciates the DOJ's efforts to craft a narrowly-tailored set of restrictions that target specific harms, will not unduly burden trade, and can be effectively implemented. However, there remains significant room for improvement in these respects, including by reconsidering some DOJ decisions regarding prior comments on the proposed Rules. CCIA strongly believes that such a complex and consequential rule should not be rushed, and will require significantly more time to get right.

As the DOJ weighs potential modifications to the proposed Rules, CCIA offers the following proposals to guide deliberation. CCIA's suggested amendments to the draft Rules are set forth in **Attachment A**.

Section 202.206 – Bulk U.S. Sensitive Personal Data

Per this Section, "The term bulk U.S. sensitive personal data means a collection or set of bulk data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted." As written, this definition risks encompassing all bulk U.S. personal data, regardless of sensitivity. The proposed Rules, however, were intended only to restrict "access to government-related data or bulk sensitive personal data."[2]

Defining the terms "bulk data" and "sensitive personal data" independently would fix this problem. CCIA recommends redefining "bulk data" as any amount of data meeting the thresholds in Section 202.205, rather than any amount of *sensitive personal* data meeting those thresholds. This Section should then define bulk U.S. sensitive data as any collection or

[1] CCIA is an international, not-for-profit trade association representing small, medium, and large communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. For more information about CCIA please see: https://www.ccianet.org/about.

[2] U.S. Dep't of Justice, Office of Pub. Affairs, Fact Sheet: Justice Department Moving Forward with Publishing a Proposed Rule to Protect Americans' Sensitive Personal Data from Countries of Concern 1 (2024), *available at* https://www.justice.gov/opa/pr/justice-department-issues-comprehensive-proposed-rule-addressing-national-security-risks.

set of data relating to U.S. persons that (1) meets the definition of bulk data under Section 202.205, and (2) meets the definition of sensitive personal data under Section 202.249.

Additionally, CCIA recommends that the DOJ exempt collections of anonymous and/or de-identified data from the restrictions on bulk U.S. sensitive personal data. We appreciate the DOJ's concerns over past incidents where data that was described as "anonymized" or "de-identified" was used to identify individuals. However, data can be described using these terms without meeting any legal standard for anonymization. Many laws create such standards, often basing them on the foreseeability that someone who could gain access to the data could re-identify it using reasonably available means such as HIPAA[3] and FERPA).[4] If the re-identification risk is sufficiently low given how the data is processed and shared, the data is anonymous. These standards have been workable for years in key US laws. A rationale for extending this rule to anonymous and de-identified data must explain why there is a major risk of re-identifying subjects using data meeting an accepted *legal standard* for anonymization or de-identification, not merely data that has been labelled using these terms.

CCIA also recommends that the definitions for "government-related data" and "bulk sensitive personal data" explicitly exclude data encrypted using industry-standard encryption. Encryption is among the most effective ways of preventing third parties from gaining unauthorized access to data. Moreover, as the DOJ underscores in its definition of "access," a third party's ability to access content can be contingent upon its decryption capabilities. Encrypted data therefore should not pose risks these Rules are intended to remedy unless a Country of Concern has the ability to decrypt such messages. While some have attempted to develop quantum computing capabilities to decipher encrypted data, such efforts are far from operational at any scale, let alone the scale required to decrypt the types of bulk data these rules contemplate. Furthermore, NIST has approved several quantum-resistant cryptographic algorithms. Including encrypted data in these definitions would therefore contradict Executive Order 14117's directive that the Attorney General protect Americans' bulk data while simultaneously "minimizing disruption to commercial activity."[5]

---

[3] U.S. Dep't of Health & Human Servs., Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule 6 (2012), *available at* https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html#standard ("Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information").

[4] Family Educational Rights and Privacy, 34 C.F.R. § 99.31(b)(1) (2024), *available at* https://www.ecfr.gov/current/title-34/part-99#p-99.31(b)(1) (deeming educational records to be de-identified "after the removal of all personally identifiable information provided that the educational agency or institution or other party has made a reasonable determination that a student's identity is not personally identifiable").

[5] Exec. Order No. 14,117, 89 Fed. Reg. 15,421 (Mar. 1, 2024), *available at* https://www.federalregister.gov/d/2024-04573/p-9.

