May 7, 2025

Data Access and National Security: A New Paradigm Under DOJ's U.S. Sensitive Data Rule

Julia Post
Covington & Burling

Ingrid Price
Covington & Burling

Joseph Whitlock
Business Software Alliance
& Global Data Alliance

Privacy+ Security Forum

National Security Context

- EO includes finding that "certain countries of concern" are using U.S. sensitive personal data to engage in a wide range of malicious activities that harm U.S. national security interests.
- Stems from view that existing law is insufficient to address these risks.
- Objective of the Rule is to categorically prohibit or restrict access by **countries of concern** (e.g., China & Russia) to Americans' **bulk sensitive personal data** and **U.S. government-related data**—even when anonymized—when such access would pose an unacceptable risk to the national security of the United States.
- Violations may result in civil or criminal penalties.

Represents the first time the U.S. government has sought to regulate U.S. personal data **for national security reasons**—as opposed to privacy or other reasons.

Countries of Concern & Covered Persons

Privacy+ Security Forum

Countries of Concern

China
(including Hong Kong & Macau)

Cuba

Iran

North Korea

Russia

Venezuela

Covered Persons

- Foreign entity organized, chartered, or with principal place of business in a CoC
- Foreign entity 50% or more owned, directly or indirectly, by one or more CoCs or covered person entities
- Foreign person who is an employee/contractor of a CoC or covered person entity
- Foreign person who is primarily resident in the territorial jurisdiction of a CoC
- A person designated by the Attorney General (wherever located)

Sensitive Personal Data

Privacy+ Security Forum

Covered Personal Identifiers – e.g., device or hardware-based identifiers, IP address, advertising ID, account authentication data, or demographic/contact info, when linked to another identifier/data.

Precise Geolocation Data – real-time or historical data that identifies the physical location of an individual or device with a precision of within 1,000 meters.

Biometric Identifiers – measurable physical characteristics or behaviors used to recognize or verify the identity of an individual.

Human 'Omic Data – human genomic data, human epigenomic data, human proteomic data, and human transcriptomic data (excludes pathogen-specific data embedded in human 'omic data sets).

Personal Health Data – e.g., health information that indicates, reveals, or describes the past, present, or future physical or mental health or condition of an individual.

Personal Financial Data – e.g., an individual's credit, charge, debit card, or bank account, including purchases and payment history.

Government-Related Data

Privacy+ Security Forum

Geolocation Data

Any precise geolocation data, **regardless of volume**, for any location within any area enumerated on the Government-Related Location Data List (the Rule includes 736 locations)

Sensitive Personal Data

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 Statement Government, including the military and Intelligence Community

Prohibited Transactions

Privacy+ Security Forum

Data Brokerage Transactions

- **Data Brokerage**: "[S]ale 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."
- Data brokerage transactions with any foreign person are prohibited unless contractual terms for onward transfers are in place

Human 'Omic Data

- Any covered data transaction that provides a country of concern or covered person with access to: Bulk human 'omic data or human biospecimens from which bulk human 'omic data can be derived.
- **Human Biospecimen**: A quantity of tissue, blood, urine, or other human-derived material; excluded if "intended by a recipient solely for use in diagnosing, treating, or preventing any disease or medical condition."

Evasions, Attempts, Causing Violations, and Conspiracies

- Any transaction that has the purpose of evading or avoiding, causes a violation of, or attempts to violate the Rule, including any conspiracy formed to violate the Rule.

Knowingly Directing

- Knowingly directing any covered data transaction that would be a prohibited transaction or restricted transaction that fails to comply with the requirements.

Restricted Transactions

Privacy+ Security Forum

Employment Agreement

Vendor Agreement

Investment Agreement

- Organizational-Level and System-Level Requirements
  - Documentation and policy requirements
  - Logical and physical access controls
  - Data risk assessments
- Data-Level Requirements
  - Data minimization/masking, encryption
  - Access to "covered data" permitted when "the combination of security mechanisms deployed fully and effectively prevents access to covered data that is *linkable, identifiable, unencrypted, or decryptable* using commonly available technology by covered persons and/or countries of concern"

SECURITY REQUIREMENTS
FOR RESTRICTED TRANSACTIONS
E.O. 14117 Implementation

JANUARY 2025

SECURITY REQUIREMENTS FOR RESTRICTED TRANSACTIONS
Pursuant To Exec. Order 14117, *Preventing Access To Americans' Bulk Sensitive Personal Data And United States Government-Related Data By Countries Of Concern*

On February 28, 2024, President Biden signed Executive Order (E.O.) 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern*, to address national-security and foreign-policy threats that arise when countries of concern and covered persons can access bulk U.S. sensitive personal data or government-related data that may be implicated by the categories of restricted transactions.

