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

U.S. DEPARTMENT OF JUSTICE

On the Advance Notice of Proposed Rulemaking

Provisions Regarding Access to Americans' Bulk Sensitive Personal Data

and Government-Related Data by Countries of Concern

89 Fed. Reg. 15,780

April 19, 2024

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Department of Justice's (DOJ) Advance Notice of Proposed Rulemaking (ANPRM) on Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, published on March 5, 2024,[1] which responds to President Biden's Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United

[1] DOJ Nat'l Sec. Div., *Advanced Notice of Proposed Rulemaking on Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern*, 89 Fed. Reg. 15780 (Mar. 5, 2024), https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and [hereinafter "DOJ NSD ANPRM"].

States Government-Related Data by Countries of Concern (EO 14117).[2] DOJ requests comments on how the Attorney General should implement a new program regulating "certain data transactions involving bulk U.S. sensitive personal data and government-related data that present an unacceptable risk to U.S. national security," pursuant to EO 14117.

EPIC is a public interest research center 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.[3] EPIC has a particular interest in safeguarding consumers' data and mitigating the harmful effects of commercial surveillance.[4]

EPIC supports the Biden administration's efforts to address the harms of commercial surveillance and the proliferation of data brokers trading in consumers' personal data. As we have made clear, "[t]he unchecked spread of commercial surveillance over the last two decades has led to a data privacy crisis for consumers in the United States[,]" and "[i]t is far past time to disrupt this data abuse, set rules of the road for our online ecosystem, and ensure that companies cannot extract private value from personal data in ways that undermine the public good."[5]

[2] Exec. Order No. 14,117, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, 89 Fed. Reg. 15421 (Feb. 28, 2024), https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related [hereinafter "Executive Order 14117"].

[3] EPIC, *About Us* (2024), https://epic.org/about/.

[4] *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 [hereinafter "EPIC FTC Comments"]; 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/.

[5] EPIC FTC Comments, *supra* note 4, at 1.

However, the ANPRM eschews a simple, effective rule and instead takes an unwieldy approach full of caveats and exceptions because it attempts to address only narrowly defined national security interests. The proposed rule is too narrow in its definition of covered data and recipients, doesn't take enough steps to safeguard the data itself, and fails to consider the myriad ways data can constitute a national security risk. Taken together, EPIC does not believe the EO 14117 and ANPRM framework is the correct approach. EPIC understands that DOJ's efforts in this ANPRM are constrained by the scope of the Executive Order. Therefore, we recommend DOJ modify its proposed rule to harmonize it—to the extent possible—with other U.S. regulatory efforts. The final rule should—at a minimum—broaden the definition of covered data to be more consistent with existing policy, engage with the re-identification problem from a technology neutral approach, not limit the covered transactions based on bulk thresholds, and provide criteria for evaluating and reevaluating "countries of concern."

I. The Narrow Scoping of the ANPRM Does Little to Ameliorate the Unsustainable Commercial Surveillance Status Quo.

The current commercial surveillance crisis is unsustainable. This "growing exploitation of Americans' sensitive personal data" threatens privacy rights, civil rights, civil liberties, and national security interests.[6] Due to the failure of policymakers in the U.S. to establish adequate data protection laws and regulations, private entities have had free reign to indiscriminately collect and commodify information about tens of millions of Americans.[7] The comprehensive cataloguing of the minutiae of Americans' daily life exposes Americans to an "ever-increasing risk of breaches, data

[6] Executive Order 14117, *supra* note 2, at 15421.

[7] *See, e.g.*, Memorandum from Chino Police Detective Jason Larkin on the Chino Police Contract with Fog Data Science 25 (Oct. 10, 2019), https://www.documentcloud.org/documents/22187494-chino_2019- 20_attachments - document/p25/a2143086 (In 2019, Fog Data Science boasted that its platform processed "250 million devices each month, 15 billion location signals each day, 10 million fenced points of interest" and more than 1 million daily events."); *see also* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

misuse, manipulation, and discrimination[,]" particularly for marginalized communities.[8] Artificial intelligence (AI) is supercharging harms from commercial surveillance by making it easier to analyze bulk data. The Office of the Director of National Intelligence (ODNI) has recognized the harms AI causes in the context of commercial surveillance, noting the ability of countries of concern to use AI to analyze and manipulate bulk sensitive personal data to render their "espionage, influence, kinetic, or cyber operations more effective."[9] Data brokers also accelerate the harms created by unchecked data collection by combining already extensive datasets and deriving inferences from data acquired via third parties. Purchasers and other downstream users often place excessive weight on these inferences, rather than treating them as essentially algorithmic speculation. Reliance on inaccurate inferences may lead to profiling, discrimination, or denial of public benefits. And when companies combine these inferences with other information to derive further inferences, these harms only compound.[10]

Despite these grave threats, the ANPRM as written fails to prevent the harms it purports to address. Rather than centering its rulemaking around the privacy and national security harms stemming from unchecked commercial surveillance, DOJ has framed it as a narrow, national security issue due to the scoping of the Executive Order. This framing undercuts the safeguards DOJ is trying to implement, leading to narrow and underinclusive categories of data, covered entities, recipients, and enforcement goals. The ANPRM text focuses heavily on harms relating to government data and military personnel, but the threats to privacy, civil liberties, civil rights, and

[8] EPIC FTC Comment, *supra* note 4, at 7, 45–55.
[9] ODNI, *Annual Threat Assessment of the U.S. Intelligence Community* 26 (Feb. 6, 2023), https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.
[10] *See, e.g.*, *TransUnion LLC, v. Ramirez*, 594 U.S. ___ (2021) (Plaintiff alleged that TransUnion, a credit reporter, mistakenly connected his name to the Treasury Department's Office of Foreign Assets Control list of known terrorists. This information was provided by TransUnion to a car dealer who was inspecting plaintiff's creditworthiness, and plaintiff alleges he was refused a loan based on this mistaken connection to the list of known terrorists.).

national security are not limited to narrowly tailored data sets or a narrow set of foreign entities. DOJ itself acknowledges the salient threats to intimidate high risk individuals such as "activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities" from engaging in free expression, peaceful assembly and to "curb political opposition."[11] DOJ should harmonize its regulation and enforcement efforts with the FTC,[12] the CFPB,[13] and Congress[14] to better protect against the harms the ODNI and DOJ have already identified.[15] Foreign adversaries and other bad actors will have fewer opportunities to access vulnerable data and cross reference it with intelligence from other sources if DOJ focuses its rulemaking on inclusive definitions of personal data and covered transactions as well as engaging in standard setting for de-identified information.