Section 202.210 – Covered Data Transactions

Section 202.201 defines the term "access" to include "logical or physical access." This Section defines covered data transactions as "any transaction that involves any access to any government-related data or bulk U.S. sensitive personal data" and a "Data brokerage; ... vendor agreement; ... employment agreement; or ... investment agreement." Taken together, these definitions risk encompassing the many routine transactions needed to maintain and store data. For instance, if a business storing bulk U.S. sensitive data hires a server technician to perform onsite maintenance work at one of its facilities, their employment agreement risks subjecting the business to the proposed Rules, since the technician would have physical access to the servers. CCIA therefore recommends amending the definition of "covered data transactions" to exclude incidental physical access to data facilities by a party who does not use the accessed data.

Similarly, CCIA recommends exempting agreements concerning 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 put the privacy and security of Americans' data at risk.

Section 202.212(b) – Covered Personal Identifiers: Exclusion

The DOJ has rightly noted that Executive Order 11417 limits this category's scope to "personally identifiable data" that can be made "exploitable by a country of concern." However, as written, this Section could extend to combinations of listed identifiers that are neither personally identifiable data nor exploitable by a country of concern. The following steps would correct this Section's scope.

First, the DOJ should state explicitly that data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such a person, cannot be a "covered personal identifier." This restriction would further the Department's stated intention in Section 202.234 that the Rule defining "covered personal identifiers" have a "much narrower" scope than "laws and policies aimed generally at protecting personal privacy."

The DOJ should also exempt any combination of the following three types of listed identifiers (unless the combination would enable a receiving transacting party to identify a US individual): (1) a device- or hardware-based identifier, (2) an advertising identifier, and (3) a network-based identifier. Covered persons often process these identifiers on behalf of U.S. entities to fulfill U.S. product and service orders, often without being able to personally identify the U.S. requestor. These modifications would reduce the capture of non-sensitive data and better align the Rules with both Executive Order 14117 and the DOJ's stated goals.

Section 202.214 – Data Brokerage

This Section defines a data brokerage as "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." However, this definition treats bulk U.S. sensitive personal data in the same manner as data not covered by the proposed Rules. CCIA recommends restricting this definition to apply only to data brokerages that engage in transactions with the bulk US sensitive personal data covered by these Rules.

Additionally, the phrase "or similar commercial transactions" is open-ended and ambiguous. CCIA recommends either removing this provision or replacing it with specific types of commercial transactions.

This Section could also be read to include businesses that service data brokers but do not buy, sell, or license data themselves. CCIA recommends clarifying that the restrictions applicable to data brokers do not extend to businesses that service data brokers but are not themselves data brokers.

Section 202.230 – Knowingly

Per this section, "the proposed rule defines 'knowingly' to mean, with respect to conduct, a circumstance, or a result, that the U.S. person had actual knowledge of, or reasonably should have known about, the conduct, circumstance, or result." CCIA recommends limiting the definition of "knowingly" to actual knowledge.

This Section states that "[t]o determine what an individual or entity reasonably should have known in the context of prohibited transactions, the Department will take into account the relevant facts and circumstances, including the relative sophistication of the individual or entity at issue, the scale and sensitivity of the data involved, and the extent to which the parties to the transaction at issue appear to have been aware of and sought to evade the application of these proposed rules." These criteria are subjective and do not give persons or entities any definite means of ensuring that they have complied with the proposed Rule. Such regulatory clarity is critical for the sectors this Section impacts– cloud service providers, for instance, would likely have to undertake invasive measures to comply with such a broad standard, undermining their efforts to preserve the privacy and confidentiality of their customer's data (e.g., by allowing customers to control the encryption of their data autonomously).

Imposing a more invasive regime on U.S. cloud computing suppliers risks driving business to rely more on suppliers from abroad, including those from the Countries of Concern specified in these Rules. Moreover, under these criteria, an entity that has made some effort to comply with the Rule could be penalized more harshly than an entity that is unaware of the Rule entirely. It is therefore more appropriate to limit this definition to cases of actual knowledge.

Section 202.241 – Personal Health Data

The Advance Notice of Proposed Rulemaking correctly chose to align the definition of personal health data with HIPAA's definition of "individually identifiable health information," but without the limitation to entities covered by HIPAA. CCIA appreciates that this lack of a covered entity limitation confused some commenters and that the DOJ has now sought to reduce confusion by removing the language incorporating HIPAA and substituting its own definition of personal

health data. However, in doing so, the Department has imposed requirements on businesses far in excess of their HIPAA obligations, extending to information such as "basic physical measurements" and "social, psychological, [and] behavioral . . . intervention[s]." The term "social intervention" lacks a clearly understood meaning, and such a definition will make it a challenge for businesses to know that they have complied with this Section's requirements.

