PRIVACY, TRUST & ACCOUNTABILITY

409 7th Street, NW; Suite 250

November 29, 2024

*Submitted via electronic form at*
*https://www.regulations.gov/commenton/DOJ-NSD-2024-0004-0001*

Mr. Lee Licata
Deputy Chief for National Security Data Risks
United States Department of Justice
National Security Division
Foreign Investment Review Section
175 N Street NE, 12th Floor
Washington, DC 20002

**Re: Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons.**

Dear Mr. Licata,

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to comment in response to the proposed rule[1] to implement Executive Order 14117[2] issued by the President of the United States on February 28, 2024 ("Proposed Rule"). The NAI shares your concerns regarding countries of concern gaining access to bulk U.S. sensitive personal data ("BUSPD") and strongly supports the efforts of the Department of Justice (the "Department" or the "DOJ") to prevent such access. The NAI also applauds the commitment to public involvement and transparency the DOJ is demonstrating through this important rulemaking process.

The NAI is a non-profit, self-regulatory association dedicated to responsible data collection and use for digital advertising. The NAI has been a leader in this space since its inception in 2000,[3] promoting the highest voluntary industry standards for member companies, which range from small startups to some of the largest companies in digital advertising. NAI's members are providers of advertising technology solutions and include ad exchanges, demand and supply side platforms, and other companies that power the digital media industry by helping digital publishers generate essential ad revenue, helping advertisers reach audiences interested in their products and services, and helping to ensure consumers are provided with ads relevant to their interests.

While the NAI's long-standing self-regulatory program was created to promote U.S. consumer privacy and protect U.S. individuals from privacy harms, it was founded on principles of responsible data collection and use for digital advertising that are consistent with the Proposed Rule's national security

[1] *Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons* (hereinafter "Proposed Rule"), 89 Fed. Reg. 15421 (proposed Oct. 29, 2024) (to be codified at 28 CFR pt. 202).
[2] *See* Exec. Order No. 14117, 89 Fed. Reg. 15421 (Feb. 28, 2024).
[3] *See History of the NAI*, The Network Advertising Initiative, https://thenai.org/about-the-nai-2/history-of-the-nai/.

goals. As an organization that prioritizes privacy safeguards in digital advertising, the NAI has a unique perspective on the Proposed Rule given our decades of experience as a leading self-regulatory association dedicated to responsible data collection and use. The NAI shares the Department's commitment to promoting an open, global, interoperable, reliable, and secure internet[4] and believes this objective goes hand-in-hand with good policy for protecting BUSPD. We offer the following comments on the Proposed Rule, which we are hopeful will assist the DOJ in meeting its objectives for the rulemaking while preserving an open, global, interoperable, reliable, and secure internet.

## I. The Department should provide as much clarity as possible regarding who covered persons are and the level of diligence businesses should undertake to avoid sharing BUSPD with them.

### A. Background

The Proposed Rule aims to enhance the DOJ's ability to address the threat posed by countries of concern gaining access to government-related data or Americans' BUSPD[5] by prohibiting certain classes of transactions involving BUSPD that the Department deems to pose an unacceptable risk to national security. Specifically, the Proposed Rule prohibits any U.S. person from knowingly engaging in a covered data transaction involving data brokerage with a country of concern or a covered person.[6] Here, "knowingly" is defined to mean that a U.S. person "had actual knowledge of, or *reasonably should have known about*, the [unlawful] conduct, circumstance, or result."[7] When analyzing a violation under this proposed knowledge standard, the Department indicates it would consider 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 the Proposed Rule.[8] Accordingly, establishing the identity of covered persons is essential to adherence to the Proposed Rule.

