PREVENTING ACCESS TO US SENSITIVE PERSONAL DATA AND GOV'T RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS

OVERVIEW OF NOTICE OF PROPOSED RULEMAKING

Table of Contents

- NPRM Objectives and Scope
- Covered Data Transactions, Types, and Thresholds
- Covered Persons & Countries of Concern
- Types of Prohibited and Restricted Transactions
  - Data Brokerage; Investment Agmts; Vendor Agmts; Employment Agmts
  - Prohibitions; Restrictions; Knowledge Standard
- Selected Exemptions
  - Corporate Group Transactions
  - Legal Compliance
  - International Agreements
  - Financial Services
  - Telecommunications
  - Personal Communications
  - Informational Materials
  - Travel
  - Official USG Business
  - CFIUS & IEEPA
- Recordkeeping
- Licensing & Enforcement

NPRM Objectives & Scope

NPRM Objectives

- NPRM seeks to mitigate national security threats that arise from countries of concern accessing government-related data or Americans' bulk U.S. sensitive personal data.
- DoJ states that the development of artificial intelligence ("AI"), high-performance computing, big-data analytics, and other advanced technological capabilities by countries of concern amplifies the threat posed by these countries' access to government-related data or Americans' bulk U.S. sensitive personal data.
  - For instance, the U.S. National Intelligence Council assessed in 2020 that "access to personal data of other countries' citizens, along with [artificial intelligence]-driven analytics, will enable [the People's Republic of China] to automate the identification of individuals and groups beyond China's borders to target with propaganda or censorship."
- Countries of concern can also exploit their access to government-related data regardless of volume to threaten U.S. national security.
  - One academic study explained that "[f]oreign and malign actors could use location datasets to stalk or track high-profile military or political targets," revealing "sensitive locations—such as visits to a place of worship, a gambling venue, a health clinic, or a gay bar—which again could be used for profiling, coercion, blackmail, or other purposes."
  - A MITRE report explained that location datasets could reveal "U.S. military bases and undisclosed intelligence sites" or "be used to estimate military population or troop buildup in specific areas around the world or even identify areas of off-base congregation to target."
  - As another example of these data risks and the relative ease with which they can be exploited, journalists were able to commercially acquire from a data broker a continuous stream of 3.6 billion geolocation data points that were lawfully collected on millions of people from advertising IDs. The journalists were then able to create "movement profiles" for tens of thousands of national security and military officials, and from there, could determine where they lived and worked as well as their names, education levels, family situations, and hobbies.

• NPRM Scope

Executive Order 14117 of February 28, 2024… directs the Attorney General to issue regulations that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest ("transaction"), where the transaction:

(a) Involves United States Government-related data ("government-related data") or bulk U.S. sensitive personal data, as defined by final rules implementing the Order;

(b) Falls within a class of transactions that has been determined by the Attorney General to pose an unacceptable risk to the national security of the United States because the transactions may enable access by countries of concern or covered persons to government-related data or bulk U.S. sensitive personal data; and

(c) Meets other criteria specified by the Order.

Data Transactions, Typologies, and Thresholds

- **202.210 – Covered Data Transaction**

(a) *Definition.* A *covered data transaction* is any transaction that involves any access to any government-related data or bulk U.S. sensitive personal data and that involves:

- (1) Data brokerage;
- (2) A vendor agreement;
- (3) An employment agreement; or
- (4) An investment agreement.

- **202.201 – Access**

The term *access* means logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information systems, information technology systems, cloud-computing platforms, networks, security systems, equipment, or software.

202.205 – Bulk

The term *bulk* means any amount of sensitive personal data that meets or exceeds the following thresholds at any point in the preceding 12 months, whether through a single covered data transaction or aggregated across covered data transactions involving the same U.S. person and the same foreign person or covered person:

- (a) Human genomic data … on more than 100 U.S. persons;
- (b) Biometric identifiers … on more than 1,000 U.S. persons;
- (c) Precise geolocation data … on more than 1,000 U.S. devices;
- (d) Personal health data … on more than 10,000 U.S. persons;
- (e) Personal financial data … on more than 10,000 U.S. persons;
- (f) Covered personal identifiers … on more than 100,000 U.S. persons; or
- (g) Combined data, meaning any collection or set of data that contains more than one of the categories in paragraphs (a) through (g) of this section, or that contains any listed identifier linked to categories in paragraphs (a) through (e) of this section, where any individual data type meets the threshold number of persons or devices collected or maintained in the aggregate for the lowest number of U.S. persons or U.S. devices in that category of data.

