1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

Friday, April 19, 2024

Via Electronic Submission

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

Re: Advance Notice of Proposed Rulemaking, "Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern" (Docket No. NSD 104)

Dear Mr. Licata,

We are pleased to provide comments on behalf of the Future of Privacy Forum (FPF) to the Department of Justice (DOJ) regarding the Advance Notice of Proposed Rulemaking on Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern (ANPRM).[1] FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of privacy and emerging technologies.[2] FPF is focused on advancing responsible data practices and provides expertise in data protection law and policy, including the privacy implications of cross-border data transfers.

FPF supports the core objectives of the ANPRM, which would seek to protect Americans' sensitive personal data from access, exploitation, and misuse by countries of concern, while upholding the "longstanding U.S. policy to promote trusted cross-border data transfers among partners that respect democratic values and the rule of law." We support a balanced approach to these goals that respects cross-border data flows while avoiding the unintended consequences of data localization legal frameworks.[3]

---

[1] Proposed Rule, 89 FR 15780, National Security Division, Department of Justice (March 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

[2] The views expressed herein do not necessarily represent the views of our Advisory Board or supporters.

[3] *See* Future of Privacy Forum, Financial Data Localization: Conflicts and Consequences (December 7, 2017), https://fpf.org/blog/financial-data-localization-info-graphic-conflicts-and-consequences/.

Ultimately, significant progress toward the noted objectives of the ANPRM could be achieved by a federal privacy law that would establish comprehensive data protection safeguards for all sensitive and non-sensitive personal information. However, to the extent that the current relative lack of regulation creates opportunities for data flows that threaten national security, we agree that other legal frameworks focused on government access, including by foreign adversaries, must increasingly address the fundamental issues raised by private sector data.

Although the proposed rule narrowly targets bulk sensitive data transfers to countries of concern, American organizations typically attempt to align their internal compliance programs with common definitions of "sensitive data" across legal regimes. Today, organizations are building and operating compliance programs based on existing definitions of "sensitive data" and related terms. As a result, the best way to accomplish the proposed rule's aims, in keeping with the DOJ's goal of "minimizing disruption to commercial activity" is to harmonize, to the extent possible, the core definitions of the DOJ's rulemaking with leading U.S. privacy frameworks and ensure that they provide sufficient protections for U.S. individuals and clarity for businesses.

In support of these rulemaking objectives and in furtherance of our general recommendations, FPF specifically recommends that the DOJ:

1) Broaden and clarify the definition of "precise geolocation data" to ensure that it applies to emerging technologies, offers sufficient protection for individuals, and harmonizes with leading U.S. frameworks. (Question 10)

2) Clarify and streamline the extent to which the scope of "U.S. device" and U.S. person" align with core definitions in leading data protection regimes, including in its relation to legal entities, households, and non-living persons. (Questions 22-25)

3) Clarify the intent and scope of the prohibition on "data brokerage" to countries of concern or covered persons, including through an advisory opinion process that could put US companies on notice of specific practices that threaten national security. (Questions 22, 24, 39, and 57)

4) Clarify the scope of exemptions for financial services, payment-processing, and regulatory-compliance-related transactions to avoid excluding a broader set of routine business activities than intended. (Questions 43-44)

We encourage the DOJ to proactively engage with consumer privacy and data protection experts as the agency develops its rules in order to maximize their effectiveness across sectors. In aligning with ongoing data protection efforts, the DOJ can ensure that the final rules are carefully tailored to address national security concerns and increase much-needed due diligence efforts across sectors, while avoiding subjecting U.S. companies to bureaucratic requirements that are not accompanied by sufficient protections for sensitive data.

1. ***Broaden and clarify the definition of "precise geolocation data" to ensure that it applies to emerging technologies, offers sufficient protection for individuals, and harmonizes with leading U.S. frameworks.*** (Question 10)

The ANPRM proposes defining "precise geolocation data" as *"data, whether real-time or historical, that identifies the physical location of an individual or a device with a precision of within [number of meters/feet] based on electronic signals or inertial sensing units"* and seeks comment on the preferred level of precision and alignment with state laws. (Question 10).

We recommend that a final definition omit the language of "based on electronic signals or inertial sensing units" in favor of a more flexible, technology-neutral definition that aligns with leading U.S. frameworks and companies' existing data mapping efforts. Such an approach is necessary to protect additional sources of precise geolocation collected from Americans. As technology advances, the number of means and methods that can be used to identify or track an individual's precise location over time has only grown. The phrasing of the current definition in the ANPRM reflects the fact that much of the current commercial marketplace relies on location data derived from smartphone apps.[4] Indeed, most precise geolocation data from apps is derived from operating system APIs that interpret electronic, inertial, and other sensors built into modern smartphones, including e.g. Wi-Fi networks and cell tower triangulation.