The Proposed Rule identifies a covered person as an individual or entity that falls into a particular class or has been designated as such by the Attorney General. The covered classes include a foreign person that: (1) is 50 percent or more owned, directly or indirectly, by a country of concern; (2) is organized or chartered under the laws of a country of concern; (3) has its principal place of business in a country of concern; or (4) is 50-percent or more owned, directly or indirectly, by a covered person.[9]

To facilitate compliance with the Proposed Rule, the Department should provide as much clarity as possible as to how it expects U.S. persons to prevent sharing BUSPD with covered persons. In the absence of clear expectations and guidance on compliance methods that are scalable by businesses, the NAI is concerned that the Proposed Rule may have disproportionate effects on small and medium-enterprises, contrary to the expectations under the Regulatory Flexibility Act (RFA) that agencies take

[4] *See Justice Department Issues Comprehensive Proposed Rule Addressing National Security Risks Posed to U.S. Sensitive Data* (Oct. 21, 2024), U.S. Department of Justice, https://www.justice.gov/opa/pr/justice-department - issues-comprehensive-proposed-rule-addressing-national-security-risks.
[5] *See* Proposed Rule at 10.
[6] *See id.* at § 202.301.
[7] *See id.* at § 202.230.
[8] *See id.*
[9] *See* Proposed Rule at § 202.211.

substantial efforts to avoid such a disproportionate burden.[10] The Proposed Rule includes an RFA analysis which estimates that "about 4,500 firms, just over 90 percent of which are small businesses (hereafter referred to as "small entities"), would be impacted by the proposed rule."[11] In addition, the Department estimates that small entities will incur compliance costs of around $32,380 per firm per year, and that many of the Proposed Rule's provisions "likely involve high fixed costs" that mean smaller entities "will likely need to pay a higher proportion of their overall budgets to comply."[12]

The U.S. digital advertising industry is large and diverse, generating $225 billion in revenue in 2023, representing a growth rate of 7 percent driven by increasing demand for digital advertising.[13] Like most industries, a small number of companies in digital advertising account for a substantial portion of revenue (65 percent of revenue by one estimate) – however, smaller businesses comprise the majority of this industry numerically and are rapidly gaining influence with user-friendly ad-tech platforms.[14] The NAI's membership reflects this dynamic, as it includes strong representation from the small and start-up business community, including many members who have fewer than 500 employees and compete fiercely with larger and more dominant players in the digital advertising sphere to help drive down costs for ad-supported businesses (including small media publishers) and make free and ad-supported content more readily available for U.S consumers.[15]

The NAI has several recommendations for how the DOJ can advance the objectives of the Proposed Rule while minimizing its impacts on small businesses, set out below.

**B. The Department should restrict "knowingly" to its ordinary meaning or, alternatively, provide clear guidance as to the due diligence that businesses are expected to conduct on counterparties to avoid unknowingly transacting with covered persons.**

The Department should reconsider its definition of "knowingly," which is at odds with how the term is traditionally understood. "Knowingly" traditionally means that someone is "aware that his conduct is of [such a] nature or that such circumstances exist" to bring the conduct within coverage of a legal rule.[16] By contrast, the Proposed Rule would define "knowingly" to include the lesser state of mind of negligence, which would ensnare businesses whom the Department believes "reasonably should have known" that a counterparty was a covered person. This creates the prospect that a small-to-medium size business with no existing national security expertise could face liability for transferring BUSPD to an entity that it did not know was a covered person —and further, that may have been actively concealing its status as a covered person. Rather, the Department should define "knowingly" consistent with its

[10] 5 U.S.C. §§ 601-612. The legislative purposes states, "when adopting regulations to protect the health, safety and economic welfare of the Nation, Federal agencies should seek to achieve statutory goals as effectively and efficiently as possible without imposing unnecessary burdens on the public." P.L 96-354 § 2, 94 Stat 1164.
[11] Proposed Rule § 9(B)(2).
[12] *Id*. The Department specifically welcomed comment on the impact on small businesses, citing the possibility that a substantial number of small firms will experience a significant impact.
[13] *See Internet Advertising Revenue* Report, PwC, https://www.iab.com/wp-content/uploads/2024/04/IAB_PwC_Internet_Ad_Revenue_Report_2024.pdf
[14] *See AdTech Market Report*, market.us, https://market.us/report/adtech-market/.
[15] *See NAI Extended Member Directory*, Network Advertising Initiative, https://sites.google.com/networkadvertising.org/extendedmemberdirectory/nai-extended-member-directory (highlighting diversity of businesses, most of which share data extensively via real-time bidding to serve programmatic digital advertising).
[16] Model Penal Code § 202(2)(b).