- **202.206 – Bulk US sensitive personal data**

The term *bulk U.S. sensitive personal data* means a collection or set of bulk data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted.

- **202.249 – Sensitive personal data**

Definition. The term *sensitive personal data* means covered personal identifiers, precise geolocation data, biometric identifiers, human genomic data, personal health data, personal financial data, or any combination thereof.

Exclusions. The term *sensitive personal data* excludes:

- (1) Public or nonpublic data that doesn't relate to an individual;
- (2) Data that is… lawfully available to the public from a Federal, State, or local government record (such as court records) or in widely distributed media (such as sources that are generally available to the public through unrestricted and open-access repositories);
- (3) Personal communications; and
- (4) Information or informational materials.

• 202.234 – Listed Identifiers

The term listed identifier means any piece of data in any of the following data fields:

(a) Full or truncated government identification or account number (such as a Social Security number, driver's license or State identification number, passport number, or Alien Registration Number);

(b) Full financial account numbers or personal identification numbers associated with a financial institution or financial-services company;

(c) Device-based or hardware-based identifier (such as International Mobile Equipment Identity ("IMEI"), Media Access Control ("MAC") address, or Subscriber Identity Module ("SIM") card number);

(d) Demographic or contact data (such as first and last name, birth date, birthplace, ZIP code, residential street or postal address, phone number, email address, or similar public account identifiers);

(e) Advertising identifier (such as Google Advertising ID, Apple ID for Advertisers, or other mobile advertising ID ("MAID"));

(f) Account-authentication data (such as account username, account password, or an answer to security questions);

(g) Network-based identifier (such as Internet Protocol ("IP") address or cookie data); or

(h) Call-detail data (such as Customer Proprietary Network Information ("CPNI")).

• 202.212 – Covered Personal Identifiers

(a) Definition. The term covered personal identifiers means any listed identifier:

(1) In combination with any other listed identifier; or

(2) In combination with other data that is disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data.

(b) Exclusion. The term covered personal identifiers excludes:

(1) Demographic or contact data that is linked only to other demographic or contact data (such as first and last name, birthplace, ZIP code, residential street or postal address, phone number, and email address and similar public account identifiers); and

(2) A network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifier, account-authentication data, or call detail data as necessary for the provision of telecommunications, networking, or similar service.

Countries of Concern & Covered Persons

• 202.211 – Covered Person

(a) *Definition*. The term *covered person* means:

- (1) A foreign entity that is 50 percent or more owned, directly or indirectly, by a country of concern, or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern;
- (2) A foreign entity that is 50 percent or more owned, directly or indirectly, by an entity described in paragraph (a)(1) of this section or a person described in paragraphs (a)(3), (4), or (5) of this section;
- (3) A foreign individual who is an employee or contractor of a country of concern or of an entity described in paragraphs (a)(1), (2), or (5) of this section;
- (4) A foreign individual who is primarily a resident in … a country of concern; or
- (5) Any person, wherever located, determined by the Attorney General:
  - (i) To be, to have been, or to be likely to become owned or controlled by or subject to the jurisdiction or direction of a country of concern or covered person;
  - (ii) To act, to have acted or purported to act, or to be likely to act for or on behalf of a country of concern or covered person; or
  - (iii) To have knowingly caused or directed, or to be likely to knowingly cause or direct a violation of this part.

• 202.701 – Designation of Covered Persons

(a) Designations. The Attorney General may designate any person as a covered person for purposes of this part if, after consultation with other agencies as the Attorney General deems appropriate, the Attorney General determines the person meets any of the criteria set forth in § 202.211(a)(5) of this part.

(b) Information considered. In determining whether to designate a person as a covered person, the Attorney General may consider any information or material the Attorney General deems relevant and appropriate, classified or unclassified, from any Federal department or agency or from any other source.

(c) Covered Persons List. The names of persons designated as a covered person for purposes of this part, transactions with whom are prohibited or restricted pursuant to this part, are published in the Federal Register and incorporated into the National Security Division's Covered Persons List. The Covered Persons List is accessible through the following page on the National Security Division's website at https://www.justice.gov/nsd.

(d) Non-exhaustive. The list of designated covered persons described in this section is not exhaustive of all covered persons and supplements the categories in the definition of covered persons in § 202.211.

