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

Dear Deputy Chief Licata:

The American Civil Liberties Union (ACLU) is pleased to offer these comments on the proposed rule by the Department of Justice[1] implementing President Biden's Executive Order "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern."[2]

As one of the nation's premier defenders of civil rights and civil liberties, the ACLU recognizes the urgency in addressing the harms posed by invasive data collection and surveillance. Consequently, the ACLU has defended and advanced privacy rights in courts and legislatures over its history, including regarding biometrics, broadband connectivity, commercial surveillance, library patronage and video rentals, healthcare, and more. Commensurate with its commitment to privacy, the ACLU also vigorously defends the right to freedom of speech and strives to harmonize privacy protections with traditional First Amendment activities such as journalism, advocacy, and robust debate on matters of public significance.

In that spirit, the ACLU offers the following comments: we raise serious concerns about the Department's reading of the Berman Amendment and its implications for First Amendment and due process rights, celebrate where the Department has appropriately narrowed the proposed rule, and offer suggestions for further clarification to avoid unintended consequences. Given the serious questions posed by the Department's proposed rule under the Berman Amendment, the First Amendment, and due process principles, the ACLU believes that it is unnecessary for the Department to proceed under "emergency" authority under the International Emergency Economic Powers Act, given that Congress has recently passed separate legislation addressing virtually the same data export issues.[3]

---

[1] 89 Fed. Reg. 86116 (Oct. 29, 2024).
[2] Executive Order 14117 of February 28, 2024, 89 Fed. Reg. 15421 (Mar. 1, 2024).
[3] Protecting Americans' Data from Foreign Adversaries Act of 2024, Pub. L. 118-50, div. I, 138 Stat. 895, 960 (2024).

AMERICAN CIVIL LIBERTIES UNION

National Political Advocacy Department
915 15th Street, NW, 6th Floor
Washington, DC 20005-2112
aclu.org

Deirdre Schifeling
Chief Political & Advocacy Officer

Anthony D. Romero
Executive Director

Deborah N. Archer
President

The DOJ's Reading of the Berman Amendment Is Overly Narrow and Likely Unworkable

The ACLU appreciates and agrees with the Department's assertion that the Berman Amendment "was designed to reach expressive information protected by the First Amendment."[4] However, the Department's forced distinction between "expressive" information and "functional" data is not supported by the text of the Berman Amendment, poses serious practical difficulties, and runs counter to First Amendment jurisprudence.

The Berman Amendment's text is broader than the Department's proposed rule acknowledges: the statute precludes the President from using IEEPA to regulate or prohibit the import or export of "information" and "informational materials" — terms that plainly encompass data beyond the limited category of "expressive material" the proposed rule identifies. As the proposed rule acknowledges, the Berman Amendment's purpose is to protect information and materials "involving the free exchange of ideas" from regulation under IEEPA.[5] But such information encompasses, for example, raw data related to scientific or technical research, journalistic reporting and investigations, and policy analysis and advocacy, regardless of whether the data itself is "expressive" in the Department's view.

Although the Department relies in significant part on canons of statutory construction,[6] "we look first to [a statute's] language, giving the words used their ordinary meaning" and "*then* apply 'established principles of interpretation.'"[7] Merriam-Webster defines "information" as "knowledge obtained from investigation, study, or instruction; intelligence, news; facts, *data*."[8] Data, in turn, is defined as "factual *information* (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation."[9] The Office of Management and Budget similarly defines "information" as "any communication or

---

[4] 89 Fed. Reg. at 86167.
[5] 89 Fed. Reg. at 86165.
[6] 89 Fed. Reg. at 86166.
[7] Tiger Lily, LLC v. United States Dep't of Hous. & Urb. Dev., 992 F.3d 518, 522 (6th Cir. 2021) (quoting Artis v. District of Columbia, 138 S. Ct. 594, 603 (2018); POM Wonderful LLC v. Coca-Cola Co., 573 U.S. 102, 134 S. Ct. 2228, 2236 (2014)) (emphasis added).
[8] Information Definition, Merriam-Webster.com, here (last visited Nov. 21, 2024) (emphasis added).
[9] Data Definition, Merriam-Webster.com, here (last visited Nov. 21, 2024) (emphasis added).

representation of knowledge such as facts, *data*, or opinions in any medium or form."[10] The plain text of the Berman Amendment underscores that "information" and "data" cannot be as readily separated as the Department suggests.

