epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

To

THE DEPARTMENT OF JUSTICE

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

89 Fed. Reg. 86,116

November 27, 2024

By notice published on October 29, 2024, the Department of Justice ("DOJ") requested comments regarding Preventing Access to U.S. Sensitive Personal Data and Government Related Data by Countries of Concern or Covered Persons (the "Proposed Rule").[1] The Electronic Privacy Information Center ("EPIC") submits these comments to urge the DOJ to (i) clarify the definition of covered data transactions, (ii) exempt internet service providers in the same manner as telecommunications providers to allow internet infrastructure to work as intended, and (iii) increase the protection of Social Security Numbers.

EPIC is a public interest research center based in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has a particular interest in safeguarding consumers' data and mitigating the harmful effects of commercial surveillance.[3]

---

[1] Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 89 Fed. Reg. 86116 https://www.federalregister.gov/documents/2024/10/29/2024-24582/provisions-pertaining-to-preventing-access-to-us-sensitive-personal-data-and-government-related-data#p-1531 [Hereinafter, the "DOJ NPRM on Preventing Access to U.S. Personal Data"].

[2] EPIC, *About Us* (2023), https://epic.org/about/.

[3] *See* EPIC, Comment on the DOJ's Proposed Rule on Access to Americans' Bulk Sensitive Personal Data and Government Related Data by Countries of Concern (Apr. 19, 2024), https://epic.org/documents/epic-comments-to-doj-regarding-anprm-on-access-to-americans-bulk-sensitive-personal-data-and-government-related-data-by-countries-of-concern/ [Hereinafter the "EPIC Comments on DOJ ANPRM"]; *See generally* EPIC, Comment on the FTC's Proposed Trade Regulation Rule on Commercial Surveillance & Data Security (Nov. 21, 2023), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRMcomments-Nov2022.pdf; EPIC, Demand Progress, & EFF, Comments on Proposed Consent Order, *In re X-Mode Social, Inc.*, FTC File No. 202-3038 (Feb. 20, 2024), https://epic.org/documents/comments-of-epic-demand-progress-and-eff-in-re-the-federal-trade-commissions-proposed-order-settlement-with-x-mode-social-inc/; EPIC, *Comments on Standards for Safeguarding Customer Information*, Docket No. 2019-04981 (Aug. 1, 2019), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Aug2019.pdf; Complaint, *In re Google LLC* (FTC, Jan. 18, 2024), https://epic.org/documents/epic-and-accountable-tech-ftc-complaint-re-google-location-data-practices-2024/.

I. EPIC Applauds the DOJ For Not Letting Industry Talking Points Erode Privacy Protections, But There are Small Changes DOJ Can Make to Clarify and Strengthen the Rule.

EPIC applauds the DOJ for recognizing the state of re-identification technology and protecting government data and bulk U.S. sensitive personal data regardless of whether it has been anonymized, pseudonymized, de-identified, or encrypted. In comments to the advanced notice of proposed rulemaking ("ANPRM") stage of this rulemaking, EPIC stressed the probability of re-identification even in datasets that have been de-identified, pseudonymized, and anonymized, especially in the wake of major artificial intelligence technological breakthroughs.[4] The DOJ recognized this re-identification crisis and refused to remove de-identified, pseudonymized, anonymized, and even encrypted data from the Proposed Rule's scope.[5] EPIC agrees with the DOJ's findings that companies' concerns that they would be required to decrypt encrypted data transiting over their channels or hosted on the company's server when they cannot hold or access encryption keys are unfounded. The standard in Section 202.230 that clarifies liability in these cases is only for "knowing" violations and would protect these edge case companies from liability. A company does not need to weaken security,[6] increase surveillance of content, or break the trust in encrypted infrastructure when the company could easily access the relevant information (the destination of the data, the amount of data, and the relative kind of data) without needing to break encryption.[7]

EPIC also applauds the DOJ's efforts to close the third-party loophole by creating both contractual clause and due diligence requirements on the transacting party's behalf. In its comments at the ANPRM stage, EPIC pointed out the glaring loophole whereby third party countries—i.e. non-U.S. persons and non-countries of concern—could easily buy the data and sell it to countries of concern and covered persons.[8] There is little to no transparency into how data brokers sell data, particularly in how data is repackaged and resold through various layers of data brokers.[9] With a distinct lack of regulation in the data broker space,[10] this Proposed Rule begins to close some of the