(e) Effective date; actual and constructive knowledge.

(1) Designation as a covered person will be effective from the date of any public announcement by the Department. Except as otherwise authorized in this part, a U.S. person with actual knowledge of a designated person's status is prohibited from knowingly engaging in a covered data transaction with that person on or after the date of the Department's public announcement.

(2) Publication in the Federal Register is deemed to provide constructive knowledge of a person's status as a covered person.

- **202.209 – Country of Concern**

The term country of concern means any foreign government that, as determined by the Attorney General with the concurrence of the Secretary of State and the Secretary of Commerce,

(1) has 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 United States persons, and

(2) poses a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or security and safety of U.S. persons.

• 202.601 – Determination of Country of Concern

(a) Countries of concern. Solely for purposes of the Order and this part, the Attorney General has determined, with the concurrence of the Secretaries of State and Commerce, that the following foreign governments have 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 U.S. persons and pose a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or security and safety of U.S. persons:

(1) China;

(2) Cuba;

(3) Iran;

(4) North Korea;

(5) Russia; and

(6) Venezuela.

(b) Effective date of amendments. Any amendment to the list of countries of concern will apply to any covered data transaction that is initiated, pending, or completed on or after the effective date of the amendment.

Predicate Acts – Prohibited & Restricted Transactions

• 202.214 – Data Brokerage

Definition. The term *data brokerage* means the sale of data, licensing of access to data, 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.

- *Example 1*. A U.S. company sells bulk U.S. sensitive personal data to an entity headquartered in a country of concern. The U.S. company engages in prohibited data brokerage.
- *Example 2*. A U.S. company enters into an agreement that gives a covered person a license to access government-related data held by the U.S. company. The U.S. company engages in prohibited data brokerage.
- *Example 3*. A U.S. organization maintains a database of bulk U.S. sensitive personal data and offers annual memberships for a fee that provide members a license to access that data. Providing an annual membership to a covered person that includes a license to access government-related data or bulk U.S. sensitive personal data would constitute prohibited data brokerage.

202.214 – Data Brokerage (cont'd)

- Example 4. A U.S. company owns and operates a mobile app for U.S. users with available advertising space. As part of selling the advertising space, the U.S. company provides the bulk precise geolocation data, IP address, and advertising IDs of its U.S. users' devices to an advertising exchange based in a country of concern. The U.S. company's provision of this data as part of the sale of advertising space is data brokerage and a prohibited transaction.

- *Example 5*. Same as Example 4, but the U.S. company provides the data to an advertising exchange based in the United States. As part of the sale of the advertising space, the U.S. advertising exchange provides the data to advertisers headquartered in a country of concern. The U.S. company's provision of the data to the U.S. advertising exchange would not be a transaction because it is between U.S. persons. The advertising exchange's provision of this data to the country of concern-based advertisers is data brokerage because it is a commercial transaction involving the transfer of data from the U.S. advertising exchange to the advertisers headquartered in the country of concern, where those country-of-concern advertisers did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. Furthermore, the U.S. advertising exchange's provision of this data to the country of concern-based advertisers is a prohibited transaction.

- *Example 6*. A U.S. information technology company operates an autonomous driving platform that collects the precise geolocation data of its cars operating in the United States. The U.S. company sells or otherwise licenses this bulk data to its parent company headquartered in a country of concern to help develop artificial intelligence technology and machine learning capabilities. The sale or license is data brokerage and a prohibited transaction.

• 202.258 – Vendor Agreement

(a) *Definition*. The term *vendor agreement* means any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration.

Example 1. A U.S. company collects bulk precise geolocation data from U.S. users through an app. The U.S. company enters into an agreement with a company headquartered in a country of concern to process and store this data. This vendor agreement is a restricted transaction.

Example 2. A medical facility in the United States contracts with a company headquartered in a country of concern to provide IT-related services. The contract governing the provision of services is a vendor agreement. The medical facility has bulk personal health data on its U.S. patients. The IT services provided under the contract involve access to the medical facility's systems containing the bulk personal health data. This vendor agreement is a restricted transaction.

Example 4. A U.S. company develops mobile games that collect bulk precise geolocation data and biometric identifiers of U.S.-person users. The U.S. company contracts part of the software development to a foreign person who is primarily resident in a country of concern and is a covered person. The contract with the foreign person is a vendor agreement. The software-development services provided by the covered person under the contract involve access to the bulk precise geolocation data and biometric identifiers. This is a restricted transaction.

