CENTER FOR DEMOCRACY & TECHNOLOGY

April 19, 2024
Via regulations.gov

Re: Department of Justice 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

CDT is a non-partisan, non-profit organization that works to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. For over a decade, we have worked to rein in the conduct of data brokers who threaten individual privacy, while at the same time ensuring that rights to free expression are protected.

We appreciate the opportunity to comment on the data broker advanced notice of proposed rulemaking (ANPRM).[1] We generally support the DOJ's goals—reducing the ability of countries of concern to collect and exploit US individuals' data. The comments below discuss concerns with and reactions to various definitions, prohibited transfers to individuals, onward transfers of data, and statutory authority.

I. Definitions

Data brokerage. CDT supports the data brokerage definition. The ANPRM proposes the following definition for data brokerage: "sale of, licensing of *access* to, or similar commercial *transactions* involving 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."

This definition appropriately scopes "data broker" activities to any entity that sells data about individuals where the recipient did not collect data directly from the relevant individuals. In other contexts, definitions of data brokers exempt companies that have a direct relationship with individuals.[2] That requirement can be gamed by data brokers: they may send emails directly to people in their databases, or may offer a "right of access" to all individuals about which they store data, thereby creating such a "relationship" and then avoiding entirely any restrictions that would otherwise be imposed on data brokers.

---

[1] Advance Notice of Proposed Rulemaking, Department of Justice, Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, Docket No. NSD 104 (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

[2] *See, e.g.*, DELETE Act, H.R. 4311, Section 2(f)(3), https://www.congress.gov/bill/118th-congress/house-bill/4311/text.

Other definitions of data brokers require a certain income share threshold from the sale of data.[3] That may work in some settings, as sometimes companies only earn a small percentage of their revenue from selling data. However, given the larger national security issues at stake in wanting to prevent data about US individuals from being sent to countries of concern, it is appropriate not to have a revenue share limit.

Sensitive personal data. We generally agree with the scope of sensitive personal data in the ANPRM. It includes many of the most important types of data that we have long felt were sensitive, including health and financial data, location data, identification numbers, biometrics, and demographic data. The DOJ could consider including some other types of data that are commonly defined as sensitive, such as data regarding children under 17, calendar information, address book information, and photos and videos of people.[4] Children's data, for example, may be of concern in the counterintelligence context because a government official or another person with access to classified information may be particularly vulnerable to pressure in the face of threats to release denigrating or embarrassing information about their child.

Bulk thresholds. The DOJ should adopt the lower bounds of the proposals for what counts as bulk data. The goal of this proceeding is to prevent as much information about US individuals from being sold to countries of concern. To best achieve that goal, and to best protect people's privacy generally, the bulk definition should be as low as reasonably possible.

We know that data brokers often traffic in the data with which the ANPRM is most concerned. In recent comments, CDT described in detail the various ways data brokers collect and monetize financial data, workers data, health data, location data, and publicly available data.[5] Limiting the sales of those and other types of personal data to countries of concern will best protect people's privacy and the nation's security interests.

Biometric and location information is particularly sensitive, and the bulk threshold should be as low as possible, and not higher than records of more than 100 people. Biometric data is immutable, it cannot be changed. Breaches and other misuse of this data, or the data ending up in the wrong hands, cause extensive harm to people, who will have limited options to make themselves whole. That is in part why laws in the U.S. are particularly protective of such data.[6]

---

[3] American Data Privacy and Protection Act, H.R. 8152, Section 2(36), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.
[4] Protecting Americans' Data from Foreign Adversaries Act of 2024, H.R. 7520, Section 2(c)(7), https://www.congress.gov/bill/118th-congress/house-bill/7520/text.
[5] Comments of Center for Democracy & Technology, Consumer Financial Protection Bureau Request for Information Regarding Data Brokers, Docket No. CFPB-2023-0020, https://cdt.org/wp-content/uploads/2023/07/CDT-Comment-to-CFPB-on-Data-Brokers-CFPB-2023-002054.pdf.
[6] *See, e.g.*, Biometric Information Privacy Act, Illinois Public Act 095-0994, https://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=095-0994; American Privacy Rights Act, Discussion Draft (Apr. 7, 2024), https://urldefense.com/v3/__https:/uovlxc5ab.cc.rs6.net/tn.jsp?f=001SWBEWTfFwQ7YTr09pFH3avTf