Moreover, HIPAA limits its definition of personally identifiable health information to data "created or received by a health care provider, health plan, employer, or health care clearinghouse"[6]– i.e. data that is actually used to identify an individual's health status or care. CCIA recommends defining "personal health data" in this manner as well. Defining "personal health data" as "health information used to identify the past, present, or future physical or mental health condition or diagnosis of an individual" would save the DOJ from being inundated with data unrelated to individuals' health status and better enable entities to ensure they are compliant.

Section 202.249(b) – Sensitive Personal Data: Exclusions

CCIA recommends clarifying that "sensitive personal data" does not include data where informational material or personal communications are transmitted together with sensitive personal data. Internet users often transmit informational material or personal communications bundled with "sensitive personal data," e.g. by sending messages voicing political views or otherwise "communicat[ing] ideas" as in Section 203 (the same principle applies to other media such as photographs and film). In such cases, the entire message should qualify as expressive content. Where "sensitive personal data" is sent alongside informational material or personal communication, the Proposed Rule may encompass them. As the DOJ's authority does not extend to regulating such informational material or personal communication,[7] this Section should exempt "sensitive personal data" incidental to the transfer of informational materials, personal communications, or any other data outside the scope of this Rule.

CCIA also appreciates the Department's further specificity regarding categories of data excluded from the definition of "sensitive personal data." However, additional clarifications narrowing the scope of the public data exclusion would be beneficial. CCIA suggests modifying the language excluding "[d]ata that is, at the time of the transaction, lawfully available to the public ... in widely distributed media (such as sources that are generally available to the public through unrestricted and open-access repositories)" using the Virginia Consumer Data Protection Act (VCDPA)'s definition of "publicly available information." Under the VCDPA, publicly available information is "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."[8] Using this established definition would still safeguard Americans' sensitive data while avoiding

[6] 42 U.S.C. § 1320d(6)(A) (2010).
[7] *See* 50 U.S.C. § 1702(b)(3) (2001).
[8] Va. Code Ann. § 59.1-575 (2023).

overbreadth, ensuring clear, consistent guidelines for covered entities, and minimizing unnecessary confusion and compliance burdens.

Section 202.302 – Other Prohibited Data-Brokerage Transactions Involving Potential Onward Transfer to Countries of Concern or Covered Persons

The comment summary for this Section instructs "U.S. persons engaged in these kinds of data brokerage transactions to take reasonable steps to evaluate whether their foreign counterparties are complying with the contractual provision as part of implementing risk-based compliance programs under the proposed rule." The phrase "reasonable steps to evaluate" is ambiguous; CCIA recommends substituting a diligence requirement. Such an instruction would provide regulatory certainty and uphold the intention of the proposed rule in targeting narrow, specifically defined circumstances necessary to safeguard security interests, while broadly upholding cross-border data flows.

Additionally, this Section should not require U.S. entities to continuously audit their foreign counterparts. A U.S. entity should be able to satisfy the requirements in this section if it has (1) secured contractual representations from its foreign counterpart that it will comply with the proposed rules, and (2) discontinues data brokerage transactions with any foreign person that the U.S. entity knows has failed to comply with the proposed Rules. This change would make more of the compliance burden fall on noncompliant foreign entities, as opposed to compliant U.S. entities.

Lastly, as this Section would require many U.S. businesses to alter the contracts on which they have based their business model, CCIA recommends allowing an 18-month grace period for U.S. entities to comply with the contractual requirements specified in this Section. Doing so would maintain the long-term benefits to U.S. data security derived from these proposed Rules while minimizing the short-term disruption to U.S. businesses.

* * * * *

We appreciate the DOJ's consideration of these comments. We look forward to continuing to participate in the DOJ's ongoing regulatory process, including reviewing and providing feedback on the series of proposed Rules. We hope the DOJ will consider CCIA a resource as these discussions progress.