202.258 – Vendor Agreement (cont'd)

- The ANPRM contemplated defining the term "cloud-computing services" as that term is defined in NIST Special Publication ("SP") 800-145.
- NIST SP 800-145 describes cloud computing in a way that includes different essential characteristics, deployment models, and service models, such as "Infrastructure as a Service (IaaS)," "Platform as a Service (PaaS)," and "Software as a Service (SaaS)."
- Because cloud computing is just one example of several types of services that may be involved in a vendor agreement, it does not appear useful to separately or specially define that term in the proposed rule at this time.
- The Department may consider issuing guidance in the future that describes cloud computing in reference to the NIST definition.

• 202.217 – Employment Agreement

(a) *Definition*. The term *employment agreement* means any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level.

- *Example 1*. A U.S. company that conducts consumer human genomic testing collects and maintains bulk human genomic data from U.S. consumers. The U.S. company has global IT operations, including individuals primarily resident in a country of concern to provide back-end services. The agreements related to employing these individuals are employment agreements. Employment includes access to the U.S. company's systems containing the bulk human genomic data. These employment agreements would be prohibited.

- *Example 3*. A U.S. company has derived U.S. persons' biometric identifiers by scraping public photos from social media platforms. The U.S. company stores the derived biometric identifiers in bulk to train facial-recognition software. The U.S. company intends to hire a foreign person, who primarily resides in a country of concern, as a project manager responsible for the database. The project manager's employment agreement would be a restricted transaction.

202.228 – Investment Agreement

(a) *Definition.* The term *investment agreement* means an agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to: (1) Real estate located in the United States; or (2) A U.S. legal entity.

(b) *Exclusion for passive investments. Investment agreement* excludes any investment that:

(1) Is made:

- (i) Into a publicly traded security…;
- (ii) Into a security offered by: (A) Any "investment company", such as index funds, mutual funds, or exchange traded funds; or (B) Any company … regulated as a business development company; or
- (iii) As a limited partner into a venture capital fund, private equity fund, fund of funds, or other pooled investment fund, if the limited partner's contribution is solely capital and [does not involve decision-making];

(2) Gives the covered person less than 10% in total voting and equity interest…; and

(3) Does not give a covered person rights beyond those reasonably considered to be standard minority shareholder protections, including (a) membership or observer rights on, or the right to nominate an individual to a position on, the board of directors or an equivalent governing body of the U.S. person, or (b) any other involvement, beyond the voting of shares, in substantive business decisions, management, or strategy of the U.S. person.

• 202.301 – Prohibited data brokerage transaction

Prohibition. [N]o U.S. person… may knowingly engage in a covered data transaction involving data brokerage with a country of concern or covered person.

- *Example 1*. An artificial intelligence chatbot in the United States … is trained on the bulk U.S. sensitive personal data of U.S. persons. … [T]he chatbot is capable of reproducing or otherwise disclosing the bulk sensitive personal health data that was used to train the chatbot when responding to queries.
- The [developer] knowingly licenses subscription-based access to that chatbot worldwide, including to covered persons [in a country of concern]. The [developer] knows or should know that the license can be used to obtain access to the U.S. persons' bulk sensitive personal training data if prompted.
- The licensing of access to this bulk U.S. sensitive personal data is data brokerage because it involves the transfer of data from the U.S. company (*i.e.*, the provider) to licensees (*i.e.*, the recipients), where the recipients did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.
- Even though the license did not explicitly provide access to the data, this is a prohibited transaction because the U.S. company knew or should have known that the use of the chatbot pursuant to the license could be used to obtain access to the training data, and because the U.S. company licensed the product to covered persons.

• 202.302 – Other prohibited data brokerage transactions

Prohibition. [N]o U.S. person … may knowingly engage in a covered data transaction involving data brokerage with any foreign person that is not a covered person unless the U.S. person:

- (1) Contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving data brokerage of the same data with a country of concern or covered person; and
- (2) Reports any known or suspected violations of this contractual requirement in accordance with paragraph (b) of this section.

Reporting known or suspected violations—

- (1) *When reports are due.* U.S. persons shall file reports within 14 days of the U.S. person becoming aware of a known or suspected violation.
- (2) *Contents of reports.* Reports on known or suspected violations shall include the following…: (i) The name and address of the U.S. person reporting the known or suspected violation; (ii) A description of the known or suspected violation, including details on the transaction, onward transfer contractual provision, contractual breach, persons involved, copies of documentation.