Although DOJ correctly identifies some of the harms posed by commercial surveillance in the context of "countries of concern," EPIC encourages DOJ to think more expansively about the kinds of harms posed by the unrestrained collection, sale, use of personal data. These harms include, but are not limited to:

[11] DOJ NSD ANPRM, *supra* note 1, at § I.

[12] FTC, *Advanced Notice of Proposed Rulemaking on Trade Regulation Rule on Commercial Surveillance and Data Security,* 87 Fed. Reg. 51273 (Aug. 22, 2022), https://www.govinfo.gov/content/pkg/FR-2022-08-22/pdf/2022-17752.pdf.

[13] CFPB, *Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information,* 88 Fed. Reg. 16,951 (June 13, 2023), https://www.federalregister.gov/documents/2023/03/21/2023-05670/request-for-information-regarding-data-brokers-and-other-business-practices-involving-the-collection.

[14] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022), [hereinafter "ADPPA"]; Protecting Americans' Data from Foreign Adversaries Act of 2024, H.R. 7520, 118th Cong. (2024), [hereinafter "Protecting Americans' Data from Foreign Adversaries Act of 2024"].

[15] *See* ODNI Senior Advisory Grp., Panel on Commercially Available Information, Report to the Dir. of Nat'l Intel. 12 (Jan. 27, 2022), *available at* https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf ("In the wrong hands, sensitive insights gained through [commercially available information] could facilitate blackmail, stalking, harassment, and public shaming.") [hereinafter ODNI SAG Report]; *see also* DOJ NSD ANPRM, *supra* note 1, at 15781 (citing Justin Sherman et al., *Data Brokers and the Sale of Data on U.S. Military Personnel* 15 (Nov. 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf).

A. Autonomy Harms Inherent to the Data Broker Business Model

While DOJ has identified discrete categories of harm stemming from the type of data transmitted by data brokers, autonomy harms that threaten civil rights, civil liberties, and national security are inherent to the data broker business model that are not addressed by the ANPRM. Disclosing personal information to third parties when that disclosure was not the primary purpose for collecting the data divests individuals of control over their data which leaves the individual more vulnerable to behavioral manipulation.[16] Individuals often do not expect their data to be disclosed to unknown third parties when they provide data to an entity. The unexpected or out-of-context disclosure of even an "innocuous piece of data" to a third party might "provide a link to other data or allow for certain inferences to be made."[17] These inferences may then be used to profile an individual, allowing bad actors to precisely target individuals based on techniques that will be most persuasive to them.[18] This practice divests the data subject of control over their data because the individuals no longer know who will have access to the data nor what those entities will do with the data.[19] Such extensive collection and sale of data can lead to "innocent" commercial outcomes such as being influenced to buy diapers[20] or could intentionally lead to more nefarious consequences, such

[16] Neil Richards, *Why Privacy Matters* 35–37 (2022) ("But the important lesson of [Target using data analytics to infer pregnancy status to tailor ads to individuals] is not actually about the power of human information analytics to find surprising correlations like the one between lotion and pregnancy. Instead, the real lesson is about the power those insights confer to *control human behavior.* The reason Target wants to know about pregnancy is because Target wants consumers to buy as much as possible of everything they sell at their big box stores—not just diapers and baby clothes, but lawn furniture and underwear, wine and electronics.") [hereinafter "*Why Privacy Matters*"]; *see also* EPIC FTC Comment, *supra* note 4, at 45–55 (noting other harms from disclosures, such as thwarted expectations, harms to contextual integrity, and discrimination harms).

[17] EPIC FTC Comment, *supra* note 4, at 17.

[18] Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in massive data breach,* Guardian (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election; *see also* Cambridge Analytica, Opinion, *In the Matter of Cambridge Analytica, LLC*., FTC File No. 9383 (Nov. 25, 2019), https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_opinionpublic.pdf.

[19] *Supra* note 15.

[20] *Why Privacy Matters*, *supra* note 16, at 36.

as influencing an individual's voting patterns.[21] Furthermore, social media has become an equalizing platform that allows anyone to go viral, proliferating social movements at an astonishing rate. Bad actors can and already have leveraged these platforms and the large datasets extracted from to engage in election interference and other malicious cyberthreats.[22] The scope constraint placed on the ANPRM by the Executive Order prevents DOJ from adequately addressing malicious behavior manipulation.

B. Revealing Sensitive Locations

DOJ recognizes that sales of personal data can allow buyers to reverse engineer sensitive locations such as military and government facilities.[23] Beyond national security risks, this data can lead to identification of places of worship, hospitals, an individual's home address, an individual's place of work, and other sensitive locations.[24] While not all home addresses are sensitive national security data, location data can be leveraged to create several types of harms. For example, journalists can be tracked back to their home and doxxed or physically harmed to stop their reporting on an issue.[25] The sale of these datasets also allows foreign adversaries to compile lists of sensitive locations that can be cross-referenced with other data to develop more granular insights into

[21] Opinion, *In the Matter of Cambridge Analytica, LLC.*, FTC File No. 9383 (Nov. 25, 2019), https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_opinionpublic.pdf/.

[22] *Id.; see also* Press Release, N.H. Dep't of Just. Off. of the Att'y. Gen., Voter Suppression AI Robocall Investigation Update, (Feb. 6, 2024), https://www.doj.nh.gov/news/2024/20240206-voter-robocall-update.html.