However, commercially available sources of geolocation data are not limited to mobile apps. Datasets consisting of precise geolocation data on Americans can also be derived from more traditional means, such as metadata attached to transactions and photographs, as well as more cutting-edge methods, such as video-based automated license plate recognition (ALPR), light proximity, signals sent by internet-connected devices and sensors, and data from vehicles. No matter where it is pulled from, location data can be just as high-risk and subject to exploitation, abuse, or mis-handling. Some of these may be included in the current definition, while others

[4] *See* Jon Keegan and Alfred Ng, The Markup, *There's a Multibillion-Dollar Market for Your Phone's Location Data* (September 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

arguably would not, and the uncertainty itself over the phrase "electronic signals" (which does not appear in privacy laws) could itself lead to commercial disruption and gaps in protections.

In creating a workable definition of "precise geolocation data," DOJ should reference leading frameworks from U.S. privacy laws. In most or all, if specific technologies are included, they are included as non-exhaustive examples ("including, but not limited to"). FPF has compiled **Table 1 (below)** to provide more information on how that definition has been drafted in comprehensive privacy laws passed by U.S. state legislatures. In addition, companies often look to self-regulatory guidance and FTC enforcement decisions that largely mirror these same frameworks.[5]

Table 1. Definitions of Precise Geolocation Data in Leading U.S. Frameworks

Source	Connecticut	California	Washington
Definition	**"Precise geolocation data"** means "information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet. 'Precise geolocation data' does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility." Conn. Gen. Stat. § 42-515(19).	**"Precise geolocation"** means "any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations." Cal. Civ. Code § 1798.140(w).	**"Precise location information"** means "information derived from technology including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. 'Precise location information' does not include the content of communications, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility." Wash. Rev. Code § 19.44.28(3)(19) ("My Health My Data Act").

[5] *See* Stacey Gray and Pollyanna Sanderson, Future of Privacy Forum, *Location Data Under Existing Privacy Laws* (Dec 2020), https://fpf.org/wp-content/uploads/2020/12/FPF_Guide_Location_Data_v2.2.pdf. More recently, FTC settlements with location data brokers may offer helpful definitions of "location data." *See, e.g.*, Federal Trade Commission, X-Mode Social, Inc., Decision and Order (April 11, 2024).

Finally, the ANPRM specifically seeks comment on the level of precision (e.g. a radius of 1,850 feet or 1,750 feet). In general, the concept of "precision" in geolocation data is inherently challenging, because the level of precision that is sufficient to identify or reveal information about a person often depends on many factors, including the specific location, population density (i.e., a rural vs. urban area), level of accuracy, and the presence and detail of a timestamp.[6] Additional sensitive locations (such as home and work, overnight "dwell" locations, and locations such as healthcare facilities or religious places of worship) can also increase the identifiability or the sensitivity of a dataset.

Today, a common industry practice is to redact a latitude-longitude to a precision of two decimal places, which approximately (if imperfectly) coincides with the geographic boundaries established in state laws (e.g. 1,850 feet). These complexities offer another good reason for the DOJ to seek to align with state laws and existing data mapping efforts of U.S. companies, while giving flexibility to address higher risk datasets in unusual cases.

2. ***Clarify and streamline the extent to which the scope of "U.S. device" and U.S. person" align with core definitions in leading data protection regimes, including in its relation to legal entities, households, and non-living persons.*** (Questions 22-25)

The ANPRM proposes defining "U.S. device" to mean "*any device that is linked or linkable to a U.S. person*," while maintaining the definition of "U.S. person" to include individuals or entities, including any "United States citizen, national, or lawful permanent resident; or any individual admitted to the United States as a refugee . . . or granted asylum . . . or any entity organized solely under the laws of the United States . . . or any *person* in the United States."

It's worth noting that the term U.S. person, which is well-established in U.S. national security law, is probably less familiar to commercial privacy practitioners, who are accustomed to the equally well-established concepts of "personally identifiable information," "data subject," "individual" or "consumer" under global, state, and federal privacy laws. Given the potential divergence between these key terms and the integral role they play in core data mapping and governance practices at the heart of compliance with the DOJ's framework, we recommend aligning the concepts as much as possible and clearly noting the extent to which they diverge. FPF has included Table 2 (below) to provide more information on how leading frameworks define personal information.

[6] Network Advertising Initiative (NAI), Guidance for NAI Members: Determining Whether Location is Imprecise (Feb 2020), https://thenai.org/wp-content/uploads/2021/07/nai_impreciselocation2.pdf.