As directed by E.O. 14117, CISA has developed the following security requirements to apply to classes of restricted transactions identified in regulations issued by the Department of Justice (DOJ). *See generally* 28 C.F.R. part 202 (identifying classes of restricted transactions at 28 C.F.R. § 202.401).

BACKGROUND

The security requirements are designed to mitigate the risk of sharing U.S. government-related data or bulk U.S. sensitive personal data with countries of concern or covered persons through restricted transactions.[1] They do this by imposing conditions specifically on the covered data, as defined below, that may be accessed as part of a restricted transaction; on the covered systems, as defined below, more broadly; and on the organization as a whole. While the requirements on covered systems and on an organization's governance of those systems apply more broadly than to the data at issue and the restricted transaction itself, CISA assesses that implementation of these requirements is necessary to validate that the organization has the technical capability and sufficient governance structure to appropriately select, successfully implement, and continue to apply the covered data-level security requirements in a way that addresses the risks identified by DOJ for the restricted transactions. For example, to ensure and validate that a covered system denies covered persons access to covered data, it is necessary to maintain audit logs of such accesses as well as organizational processes to utilize those logs. Similarly, it is necessary for an organization to develop identity management processes and systems to establish an understanding of what persons may have access to different data sets.

In addition to requirements on covered systems, applying security requirements on the covered data itself that may be accessed in a restricted transaction is also necessary to address the risks. The specific requirements that are most technologically and logistically appropriate for different types of restricted transactions may vary. For example, some transactions may be amenable to approaches that minimize data or process it in such a way that does not reveal covered data to covered persons. In other cases, techniques such as access control and encryption may be more appropriate to deny any access by covered persons to covered data. The security requirements contemplate multiple options to minimize the risk to covered data, though all of the options build upon the foundation of the requirements imposed on covered systems and the organization as a whole. While U.S. persons engaging in restricted transactions must implement all of the organizational- and covered-system level requirements, such persons will have some flexibility in determining which

[1] CISA notes that these security requirements are, as required by the E.O., designed to "address the unacceptable risk posed by restricted transactions, as identified by the Attorney General." E.O. 14117 Sec. 2(d). They are not intended to reflect a comprehensive cybersecurity program. For example, several areas addressed in CISA's Cross-Sector Cybersecurity Performance Goals (CPGs), available at https://www.cisa.gov/cross-sector-cybersecurity-performance-goals, are not reflected in the data security requirements, even though the CPGs themselves are a common set of protections that CISA recommends all critical infrastructure entities voluntarily implement to enhance their baseline security posture. As the nation's cyber defense agency and the national coordinator for critical infrastructure security and resilience, CISA recommends that all U.S. persons implement cybersecurity best practices in light of the risk and potential consequence of cyber incidents.

CISA | DEFEND TODAY, SECURE TOMORROW

CISA-ExternalAffairs@hq.dhs.gov

Restricted Transaction Compliance Requirements

Privacy+ Security Forum

Diligence and Audit

- Data compliance program must have procedures for verifying the data flows and the identity of vendors involved.
- Must conduct annual audits by an "independent" auditor.

Data Compliance Policy and Recordkeeping

- U.S. persons engaging in covered data transactions must keep a full and accurate record of each such transaction and maintain such record for ten years.
- U.S. persons engaging in restricted transactions have additional records requirements, including maintaining a written policy that describes data compliance program.

Reporting

- U.S. persons who have "received and affirmatively rejected (including automatically rejecting using software, technology, or automated tools) an offer from another person to engage in a prohibited transaction involving data brokerage" within 14 days of rejection.
- Additional reporting requirements in select circumstances, and DOJ may require additional reports to be furnished on demand.