Sincerely,

Jesse Lieberfeld
Policy Counsel– Privacy, Security, and Emerging Technologies
Computer & Communications Industry Association

ATTACHMENT A

Suggested Amendments to Revised Draft Rules

This Attachment contains CCIA's suggestions for specific modifications to the Revised Draft Rules. The text below is the draft Rules text after the Department of Law's revisions. CCIA's proposed deletions are in red and proposed new language is in green.

§ 202.205 – Bulk: The term bulk means any amount of ~~sensitive personal~~ data that meets or exceeds the following thresholds at any point in the preceding 12 months, whether through a single covered data transaction or aggregated across covered data transactions involving the same U.S. person and the same foreign person or covered person....

§ 202.206 – Bulk U.S. Sensitive Personal Data: The term bulk U.S. sensitive personal data means a collection or set of bulk data relating to U.S. persons that meets the criteria for sensitive data as defined in § 202.249, in any format, unless ~~regardless of whether~~ the data is anonymized, pseudonymized, de-identified, or encrypted using industry-standard encryption.

§ 202.210 – Covered Data Transactions: A covered data transaction is any transaction that involves any access to any government-related data or bulk U.S. sensitive personal data, apart from incidental physical access to data facilities by a party who does not use the accessed data, and that involves:

(1) Data brokerage;

(2) A vendor agreement, except those governing the exchange of telecommunications and Internet traffic over subsea cables or terrestrial telecommunication facilities;

(3) An employment agreement; or

(4) An investment agreement.

§ 202.212(b) – Covered Personal Identifiers: *Exclusion.* The term covered personal identifiers excludes:

(1) Demographic or contact data that is linked only to other demographic or contact data (such as first and last name, birthplace, ZIP code, residential street or postal address, phone number, and email address and similar public account identifiers);~~ and~~

(2) A network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifier, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar service;~~.~~

(3) Data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such a person, or data encrypted using industry-standard encryption; and

(4) Device- or hardware-based identifiers, advertising identifiers, and/or network-based identifiers, or any combination thereof, unless the identifier or combination of identifiers would enable a receiving transacting party to identify a US individual.

§ 202.214 – Data Brokerage: The term data brokerage means the sale or licensing of bulk U.S. sensitive personal data, ~~licensing of access to data, or similar commercial transactions~~ involving the transfer of such 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. This definition does not extend to a business that services a data brokerage but is not itself a data brokerage.

§ 202.230 – Knowingly: The term knowingly, with respect to conduct, a circumstance, or a result, means that a person has actual knowledge~~, or reasonably should have known,~~ of the conduct, the circumstance, or the result.

§ 202.241 – Personal Health Data: The term personal health data means health information that identifies the past, present, or future physical or mental health condition or diagnosis of an individual ~~that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. This term includes basic physical measurements and health attributes (such as bodily functions, height and weight, vital signs, symptoms, and allergies); social, psychological, behavioral, and medical diagnostic, intervention, and treatment history; test results; logs of exercise habits; immunization data; data on reproductive and sexual health; and data on the use or purchase of prescribed medications~~.

§ 202.249(b) – Sensitive Personal Data: *Exclusions.* The term sensitive personal data excludes:

(1) Public or nonpublic data that does not relate to an individual, including such data that meets the definition of a "trade secret" (as defined in 18 U.S.C. 1839(3)) or "proprietary information" (as defined in 50 U.S.C. 1708(d)(7));

(2) Data that ~~is~~, at the time of the transaction, the disclosing transacting party has a reasonable basis to believe is lawfully available to the public ~~from a Federal, State, or local government record (such as court records) or in~~ through widely distributed media (such as sources that are generally available to the public through unrestricted and open-access repositories), 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;

(3) Personal communications; ~~and~~

(4) Information or informational materials; and~~.~~

(5) Data where informational material or personal communications are transmitted together with sensitive personal data.

§ 202.302 – Other Prohibited Data-Brokerage Transactions Involving Potential Onward Transfer to Countries of Concern or Covered Persons: Beginning 18 months from the Effective Date of this Section, ~~E~~except as otherwise authorized pursuant to this part, no U.S. person, on or after the effective date, may knowingly engage in a covered data transaction involving data brokerage with any foreign person that is not a covered person unless the U.S. person:

(1) Contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving data brokerage of the same data with a country of concern or covered person; and

(2) Reports any known ~~or suspected~~ violations of this contractual requirement in accordance with paragraph (b) of this section.