---

[4] EPIC Comments on DOJ ANPRM, *supra* note 2 at 3-11.
[5] DOJ NPRM on Preventing Access to U.S. Personal Data, *supra* note 1 at 86126-27.
[6] Insider threats are a "central concern" in cybersecurity efforts. Jonathon W. Penney & Bruce Schneier, *Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group*, 36 Berkeley Tech. L. J. 102, 105 (2021) (Citing Jonathan Mayer, Cybercrime Litigation, 164 U. PA. L. REV. 1453, 1493 (2016) (noting in Table 4 that well over half of cybercrime was committed by a combination of employees, consultants, and contractors, users or customers, and business partners); Eric J. Sinrod & William P. Reilly, Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, 16 Santa Clara High Tech. L.J. 177, 184 (2000) ("According to recent FBI assessments, disgruntled insiders are a principal source of computer crimes."); *see also* Lucas Wright, *People, Risk, and Security* 40–43 (2017) (discussing insider threats)). By allowing intermediary companies to break encryption to monitor data flows for prohibited transactions, far more threats would be created than prohibited transactions would be flagged.
[7] DOJ NPRM on Preventing Access to U.S. Personal Data, *supra* note 1 86126-29.
[8] EPIC Comments on DOJ ANPRM, *supra* note 2 at 19-24.
[9] For example, Justin Sherman, Fellow and Research Lead at Duke University's Data Brokerage Project, also noted that "based on the copious evidence of data brokerage-linked harms (from domestic violence to consumer exploitation), there is very little to suggest data brokers implement controls to prevent harmful uses of their data once sold. *Promoting Competition, Growth, and Privacy Protection in the Technology Sector Before the Sen. Comm. on Fin. Subcomm. Fiscal Responsibility & Econ. Growth,* 117th Cong. (2021), https://www.finance.senate.gov/imo/media/doc/Written%20Testimony%20-%20Justin%20Sherman.pdf (statement of Justin Sherman, Fellow and Research Lead, Data Brokerage Project at Duke Univ. Sanford Sch. of Pub. Pol'y).
[10] *But see* EPIC Comments on DOJ ANPRM, *supra* note 2 at 22-23 (discussing the limited existing and proposed data broker regulations, such as the CFPB's potential rulemaking using its FCRA authority).

gaps and build an infrastructure where data brokers will need to monitor data flows and otherwise engage in due diligence measures to ensure that national security concerns are properly mitigated.

Finally, EPIC applauds the DOJ for refusing to create a consent exemption whereby a data subject could consent to their data being disclosed in otherwise prohibited or restricted transactions.[11] Notice and consent regimes are notoriously fallible as consumers often do not know their data is being transacted in the first place and rarely have adequate information or ability to make informed decision about where their data is going or how it is going to be used.[12] The DOJ recognizes that these decisions, in aggregate, "help create the national security risk" the Proposed Rule is trying to mitigate.[13]

However, the Proposed Rule still fails to comprehensively protect national security interests. The DOJ declined to extend the scope of covered personal identifiers and did not address EPIC's concern about the bulk threshold limits being reset every twelve months. The reason privacy laws include various types of personal data categories is the increasing ease with which individuals can be re-identified based on more remote categories of data.[14] Properly scoped privacy regulations and principles, such as data minimization, can further national security interests by keeping key authentication datapoints like Social Security Numbers out of the hands of malicious actors.[15] The DOJ's refusal to extend the definition of covered personal identifiers puts compliance costs and the bottom line of multimillion dollar corporations ahead of the security of major digital infrastructure and fails to adequately protect individuals, including current and former government officials, from impersonation and other grievous harms. EPIC provides the following narrow changes to ameliorate some of the issues with the Proposed Rule.

a. The Definition of Covered Data Transactions Should Make Clear that the Proposed Rule Only Limits Countries of Concern and Covered Persons from Accessing Government-Related Data and Bulk U.S. Sensitive Data, Not U.S. Persons' Access.