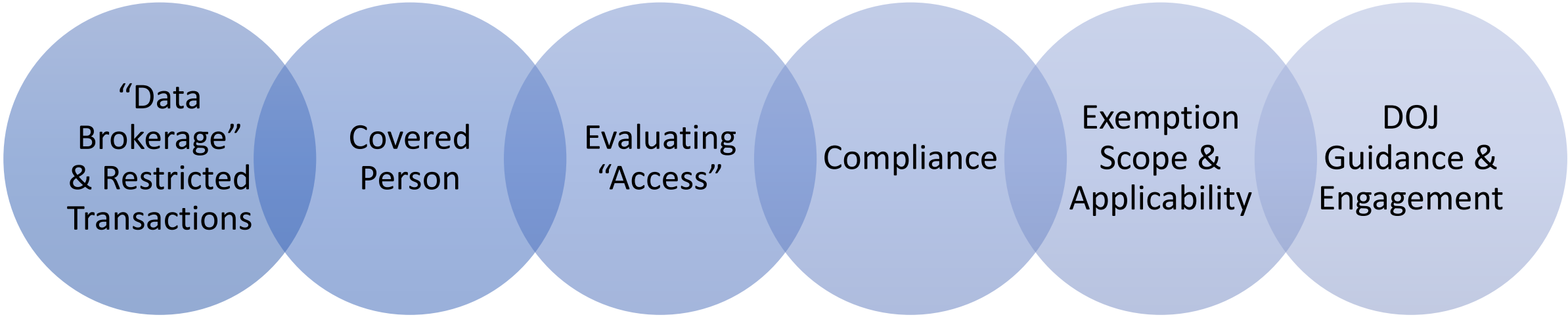
Exemptions

Privacy+ Security Forum

1	Corporate Group Transactions
2	Financial Services
3	Official Business of the U.S. Government
4	Travel
5	Personal Communications
6	Information or Informational Materials
7	Transactions Required or Authorized by U.S. Federal Law or International Agreements
8	Life Sciences Exemptions
9	Investment Agreements Subject to a CFIUS Action
10	Telecommunications Services