Location information is also particularly sensitive and often identifying. Most people will be at home in the evenings and overnight, and at work during the day. That information is likely to be unique to individuals, and one study showed that a mere four location data points is enough to identify most people.[7]

Health and finance data and individual identifiers are similarly sensitive, private information that should be protected. Many of these same types of data would be protected by the Protecting Americans' Data from Foreign Adversaries Act, recently passed by the US House of Representatives.[8] Therefore, they should be protected, with the lowest bulk definition possible, from being shared with countries of concern.

Personal health data. The DOJ should modify the definition of "personal health data'" to ensure it captures health data collected and held by all entities, including websites and apps. The ANPRM proposes to define "personal health data" the same as "individually identifiable health information" in the Health Insurance Portability and Accountability Act (HIPAA), "regardless of whether such information is collected by a 'covered entity' or 'business associate.'"[9] HIPAA is a logical place to look for critical definitions regarding health data, but because the HIPAA definition is expressly limited to information created or received by certain health-related organizations, it makes more sense to simply define the data the DOJ seeks to cover without reference to HIPAA itself.

The DOJ should be crystal clear on what personal health data includes. The clearest way to define personal health data is simply to affirmatively and separately define the term without direct reference to another statute. For instance, the definition could read, generally, identified or identifiable information that "relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."[10] Or, the DOJ could look at the definitions in the Protecting Americans' Data from Foreign Adversaries Act, and define personal health data as "[a]ny information that describes or reveals the past, present, or future

---

5yk_toRSbXD-wojbxNtqFE_gNiMQYKrlWM0r5UdGGhI5cPhonzCQCoyGcphFzsB92ImTSo3FP3fNUsg MKw4sEaxhlIQsYj_CMV856PX7QUCuCyDovA8CqFjhtpGyo2hbvNpZ9YADfEdFXD5Sk_f8bZTEQ7auq5 NQj1Z5LmibEgkXMKppZl6PWpLR2qFxnQ==&c=CvMcFQEsXc-dUyZUECxuwkwAaVrife3biuFN431hno sonUX_dXb7lQ==&ch=-l71mn7luw8whfI5e2gSOB3FbmlKBxug77depRGHkogIaecJxc27EQ==__;!!Bg5e asoyC-OII2vlEqY8mTBrtW-N4OJKAQ!M7Gc0_h3VtXe8ITD1aawpyUqbt8Brw_m23tn2CZ6phnovisLch N400qCaW1zs21uouSglkRorAgYIyLpOdzD4u5blaYtvqBPKEQSPL7ABr_rtLweyQWvSg$.

[7] Yves-Alexandre de Montjoye *et al.*, *Unique in the Crowd*, Nature (Mar. 25, 2013), https://www.nature.com/articles/srep01376.

[8] Protecting Americans' Data from Foreign Adversaries Act of 2024, H.R. 7520, Section 2(c)(7), https://www.congress.gov/bill/118th-congress/house-bill/7520/text.

[9] Department of Health & Human Services, Summary of the HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[10] 45 CFR 160.103 (HIPAA rule definition, removing the covered entity requirement).

physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual."[11]

This proposed definition removes any potential ambiguities regarding the relevance of the type of entity that holds personal health data that may arise from the cross-referenced definition and thereby clearly encompasses entities such as health app providers, while retaining the core definitional elements that correctly identify the universe of health data that should be covered by the rule.

II. Scope of "covered persons"

The class of "covered persons" with respect to whom transactions in personal data are restricted or prohibited is overly broad, difficult to administer and to comply with, and, with respect to the largest class of such persons, of limited national security risk. Under the ANPRM, any individual who is a non-U.S. person primarily resident in a country of concern would be a covered person regardless of whether they are listed as such on the list to be maintained by the DOJ, regardless of whether their citizenship and allegiance is to a close U.S. ally, and regardless of whether they have a close relationship with the government of a country of concern that would make them particularly vulnerable to governmental pressure, such as being an employee, official, or agent of such government.