For example, DOJ should consider:

- ***Limiting protections only to natural persons.*** Leading data protection laws establish protections only for information related to natural persons, and do not typically protect information collected about legal entities, such as businesses, institutions, or non-profits. In contrast, the term "U.S. person" in the ANPRM has a much broader scope. As a result, the ANPRM risks creating a significant new compliance burden that will be 1) novel for in-house privacy experts and 2) not necessarily bring concurrent privacy safeguards that would address the core concerns raised in the ANPRM regarding countries of concern "track[ing] and build[ing] profiles on U.S. individuals," or "collect[ing] information on activists, academics, journalists, dissidents, political figures, or [others]."
- ***Expressly including protections for households.*** In most cases, leading U.S. and global data protection laws provide protections for data related to households (for example, residential utility usage). In U.S. privacy laws, household data is often, but not always, expressly included by statute. In laws that do not expressly refer to households, such data is often included anyway insofar as most household-level information is related to specific identified or identifiable persons. While there may be some examples of household data that is not linked or linkable to specific persons, the DOJ should make it clear that when it is, household-level information would be similarly protected.
- ***Expressly excluding protections for non-living persons.*** The definition of personal data under EU's General Data Protection Regulation (GDPR) does not extend to non-living persons, although individual member states in the EU can choose to extend such protections.[7] Similarly, U.S. privacy laws typically protect only living individuals.

Table 2. *Definitions of Personal Data in Leading Frameworks*

Source	**GDPR**	**Colorado**	**Virginia**
Definition of Personal Data (Or Equivalent)*	**"Personal data"** is defined as "any information relating to an identified or identifiable natural person ('data subject')." GDPR Art. 4(1).	**"Personal data"** is defined as "information that is linked or reasonably linkable to an identified or identifiable individual" and "does not include de-identified data or publicly available information." Colo. Rev. Stat. § 6-1-1303.	**"Personal data"** is defined as "any information that is linked or reasonably linkable to an identified or identifiable natural person," and "does not include de-identified data or publicly available information." Va. Code § 59.1-575.

[7] Recital 27, General Data Protection Regulation (GDPR), https://gdpr-info.eu/recitals/no-27/.

3. ***Clarify the intent and scope of the prohibition on "data brokerage" to countries of concern or covered persons, including through an advisory opinion process that could put US companies on notice of specific practices that threaten national security.*** (Questions 22, 24, 39, and 57)

The DOJ proposes a general prohibition, subject to authorized exemptions, on any U.S. person "knowingly engag[ing] in a *covered data transaction* with a *country of concern* or *covered person*," and seeks comment on the feasibility of contracting with prospective customers to prevent pass-through sales, re-sale, or onward transfer of bulk U.S. sensitive personal data to countries of concern or covered persons. (Question 39). Under the proposed framework, *covered data transactions* would include "data brokerage," and the DOJ specifically seeks comment on ways to enhance the term's clarity or address elements of the data brokerage ecosystem that are not covered by the term as currently defined (Questions 22 and 24). Finally, the DOJ seeks comment on the potential role of interpretive guidance (Question 57).

Overall, the proposed definition of "data brokerage" expands significantly beyond both common understandings of the term and the leading statutory definitions in U.S. state laws. For example, California's Data Broker Registration Statute defines "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."[8] In contrast, the DOJ has proposed a definition of "data brokerage" to include "the transfer of data from any person (the provider) to any other person (the recipient), where the *recipient* did not collect or process the data directly from the individuals linked or linkable to the collected or processed data." (emphasis added).

While a broad definition may serve the national security interests articulated in the ANPRM, its breadth will encompass a very wide range of routine commercial activity. As a result, the current definition could provoke a modest increase in overall due diligence with respect to all or nearly all transfers of personal data in the United States. Given the additional compliance obligations that this would require, the definition and its coinciding requirements should be carefully tailored and clear in both intent and scope.

In this context, we recommend further analysis into the relative prevalence of *deliberate and knowing* sales of bulk sensitive data on Americans to countries of concern, as compared to

[8] California Department of Justice, Data Broker Registry, https://oag.ca.gov/data-brokers. *See also*, California SB-362 (Data broker registration), *available at* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB362.

transfers of data through open and unrestricted marketplaces, either unknowingly or incidentally, though perhaps with equal risk to the individual or the state. Restricting the former is a clear objective of the ANPRM. We recommend further clarification regarding if and to what extent activities constituting the latter are also meant to fall within scope of the DOJ's intended objectives. For more information, here are two potential regular commercial transactions that DOJ should consider:

- ***Auction-based digital ad exchanges.*** Much of the current online advertising ecosystem relies on relatively open, auction-based systems for delivering targeted advertising across platforms and devices. It has been demonstrated that companies can scrape large amounts of bulk information on U.S. devices from digital advertising exchanges through participation in real time bidding auctions.[9] However, a company that participates in an exchange may not be purchasing or licensing bulk data directly, and therefore may not fall under the auspices of "data brokerage." The DOJ should directly address whether these kinds of arrangements are meant to be within scope of the term "data brokerage," and if so, require clear and specific due diligence measures.
- ***First-party targeting***. Platforms with access to large amounts of consumer-facing data may offer advertisers the ability to target personalized content to their users.[10] Unlike in an open exchange, however, advertisers may not receive direct access to underlying data, receiving instead, for example, an aggregated report of impressions and overall ad effectiveness. Nonetheless, under some interpretations, the data has been "accessed" in the sense that users have been targeted or influenced. The DOJ should directly address whether this scenario is within the intended scope.