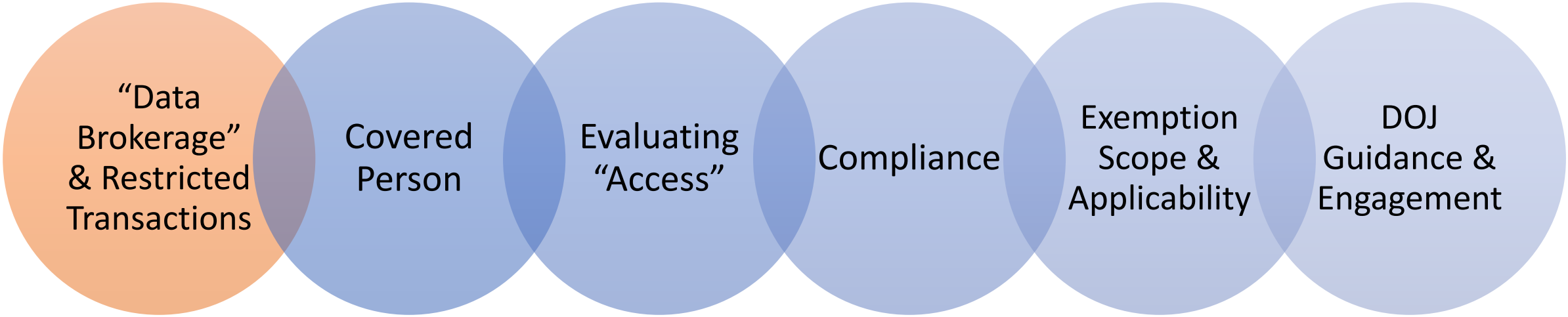
Key Areas of Consideration

Privacy+ Security Forum

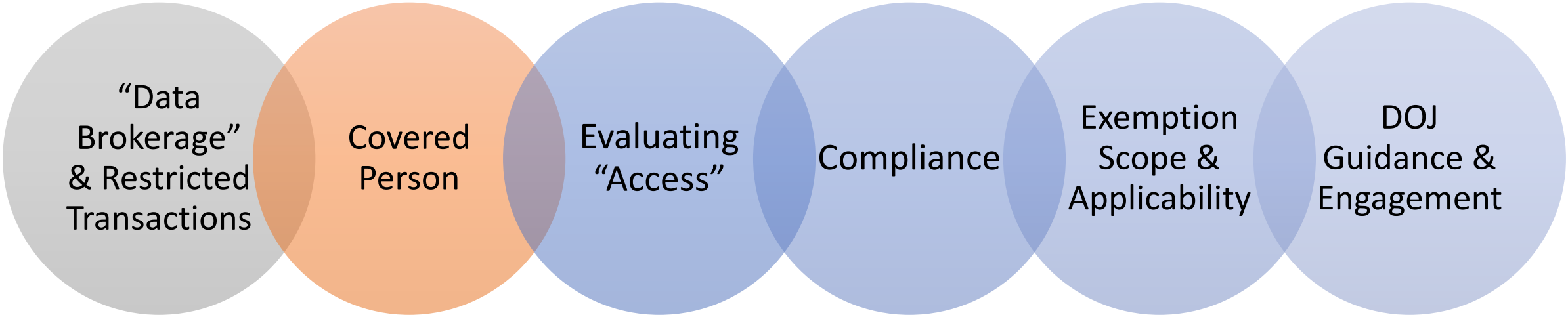


Key Areas of Consideration

Privacy+ Security Forum

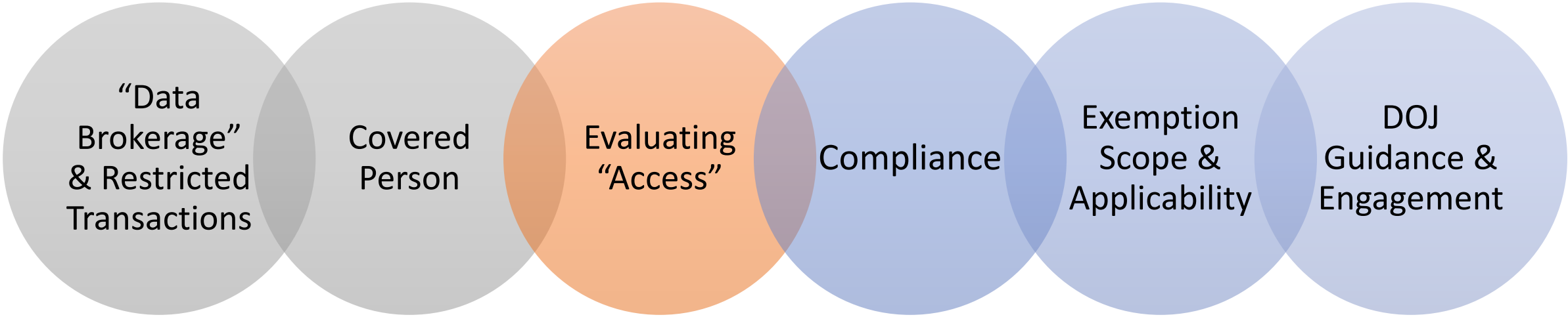


Key Areas of Consideration

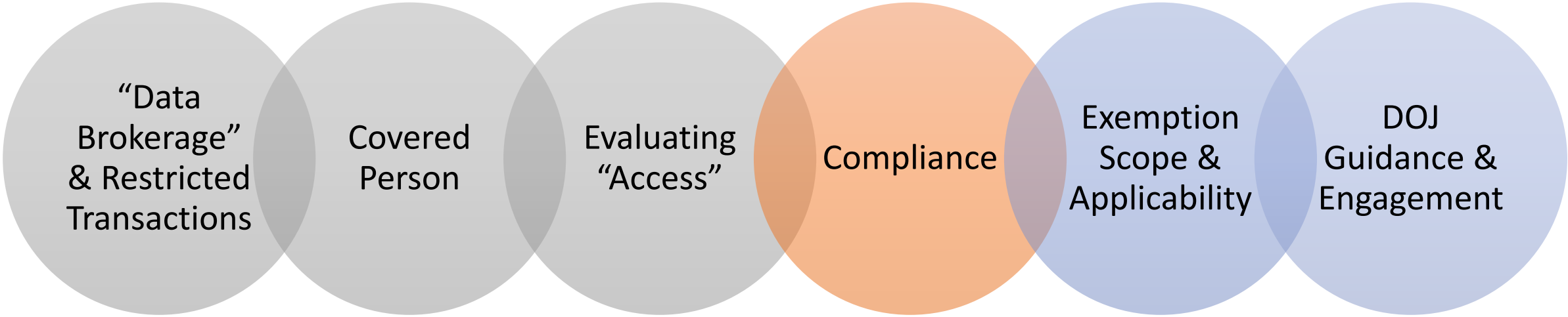


Key Areas of Consideration

Privacy+ Security Forum

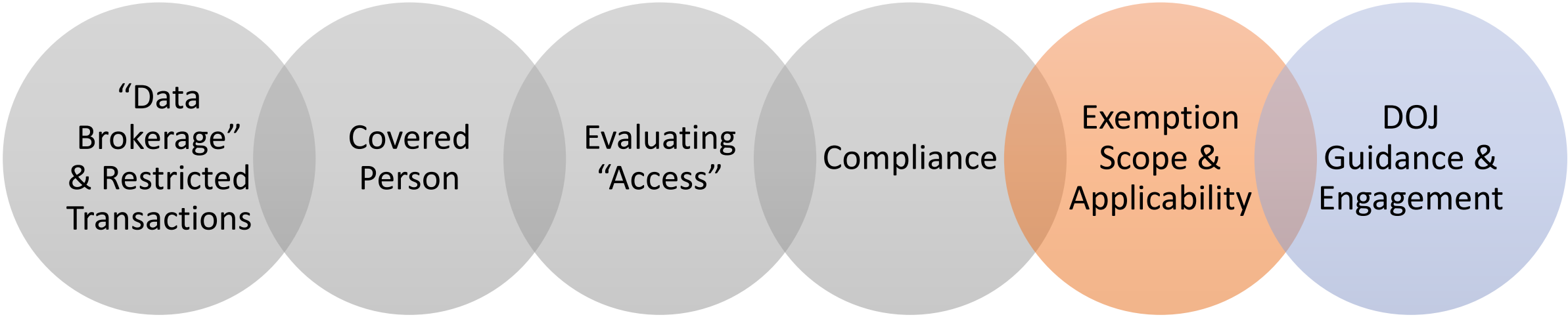


Key Areas of Consideration