[23] DOJ NSD ANPRM, *supra* note 1, at 15781 (citing Richard Pérez-Peña & Matthew Rosenberg, *Strava Fitness App Can Reveal Military Sites, Analysts Say*, N.Y. Times (Jan. 29, 2018), https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html; Jeremy Hsu, *The Strava Heat Map and the End of Secrets,* WIRED (Jan. 29, 2018), https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy).

[24] *See* Press Release, FTC, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

[25] *See, e.g.*, Marina E. Franco, *Mexican president's dox of journalist shows perils of reporting in country*, Axios (Feb. 27, 2024), https://www.axios.com/2024/02/27/mexico-amlo-new-york-times-journalist; *see also* DOJ NSD ANPRM, *supra* note 1, at § I ("Countries of concern can also use access to U.S. persons' bulk sensitive personal data to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.").

Americans. For this reason, EPIC strongly recommends using a different system to determine what transactions are covered (rather than bulk thresholds) to ensure that as few location data points are exposed as possible.

C. Reputationally Damaging Information

Location data isn't the only kind of data that can derive or lead to inferences of reputationally damaging information, and by protecting a broader swath of data, DOJ can reduce the ability of bad actors to blackmail or otherwise influence individuals.[26] Location data can lead to reputationally damaging inferences, such as possible sexual partners.[27] However, information as innocuous as what time the smart lights turn on in an individual's home can let a bad actor know an individual's daily routine, facilitating stalking (physical harm) or possible robbery of an individual's home (financial harm).[28] The overarching impact of data broker transactions is that the data brokers become a hub for connecting different datasets to increase granularity of inferences that can be made, and often, the data brokers advertise based on this value add to the market.[29] DOJ will not be able to address reputationally damaging inferences that can be made about an individual unless it uses an expansive definition of personal data with appropriate de-identification procedures.[30]

[26] *See* ODNI SAG Report, *supra* note 15 ("In the wrong hands, sensitive insights gained through [commercially available information] could facilitate blackmail, stalking, harassment, and public shaming.").

[27] *See, e.g.*, Michelle Boorstein & Heather Kelly, *Catholic group spent millions on app data that tracked gay priests*, Wash. Post (Mar. 9, 2023), https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/; *see also* Jen Caltrider et al., *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*, Mozilla Found. (Sep. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.

[28] *See* Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. Times (Jun. 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html; Kashmir Hill, *Federal Regulator Questions Carmakers About Unwanted Tracking via Their Apps*, N.Y. Times (Jan. 11, 2024), https://www.nytimes.com/2024/01/11/technology/fcc-car-apps-stalking.html; Joseph Cox, *I Tracked an NYC Subway Rider's Movements with an MTA 'Feature,'* 404Media (Aug. 30, 2023), https://www.404media.co/i-tracked-nyc-subway-rider-home-omny-mta/.

[29] *See, e.g.*, Thompson Reuters, *Thomson Reuters CLEAR: The Smarter Way to Get Your Investigative Facts Straight* (2015), https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/legal/fact-sheet/clear-brochure.pdf.

[30] *Infra* Section II(b).

D. Genomic & Biometric Data

Genomic and biometric data can be used not only to target individuals, but acquiring this data also leads to impersonations which can create major security issues as well as financial harm, physical harm, national security issues, election interference, and a plethora of other issues. DOJ identified issues of using genomic data (genetic test results such as 23andMe) to target individuals such as combining genomic data with other datasets to re-identify individuals and identify exploitable health information.[31] Genomic data is also dangerous because it can be used to find individuals who are genetically related to the sample provider.[32] Inferences can also be made about an individual's health as well as other categories of data such as ancestry, allowing for more in depth profiling of individuals.[33] Allowing foreign adversaries to acquire genomic and/or biometric data (such as fingerprints and facial prints) can also create physical security issues. Bad actors can use legally obtained facial prints to bypass biometric security measures or create fraudulent identities.[34] Beyond security measures, though, impersonating an individual can lead to other harms such as election interference. The American election cycle is already experiencing deepfakes of political

[31] Executive Order 14117, *supra* note 2, at § 3(b).

[32] Nat'l Inst. of Just., *In-Brief: An Introduction to Forensic Genetic Genealogy Technology for Forensic Science Service Provide*rs 3 (Sept. 2022), https://forensiccoe.org/private/6320f16805925.

[33] *What Unexpected Things Might I Learn From 23andMe?*, 23andMe, https://customercare.23andme.com/hc/en-us/articles/202907980-What-Unexpected-Things-Might-I-Learn-From-23andMe (last visited Apr. 18 2024) (listing what consumers can expect from the results of a 23andMe genetic test, including health information, ancestry information, and connections to family members). *But see* Brian Resnick, *The limits of ancestry DNA tests, explained*, Vox (May 23, 2019), https://www.vox.com/science-and-health/2019/1/28/18194560/ancestry-dna-23-me-myheritage-science-explainer (discussing the limitations of genomic ancestry data, i.e., inferences about what geographical areas an individual's ancestors may have come from based on commonalities in genes between the test sample and the test company's database).

[34] Jessica Hallman, *Deepfakes expose vulnerabilities in certain facial recognition technology*, Penn St. Info. Sec. & Tech. (Aug. 11, 2022), https://www.psu.edu/news/information-sciences-and-technology/story/deepfakes-expose-vulnerabilities-certain-facial/.

candidates, and decisionmakers are scrambling to keep up with regulating the technology.[35] Individuals cannot avoid these harms short of undertaking extensive cosmetic surgery.[36] Even then, some data like genomic data is truly unchangeable, allowing a single data breach to haunt an individual for the rest of their life. Impersonations using voice prints or face prints can also lead to scams that exploit individuals for money—leading to psychological, relationship, and financial harms.[37] The ANPRM's focus on bulk thresholds to decide what transactions are covered would expose Americans to these various harms up to the bulk threshold defined by DOJ. While EPIC recommends a different approach to determining what transactions are covered,[38] at minimum EPIC urges DOJ to place lower thresholds on transmission of genomic and biometric data to ensure as much data is protected as possible.