ordinary meaning, which requires actual awareness. Making this change would protect small-to-medium sized business from surprise liability under the Proposed Rule while still enabling the Department to enforce it in cases of willful blindness, which an actual knowledge standard would continue to encompass.[17]

If, however, the Department maintains a negligence standard of "knowingly" for the Proposed Rule, it should develop a compliance framework that establishes a clear set of requirements and practices that will enable businesses to meet the DOJ's expectations as to the type and amount of due diligence a business must conduct to avoid the accusation that it "reasonably should have known" the true status of a counterparty as a covered person.

One method the Department could pursue to this end would be establishing a safe harbor program for businesses focused on diligence steps companies can take to meet a "reasonably should know" standard, so that in the event that a business unknowingly transacts with a covered person, it can still operate with a level of assurance that it has complied with the Proposed Rule's knowledge standard by conducting the diligence expected by the Department. A promising approach would be to have sectoral or industry self-regulatory initiatives similar to the Safe Harbor Program under the Children's Online Privacy Protection Act (COPPA).[18] Under the COPPA Safe Harbor Program, industry groups can apply to the Federal Trade Commission (FTC) for approval of self-regulatory guidelines that include: 1) substantially the same protections as those in the regulations; 2) a mechanism for independent assessment of operators' compliance; and 3) disciplinary actions for operators' non-compliance. The approved guidelines are subject to recordkeeping and reporting requirements to the Commission and are subject to revocation of their approval for non-compliance with the regulations.[19] If the DOJ follows this approach for a self-regulatory safe harbor program and approves one or more programs to implement it, industry participants would be able to receive a safe harbor certification for reasonable compliance measures. This approach would promote a transparent and manageable way to comply with the Proposed Rule at scale and without the need for many additional resources from the Department.

Conversely, a lack of clear requirements could result in businesses lacking a clear understanding of the data transfers the DOJ seeks to prevent. This could both (1) lead to businesses undertaking transactions the DOJ would otherwise seek to prevent; and (2) lead to an overly conservative approach by businesses that would drastically limit transactions undertaken for legitimate, beneficial purposes that do not pose the security risks the DOJ is seeking to minimize through the Proposed Rule.

### C. The Department should develop a robust list of designated covered persons

Under the Proposed Rule the Department reserves the right to include as a covered person an entity or individual "that the Attorney General has designated as a covered person" even if they would not otherwise meet the relevant thresholds.

We support the DOJ's plan to maintain a list of designated covered persons as this would provide U.S. persons necessary insight as to who may be a covered person, especially since the

---

[17] *See United States v. Ravenell*, 66 F.4th 472, 490 (4th Cir. 2023) ("[T]he government may prove knowledge by establishing that the defendant deliberately shielded himself from clear evidence of critical facts that are strongly suggested by the circumstances.") (quotations omitted).

[18] 15 U.S.C. §§ 6501-6506; 16 C.F.R. § 312.

[19] U.S.C. § 6503; 16 C.F.R. § 312.11; described at https://www.ftc.gov/enforcement/coppa-safe-harbor-program).