• 202.401 – Authorization to conduct restricted transactions

Restricted transactions. [N]o U.S. person… may knowingly engage in a covered data transaction involving a vendor agreement, employment agreement, or investment agreement with a country of concern or covered person unless the U.S. person complies with the security requirements [& other requirements].

- *Example 1*. A U.S. company engages in an employment agreement with a covered person to provide information technology support. As part of their employment, the covered person has access to personal financial data. The U.S. company implements and complies with the security requirements. The employment agreement is authorized as a restricted transaction because the company has complied with the security requirements.

- *Example 2*. A U.S. company engages in a vendor agreement with a covered person to store bulk personal health data. Instead of implementing the security requirements as identified by reference in this subpart, the U.S. company implements different controls that it believes mitigate the covered person's access to the bulk personal health data. Because the U.S. person has not complied with the security requirements, the vendor agreement is not authorized and thus is a prohibited transaction.

• 202.230 – Knowingly

Definition. The term *knowingly,* with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or reasonably should have known, of the conduct, the circumstance, or the result.

Example. A U.S. service provider provides a software platform on which a U.S. company processes the bulk U.S. sensitive personal data of its U.S.-person customers. While the U.S. service provider is generally aware of the nature of the U.S. company's business, the U.S. service provider is not aware of the kind or volume of data that the U.S. company processes on the platform, how the U.S. company uses the data, or whether the U.S. company engages in data transactions. The U.S. company also primarily controls access to its data on the platform, with the U.S. service provider accessing the data only for troubleshooting or technical support purposes, upon request by the U.S. company. Subsequently, without the actual knowledge of the U.S. service provider and without providing the U.S. service provider with any information from which the service provider should have known, the U.S. company grants access to the data on the U.S. service provider's software platform to a covered person through a covered data transaction, in violation of this part. The U.S. service provider itself, however, has not knowingly engaged in a restricted transaction by enabling the covered persons' access via its software platform.

Example. Same as prior Example, but in addition to providing the software platform, the U.S. company's contract with the U.S. service provider also outsources the U.S. company's processing and handling of the data to the U.S. service provider. As a result, the U.S. service provider primarily controls access to the U.S. company's bulk U.S. sensitive personal data on the platform. The U.S. service provider employs a covered person and grants access to this data as part of this employment. Although the U.S. company's contract with the U.S. service provider is not a restricted transaction, the U.S. service provider's employment agreement with the covered person is a restricted transaction. The U.S. service provider has thus knowingly engaged in a restricted transaction by entering into an employment agreement that grants access to its employee because the U.S. service provider knew or should have known of its employee's covered person status and, as the party responsible for processing and handling the data, the U.S. service provider was aware of the kind and volume of data that the U.S. company processes on the platform.

Selected Exemptions

202.506 – Corporate Group Transactions

Exemption for data transactions:

(1) Between a U.S. person and its subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction, or control of) a country of concern; and

(2) Ordinarily incident to and part of administrative or ancillary business operations, including:

- (i) Human resources;
- (ii) Payroll, expense monitoring and reimbursement, and other corporate financial activities;
- (iii) Paying business taxes or fees;
- (iv) Obtaining business permits or licenses;
- (v) Sharing data with auditors and law firms for regulatory compliance;
- (vi) Risk management;
- (vii) Business-related travel;
- (viii) Customer support;
- (ix) Employee benefits; and
- (x) Employees' internal and external communications.

202.505 – Financial Services

Exemption for data transactions that are ordinarily incident to and part of the provision of financial services, including:

- (1) Banking, capital-markets (including investment-management services), or financial-insurance services; (2) A financial activity authorized for national banks by 12 U.S.C. 24 (Seventh) and rules and regulations and written interpretations of the Office of the Comptroller of the Currency thereunder;
- (3) An activity that is "financial in nature or incidental to such financial activity" or "complementary to a financial activity," section (k)(1), as set forth in section (k)(4) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)) and rules and regulations and written interpretations of the Board of Governors of the Federal Reserve System thereunder;
- (4) The transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services (such as the purchase, sale, or transfer of consumer products and services through online shopping or e-commerce marketplaces);
- (5) The provision or processing of payments or funds transfers (such as person-to-person, business-to-person, and government-to-person funds transfers) involving the transfer of personal financial data or covered personal identifiers, or the provision of services ancillary to processing payments and funds transfers (such as services for payment dispute resolution, payor authentication, tokenization, payment gateway, payment fraud detection, payment resiliency, mitigation and prevention, and payment-related loyalty point program administration); and
- (6) The provision of investment-management services that manage or provide advice on investment portfolios or individual assets for compensation (such as devising strategies and handling financial assets and other investments for clients) or provide services ancillary to investment-management services (such as broker-dealers executing trades within a securities portfolio based upon instructions from an investment advisor).