E. AI Acceleration of Harms

DOJ rightly discusses the harms posed by artificial intelligence's ability to accelerate the harms already present from the mere existence of these datasets.[39] Artificial intelligence systems can speed up the re-identification process, link novel pieces of data that might not have otherwise been linked, make inferences based on the data, and perform many other functions.[40] AI can not only

[35] Matt O'Brien, *AI image generator Midjourney blocks images of Biden and Trump as election looms*, Associated Press (Mar. 13, 2024), https://apnews.com/article/midjourney-ai-imagegenerator-biden-trump-deepfakes-bc6c254ddb20e36c5e750b4570889ce1; *see also* N.H. Dept. of Just. Off. of the Att'y. Gen., *Voter Suppression AI Robocall Investigation Update*, (Feb. 6, 2024), https://www.doj.nh.gov/news/2024/20240206-voter-robocall-update.html.
[36] For example, Apple allows users to use its facial recognition software to recognize an individual even if the individual is wearing a facial covering. *Use Face ID While wearing a mask with iPhone 12 and later*, Apple Support, https://support.apple.com/en-us/102452 (last visited Apr. 18, 2024).
[37] *See, e.g.*, Charles Bethea, *The Terrifying A.I. Scam that Uses Your Loved One's Voice*, New Yorker (Mar. 7, 2024), https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice (describing an illegal robocall campaign where fraudsters created deepfakes of an individual's voice and called the individual's family members, pretending to harm the individual to ransom money from the family).
[38] *Infra* Section II(c).
[39] DOJ NSD ANPRM, *supra* note 1, at n.2–5 and accompanying text.
[40] *See generally* Luc Rocher, Julien M. Hendrickx, & Yves-Alexandre de Montjoye, *Estimating The Success of Re-Identifications in Incomplete Datasets Using Generative Models*, 10 Nature Commc'ns 3069 (2019), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6650473/.

assist on the back end, it can also generate mis/disinformation at scale.[41] EPIC applauds DOJ for stepping up and beginning the regulatory process in the face of these salient factors, but the ANPRM must go further to properly address privacy, civil rights, civil liberties, and national security concerns.

II. DOJ's Proposed Rules — Constrained by EO 141147 — Will Not Adequately Address Commercial Surveillance Harms and Are Inconsistent with Efforts by Other U.S. Regulators.

As EPIC has noted above, the commercial surveillance status quo is harmful to consumers and deeply unsustainable.[42] While DOJ's proposed rule would protect consumers from a very narrow set of commercial surveillance practices, it doesn't do enough. To be clear, EPIC understands that DOJ's ANPRM explicitly acknowledges the proposed rules are no substitute for a comprehensive data privacy law that protects consumers from the underlying commercial surveillance ecosystem.[43] However, as currently drafted, the ANPRM's piecemeal approach ignores documented harms from other countries and narrows the scope of enforcement. In short, this approach won't work. The types of data, the amount of data, the types of covered entities, the types of recipients—everything is laid out in excruciating and restrictive detail that creates unnecessary loopholes and renders privacy and national security protections inert. DOJ should simplify its ANPRM to be consistent with existing (and proposed) legislation to increase privacy, civil liberty, civil rights, and national security protections.

Below, EPIC sets out recommendations to broaden the definition of covered data to be more consistent with existing policy, to engage with the re-identification problem from a technology

[41] Tate Ryan-Mosley, *How generative AI is boosting the spread of disinformation and propaganda*, MIT Tech. Rev. (Oct. 4, 2023), https://www.technologyreview.com/2023/10/04/1080801/generative-ai-boosting-disinformation-and-propaganda-freedom-house/.

[42] *See supra* Section I.

[43] *See* DOJ NSD ANPRM, *supra* note 1, at 15783 ("The program is not intended as a commercial regulation of all cross-border data flows between the United States and our foreign partners, or as a comprehensive program to regulate Americans' data privacy.").

neutral approach, to apply the protections currently reserved for bulk transactions more broadly, and to provide means of reevaluating any list of countries of concern.

A. Broad Definitions of Sensitive Data Set Stronger Safeguards and are Consistent with Current Legislation.

The scope of data covered by DOJ's rulemaking should be broad and hinge on the data's connection to the data subject rather than possible exploitability by countries of concern. The definition of sensitive data should include data that is explicitly associated with a particular individual, household, or device as well as data from which it is possible to infer and/or derive the identity of a particular individual, household, or device.[44] When linked with other types of data, almost any type of data can lead to inferences about sensitive categories of information about an individual, so the scope of DOJ's rulemaking should cover a broad swath of personal data to ensure proper protection of privacy, civil rights, and civil liberties.[45] The ANPRM explicitly acknowledges the enhanced risk of identification from multiple, seemingly unrelated pieces of data in its definition of "covered personal identifiers[]" by covering listed identifiers in combination with other listed identifiers, even across multiple data sets.[46] The ANPRM further points to the risks of artificial intelligence accelerating the ability of entities to re-identify individuals from those linked data points, meaning that a broad definition of personal data is imperative to protect Americans from the harms stemming from covered transactions.[47]

[44] EPIC & US PIRG, *State of State Privacy* 22 (Feb. 2024), https://epic.org/wp-content/uploads/2024/01/EPIC-USPIRG-State-of-Privacy.pdf; EPIC FTC Comments, *supra* note 4, at 24.
[45] *See supra* note 27.
[46] DOJ NSD ANPRM, *supra* note 1, § III(b)(1).
[47] DOJ NSD ANPRM, *supra* note 1, § I (citing an ODNI report); *see infra* Section II(b).