Department suggests that there will be covered persons - such as some U.S. persons - that will not fall under the other classes as defined by the Proposed Rule.[20] As such, a list of designated covered persons is essential to the objective of protecting BUSPD as well as government-related data. Such a list may be managed by the government, drawing for instance upon the experience of the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") sanctions lists.[21]

Further, to the extent the Department is aware that certain entities are Covered Persons under any of the other thresholds under the Proposed Rule, the NAI urges the Department to create reference lists for those entities as well. We believe this will help businesses meet the Department's goals of preventing transfers of BUSPD to covered persons. The alternative of expecting each business to individually determine whether a counterparty is a covered person – particularly where some businesses have different access to relevant information and would not otherwise (reasonably) know that an entity is a covered person – is less likely to prevent transfers of BUSPD to entities known by the Department to be covered persons. Creating robust reference lists of covered persons under any relevant threshold would promote the goal of preventing BUSPD from reaching covered persons, even unknowingly, and would ease administration of the Proposed Rule for businesses.

Finally, we urge the Department to develop and maintain its list of designated covered persons on a publicly announced timeline to enable businesses to plan for adopting it and to create more certainty about when compliance with the list is expected.

**D. The Department should recognize and promote adequate contractual requirements as a due diligence method that satisfies the "*reasonably should have known*" requirement.**

As previously noted, the Proposed Rule currently defines "knowingly" to mean that a U.S. person had actual knowledge of, or *reasonably should have known about*, the [unlawful] conduct, circumstance, or result. To clarify the Department's expectations for what a U.S. person *reasonably should have known about*, the NAI recommends that the DOJ promote contractual representations and warranties as a method for businesses to meet this standard. The Department could encourage businesses subject to the Proposed Rule to include in their contracts governing sales of BUSPD representations and warranties that their counterparty is not a "covered person" and promote inclusion of such contract provisions as a way to satisfy the Department's expectations for diligence.

For example, a contract between a U.S. person and a foreign person may include the following model contract provision:

> *[Foreign Person] hereby represents and warrants that it is NOT:*
>
> *(1) 50 percent or more owned, directly or indirectly, by the People's Republic of China, the Republic of Cuba, the Islamic Republic of Iran, the Russian Federation, the Bolivarian*

[20] *E.g. id.* at 132 ("As described in the ANPRM, including its Example 33, anyone in the United States (including temporarily in the United States) would be considered a U.S. person, and no U.S. persons (including those temporarily in the United States) would be categorically treated as covered persons.216 A U.S. person (including a temporary traveler to the United States) would be a covered person only if they had been designated by the Department. The proposed rule adopts this proposal unchanged from the ANPRM.").

[21] OFAC provides its Specially Designated Nationals List, and its other sanctions lists for download on its website, as well as its Sanctions List Service to search across its lists, *see* https://ofac.treasury.gov/sanctions-list-service.

*Republic of Venezuela, or the People's Republic of Korea (collectively "Countries of Concern");*
*(2) organized or chartered under the law of a Country of Concern;*
*(3) have its principal place of business in a Country of Concern; or*
*(4) 50 percent or more owned, directly or indirectly, by an entity as described in (1)-(3) above.*

The inclusion of a contractual provision like this would indicate that a business subject to the Proposed Rule is aware of its obligations under the Proposed Rule, is taking steps to avoid transferring BUSPD in violation of the rule, and is requiring its counterparties to guarantee that they do not meet the relevant thresholds. While a counterparty could still affirmatively mislead a business by agreeing to a false representation and warranty, this goes beyond the reasonableness standard. Further, in cases where a covered persons is discovered to have fraudulently agreed to these representations and warrantees, the Department could add the relevant entity to a definitive reference list of covered persons, as discussed above. This also highlights the importance of the Department developing a more robust list of entities that may be likely to engage in this type of fraud to evade the Proposed Rule's prohibitions.