The combined populations of the covered countries is roughly 1.7 billion people. They include non-U.S. persons from all or virtually all of the countries in the world, all of whom would be covered persons under the ANPRM. Many of them move around; some have more than one residence, and their place of residence may be unknown or unverifiable by the entity in the U.S. from which they are seeking data. A small portion of them will be citizens of countries that are close U.S. allies and/or dissidents, journalists, human rights defenders, and aid workers whose access to covered data could advance U.S. interests, but for whom due diligence or licensing requirements attendant to such access could put them at risk.

The Department of Justice should limit the class of covered persons by omitting this large class of individuals who merely reside in covered countries, and focus on the other covered persons such as employees and contractors of governments of countries of concern, entities under the control of such countries, and other non-U.S. persons the Attorney General has designated.

III. Onward transfers

CDT supports the limitations placed on onward transfers of data sold by data brokers. Without this limit, merely including a "middle-man" in the sale process would be a straightforward

[11] Protecting Americans' Data from Foreign Adversaries Act of 2024, H.R. 7520, Section 2(c)(7)(B). https://www.congress.gov/bill/118th-congress/house-bill/7520/text#HAA3E64C9AB014CE0AE8DABE2E1AA6528.

workaround to the requirements, such as a US data broker selling to a European data broker, who in turn sells to a country of concern. The DOJ should not allow for this type of workaround, so the rule should include limits on onward transfer of data.

Enforcement of a contractual provision prohibiting such onward transfers may, however, be difficult. The government may want to publicly identify foreign data brokers that engage in such onward transfers so that US data brokers are aware of the risk of selling sensitive personal data to such brokers. The government may want to work with allies and other nations to encourage them to adopt similar restrictions on data sales to countries of concern, so that brokers in those countries could not serve a middle-man role.

IV. Statutory authority

The DOJ should, in the notice of proposed rulemaking that will follow this ANPRM, clarify its interpretation of the statutory authority for issuing the proposed rule. In short, the primary statutory authority for the rule cited in ANPRM does not permit the President to regulate the flow of information, and yet the ANPRM seems to contemplate restricting or prohibiting certain flows of information to countries of concern.

The ANPRM cites three statutes for this authority, the most important of which is the International Emergency Economic Powers Act (IEEPA).[12] IEEPA authorizes the President to declare a national emergency that triggers economic sanctions, which the President did on February 28, 2024 in the Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United State Government-Related Data by Countries of Concern.[13] However, the authority IEEPA confers is limited. In imposing sanctions, the President may not, "regulate or prohibit, directly or indirectly … the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of *any information or informational materials*, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks and news wire feeds."[14] Court decisions blocked President Trump's executive order banning TikTok in part based on this language.[15]

---

[12] 50 USC 1701 *et seq*.
[13] Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.
[14] 50 USC 1703(b)(2) (emphasis added).
[15] TikTok et al. v. Trump (D.DC 2020), https://cases.justia.com/federal/district-courts/district-of-columbia/dcdce/1:2020cv02658/222257/30/0.pdf?ts=1601371372.

According to the DOJ Fact Sheet[16] issued to explain the ANPRM, the DOJ does not intend to restrict the export of "expressive information under 50 USC 1702(b)(3) such as videos, artwork or publications." While the ANPRM does not focus on videos, artwork or publications, nor on expression that might be found in TikTok videos, it seemingly would restrict or prohibit the export of "information" such as personal identifiers, personal health data, personal financial data, and precise geolocation data. Although the statutory language includes a non-exhaustive list of types of information that IEEPA declarations cannot restrict and those arguably could all be characterized as "expressive," the exception covers "any information" and expressly says that this term is "not limited to" the listed examples. The DOJ should explain why it views the data that is the subject of the ANPRM as being outside the realm of the "information" IEEPA does not permit the government to restrict.

V. Conclusion

CDT supports the DOJ's goals in this proceeding, which is to reduce the ability of countries of concern to collect and exploit US individuals' data. We urge the DOJ to account for the concerns we have outlined here as it puts together the NPRM that is expected to follow.

[16] DOJ Fact Sheet on data broker ANPRM (Feb. 28, 2024), https://www.justice.gov/d9/2024-02/data_security_eo_fact_sheet.pdf, at 3.