The definition of covered data transactions should be revised to clarify that transactions prohibited under the Proposed Rule are only those where a country of concern and/or a covered person gains access to government related data or bulk U.S. sensitive personal data. Both the text describing the Proposed Rule and each example in the Proposed Rule imply that the only prohibited transactions are those in which a U.S. person engages in a covered data transaction where a country of concern or covered person is the party that receives access to government related data or bulk U.S. sensitive personal data. However, the definition of "covered data transaction" is too vague and

---

[11] DOJ NPRM on Preventing Access to U.S. Personal Data, *supra* note 1 at 86121.
[12] *See e.g.*, Neil M. Richards & Woodrow Hartzog, *Pathologies of Digital Consent*, 96 Wash. Univ. L. Rev. 1461 (2019).
[13] DOJ NPRM on Preventing Access to U.S. Personal Data, *supra* note 1 at 86,121.
[14] *See e.g.* Luc Rocher et al., *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models,* 10 Nature Commc'ns, at 1 (2019), https://www.nature.com/articles/s41467-019-10933-3.pdf [https://perma.cc/SYJ7-KA95]; *see also* Alex Hern, *`Anonymised' Data Can Never Be Totally Anonymous, Says Study,* The Guardian (Jul. 23, 2019), https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds.
[15] Justin Sherman, *Tackling Data Brokerage Threats to American National Security*, Lawfare (Nov. 25, 2024), https://www.lawfaremedia.org/article/tackling-data-brokerage-threats-to-american-national-security; Justin Sherman et al., *Data Brokers, Military personnel, and National Security Risks*, Lawfare (Nov. 16, 2023), https://www.lawfaremedia.org/article/data-brokers-military-personnel-and-national-security-risks.

does not clarify the direction of the transaction, which may imply that the restrictions flow both ways (such that U.S. persons would be restricted from receiving access to the data in question).

While the definitions of "covered data transactions," "data brokerage," "vendor agreements," "employment agreements," and "investment agreements" are also drafted vaguely, they do not have the same impact as "covered data transactions." The remainder of the text implies that the DOJ does not intend the Proposed Rule to prohibit transactions where U.S. persons gain access to government related data and/or bulk U.S. sensitive personal data, but rather that this NPRM is only concerned with transactions that "enable countries of concern or covered persons to access government-related data or bulk U.S. sensitive personal data to harm U.S. national security."[16] Out of 112 examples in the text of the Proposed Rule, there are no examples in which a U.S. person gaining access to government related data or bulk U.S. sensitive personal data is a prohibited or restricted transaction. In fact, several examples illustrate that a particular situation would not be prohibited or restricted because a country of concern and/or covered person is not receiving access to government related data or bulk U.S. sensitive personal data.[17] The DOJ even explicitly states in some examples that because a covered person could become a U.S. person while physically in the United States, a transaction would not be prohibited, unless other conditions were met such as the transacting parties traveling to the United States for the purpose of evading the rule.[18]

Still, despite the implication based on other portions of the Proposed Rule that U.S. persons would not be prosecuted for receiving government-related data or bulk U.S. sensitive personal data, the definition of covered data transactions should be updated to explicitly exclude these transactions to ensure that U.S. persons' free speech rights are not unduly burdened. Investigative journalists acquire information from various sources, including individuals and entities in countries of concern that would constitute covered persons. In some cases, journalists go to countries of concern for information on the U.S. government explicitly because those countries have adverse relationships with the United States. Government officials engaging in suspicious behavior in countries of concern is newsworthy, and major reporting like the Panama Papers would not have been possible if these information sources were blocked by a rule such as the one proposed in this NPRM. To be clear, the First Amendment violation does not stem from the idea that the data being transacted is expressive speech, which would implicate the Berman Amendment and other downstream consequences. Commercial data transactions are not speech, nor is the data itself expressive.[19] Instead, the violation stems from the fact that journalists' ability to engage in expressive speech, such as creating news articles, would be burdened by the possibility that accessing certain information is criminalized. The DOJ should foreclose any possibility of this Proposed Rule being weaponized to punish journalists for investigating and reporting on the U.S. government.