Alternative methods of due diligence that put greater burdens on transferors of BUSPD are not likely to produce better results. For example, The Proposed Rule states that the provisions defining a Covered Person are similar to those sanctions issued by the Office of Foreign Assets Control ("OFAC") and that "businesses and third-party service providers have developed tools and services to assist with screening and due diligence based on corporate ownership in the sanctions, anti- money laundering, and other regulatory contexts."[22] Yet, when foreign persons may be owned by layers of shell companies and trusts, it would be challenging, if not impossible in many cases, for U.S. businesses covered by the Proposed Rule to determine with reasonable certainty whether an entity is 50-percent or more owned indirectly by a covered person, as the Proposed Rule requires. Using contractual representations and warranties is a way to manage this uncertainty by requiring acquirers of BUSPD to understand their own ownership structure and make corresponding representations and warranties instead of relying on their counterparties to investigate and discover it, particularly when that type of external investigation into corporate structure may not be possible to undertake with accuracy or at scale.

Finally, we encourage the DOJ to look to existing precedents for utilizing contracts to satisfy requirements for international data transfers. The Proposed Rule itself recognizes the importance of contractual limitations in its restrictions on transfers by U.S. businesses to foreign persons.[23] In addition, the European Union's General Data Protection Regulation provides a strong analogue to the activity addressed by the Proposed Rule and recognizes standard contractual clauses as a valid transfer mechanism for international data transfers.[24] To promote the use of standard contract language, the Department could undertake to draft such clauses itself, as the European Union Commission has done by promulgating standard contractual clauses ("SCCs") for transfers of personal data out of the European Union.[25] Alternatively, the Department could draw on sectoral and industry expertise and

[22] *Id.*
[23] *See id.* at § 202.302.
[24] *See* General Data Protection Regulation, Art. 28, https://gdpr-info.eu/art-28-gdpr/.
[25] The European Commission 2021/914, 2021 O.J (L 199) 31 (EU), text at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

authorize self-regulatory processes to draft and use SCCs. These self-regulatory SCCs could be submitted for approval to the Department, again with a process similar to FTC approval of self-regulatory methods for complying with COPPA.

### E. The Department should provide standard contractual clauses for the requirement that a foreign person refrain from engaging in a subsequent covered data transaction involving BUSPD with a country of concern or covered person and delay enforcement of this requirement by 18 months after the date the Proposed Rule goes into effect.

Pursuant to § 202.302 of the Proposed Rule, U.S. persons seeking to engage in covered data transactions with a foreign person must contractually require the foreign person to refrain from engaging in a subsequent covered data transaction involving that data with a country of concern or covered person.[26] The Department should provide standard contractual clauses that business may use to satisfy the requirement that a foreign person refrain from engaging in a subsequent covered data transaction involving sensitive data with a country of concern or covered person.[27] Providing pre-approved standard contractual clauses would allow for businesses subject to the rule to efficiently make required contractual changes with their counterparties without negotiating over terms that may not advance the objectives of the Proposed Rule. The Department should also delay enforcement of this requirement by 18 months after the date the Proposed Rule goes into effect to allow for the necessary contractual changes to occur throughout the business ecosystem.

## II. The Department should ensure that definitions for "Covered Personal Identifier" and "Bulk U.S. Sensitive Data" are consistent throughout the Proposed Rule.

The NAI recommends the Department amend certain definitions of key terms throughout the Proposed Rule to ensure their internal consistency.

### A. The Department should clarify that the definition of "Covered Personal Identifier" includes a listed identifier in combination with "other Sensitive Personal Data."

The Proposed Rule defines "Covered Personal Identifier" in § 202.212 as consisting of three subcategories:

(1) listed identifiers in combination with any other listed identifier;
(2) listed identifiers in combination with other sensitive personal data; and
(3) listed identifiers in combination with other data that are disclosed by a transacting party pursuant to the transaction that makes the listed identifier exploitable by a country of concern, if they could be used to identify an individual from a dataset or to link data across multiple datasets to an individual.[28]

However, in Subpart B, the Department offers a different definition for "Covered Personal Identifier" as any listed identifier:

(1) In combination with any other listed identifier; or

[26] *See* Proposed Rule at § 202.302.
[27] *See also* Section I.B. *supra* for discussion on the use of standard contractual clauses as a form of diligence for avoiding transactions with covered persons directly.
[28] *See* Proposed Rule at § 202.212.