202.509 – Telecommunications

- Exemption for data transactions … ordinarily incident to and part of the provision of telecommunications services, including international calling, mobile voice, and data roaming.

- *Example*. A U.S. telecommunications service provider collects precise geolocation data on its U.S. subscribers. The U.S. telecommunications service provider sells this precise geolocation data in bulk to a covered person for the purpose of targeted advertising. This sale is not ordinarily incident to and part of the provision of telecommunications services and remains a prohibited transaction.

- *Example*. A U.S. telecommunications service provider collects covered personal identifiers from its U.S. subscribers. Some of those subscribers travel to a country of concern and use their mobile phone service under an international roaming agreement. The local telecommunications service provider in the country of concern shares these covered personal identifiers with the U.S. service provider for the purposes of either helping provision service to the U.S. subscriber or receiving payment for the U.S. subscriber's use of the country of concern service provider's network under that international roaming agreement. The U.S. service provider provides the country of concern service provider with network or device information for the purpose of provisioning services and obtaining payment for its subscribers' use of the local telecommunications service provider's network. Over the course of 12 months, the volume of network or device information shared by the U.S. service provider with the country of concern service provider for the purpose of provisioning services exceeds the applicable bulk threshold. These transfers of bulk U.S. sensitive personal data are ordinarily incident to and part of the provision of telecommunications services and are thus exempt transactions.

202.501 – 202.504, 508: Personal Communications, Informational Materials, Travel, Official USG Business

Exemptions for data transactions to the extent that they:

- Involve any postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value.
- Involve the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials.
- Are ordinarily incident to travel to or from any country, including importation of accompanied baggage for personal use; maintenance within any country, including payment of living expenses and acquisition of goods or services for personal use; and arrangement or facilitation of such travel, including nonscheduled air, sea, or land voyages.
- Are for the conduct of the official business of the United States Government by its employees, grantees, or contractors; any authorized activity of any United States Government department or agency…; or transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government.
- Are covered by CFIUS investment agreements or provisions of IEEPA.

- **202.507: Transactions required or authorized by Federal law or int'l agreements, or necessary for compliance with Federal law**

Exemptions for data transactions to the extent that they are:

- Required or authorized by Federal law or pursuant to an international agreement to which the United States is a party, including the: (1) Convention on Internation Civil Aviation; (2) Convention on the Facilitation of Int'l Maritime Traffic; (3) Postal Payment Services Agreement; (4) Constitution of the World Health Organization; (5) US-China Mutual Assistance Agreement on Customs Matters; (6) US-China Agreement on Mutual Legal Assistance in Criminal Matters; (7) US-China Agreement on Avoidance of Double Taxation; (8) US-Macao Cooperation Agreement on FATCA; (9) US-China Agreement on Cooperation in the Science and Technology of Medicine & Public Health (and later-agreed protocols).

- Required or authorized by the following: (1) The Pandemic Influenza Preparedness and Response Framework; and (2) The Global Influenza Surveillance and Response System.

- Ordinarily incident to and part of ensuring compliance with any Federal laws and regulations, including the Bank Secrecy Act; the Securities Act of 1933; the Securities Exchange Act of 1934; the Investment Company Act of 1940; the Investment Advisers Act of 1940; the International Emergency Economic Powers Act; the Export Administration Regulations; or any notes, guidance, orders, directives, or additional regulations related thereto.

Recordkeeping

202.1101 – Recordkeeping

Records. Except as otherwise provided, U.S. persons engaging in any transaction subject to the provisions of this part shall keep a full and accurate record of each such transaction engaged in, and such record shall be available for examination for at least 10 years after the date of such transaction.