Such strong definitions of personal data already exist at the state level, such as California[48] and Colorado's[49] enacted privacy laws. Proposed federal legislation[50] and enacted laws in the EU[51] and the UK[52] have incorporated similar expansive definitions of covered, personal data. In addition to broad, baseline safeguards for personal data, these laws also highlight uniquely sensitive categories of data, such as precise location data, where **additional** protections attach.[53] Generally, these categories of sensitive data that enjoy heightened safeguards include:

- government issued identifiers;
- health information;
- biometric and genetic data;
- financial information;
- sexual orientation and behavior;
- religious or philosophical belief;
- union membership;
- race and national origin; and
- children's information.[54]

[48] California Consumer Privacy Act, Cal. Civ. Code § 1798.140(o)(1) (2018) (personal information is "information that identifies, relates to, describes, is reasonably associated with, or could reasonably be linked, directly or indirectly, with a particular consumer"—this includes identifiers that could be linked with a particular household) [hereinafter "CCPA"].

[49] Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1303(17)(a) (2021) (personal data is "information that is linked or reasonably linkable to an identified or identifiable individual") [hereinafter "CPA"].

[50] ADPPA, *supra* note 13, at § 2(8)(A) (covered data is "information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual and may include derived data and unique identifiers"); Protecting Americans' Data from Foreign Adversaries Act of 2024, *supra* note 13, at § 2(b)(5) (personally identifiable sensitive information is "any sensitive data that identifies or is linked or reasonably linkable, alone or in combination with other data, to an individual or a device that identifies or is linked ore reasonably linkable to an individual.").

[51] Commission Regulation (EU) 2016/679, art. 4(1), 2016 O.J. (L 119) 1 (EU) (personal data includes "any information relating to an identified or identifiable natural person," including both direct and indirect identifiers).

[52] Data Protection Act 2018 c. 12 (Eng.) (defining personal data as "any information relating to an identified or identifiable living individual").

[53] *See, e.g.*, CCPA, *supra* note 48, at § 1798.121 (describing Consumers' right to limit use and disclosure of sensitive data).

[54] *See, e.g.*, *id.* at § 1798.140(ae) (defining sensitive personal information as including personal information that reveals social security, driver's license, state ID card, or passport number; account; log-in, financial account, debit or credit card number along with security/access code, password, or credentials allowing account access; precise geolocation; racial or ethnic origin, religious or philosophical belief, or union membership; contents of communications; genetic data; processing of biometric data for identification purposes; health data; and sex life or sexual orientation); *see also* CPA, *supra* note 49, at § 6-1-1303(24)(defining sensitive data as including personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status, genetic or biometric data used to identify an individual, or personal data from a known child).

EPIC applauds DOJ's inclusion of several of these types of sensitive data in its definition of "sensitive personal data" and "covered personal identifiers[,]"such as location data, financial transactions, and purchase history. However, EPIC urges DOJ to use a broad, baseline definition of covered personal data, by including the categories of data listed above as well as web browsing data and data that identifies or could lead to inferences about protected class membership.[55] The above list covers race, religion, and national origin directly, as well as sex, age, and disability status indirectly through the broader "health information" and "biometric and genetic data" categories. Although EPIC recommends explicitly covering each protected class in its definitions to ensure that this sensitive information cannot be used by countries of concern to discriminate against Americans.

Even recently proposed national security focused data broker legislation goes further than DOJ's current list of sensitive data categories, including information that identifies membership in a protected class, children's data, and web browsing information.[56] The Federal Trade Commission (FTC) has engaged in Section 5 rulemaking on commercial surveillance writ large[57] as well as a series of discrete enforcement actions against data brokers—signaling the Commission's interest in tackling major categories of sensitive data. In particular, the FTC has explicitly stated that web

[55] Title VII of the Civil Rights Act of 1964 (as amended) protects individuals from discrimination in employment settings based on race, color, religion, sex, or national origin. Civil Rights Act of 1964, 42 U.S.C. § 2000e *et seq; see also Bostock v. Clayton Cnty.*, 590 U.S. 644 (2020) (holding that gender identity and sexual orientation were covered under the definition of sex for the purpose of Title VII of the Civil Rights Act of 1964).
[56] Protecting Americans' Data from Foreign Adversaries Act of 2024, *supra* note 13, at § 2(e)(7)(N).
[57] *See supra* note 12.

browsing data[58] and health data[59] are sensitive categories of data. While web browsing data is not a traditional form of PII, the FTC pointed to the breadth of inferences about a person that can be made from web browsing data in a recent enforcement action, such as data points like a Google search for government jobs in Fort Meade, Maryland with a salary greater than $100,000 which could lead to an inference that the individual is looking for a job at the NSA.[60] In a similar vein, the Director of the FTC's Bureau of Consumer Protection directly stated that "consumer health data should be handled with extreme caution[,]" particularly in relation to the various health information related enforcement actions the Commission had taken on in the past few years.[61]

B. Present Day Technology Makes Re-Identification Inevitable, Efficient, and Accurate Which Necessitates Strong De-Identification Standards.

The advent of artificial intelligence has irrevocably made re-identification of individuals, devices, and households easier, quicker, and more accurate.[62] DOJ should create clear standards for anonymization and de-identification to lower the risk of re-identification.

[58] FTC, *FTC Cracks Down on Mass Data Collectors: A Closer Look at Avast, X-Mode, and InMarket* (Mar. 4, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/03/ftc-cracks-down-mass-data-collectors-closer-look-avast-x-mode-inmarket.

[59] Press Release, FTC, *Alcohol Addiction Treatment Firm will be Banned from Disclosing Health Data for Advertising to Settle FTC Charges that It Shared Data Without Consent* (Apr. 11, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/04/alcohol-addiction-treatment-firm-will-be-banned-disclosing-health-data-advertising-settle-ftc [hereinafter "FTC Monument Press Release"]; Press Release, FTC, *Proposed FTC Order will Prohibit Telehealth Firm Cerebral from Using or Disclosing Sensitive Data for Advertising Purposes, and Require it to Pay $7 Million* (Apr. 15, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/04/proposed-ftc-order-will-prohibit-telehealth-firm-cerebral-using-or-disclosing-sensitive-data.