(2) In combination with other data that is disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data.[29]

For the sake of clarity, we recommend aligning these two definitions by replacing the definition of Subpart B with the definition that appears in § 202.212. We believe the formulation in § 202.212 is clearer because it relies on other defined terms like "sensitive personal data" instead of undefined terms like "other data" as does the definition in Subpart B.

### B. The Department Should Clarify that the Definition of "Bulk U.S. Sensitive Data" is a Collection or Set of *Sensitive Personal Data* Relating to U.S. Persons

Section 202.206 defines "Bulk U.S. Sensitive Data" as a collection or set of **sensitive personal data** relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted.[30] (emphasis added). However, under Subpart B "Bulk U.S. Sensitive Data" is defined as "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."[31] (emphasis added). The NAI recommends the Department align the two different definitions of "Bulk U.S. Sensitive Data" by removing the existing definition in Subpart B and replacing it with the one that appears in § 202.206.

## III. Rather than treating both identified and de-identified data the same under the definition of "bulk U.S. sensitive personal data," the Department should provide a definition for de-Identified data that addresses the Department's concerns about re-identification.

The Proposed Rule's definition of "Bulk U.S. Sensitive Data" specifies that it consists of certain sensitive data, "in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted."[32] The Department declined requests from several comments given in response to the ANPRM[33] to exclude encrypted, pseudonymized, de-identified, or aggregated data from the Proposed Rule's coverage and asserted in response that "anonymized data is rarely, if ever, truly anonymous."[34] The Department also cites several studies primarily focusing on how bulk precise location data may be used to identify sensitive information such as the location of military and government employees, facilities, and activities.[35]

The DOJ appears to be addressing two distinct risks in its response to the initial comments on de-identified data for the ANPRM. The first risk is that data that is intended to be de-identified can nevertheless be associated with an identified or identifiable individual – in other words, the risk that certain procedures intended to achieve de-identification can be defeated. The second risk is that even

[29] *See id.* at Subpart B.
[30] *See id.* at § 202.206.
[31] *See id.* at Subpart B.
[32] *See id.* at § 202.206.
[33] *Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern*, 89 Fed. Reg. 15421 (proposed Mar. 4, 2024) (to be codified at 28 CFR pt. 202).
[34] *See id.* at § 202.206 (quoting *In Camera*, *Ex Parte* Classified Decl. of David Newman, Principal Deputy Assistant Att'y Gen., Nat'l Sec. Div., U.S. Dep't of Just., Doc. No. 2066897 at Gov't App. 74–75 ¶¶ 100–01, *TikTok Inc. v. Garland*, Case Nos. 24-1113, 24-1130, 24-1183 (D.C. Cir. July 26, 2024) (publicly filed redacted version)).
[35] *See* Proposed Rule at § 202.206 n.41-44.

data that is successfully de-identified and is never re-associated with identified or identifiable individuals may nevertheless pose risks to national security by, for instance, revealing the location of sensitive locations. The NAI believes that the DOJ can address both types of risk without imposing a general restriction on the transfer of de-identified and aggregate data by including it in the definition of BUSPD.

To address the first risk – *i.e.*, the risk of re-identification – the NAI recommends that the DOJ amend the Proposed Rule to exclude de-identified and anonymized data from the definition of BUSPD while directing the Department of Homeland Security ("DHS") to establish a set of criteria for de-identification and anonymization that sufficiently address the re-identification risks identified by the DOJ in connection with the Proposed Rule. This would allow the DOJ to address its concerns through strong de-identification requirements without limiting data transfers that do not present a risk to national security due to re-identification risk. As a related or alternative approach, the Department could consider the "expert" de-identification process recognized in the Health Insurance Portability and Accountability Act (HIPAA), where an independent expert certifies whether a de-identification method succeeds in creating a very low risk of re-identification.[36] Further, if the if the Proposed Rule continues to apply to data once it is properly de-identified, one consequence is that commercial actors will have less incentive to implement effective anonymization techniques, reducing privacy and increasing the chance that a malicious actor can re-identify the data.