Moreover, the Department's reading of the statute fails one central canon of statutory construction: it focuses solely on the term "informational materials," effectively ignoring the term "information" and violating the canon against surplusage.[11] Because "information" is a distinct category from "informational materials," the term "information" must be given its own meaning in construing the scope of the statute's protection.

The Department's reliance on the canon of *noscitur a sociis* to justify narrowly limiting the statute to "expressive materials" is also misplaced. Contrary to the proposal's claim, not all the words used in the statute's list are inherently or necessarily expressive in nature. A number of the terms — "microfiche, tapes, compact disks, CD ROMs" — are simply mediums on which information of virtually any kind may be stored and transmitted, including many of the most common mediums for transmitting information when the Berman Amendment was adopted by Congress in 1988 and amended in 1994. Because the terms in the statute are not uniformly expressive in nature, there is no basis for artificially limiting the broad term "information" to "expressive material" based on "the company it keeps" in the Berman Amendment.

Moreover, such a distinction is unworkable, as there is no practical way to separate "expressive" activities such as journalism or advocacy from the facts and data on which they rely. As the Supreme Court has observed, "Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs,"[12] and determining when data or facts become speech or expressive informational materials is likely futile. For example, recent data-driven journalism used data purchased from data brokers to track the movements and relationships of associates of a convicted sex trafficker;[13] another tracked the impact of visits by Securities and Exchange Commission employees to corporate

---

[10] OMB Circular A-130 at 29 (2014), here (emphasis added).
[11] *See* Kungys v. United States, 485 U.S. 759, 778 (1988) (plurality opinion of Scalia, J.) (describing the "cardinal rule of statutory interpretation that no provision should be construed to be entirely redundant").
[12] Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011).
[13] Dhruv Mehrotra & Dell Cameron, *Jeffrey Epstein's Island Visitors Exposed by Data Broker*, Wired (Mar. 28, 2024), here.

headquarters on stock prices.[14] In each example, identifying just when the underlying data is transformed into "expressive" information is impossible — had the journalists or researchers released the data to support their reporting, would it be "expressive" or "functional"? What if they had released it independent of their reporting for others to report on?

Finally, First Amendment jurisprudence does not support the Department's categorical distinction between "informational materials" and "functional data." The Department contends that "[t]he Berman Amendment was designed to reach expressive information protected by the First Amendment,"[15] but the Supreme Court has recognized that "the creation and dissemination of information are speech within the meaning of the First Amendment,"[16] and, in part for that reason, the First Amendment's protection can reach "even dry information, devoid of advocacy, political relevance, or artistic expression."[17] Because the First Amendment does not recognize a black-and-white distinction between "expressive" informational material and "data that is technical, functional, or otherwise non-expressive,"[18] neither does the Berman Amendment. Perhaps some bodies of data may not constitute "speech" under the First Amendment, but the Department fails entirely to limit its proposed rule to such data.

This is not to claim that the regulation of data brokers and data brokerage is not permitted by the First Amendment — it likely is[19] — but only that the approach taken by the Department is not permitted by the Berman Amendment. Whereas the identification of data as "speech" is only the beginning of the inquiry under the First Amendment, it is the end of the inquiry under Berman. As one court observed, the Berman Amendment "totally *exempts* from prohibition or regulation the import of ideas and information protected by the First Amendment."[20] In contrast, the First Amendment inquiry would next

---

[14] William Christopher Gerken et al., *Watching the Watchdogs: Tracking SEC Inquiries Using Geolocation Data*, SSRN (Sept. 19, 2024), here.
[15] 89 Fed. Reg. at 86167.
[16] *Sorrell*, 564 U.S. at 570.
[17] *Id.* (quoting IMS Health Inc. v. Sorrell, 630 F.3d 263, 271 (2d Cir. 2010)).
[18] 89 Fed. Reg. at 86209.
[19] For example, the Fair Credit Reporting Act, which regulates the related consumer reporting industry, has been upheld against multiple First Amendment challenges. King v. Gen. Info. Servs., Inc., 903 F. Supp. 2d 303, 306 (E.D. Pa. 2012); Trans Union LLC v. F.T.C., 295 F.3d 42, 53 (D.C. Cir. 2002); Trans Union Corp. v. F.T.C., 267 F.3d 1138, 1141 (D.C. Cir. 2001); Trans Union Corp. v. F.T.C., 245 F.3d 809, 818 (D.C. Cir. 2001).
[20] Cernuda v. Heavey, 720 F. Supp. 1544, 1550 n.10 (S.D. Fla. 1989) (emphasis in original).