In the context of companies that abuse the restrictions in open commercial marketplaces, contractual limitations are typically not sufficient. As a result, we caution that the ANPRM risks adding a compliance burden for U.S. companies without any accompanying increase in protections for sensitive personal data. The DOJ could more effectively enforce additional due diligence protections, including through technical means, by clarifying the intent and scope of the data brokerage prohibition – for example, by tailoring it more closely to a typical definition of "data broker" in the United States, by clearly including (or excluding) situations that involve

---

[9] *See* Office of Senator Ron Wyden, Press Release, *Wyden, Bipartisan Senators, Question Online Ad Exchanges on Sharing of Americans' Data with Foreign Companies* (April 2, 2021), *available at* https://www.wyden.senate.gov/news/press-releases/wyden-bipartisan-senators-question-online-ad-exchanges-on-sharing-of-americans-data-with-foreign-companies

[10] *See, e.g.*, Meta Business Help Center, *About Custom Audiences* (last accessed April 19, 2024), https://www.facebook.com/business/help/744354708981227?id=2469097953376494

access to platforms without intentional sales, or providing a greater number of clear examples that address digital advertising use cases.

Finally, we are optimistic about the potential role that an advisory process could play with respect to these specific provisions, given their broad scope and the critical role of the knowledge standard. (Question 57) For example, the DOJ could put companies on notice of specific known bad actors, or of specific practices, such as bidstream data scraping, that participating companies *should* know are leading to transfers of data to countries of concern. In particular, business practices related to advertising are evolving rapidly in response to platform and regulatory pressures.[11] An advisory process may help ensure that regulations remain effective over time.

4. ***Clarify the scope of exemptions for financial services, payment-processing, and regulatory-compliance-related transactions to avoid excluding a broader set of routine business activities than intended.*** (Questions 43-44)

Among other exemptions, the proposed rules would exempt transactions "to the extent that they are ordinarily incident to and part of the provision of financial services," including banking, capital markets, financial insurance services, or transactions required for federal regulatory compliance, and seeks comments on any modifications that could be made to enhance clarity and prevent unintended consequences (Questions 43-44).

In keeping with the objectives of the ANPRM, we recommend that the final rules clearly articulate the boundaries of the financial exemption to ensure that it does not unintentionally include emerging consumer-facing products and services that are financial in nature but not regulated similarly to banks and financial institutions. For example, data derived from personal budgeting or shared expense apps like YNAB ("You Need a Budget"), PocketGuard, or Splitwise, could be considered "financial" but may not be intended to fall into this exemption.

Similarly, the current exemption for "regulatory-compliance-related transactions" exempts transactions that are incident to and part of compliance with "any Federal laws and regulations," and provides a list of laws and regulations such as the Bank Secrecy Act and the Securities Act of 1933. The broad phrasing and non-exhaustive list suggests that this would include compliance with other laws, such as anti-money-laundering (AML) laws, the Know-Your-Customer provisions of Title III of the Patriot Act, as well as to compliance with credit reporting and identity theft

[11] *See* Stacey Gray, Future of Privacy Forum, *Examining Novel Advertising Solutions: A Proposed Risk-Utility Framework* (April 1, 2024), https://fpf.org/blog/examining-novel-advertising-solutions-a-proposed-risk-utility-framework/.

regulations under the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act of 2003 (FACTA). For example, the furnishing of credit reports, the notification of an adverse action taken based on information in a credit report, and similar activities, while they may be incidental to compliance with FCRA, may create risks for American consumers if the underlying data were to be accessed by countries of concern. The final rules should clarify the specific boundaries of the exemption.

In all of the above considerations, we recommend that the DOJ engage with the privacy and data protection community, including compliance-oriented practitioners, as well as academics, consumer protection enforcers and policymakers. We welcome further engagement and would be happy to follow up on any of our recommendations.

Sincerely,

Stacey Gray, *Senior Director, US Policy, Future of Privacy Forum*
Amie Stepanovich, *VP of US Policy, Future of Privacy Forum*
Ryan Campbell, *Spring 2024 US Policy Intern, Future of Privacy Forum*

Please contact: info@fpf.org