To address the second risk – *i.e.*, the risk posed to revealing sensitive locations, the NAI recommends that the DOJ adopt a definition of "sensitive locations" in keeping with the NAI's Precise Location Information Solution Provider Voluntary Enhanced Standards[37] and recent FTC enforcement activity[38] that includes categories of sensitive locations the DOJ views as posing a risk to national security (for example, military installations). This would enable the DOJ to ban the transfer of any type of data related to defined categories of sensitive locations that pose such a risk without requiring a blanket prohibition on transferring any de-identified or aggregate data.

## IV. The Department and the FTC Should Enter into a Formal Bilateral Agreement with the Objective of Aligning the Parallel Authorities and Enforcement.

The NAI appreciates the Department's consideration of "the potential interaction between Proposed Rule's application to data-brokerage transactions with the Protecting Americans Data from

---

[36] *See* 45 C.F.R § 164.514(b) "A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination[.]"

[37] *See Precise Location Information Solution Provider Voluntary Enhanced Standards*, The Network Advertising Initiative, https://thenai.org/accountability/precise-location-information-solution-provider-voluntary-enhanced-standards/.

[38] *See In re X-Mode Social and Outlogic*, Docket No. C-4802 F.T.C., https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf.

Foreign Adversaries Act of 2024 (PADFAA)"[39] and a consultation process on this issue with the Federal Trade Commission (FTC) and other agencies.[40] We also recognize the significant differences between PADFAA and the Proposed Rule, including the different criteria for determining whether a person is "covered," and the Proposed Rule's establishment of process for the DOJ to designate covered persons, which the PADFAA lacks.[41] The NAI also supports the Department's intention to "coordinate closely [with the FTC] to ensure that these authorities are exercised in a harmonized way to minimize any conflicting obligations or duplicative enforcement."[42]

In addition to the intentions expressed by the Department and the FTC to "coordinate, as appropriate, on licensing decisions and on any potential enforcement actions under the PADFAA with respect to activities that may be authorized, exempt, or licensed under the proposed rule," the NAI recommends that the agencies establish a Memorandum of Understanding (MOU) to formalize this collaboration. The NAI believes that the primary objectives of an MOU should be to enable the FTC to leverage the expertise and resources of the Department, with the critical goal of establishing to the greatest extent possible a single, clear set of entities considered to be controlled by foreign adversaries and hence covered under both PADFAA and the Proposed Rule.

In the absence of close coordination between the FTC and DOJ, U.S. businesses could be forced to comply with parallel legal regimes whereby a different set of businesses are covered by data sharing restrictions. Even worse, given the FTC's lack of resources and expertise in national security compared to its traditional consumer protection and competition expertise, it is possible that PADFAA would be implemented and enforced in a way where there is insufficient clarity with respect to who covered persons are.

## V. Conclusion

Thank you for your continued commitment to public involvement and transparency in this important rulemaking process. The NAI is grateful for this opportunity to comment on the Proposed Rule. If the NAI can provide any further input that would be helpful as the Department works toward finalizing the Proposed Rule, please do not hesitate to contact me at david@networkadvertising.org.

Respectfully Submitted,

David LeDuc
Vice President, Public Policy
Network Advertising Initiative (NAI)

[39] Protecting Americans' Data from Foreign Adversaries Act of 2024, H.R.7520, 118th Cong. (2024), https://www.congress.gov/bill/118th-congress/house-bill/7520/text.
[40] *See Proposed Rule* at § 202.1305(K).
[41] *See generally* Protecting Americans' Data from Foreign Adversaries Act of 2024, H.R.7520, 118th Cong. (2024), https://www.congress.gov/bill/118th-congress/house-bill/7520/text.
[42] *See Proposed Rule* at § 202.1305(K).