determine what level of scrutiny applies and whether the government action or regulation at issue satisfies it[21] — crucial questions not contemplated by Berman.

Consequently, the bar imposed by the Berman Amendment does not preclude regulation in this space entirely but leaves the matter for Congress to address through legislation, as it already has.[22]

The Department's Interpretation of the Berman Amendment Is Unlikely to Receive Judicial Deference

Moreover, the Department's interpretation of the Berman Amendment is unlikely to receive judicial deference, despite the cases the Department cites.[23] Each of those cases expressly[24] relies on deference awarded to executive agencies' legal interpretations under *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*,[25] which has since been overturned in the Supreme Court's decision *Loper Bright Enterprises v. Raimondo*.[26]

To be sure, the *Loper Bright* Court did recognize that deference may be appropriate under *Skidmore v. Swift & Co.*[27] or where the statute gives the agency "authority to give meaning to a particular statutory term," "fill up the details" of a statutory scheme, or to act within the limits of a term such as "reasonable."[28] Even in those cases, however, the

---

[21] *E.g. Sorrell*, 564 U.S. at 571-72 (assuming *Central Hudson* scrutiny applies to regulation of data brokerage); Trans Union LLC v. F.T.C., 295 F.3d 42, 52 (D.C. Cir. 2002) (applying *Central Hudson* scrutiny to regulation of consumer reporting agencies under the Fair Credit Reporting Act).

[22] Protecting Americans' Data from Foreign Adversaries Act of 2024, Pub. L. 118-50, div. I, 138 Stat. 895, 960 (2024).

[23] 89 Fed. Reg. at 86165 n.339 (citing Zarmach Oil Servs., Inc. v. U.S. Dep't of Treas., 750 F. Supp. 2d 150, 156 (D.D.C. 2010); Holy Land Found. v. Ashcroft, 333 F.3d 156, 162-63 (D.C. Cir. 2003); United States v. Lindh, 212 F. Supp. 2d 541, 562-63 & n.52 (E.D. Va. 2002); Consarc Corp. v. U.S. Dep't of Treas., Off. of Foreign Assets Control, 71 F.3d 909, 914-15 (D.C. Cir. 1995); Consarc Corp. v. Iraqi Ministry, 27 F.3d 695, 701 (D.C. Cir. 1994)).

[24] *See Zarmach*, 750 F. Supp. 2d at 156; *Consarc Corp. v. OFAC*, 71 F.3d at 914; *Consarc Corp. v. Iraqi Ministry*, 27 F.3d at 702; *cf. Holy Land, 333 F.3d* at 162 (deferring to agency's fact finding).

[25] 467 U.S. 837, 843-44 (1984).

[26] 144 S. Ct. 2244, 2273 (2024).

[27] 323 U.S. 134, 139–40 (1944) (noting that the "interpretations and opinions" of the relevant agency, "made in pursuance of official duty" and "based upon ... specialized experience," "constitute[d] a body of experience and informed judgment to which courts and litigants [could] properly resort for guidance," even on legal questions). The Department does not contend that it is entitled to *Skidmore* deference.

[28] *Id.* at 2263.

reviewing court is "to independently interpret the statute and effectuate the will of Congress subject to constitutional limits."[29] Under the traditional role of a reviewing court, "respect [is] warranted when an Executive Branch interpretation was issued roughly contemporaneously with enactment of the statute and remained consistent over time."[30] In such cases, "[t]he views of the Executive Branch could inform the judgment of the Judiciary, but did not supersede it."[31] That, however, is not the case here, where thirty years after the Berman Amendment was last amended, the Department is promulgating a starkly new and narrower interpretation of the Amendment.