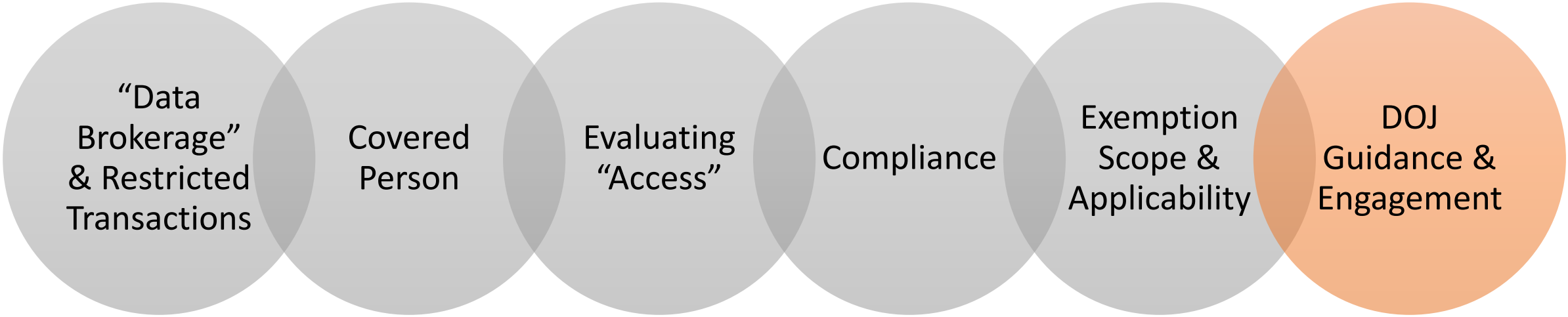
Key Areas of Consideration

Privacy+ Security Forum



Key Areas of Consideration

Privacy+ Security Forum



Questions & Contacts

Privacy+ Security Forum

Julia Post

Of Counsel
Covington & Burling

Ingrid Price

Special Counsel
Covington & Burling

Joseph Whitlock

Executive Director,
Global Data Alliance
Senior Director, Policy Business
Software Alliance