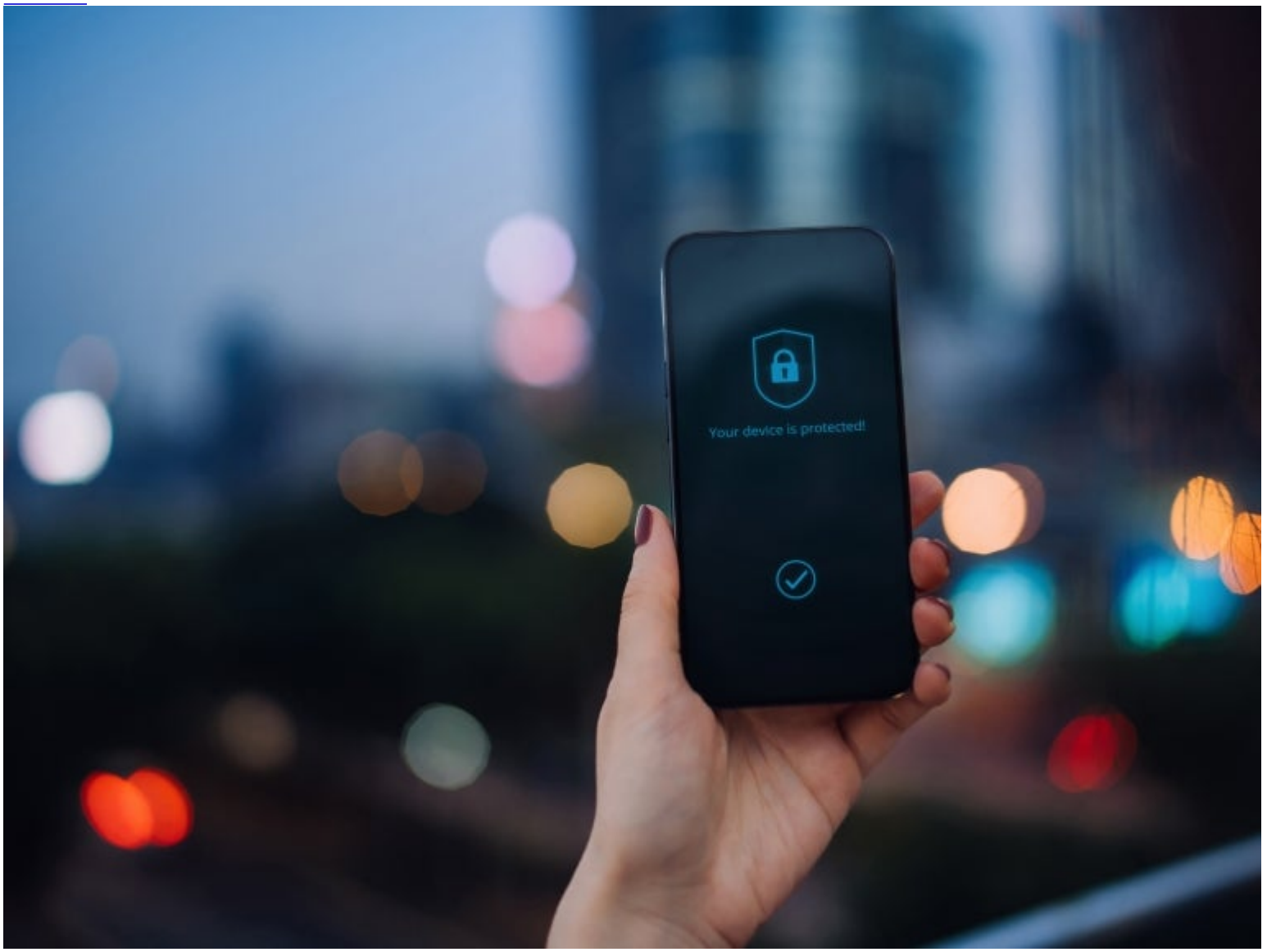
Articles



In October 2024, the U.S. Department of Justice (DOJ) issued a 420-page Notice of Proposed Rulemaking (NPRM) to implement Executive Order (EO) 14117, which directed DOJ to issue implementing regulations and directed the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) to develop related security measures for classes of transactions related to countries' access to sensitive personal data and government-related data. DOJ's NPRM is highly anticipated, and while it is similar to DOJ's March 2024 Advance Notice of Proposed Rulemaking (ANPRM), it includes changes in response to public comments on the ANPRM.