Moreover, the authority cited by the Department as establishing deference to its IEEPA rulemaking[32] amounts to nothing more than a general grant of rulemaking authority; its authorization for the Department to "prescribe[e] definitions"[33] lacks the specific authorization to "give meaning to a particular statutory term" envisioned by *Loper Bright* as meriting some level of "respect."[34]

Further, even prior to *Loper Bright*, where the interpretative issue was of constitutional provisions (such as is the case here by reference), there was — and is — no deference.[35]

The Proposal Leaves Too Many Crucial Questions to the Discretion of the Attorney General, Raising Significant Due Process Concerns

The proposed rule leaves significant questions to the Attorney General's discretion, including basic aspects of the rule's scope. That discretion includes the granting of licenses to U.S. persons and adding to the list of countries of concern,[36] each of which is significant.

---

[29] *Id.*
[30] *Id.* at 2258
[31] *Id.*
[32] 89 Fed. Reg. 86165 (citing 50 U.S.C. § 1704).
[33] 50 U.S.C. § 1704.
[34] *See Loper*, 144 S. Ct. at 2263 n.5 (citing statutes that authorize definitions of particular terms).
[35] *Loper*, 144 S. Ct. at 2247 ("[The APA] makes clear that agency interpretations of statutes—like agency interpretations of the Constitution—are not entitled to deference.").
[36] 89 Fed. Reg. at 86151, 86152, 86141 ("During the ANPRM's comment period, commenters requested that the proposed rule include criteria and a transparent process for the Department of Justice to designate countries of concern, including by conducting robust interagency discussion and soliciting public comment. The proposed rule makes no change in response to this comment.").

However, the most concerning component of the Attorney General's broad discretion is their authority to unilaterally designate "any person, wherever located" — including U.S. persons — as a "covered person."[37] That designation hinges on three broad factors, as "determined by the Attorney General," including whether the person is "controlled by" or "likely to act on behalf of" country of concern.[38]

Crucially, the designation is made with neither notice nor an opportunity to be heard, no rules of evidence, and virtually no recourse. Instead, the designation is made by simple publication in the Federal Register — with no public comment period — and is effective immediately.[39] The designation may be based on "any information or material the Attorney General deems relevant and appropriate, classified or unclassified, from any Federal department or agency or from any other source,"[40] and it may be made whether the person's relationship with the country of concern is "voluntary or involuntary."[41] Recourse for affected individuals is limited to petitioning the Attorney General to reconsider the designation.[42]

This truncated process raises serious due process concerns, especially given that it may restrict the fundamental liberty interests of U.S. persons to disclose and receive information. "An essential principle of due process is that a deprivation of life, liberty, or property 'be preceded by notice and opportunity for hearing appropriate to the nature of the case.'"[43]

The proposed rule fails to meet even that constitutional minimum, as the deprivation takes place with no notice to the affected individuals and is effective *immediately* upon publication. Moreover, the ability to petition the Attorney General for reconsideration is insufficient; that procedure provides an opportunity to be heard only *after* the

---

[37] 89 Fed. Reg. at 86206 (to be codified at § 202.211(a)(5)).
[38] *Id.*
[39] *Id.* at 86151, 86221 (to be codified at § 202.701(c), (e)).
[40] *Id.* at 86221 (to be codified at § 202.701(b)).
[41] *Id.* at 86151.
[42] *Id.* at 86221 (to be codified at § 202.702).
[43] Cleveland Bd. of Educ. v. Loudermill, 470 U.S. 532, 542 (1985) (quoting Mullane v. Central Hanover Bank & Trust Co., 339 U.S. 306, 313 (1950)); *accord* Mathews v. Eldridge, 424 U.S. 319, 333 (1976) ("[The] essence of due process is the requirement that 'a person in jeopardy of serious loss (be given) notice of the case against him and opportunity to meet it.'" (quoting Joint Anti-Fascist Comm. v. McGrath, 341 U.S. 123, 171-172 (Frankfurter, J., concurring))); Goldberg v. Kelly, 397 U.S. 254, 266 (1970); Armstrong v. Manzo, 380 U.S. 545, 552 (1965)).

deprivation,[44] and vesting the Attorney General with authority both as the original decisionmaker and the adjudicator of the petition for reconsideration raises "substantial" due process concerns.[45]

To avoid these serious constitutional questions, the Department should consider limiting the Attorney General's designation authority in proposed § 202.211(a)(5) to foreign persons if it promulgates a final rule.