Additional recordkeeping requirements. U.S. persons engaging in any restricted transaction shall create and maintain, at a minimum, the following records in an auditable manner:

- (1) A written policy that describes the data compliance program and that is certified annually by an officer, executive, or other employee responsible for compliance;
- (2) A written policy that describes the implementation of any applicable security requirements as defined in § 202.248 of this part and that is certified annually by an officer, executive, or other employee responsible for compliance;
- (3) The results of any annual audits that verify the U.S. person's compliance with the security requirements and any conditions on a license;
- (4) Documentation of the due diligence conducted to verify the data flow involved in any restricted transaction, including:
  - (i) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;
  - (ii) The identity of the transaction parties, including any direct and indirect ownership of entities or citizenship or primary residence of individuals; and
  - (iii) A description of the end-use of the data;
- (5) Documentation of the method of data transfer;
- (6) Documentation of the dates the transaction began and ended;
- (7) Copies of any agreements associated with the transaction;
- (8) Copies of any relevant licenses or advisory opinions;
- (9) The document reference number for any original document issued by the Attorney General, such as a license or advisory opinion;
- (10) A copy of any relevant documentation received or created in connection with the transaction; and
- (11) An annual certification by an officer, executive, or other employee responsible for compliance of the completeness and accuracy of the records documenting due diligence.

202.1102 – Reports to be furnished on demand

- Every person is required to furnish under oath, in the form of reports or otherwise, as may be required by DoJ, complete information relative to any act or transaction…
- DoJ may require that such reports include the production of any books, contracts, letters, papers, or other hard copy or electronic documents, in the custody or control of the persons required to make such reports.
- DoJ may, through any person or agency, conduct investigations, hold hearings, administer oaths, examine witnesses, receive evidence, take depositions, and require by subpoena the attendance and testimony of witnesses and the production of any books, contracts, letters, papers, and other hard copy or electronic documents relating to any matter under investigation.

202.1103 – Annual Reports

- *Who must report*. An annual report must be filed by any U.S. person that is engaged in a restricted transaction involving cloud-computing services, and that has 25% or more of the U.S. person's equity interests owned (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise) by a country of concern or covered person.
- *Primary responsibility to report*. Primary responsibility for reporting… rests with the actual U.S. person engaging in the data transaction. No U.S. person is excused from filing a report by reason of the fact that another U.S. person has submitted a report with regard to the same data transaction, except where the U.S. person has actual knowledge that the other U.S. person filed the report.
- *When reports are due*. A report on the data transactions engaged in as of December 31 of the previous year shall be filed annually by March 1 of the subsequent year.
- *Contents of reports*. Annual reports on the data transactions described in § 202.1103(a) shall include the following:
  - (1) The name and address of the U.S. person engaging in the covered data transaction, and the name, telephone number, and email address of a contact from whom additional information may be obtained;
  - (2) A description of the covered data transaction, including: (i) The date of the transaction; (ii) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction; (iii) The method of data transfer; and (iv) Any persons participating in the data transaction and their respective locations, including the name and location of each data recipient, the ownership of entities or citizenship or primary residence of individuals, the name and location of any covered persons involved in the transaction, and the name of any countries of concern involved in the transaction;
  - (3) A copy of any relevant documentation received or created in connection with the transaction; and
  - (4) Any other information that the Department of Justice may require.

202.1104 – Reports on Rejected Prohibited Transactions

- (a) *Who must report*. A report must be filed by any U.S. person that has received and affirmatively rejected (including automatically rejected using software, technology, or automated tools) an offer from another person to engage in a prohibited transaction involving data brokerage.
- (b) *When reports are due*. U.S. persons shall file reports within 14 days of rejecting a transaction prohibited by this part.
- (c) *Contents of reports*. Reports on rejected transactions shall include the following, to the extent known and available to the person filing the report at the time the transaction is rejected:
  - (1) The name and address of the U.S. person that rejected the prohibited transaction, and the name, telephone number, and email address of a contact from whom additional information may be obtained; (2) A description of the rejected transaction, including:
    - (i) The date the transaction was rejected;
    - (ii) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;
    - (iii) The method of data transfer;
    - (iv) Any persons attempting to participate in the transaction and their respective locations, including the name and location of each data recipient, the ownership of entities or citizenship or primary residence of individuals, the name and location of any covered persons involved in the transaction, and the name of any countries of concern involved in the transaction;
    - (v) A copy of any relevant documentation received or created in connection with the transaction; and
    - (vi) Any other information that the Department of Justice may require.

GLOBAL DATA ALLIANCE

TRUST ACROSS BORDERS

Please direct any questions to gdainfo@bsa.org