[60] *FTC Cracks Down on Mass Data Collectors*, *supra* note 58.

[61] FTC Monument Press Release, *supra* note 59.

[62] Exec. Order No. 14,110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 88 Fed. Reg. 75191 (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence; *See* EPIC, Comment on the CFPB's Proposed Rule on the Small Business Advisory Review Panel for Consumer Reporting 14–15 (Oct. 30, 2023), https://epic.org/wp-content/uploads/2023/10/EPIC-CFPB-FCRA-SBREFA-Comment.pdf [hereinafter "EPIC CFPB Comments"] (citing Luc Rocher et al., *Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models*, 10 Nature Commc'ns 1, 2 (2019)).

Anonymization and de-identification are confusing and sometimes interchangeable terms, particularly in the advertising done by data brokers themselves.[63] As the ODNI Senior Advisory Group report on commercially available information emphasizes at length, information can be combined to "reverse engineer identities or deanonymize various forms of information," underscored by a *New York Times* project that deanonymized persistent location data on U.S. persons within minutes.[64]

To remove any ambiguity and to maximize the protection of privacy and national security, DOJ should define de-identification in clear, robust terms. The definition should also be tech-neutral to ensure flexible enforcement of a rapidly evolving field. DOJ should look to the following de-identified data standard, which EPIC has endorsed:

> "DE-IDENTIFIED DATA.—The term "de-identified data" means information that does not identify and is not linked or reasonably linkable to a distinct individual or a device, regardless of whether the information is aggregated, and if the covered entity or service provider—
>
> > (A) takes reasonable technical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual;
> >
> > (B) publicly commits in a clear and conspicuous manner—
> >
> > > (i) to process and transfer the information solely in a de-identified form without any reasonable means for re-identification; and
> > >
> > > (ii) to not attempt to re-identify the information with any individual or device that identifies or is linked or reasonably linkable to an individual; and

[63] *See, e.g.*, *Privacy Policy*, Outlogic, https://outlogic.io/privacy-policy/ (last visited Apr. 18, 2024) (defining de-identified data as "altered it in such a way that it cannot be linked to Personal Data" as well as later admitting to using the so-called de-identified information for marketing.); *see also* Michael D. Smith & Jim Waldo, *Anonymity, De-Identification, and the Accuracy of Data*, Harv. Online (Aug. 28, 2023), https://www.harvardonline.harvard.edu/blog/anonymity-de-identification-accuracy-data (discussing the differing definitions of anonymized and de-identified data under different statutes such as HIPAA, FERPA, and the U.S. Census Bureau's data standards.).

[64] ODNI SAG Report, *supra* note 15, at 5, 35; *see* Thompson & Warzel, *supra* note 7.

> (C) contractually obligates any person or entity that receives the information from the covered entity or service provider—
>
>> (i) to comply with all of the provisions of this paragraph with respect to the information; and
>>
>> (ii) to require that such contractual obligations be included contractually in all subsequent instances for which the data may be received."[65]

Finally, the inferences that can be made from publicly accessible information, particularly when cross-referenced with the data covered by the ANPRM, are not less sensitive than the inferences that can be made from non-public information, especially when gathered in bulk. From social media accounts to government licensing information to public county records, data brokers have access to unimaginable quantities of personal information on the internet at a minimal cost.[66] The ODNI explicitly calls out the threats that can arise from bad actors distorting publicly available information, particularly in conjunction with the use of artificial intelligence which can accelerate both the pace at which the data is collected and the speed and granularity with which the data is analyzed.[67] Publicly accessible information is a vast resource with which to cross-reference the data covered by the ANPRM to more easily re-identify individuals, households, and devices.[68] The unrestricted collection and dissemination of such information makes it all the more important to limit transactions of non-public data to minimize the total quantity of information being collected by countries of concern.

[65] ADPPA, *supra* note 13, at § 2(12).
[66] EPIC CFPB Comment, *supra* note 65, at 3–5 (listing the types of "insights" offered by data brokers).
[67] *See supra* Section I(e); *see also* Nat'l Intel. Council, *Assessment: Cyber Operations Enabling Expansive Digital Authoritarianism* 3 (Apr. 7, 2020), https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407--2022.pdf.
[68] DOJ NSD ANPRM, *supra* note 1, n.4–5 and accompanying text.

C. DOJ Must Not Limit Covered Transactions with Bulk Data Thresholds Because Time and Quantity Requirements are a Red Herring.

The ANPRM should not frame the scope of covered transactions through quantities of data over a certain time period because these limits create a logistical nightmare, explicitly condone harm up to a certain amount, and fail to meaningfully address the threats posed by present-day data reidentification capabilities. Instead, EPIC recommends regulating these transactions writ large, regardless of quantity and time frame.

EPIC is concerned that defining quantity and time limits will undermine effective enforcement. Although the proposed rule has laudable reporting and certifications, which—coupled with DOJ's enforcement authority—will hopefully have some deterrent effect, the quantity and time limits may invite gamesmanship. Though the rule may impede transfers in bulk, covered entities may be incentivized to sell data up to the very limit set by DOJ. And countries of concern will remain able stockpile data over a long period of time, albeit with some added friction. Similarly, time limits are not a useful measure for defining covered transactions because present day re-identification technology allows for data to be linked across datasets whether the data was collected within the same transaction or twelve months and one day apart.[69] Countries of concern, having stockpiled data over the course of years, can obtain the same highly detailed picture of sensitive information by cross referencing or combining datasets. Therefore, if DOJ decides to use bulk thresholds, it should not include a time limit. DOJ should instead rely on total quantity of data provided to the recipients.

[69] *See supra* Section II(b).