The Proposed Rule Includes Several Tailored Provisions that Should Not Be Expanded in Any Final Rule

If the Department promulgates a final rule, the proposed rule includes several crucial narrowing provisions that should be maintained:

- The inclusion of bulk data thresholds will, as a practical matter, reduce the impact of the rule on ordinary speech activities while tailoring its focus on the harms at the center of the proposal: data brokerage.
- The geofences prescribed in § 202.1401 are focused on specific, defined governmental campuses. In all but one case, the defined campuses are no larger than a city block. This approach is significantly more targeted than attempts to protect all governmental facilities or all critical infrastructure, as defined by the Cybersecurity and Infrastructure Security Agency, which can overbroadly cover everything from K-12 public schools to federal intelligence agencies.[46]
- Limiting government-related data to that which is "market[ed]" as such will avoid incentivizing — or requiring — entities involved in transferring data to engage in even more profiling of U.S. persons and surveilling the data they transfer. Without such a limitation, data processors would effectively be required to surveil the data they collect and distribute to expressly identify individuals as governmental officials and employees, a

[44] *Cf.* Farhat v. Jopke, 370 F.3d 580, 595–96 (6th Cir. 2004) ("We also have held that in the pretermination stage, the [public] employee does not have a right to, and the Constitution does not require, a neutral and impartial decisionmaker. . . . It is at the post-deprivation stage where a neutral decisionmaker is needed to adjudicate the evidence.").

[45] *Cf.* Withrow v. Larkin, 421 U.S. 35, 51–52 (1975) ("That is not to say that there is nothing to the argument that those who have investigated should not then adjudicate. The issue is substantial, it is not new, and legislators and others concerned with the operations of administrative agencies have given much attention to whether and to what extent distinctive administrative functions should be performed by the same persons.").

[46] *See, e.g.*, Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act of 2023, S. 1631, 118th Cong. (2023).

scenario that would be compounded by the fact that there are no bulk thresholds for government-related data.

- Similarly, the "knowing" mental state avoids imposing due diligence requirements on entities involved in transferring data to engage in surveillance of those using their services. For example, a strict liability, negligence, or recklessness standard could impose liability on entities, even when they have no awareness of the data they are transferring. This is particularly true for messaging applications, broadband service, and potentially cloud service, where the providers should have little to no insight into the content of the data they are transferring.[47] Any lower standard than knowledge would have particularly detrimental effects on encrypted communications, where technical security and privacy measures make it impossible for prying eyes to analyze the content of our communications. The ACLU particularly appreciates Examples 2 and 5 included in proposed § 202.230, which underscore that providers of communications infrastructure such as broadband service or cloud storage handling encrypted data generally will not have actual knowledge of the nature of the data they handle.[48]
- The exclusion of personal communications, expressive materials, and telecommunications helps ensure that core First Amendment activities are not overly burdened.

Each of these provisions is a step in the appropriate direction in ensuring that proposed rule is narrowly tailored to the harms it seeks to address.

[47] 89 Fed. Reg. at 86132 ("[I]f a U.S. entity merely provides a software platform or owns or operates infrastructure for a U.S. customer, and thus does not know or reasonably should not know of the kind or volume of data involved, then the U.S. entity generally would not 'knowingly' engage in a prohibited transaction if the U.S. customer uses their platform or infrastructure to engage in a prohibited transaction. . . . Likewise, if a U.S. entity merely stores encrypted data on behalf of a U.S. customer and does not have access to the encryption key (or has access only to an emergency backup encryption key usable only at the customer's explicit request), and if the U.S. entity is reasonably unaware of the kind or volume of data involved, the U.S. entity generally would not meet the 'knowingly' standard of the proposed rule.").

[48] 89 Fed. Reg. at 86210-11.