To clarify this issue, the language of Section 202.210(a) should be revised. The definition of "covered data transaction" provides the scope of the Proposed Rule and is best suited to explicitly

[16] DOJ NPRM on Preventing Access to U.S. Personal Data, *supra* note 1 at 86121.
[17] *See e.g.* DOJ NPRM on Preventing Access to U.S. Personal Data, *supra* note 1 at § 202.506(b)(5).
[18] *See e.g.* DOJ NPRM on Preventing Access to U.S. Personal Data, *supra* note 1 at § 202.304(b)(1).
[19] Megan Iorio, *NetChoice v. Bonta: The Case That Threatens the Future of Privacy*, EPIC (Oct. 19, 2023), https://epic.org/netchoice-v-bontathe-case-that-couldthreaten-the-future-of-privacy/ (Discussing how the First Amendment is implicated when a protected category of speech is burdened, and how data protection laws do not necessarily implicate the First Amendment under *Sorrell v. IMS Health*).

clarify that U.S. persons accessing government-related data or bulk U.S. sensitive personal data is not prohibited under the Proposed Rule. Section 202.210(a) should read as follows:

> Definition. A covered data transaction is any transaction that involves any access **by countries of concern and/or covered persons** to any government-related data or bulk U.S. sensitive personal data and that involves: (1) data brokerage; (2) a vendor agreement; (3) an employment agreement; or (4) an investment agreement.

b. A Stronger Designation for Social Security Numbers Would Reduce Its Unnecessary Collection While Imposing Minimal Compliance Costs On Regulated Entities.

EPIC urges the DOJ to counter the data collection efforts of countries of concern by classifying Security Numbers ("SSNs") as "covered personal identifiers." Both public and private sectors continue to rely on SSNs for convenient identity verification, preserving their central role in U.S. identity systems despite the fact that data breaches have compromised their reliability as personal identifiers.[20] This low-cost yet effective measure would strengthen protections for U.S. citizens' data.

First, classifying SSNs as "covered personal identifiers" would impose minimal costs on regulated entities. Most organizations already have systems in place to safeguard SSNs under existing privacy laws, such as the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act. Modern data classification tools further simplify SSN detection, making compliance incremental rather than burdensome. Second, even small compliance costs would incentivize organizations to reduce SSN collection. By classifying SSNs as "covered personal identifiers," the DOJ would encourage organizations to adopt alternative authentication methods to limit compliance obligations. This reduced reliance on SSNs aligns with longstanding federal policy designed to minimize SSN use.[21] Over time, as SSN collection declines, the DOJ's monitoring costs would also decrease.

c. To Prevent the Criminalization of Providing Basic Internet Connectivity, Internet Service Providers Should Receive the Same Exemptions as Telecommunications Providers.

Internet service providers ("ISPs") should receive the same narrowly tailored exemption as telecommunications providers to ensure that this Proposed Rule does not limit the provision of basic internet connectivity to people in countries of concern and unduly burden ISPs outside of countries of concern. In the process of providing basic connectivity services, entities may provide various listed identifiers together in a way that triggers bulk thresholds. For example, ISPs may provide access to bulk amounts of both mobile advertising IDs and IP addresses over a 12-month period by

---

[20] Suzanne Rowan Kelleher, *Everyone's Social Security Number Has Been Compromised. Here's How To Protect Yourself*, Forbes (Aug. 1, 2019), https://www.forbes.com/sites/suzannerowankelleher/2019/08/01/everyones-social-security-number-has-been-compromised-heres-how-to-protect-yourself/?sh=6ea189929ac7.

[21] *See, e.g.*, U.S. Fed. Trade. Comm'n, *Security in Numbers: Social Security Numbers and Identity Theft*, 5 (Dec. 2008) (suggesting the private sector to reduce reliance on SSNs by enhancing authentication methods and minimizing the display and transmission when unnecessary).

connecting one server to another in the course of connecting a device to a website.[22] A peering agreement is an arrangement between servers to move packets of data, either for money or for free.[23] This may constitute a vendor agreement under Section 202.258, which would subject the transactions to the prohibitions and restrictions of this Proposed Rule.