D. The EO's focus on "countries of concern" will make this regime difficult to enforce and is inconsistent with efforts by other U.S. regulators.

This EO and proposed rule reflect, as CFPB Chair Rohit Chopra noted recently, an "emerging consensus that intrusive surveillance and aggregation of personal data can create the conditions for harming national security and undermining freedom."[70] However, this EO framework does not reflect the consensus among Congress and other regulators, who have generally focused on collection and sale more broadly, rather than individual recipients of that data. The EO and proposed rule's focus on a limited number of "countries of concern" will make this framework difficult to effectively enforce.

According to the proposed rule, DOJ is considering adopting the EO's definition of "country of concern" without elaboration or amendment.[71] In a similar context, the Department of Commerce identified the following countries as "having engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of the United States": the People's Republic of China, along with the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau; the Russian Federation; the Islamic Republic of Iran; the Democratic People's Republic of Korea; the Republic of Cuba; and the Bolivarian Republic of Venezuela.[72] As an initial matter, the proposed rules also do not include any indication of how this list of "countries of concern" may be updated or modified. EPIC recommends that at a minimum, the government must set out clear criteria for the evaluation—and reevaluation—of covered and non-covered countries to ensure proper coverage, and that DOJ proposed rules should create space for such reevaluation. However, as discussed below, EPIC believes that short of

[70] Rohit Chopra, Dir., CFPB, Prepared Remarks at the White House on Data Protection and National Security (Apr. 2, 2024), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-at-the-white-house-on-data-protection-and-national-security/.

[71] *See* DOJ NSD ANPRM, *supra* note 1, Sec. E.

[72] *Id.*

a comprehensive law protecting consumers' data, a better approach is a tiered approach to foreign data exports based on a more robust list of criteria.[73]

More fundamentally, by cabining these rules to a short list of "countries of concern" the EO and proposed rule ignores the much more pervasive ecosystem of foreign countries and actors taking advantage of commercial surveillance. For example, this framework would not cover many of the entities based in other countries who have been known to facilitate surveillance of Americans, whether through purchase of commercial information or the deployment of advanced surveillance technology such as spyware.[74] This framework would likewise do nothing to protect Americans from having their sensitive personal data purchased from such entities, including those linked to authoritarian governments like Saudi Arabia and the United Arab Emirates. Similarly, this framework does not apply to many of the countries that have regularly engaged in transnational repression, including digital repression, despite the clear links between access to sensitive personal data and repressive tactics.[75] And finally, unlike similar regulatory approaches proposed by Congress,[76] it does not take into consideration the adequacy and enforcement of a given country's data protection, surveillance, and export control laws, meaning that it does not apply to many

[73] *See infra* notes 87–90 and accompanying text.
[74] *See, e.g.*, Joseph Cox, *Inside a Global Phone Spy Tool Monitoring Billions*, 404Media (Jan. 24, 2024), https://www.404media.co/inside-global-phone-spy-tool-patternz-nuviad-real-time-bidding/ (reporting on an Israeli startup collecting data from billions of users through real-time bidding to package and sell for surveillance); Byron Tau & Dustin Volz, *How Ads on Your Phone Can Aid Government Surveillance*, Wall St. J. (Oct. 13, 2023), https://www.wsj.com/tech/cybersecurity/how-ads-on-your-phone-can-aid-government-surveillance-943bde04 (reporting on an India-based data broker collecting and selling geolocation data derived from advertising networks); U.S. Gov't Accountability Off., GAO-24-106183, *Human Rights: Agency Actions Needed to Address Harassment of Dissidents and Other Tactics of Transnational Repression in the U.S*. 10 (2023), https://www.gao.gov/assets/D23106183.pdf ("The United Arab Emirates used a messaging application downloaded by millions worldwide, including some in the U.S., to surveil and track users in 2019.") [hereinafter "GAO TNR Report"].
[75] *See Protecting Americans' Private Information from Hostile Foreign Powers Before the Sen. Jud. Subcomm. on Privacy, Tech., & L.*, 117th Cong. (2022), https://www.judiciary.senate.gov/imo/media/doc/Testimony - Klein - 2022-09-14.pdf (statement of Adam I. Klein, Dir., Robert Strauss Ctr. on Int'l Sec. & L. Univ. of Texas at Austin) (emphasizing the link between transnational repression and lax data controls in the context of China). *See generally* GAO TNR Report, *supra* note 74.
[76] *See infra* notes 88–90 and accompanying text.

countries that have acted as havens for surveillance pass-throughs in other contexts (such as with spyware), or protect against a much broader set of privacy and nationals security harms, such as blackmail, extortion, or other exploitation for foreign intelligence purposes.[77]

Limiting the proposed rule to these countries of concern also makes effective enforcement all the more difficult. EPIC recognizes that implementation of know-your-customer obligations is a step in the right direction. Researchers at Duke University have found that data brokers "conduct varying degrees of know-your-customer due diligence: some appear to conduct some due diligence before initiating a data purchase agreement, some appear to conduct a little due diligence, and some appear to conduct none at all. For those that appear to conduct some due diligence, it is unclear how comprehensive that vetting is in practice."[78] 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."[79] Therefore, to the extent this proposed rule—and threatened enforcement actions—shifts data brokers' incentives toward meaningful controls, that is a step in the right direction.

However, even if data brokers are incentivized to know their initial customers, these controls are likely to be difficult to effectively enforce at various degrees of separation, especially across countries and jurisdictions. Ultimately, without some baseline level of protection against the collection and sale of this sensitive personal data—to anyone—it will be hard to prevent this shell game. EPIC recommends DOJ advocate for broader regulation in order to mitigate these risks.

[77] *Id.*
[78] *See 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).
[79] *Id.*

Nonetheless, by focusing on only certain "countries of concern," these piecemeal restrictions are likely to make enforcement difficult in practice.