Several Provisions of the Proposed Rule Should Be Narrowed to Avoid Chilling Speech-Related Activities

Despite the tailored provisions throughout the proposed rule, several aspects of the rule will still broadly sweep in core speech-related activities, and further narrowing is needed to avoid burdening speech-related activities if the Department promulgates a final rule.

In particular, the provisions on government-related data do not include quantitative bulk thresholds but instead apply to even a single transaction. Similarly, the definitions of "covered data transaction," "data brokerage," and "employment," "vendor," and "investment" agreements do *not* specify that the transfer of data must be *to* a covered person. For example, "data brokerage" is defined as "the sale of data . . . involving the transfer of data from *any person* (the provider) to *any other person* (the recipient)."[49] Nothing in that definition limits its application to transfers of data *to* a covered person, and the other relevant definitions are similarly open ended.[50]

Thus, those definitions would facially reach transactions involving the transfer of data on a *single* governmental official to U.S. persons, such as a U.S.-based newspaper contracting with a covered person to compile information on U.S. officials' financial transactions in a country of concern. The informant then obtains, compiles, and transfers the information back to the U.S. newspaper. Depending on whether the arrangement is viewed as data brokerage or a vendor agreement, the transaction may be prohibited or restricted.

This concern is not merely hypothetical. Similar consequences have arisen from laws known as "Daniel's Law," which seek to protect the personal information of judges, police officers, and other

[49] 89 Fed. Reg. at 86207 (to be codified at § 202.214).

[50] *Id.* at 86208 (to be codified at § 202.217) ("employment agreement means any agreement or arrangement in which an individual . . . performs job functions directly for a person in exchange for payment or other consideration . . . .") *id.* at 86209 (to be codified at § 202.228) ("investment agreement means an agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to" U.S. real estate or legal entities); *id.* at 86213 (to be codified at § 202.258) ("vendor agreement means any agreement or arrangement . . . in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration").

government officials from publication. The law has resulted in journalists being prohibited from publishing matters of public importance, obtained from public records, such as a city police chief having a primary residence more than two hours from the town he served.[51] This approach runs counter to the principles undergirding the First Amendment, where speech about public officials, public figures, and matters of public significance is awarded the highest levels of protection.[52]

The proposed rule might similarly disrupt basic internet connectivity and other online services, despite exceptions built into the proposed rule. The proposed rule includes several identifiers that are necessary or commonly used to operate broadband services or online platforms — or that are ordinarily transferred in the operation of those services. For example, establishing a connection with a remote server, such as one hosting the content of a website, will require transmission of the user's IP address to the server; cookie data will also be transmitted to establish a session state, such as whether a user is logged in or if they have items in their cart.[53]

More concerningly, any device using traditional IPv6 stateless address allocation will effectively globally transmit both its IP address and its MAC address in a way that is visible to any remote network operator or peer.[54] This suggests that any network service provider passing U.S. device IPv6 packets to any remote party (or through any remote network) operated by a covered person is at risk under the proposed rule. Broadband service will also entail the transfer of other sensitive personal data, such as financial data or governmental identifiers, as described below, in serving customers. In establishing and maintaining that service, countless entities

---

[51] Caitline Vogus, *NJ Court to Journalist on Publication of Official's Address: Do You Feel Lucky, Punk?*, Freedom of the Press Foundation (Apr. 30, 2024), here; Terrence McDonald, *Daniel's Law Is Bad for N.J. Journalists – And Everyone Who Wants Government Accountability*, New Jersey Monitor (July 27, 2023), here

[52] Philadelphia Newspapers v. Hepps, 475 U.S. 767 (1986); Gertz v. Welch, 418 U.S. 323 (1974); New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

[53] *How Websites and Apps Collect and Use Your Information*, Federal Trade Commission (Sept. 2023), here.

[54] Said Jawad Saidi et al, One Bad Apple Can Spoil Your IPv6 Privacy, arXiv (Mar. 16, 2022), here/

would transfer that data throughout the internet "stack," often on the basis of agreements.[55]

Consequently, those identifiers — among many others — could constitute a covered personal identifier, and the entities involved in transferring that information over the internet backbone could be engaged in vendor agreements and face liability under the rule. This could have serious consequences; the volume of connections between the United States and China alone that could qualify as "covered data transactions" is likely innumerable, easily clearing the bulk data thresholds.