The NPRM raises important considerations for all businesses that sell, license, or otherwise transfer data or give access to data, whether through direct transactions or through vendor, employment, or investment agreements.

The proposed rule is not a privacy rule. It is a national security rule. As a result, although privacy regimes and the NPRM cover much of the same territory, the NPRM is drafted with a different approach that may be unfamiliar to data privacy professionals. For example, the NPRM does not exempt encrypted or anonymized data from its scope. It does not distinguish among different categories of participants in a data transaction or between controllers and processors of data. Terms such as "data brokerage" refer to a type of data transfer, not to a specific category of business.

Notable Updates from the ANPRM

While the NPRM generally tracks the ANPRM, DOJ has solicited, received, and addressed feedback. Updates include:

- Addressing third-party provider concerns in an expanded discussion of the "knowingly" standard.
- Refining the discussion of intra-entity data transfers, now referred to as "Corporate Group Transactions."
- Defining "Precise Geolocation Data" to include IP address geolocation under some circumstances.
- Modifying the definition of "personal health data."
- Focusing on data disclosures through artificial intelligence and advertising.
- Defining bulk thresholds.
- Providing additional description of exempt transactions.
- Including specific provisions related to medical research.
- Cross-referencing new security controls proposed by CISA.
- Providing more description of licensing, compliance, and enforcement proposals.
- Confirming that inconsistencies between the NPRM and more common privacy controls are intentional and based on national security considerations.
- Confirming DOJ's commitment to covering encrypted and anonymized data.

Scope

At a high level, the NPRM focuses on reducing access by "countries of concern" (CoCs) to sensitive data of U.S. persons, whether directly or through "covered persons" (CPs). The NPRM lists six categories of data as "sensitive personal data" that are subject to prohibitions and restrictions, including (1) covered personal identifiers, (2) precise geolocation data, (3) biometric identifiers, (4) human genomic data, (5) personal health data, and (6) personal financial data. The NPRM's restrictions only apply to data transactions involving these categories of sensitive personal data if they exceed "bulk thresholds" at any point in the preceding 12 months.

In addition to sensitive personal data, the NPRM also proposes regulations on government-related data, regardless of its volume, which includes (1) precise geolocation data for locations within DOJ's Government-Related Location Data List and (2) sensitive personal data marketed as linked or linkable to current or recent former U.S. government employees or contractors or to former senior U.S. government officials.

Prohibited and Restricted Transactions

The NPRM *prohibits* certain covered data transactions with a CoC or CP, specifically (1) data brokerage and (2) covered data transactions involving access to bulk human data or biospecimens. The NRPM also *restricts* three categories of covered data transactions with a CoC or CP: (1) vendor agreements, (2) employment agreements, and (3) investment agreements (other than passive investments). Restricted transactions are only permitted if they comply with the new CISA security requirements. For both prohibited and restricted transactions, the U.S. person must knowingly engage in those covered transactions for the NPRM to apply.

Violations of the NPRM can result in both civil and criminal penalties, with willful violations leading to substantial criminal fines and up to 20 years of imprisonment.

Considerations for Businesses

U.S. businesses should assess whether they expose covered U.S. person or U.S. government-related data to countries of concern or to covered persons. A business does not have to be a "data broker" or even transact primarily in data for the proposed rule to have substantial implications. Outsourced data processing and storage or information technology services, for example, may present unanticipated risk. Reliance on encryption for privacy compliance purposes will not be sufficient under the new national security rule.

Third-party providers of communication-related services should assess whether their customers' use of their services could be imputed to the provider under the "knowingly" standard.

Businesses that engage in restricted (and even exempt) transactions should develop risk-based compliance programs, which are covered in a separate Update.

Businesses should also review the substance of the NPRM and consider offering comments and feedback on the NPRM to DOJ by the **commenting deadline on November 29, 2024**.

Related Content for Businesses to Review

To read more about the NPRM-related proposed regulations by DHS CISA, please see here.

Authors

David Aaron

Senior Counsel
DAaron@perkinscoie.com

Stephanie Olson

Counsel
SOlson@perkinscoie.com 206.359.3025

Stephanie Duchesneau

Associate
SDuchesneau@perkinscoie.com 202.434.1671

Mason Ji

Associate
MJi@perkinscoie.com 206.359.6308

Explore more in

Privacy & Security Life Sciences & Healthcare Technology & Communications