As currently written, this prohibition would cut off internet traffic between the U.S. and countries of concern under Section 202.301(a). However, it would also create major problems under the restrictions on other transactions in Section 202.401. The internet is a complex network of servers that connect with each other in different ways; if peering agreements constitute vendor agreements, then ISPs would need to engage in contractual clauses and due diligence measures to prohibit the receiving party from transferring access to data to covered persons and/or countries of concern. The CISA security rules also require that security mechanisms be "sufficient to prevent access to covered data by covered persons,"[24] which may help create safeguards against malicious cyberattacks like border gateway protocol hijacking.[25] However, this broad language could also preclude infrastructure vendors from accessing aspects of the TCP/IP protocol packets (which include various listed identifiers)[26] necessary to provide basic connectivity to individuals.

The DOJ believes that Americans should be able to "communicate globally, including with and in countries of concern" and "does not intend for these regulations to impede telecommunications service providers to operate."[27] Americans communicate not only through telecommunication channels, but also over the internet through Wi-Fi based social media platforms such as Instagram and messaging applications such as Discord. It is uncertain whether ISPs will be consistently treated as telecommunications providers,[28] so ISPs should have a separate exemption to ensure that internet infrastructure is not affected by this Proposed Rule. However, similar to the telecommunications provider exemption,[29] this ISP exemption should be narrowly tailored to only

[22] *See e.g. How Does the Internet Work,* Cloudflare, https://www.cloudflare.com/learning/network-layer/how-does-the-internet-work/ (last visited Nov. 26, 2024).
[23] *See e.g. What is an Internet Exchange Point | How do IXPs work?,* Cloudflare, https://www.cloudflare.com/learning/cdn/glossary/internet-exchange-point-ixp/ (Last visited Nov. 26, 2024).
[24]Request for Comment on Security Requirements for Restricted Transactions Under Executive Order 14117, 89 Fed. Reg. 85,976, https://www.federalregister.gov/documents/2024/10/29/2024-24709/request-for-comment-on-security-requirements-for-restricted-transactions-under-executive-order-14117.
[25] *What is BGP Hacking?,* Cloudflare, https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/ (last visited Nov. 26, 2024).
[26] *What is TCP/IP?,* Cloudflare, https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/ (last visited Nov. 26, 2024).
[27] DOJ NPRM on Preventing Access to U.S. Personal Data, *supra* note 1 at 86137.
[28] Earlier this year, the FCC enacted a rule that re-classified ISPs as telecommunications providers, but this rule has been stayed pending a challenge in the Sixth Circuit. *See, e.g.*, *In re Safeguarding and Securing the Open Internet, Restoring Internet Freedom*, Declaratory Ruling, Order, Report and Order, and Order on Reconsideration, WC Dkt. Nos. 23-320, 17-108 (Rel. May 7, 2024), https://docs.fcc.gov/public/attachments/FCC-24-52A1.pdf [hereinafter "FCC Title II Order"], *but see* Order to Stay Pending Review, *In re: MCP No. 185 Open Internet Rule (FCC 24-52)* No. 24-7000 (6*th* Cir. Aug. 1, 2024). The saga of ISP classification and re-classification has been decades-long and the subject of much litigation. *See* FCC Title II order at ¶¶4-15. Whether ISPs are classified as telecommunications carriers has several implications for data protection regulatory authority. *See, e.g.*, Fed. Trade Comm'n, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* at 4-10 (2021), *available at* https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.
[29] DOJ NPRM on Preventing Access to U.S. Personal Data, *supra* note 1 at 86137.

cover "the extent that [the transactions] are ordinarily incident to and part of the provision of internet services, like basic connectivity."

II. Conclusion

For too long, the United States has failed to protect consumers from the proliferation and evolution of commercial surveillance practices, leaving consumers vulnerable to harms perpetrated by parties willing to open their wallets. This includes adversarial countries and allied governments, as well as our own law enforcement and intelligence agencies. It is time that the government protect consumers from the full range of commercial surveillance harms. EPIC commends the DOJ for beginning to acknowledge the harms of unchecked surveillance capitalism but remains disappointed by this NPRM's overly narrow focus and unresolved issues from the ANPRM stage. The DOJ should take advantage of this opportunity to correct its course. EPIC looks forward to engaging with the DOJ further on these urgent issues, and we stand by to assist your agency however we can.

Respectfully submitted,

Jeramie D. Scott
Director, EPIC Project on Surveillance Oversight
Senior Counsel

Maria Villegas Bravo
EPIC Law Fellow

Phillipe Lin
EPIC IPIOP Clerk