The proposed rule's exception to the definition of "covered personal identifiers" for networking is likely insufficient to address this concern. The exception would exclude 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" from the definition of a "covered personal identifier."[56] The exception is likely insufficient for two reasons:

- First, it is not clear to what extent key identifiers such as session state information preserved in cookies are "necessary" for networking services.
- Second, many other types of listed identifiers and sensitive personal data will be transmitted by broadband providers "in combination" with network identifiers, such as a broadband service transmitting bank account numbers along with IP addresses when establishing connectivity for a financial transaction. The fact that the account numbers will almost certainly be encrypted is irrelevant under the proposed rule, as the definition of "bulk U.S. sensitive personal data" expressly applies to encrypted data.[57]

Further, the exception for expressive informational materials may not be sufficient to address concerns around broadband connectivity. The Department states that "expressive content and associated *metadata that is not sensitive personal data* would be categorically outside the scope of . . . the proposed regulations."[58]

---

[55] Internet Society, Internet Interconnections: Proposals For New Interconnection Model Comes Up Short (2012), here.
[56] 89 Fed. Reg. at 86206 (to be codified at § 202.212(b)(2)).
[57] 89 Fed. Reg. at 86205 (to be codified at § 202.206).
[58] 89 Fed. Reg. at 86169 (emphasis added).

However, this statement is circular — metadata is excluded as "sensitive personal data" only to the extent it "is not sensitive personal data" to begin with. That is, the metadata is exempted from the proposed rule, but only to the extent that it is not covered by the rule in the first place. Under that framing, the proposed rule could eviscerate basic broadband connectivity.[59]

To address these potential consequences, the ACLU suggests the following redlines if the Department decides to promulgate a final rule:

- Ensure that the definitions regarding "covered data transactions" apply only to data that is transferred *to* covered persons; the ACLU recommends amending the definition of "access" in proposed § 202.201 to read: "The term access means logical or physical access **provided to a country of concern or a covered person**, including . . . ."
- Provide a definition for "sale of data" as follows: "sale of data means the exchange of personal sensitive data to a country of concern or a covered person in exchange for monetary consideration, but excluding: (1) the disclosure of personal data to a processor that processes the personal data on behalf of the provider; (2) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; (3) the disclosure or transfer of personal data to an affiliate of the controller; (4) the transfer of publicly available information."[60]
- Extend the telecommunications exception in proposed § 202.509(a) to "**broadband internet access service, as defined in 47 C.F.R. § 8.1(b), or any successor regulation, or any internet protocol-based transmission or networking service, or the functional equivalent of any of those services**."
- Clarify that the exemption for "expressive" "information or informational materials" in proposed § 202.502 also extends to

[59] The proposed rule could also potentially impact online platforms that of course depend on broadband connectivity, such as features that would connect people from the United States to those in covered countries. However, the ACLU understands the Department's proposed exception for "expressive" information materials to include features of and communications through online platforms. *See* 89 Fed Reg. at 86166 n.348 ("The United States Government did not dispute that these expressive communications exchanged on TikTok were 'informational materials' under the Berman Amendment.").

[60] This definition focuses on the harm identified as the focus of the proposed rule, "the outright sale" of data, 89 Fed. Reg. at 86131, and excludes other transfers covered by other dimensions of the proposed rule, such as vendor agreements.

"**associated metadata, whether or not the metadata on its own constitutes sensitive personal data**."

- Add examples to the provisions regarding exempt transactions in subpart E to clarify that broadband service, internet connectivity, and internet protocol-based network are "ordinarily incident" to the transactions, especially regarding travel, financial services, and telecommunications services.
- Add an exception to subpart E for encrypted data as follows: "Subparts C and D of this part do not apply to data transactions to the extent that the relevant sensitive personal data is encrypted, and no covered person has access to the encryption key and cannot reasonably access the sensitive personal data in plaintext."

ACLU
AMERICAN CIVIL LIBERTIES UNION

Thank you for your consideration. If you have any questions about these comments, please do not hesitate to contact us at cvenzke@aclu.org.

Sincerely,

Cody Venzke
Senior Policy Counsel
National Political Advocacy Department