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

GOVERNMENT DATA

Agenda for Discussion

- Explanation for NPRM Coverage of Gov't-Related Data
- Definition of "Government-Related Data"
- Prohibitions and Restrictions Related to Government Data
- Examples of Government-related Data Transactions

NPRM Explanation for Coverage of Gov't-Related Data

- 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.
- Countries of concern can 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.
  - It has become increasingly evident in recent years that government-related location data is at risk of being exploited by countries of concern through location information collected from electronic devices, including cell phones and fitness apps. Such data can be used to not only track the movements of targeted government associates but also to link them with sensitive activities and vices, such as gambling or prostitution. This information can then be used to pressure these persons to reveal sensitive information, thereby compromising U.S. national security. Methods include malicious cyber-enabled activities, espionage, and blackmail. As of July 2021, one of the largest data brokers, Acxiom, sold products that purported to cover 45.5 million current and former U.S. military personnel and 21.3 million current and former government employees.

Definitions of "Government-Related Data"

• 202.201 – "Scope" Application to Government-related Data

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.

• 202.222 – Government-related Data

(a) Definition. The term government-related data means the following:

Any **precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List** in § 202.1401 which the Attorney General has determined poses a heightened risk of being exploited by a country of concern to reveal insights about locations controlled by the Federal Government, including insights about facilities, activities, or populations in those locations, to the detriment of national security, because of the nature of those locations or the personnel who work there. Such locations may include:

(i) The worksite or duty station of Federal Government employees or contractors who occupy a national security position as that term is defined in 5 CFR 1400.102(a)(4);

(ii) A military installation as that term is defined in 10 U.S.C. 2801(c)(4); or

(iii) Facilities or locations that otherwise support the Federal Government's national security, defense, intelligence, law enforcement, or foreign policy missions.

(2) Any sensitive personal data, regardless of volume, that a transacting party markets as linked or **linkable to current or recent former employees or contractors, or former senior officials, of the United States Government**, including the military and Intelligence Community.

202.222 - Government-related Data (cont'd)

- Bulk thresholds do not apply to transactions involving government-related data. This means that any prohibitions and restrictions apply to such transactions even if the data involves only a single government official or a single government-related location.
- The proposed rule defines subcategories of government-related data for locations and personnel.

Government-related Location Data

- The location subcategory covers any precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List in § 202.1401 that the Attorney General has determined poses a heightened risk of being exploited by a country of concern to reveal insights to the detriment of national security about locations controlled by the Federal Government, including insights about facilities, activities, or populations in those locations, because of the nature of those locations or the personnel who work there.
- The purpose of this list is to prevent countries of concern from exploiting the geolocation data in these locations, such as by using aggregated geolocation data to draw inferences about facilities, activities, or populations located there that could undermine U.S. national security or foreign policy or to conduct intelligence or counterintelligence operations against government employees or contractors, or against government facilities.
- The locations that the Department might add to this list may include the worksites or duty stations of Federal Government employees or contractors who occupy national security positions, as that term is defined in 5 CFR 1400.102(a), wherever they are located.
- The locations may also include military installations, embassies or consulates, or other facilities worldwide that support the Federal Government in achieving its national security, defense, intelligence, law enforcement, or foreign policy missions.

Government-related Personnel Data

- The personnel subcategory cover any sensitive personal data, regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the United States Government, including the military and intelligence community.
- The proposed rule defines "recent former employees or contractors" as employees or contractors who have worked for or provided services to the United States Government, in a paid or unpaid status, within the 2 years preceding a proposed covered data transaction. See § 202.245.
- The proposed rule defines a "former senior official" as either a "former senior employee" or "former very senior employee," as those terms are defined in the ethics regulations pertaining to post-employment conflicts of interest for former Executive Branch or independent agency employees. 5 CFR 2641.104. See § 202.220.
- DoJ defines the personnel subcategory based on how the U.S. person markets the data, not on whether a particular dataset contains data on former government employees or contractors. In other words, the personnel subcategory applies only to transactions in which the U.S. person has already identified and described sensitive personal data as being about certain government personnel. This subcategory does not apply on the basis of the presence or absence of data linked to certain government personnel in the underlying sensitive personal data.
- DoJ is still considering how to address the national security risk where – even in the absence of such marketing activity – sensitive personal data could be used to identify current or certain former government personnel. The Department is still considering how to address this issue, specifically whether to include, and how to define, this category of information in the proposed rule while minimizing the unintended consequence described above in this section. The Department appreciates any views from the public.

• Examples of Government-related Data

Examples of government-related data marketed by a transacting party.

(1) Example 1. A U.S. company advertises the sale of a set of sensitive personal data as belonging to "active duty" personnel, "military personnel who like to read," "DoD" personnel, "government employees," or "communities that are heavily connected to a nearby military base." The data is government-related data.

(2) Example 2. In discussing the sale of a set of sensitive personal data with a covered person, a U.S. company describes the dataset as belonging to members of a specific named organization. The identified organization restricts membership to current and former members of the military and their families. The data is government-related data.

Prohibitions and Restrictions Involving Government-Related Data

- **202.210 – Covered Data Transaction (involving government-related data)**

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.

Examples of Prohibited Data Brokerage Transactions involving government-related data

- Example 1. 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 2. 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.

- **Examples of Prohibited Data Brokerage Transactions involving government-related data**

- *Example* 3. A foreign person who is a covered person asks a U.S. company for a list of Media Access Control ("MAC") addresses from devices that have connected to the wireless network of a U.S. fast-food restaurant located in a particular government building.

- The U.S. company then sells the list of MAC addresses, without any other listed identifiers or sensitive personal data, to the covered person.

- The disclosed MAC addresses, when paired with the other data disclosed by the covered person—that the devices "have connected to the wireless network of a U.S. fast-food restaurant located in a particular government building"—makes it so that the MAC addresses are linked or linkable to other sensitive personal data, in this case precise geolocation data of the location of the fast-food restaurant that the national security-related individuals frequent with their devices.

- This combination of data therefore meets the definition of covered personal identifiers.

GLOBAL DATA ALLIANCE

TRUST ACROSS BORDERS

Please direct any questions to gdainfo@bsa.org