Because of the sheer scale of the data protection crisis facing American consumers[80]— itself due to the failure to pass a comprehensive privacy law and continued reliance on weaker, piecemeal regulations—other U.S. regulators have focused on setting forth broad rules on the collection, use, and sale of personal data. For example, in the FTC's commercial surveillance rulemaking and other actions, the Commission has focused more broadly on the collection and use of personal data rather than the sale or transfer to particular entities.[81] Even where the FTC has focused specifically on the data broker ecosystem, it has generally focused on the broad sale and transmission of personal data, not on that sale and transmission to particular third parties.[82]

Similarly, the Consumer Financial Protection Bureau (CFPB)'s contemplated regulations for the Fair Credit Reporting Act (FCRA) are not concerned with the identity of the purchaser or recipient.[83] FCRA delineates the permissible purposes for which a consumer report can be furnished and limits how that consumer report information can then be used.[84] This broader, purpose-based approach embodied in FCRA and carried out by the CFPB are consistent with other purpose-based approaches adopted by the FTC.

[80] *See supra* Section I.

[81] *See, e.g.*, Lina M. Khan, Chair, FTC, Statement Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking (Aug. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Statement%20of%20Chair%20Lina%20M.%20Khan%20on%20Commercial%20Surveillance%20ANPR%2008112022.pdf (detailing the FTC's focus on collection and use of personal data).

[82] Notably, however, one area in which the FTC has drawn a distinction is the sale of sensitive personal data to U.S. government contractors for national security purposes. *See* Complaint, *In the Matter of X-Mode Social, Inc.*, FTC File No. 202-3038 5 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-Complaint.pdf.

[83] EPIC CFPB Comment, *supra* note 65, at 7 (noting FRCA's purpose-based approach to regulation of data collection, sales, and retention).

[84] 15 U.S.C. § 1861(b).

Congress has also generally focused on passing a comprehensive federal privacy law that would address the collection, use, and sale of personal data rather than its transfer to particular classes of third parties.[85] Even where Congress has introduced legislation focusing on sales and transmissions of personal data to foreign entities, its focus has generally been broader.[86] For example, while The Protecting Americans' Data from Foreign Surveillance Act targets exports of personal data to high-risk countries, it seeks to create a tiered system. Under this system, identified low-risk countries would not need an export license for covered personal data, while identified high-risk countries would be subject to presumptive denial of an export license.[87] The bill does not contain a specific list of high-risk countries, but rather calls for an evaluation based on several criteria, including:

- "the adequacy and enforcement of the country's privacy and export control laws";[88]
- "the circumstances under which the foreign government can compel, coerce, or pay a person in that country to disclose personal data";[89] and
- "whether that foreign government has conducted hostile foreign intelligence operations against the United States."[90]

[85] *See, e.g.*, ADPPA, *supra* note 13. Even at the state level, data broker bills focus on collection and sale rather than focus narrowly on foreign actors. *See, e.g.*, CCPA *supra* note 48. One area where Congress—and several states—have been particularly active of late in focusing on sales to particular entities is on the *U.S. government's* purchase of sensitive information. *See* Derek B. Johnson, *House passes bill to limit personal data purchases by law enforcement, intelligence agencies*, Cyberscoop (Apr. 17, 2024), https://cyberscoop.com/house-passes-4th-amendment-is-not-for-sale-act/. However, this distinction between U.S. intelligence and law enforcement agencies and other recipients is appropriate because there are *already* constitutional and statutory rules restricting the government's ability to acquire certain information.

[86] *But see* Protecting Americans' Data from Foreign Adversaries Act of 2024, *supra* note 13 (seeking to apply many of the same restrictions contained within these proposed rules, though through FTC enforcement).

[87] Protecting Americans' Data From Foreign Surveillance Act of 2022, S. 4495, 117th Cong. § 3 (2022).

[88] *Id.*

[89] *Id.*

[90] *Id.*

In addition to these categories, all other countries would require a license, essentially creating a tiered data protection system rather than the piecemeal system set forth in the EO and DOJ's proposed rules.[91] Although EPIC recognizes that DOJ's proposed rules are constrained by EO 14117, EPIC recommends that DOJ not simply adopt the EO definition of "countries of concern" without amendment, but rather flesh out a broader set of criteria by which DOJ will evaluate and reevaluate risk.

Ultimately, by scoping this order to "countries of concern" but leaving untouched data sales to other countries and the United States government itself, this framework implicitly entrenches the legitimacy of those unregulated sales. While other U.S. regulators are focused on reining in the data broker industry and the commercial surveillance system at a foundational level, the EO framework—coupled with other public opposition to consistent protections[92]—indicates an unfortunate and disappointing unwillingness by some government agencies to divorce themselves from the data broker industry.

III. 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, 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 DOJ for beginning to acknowledge the harms of unchecked surveillance capitalism but remains disappointed

[91] *Id.*

[92] White House, *The SAFE Act Raises Profound Risks for National Security and Public Safety* (2024), *available at* https://www.eff.org/files/2024/04/04/white-house-four-pager-on-the-durbin-lee-bill-to-re-up-section-702_1.pdf; OMB, *Statement of Administration Policy: H.R. 4639 — Fourth Amendment Is Not For Sale Act* (Apr. 16, 2024), (opposing a House bill to regulate U.S. intelligence and law enforcement agencies' purchase of certain personal data, in part because the bill "does not affect the ability of foreign adversaries or the private sector to obtain and use the same information.").

by this ANPRM’s overly narrow focus and its continued opposition to legislative safeguards on the U.S. government’s own purchase of sensitive data. DOJ and the Biden administration should take advantage of this opportunity to chart a new course. EPIC looks forward to engaging with DOJ further on these urgent issues, and we stand by to assist your agency however we can.

Respectfully submitted,

Jeramie Scott
Jeramie Scott
EPIC Senior Counsel
Director of the EPIC's Project on Surveillance Oversight

Chris Baumohl
Chris Baumohl
EPIC Law Fellow

Maria Villegas Bravo
Maria Villegas Bravo
EPIC Law Fellow