Evading DOJ Crosshairs As Data Security Open Season Starts

By **Christian Everdell and Marvin Lowenthal** (July 7, 2025)

Christian Everdell

Marvin Lowenthal

The U.S. Department of Justice has added a new weapon to its enforcement arsenal, aimed at enhancing its ability to prevent foreign adversaries from accessing and exploiting government-related data and sensitive personal data of U.S. citizens — and this one has teeth.

The data security program was enacted under Executive Order No. 14117 on preventing certain countries from accessing Americans' sensitive data and U.S. government-related data. The DSP gives the DOJ's National Security Division the ability to pursue civil enforcement actions and criminal prosecutions against U.S. nationals and companies that engage in a wide range of data transactions that allow access to sensitive U.S. personal data and government data to designated countries of concern, as well as people and entities associated with those countries.

The scope of the DSP is broad and has the potential to affect any U.S. company that collects bulk quantities of sensitive data, including personal financial data, geolocation data, biometric data and personal health data.

The DSP's prohibitions and restrictions took effect on April 8, but the DOJ provided a 90-day grace period to give time for U.S. companies to bring their policies and business activities into compliance with the new rules. That grace period ends on July 8, and open season begins.

It remains to be seen how aggressively the DOJ will use this new enforcement tool. But with potentially steep civil penalties and even criminal prosecution at stake, U.S. companies will need to understand the contours and potential pitfalls of the DSP regulations to avoid falling into the DOJ's crosshairs.

Origins of the DSP

The DSP rules enact a regulatory framework to implement the goals of Executive Order No. 14117, issued by then-President Joe Biden on Feb. 28, 2024, pursuant to his authority under the International Emergency Economic Powers Act.[1]

The executive order addressed the new threat posed by the growth of artificial intelligence, which has magnified the danger of foreign adversaries systematically accessing and exploiting Americans' sensitive personal data.

U.S. companies across a wide range of business sectors now collect, store, and sometimes license or sell large volumes of sensitive data, such as demographic details, contact information, genomic sequences, biometric identifiers, geolocation trails, health data and financial records.

Executive Order No. 14117 recognized that foreign adversaries who have access to this type of bulk sensitive personal data, or sensitive government data, could use AI to analyze and

manipulate that data to engage "in a wide range of malicious activities" that threaten the "security, privacy, and human rights" of all Americans.[2]

Accordingly, the executive order directed the attorney general, in coordination with the secretary of homeland security and in consultation with other agencies, to craft enforceable regulations aimed at preventing countries of concern from obtaining bulk sensitive or government-related data.[3] The DSP regulations, codified in Title 28 of the Code of Federal Regulations, Part 202, are the result of that effort.

The DSP's Prohibitions and Restrictions

At its core, the DSP regulations limit the ability of U.S. persons — which include U.S. nationals wherever they are located, U.S.-based companies and their foreign branches, and anyone physically present in the U.S.[4] — from engaging in a covered data transaction.

A "covered data transaction" is defined as "any transaction that involves any access by a country of concern or covered person 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."[5]

The DSP regulations provide lengthy and nuanced definitions for each of these terms. We do not repeat them in full here, and instead summarize certain key definitions as follows:

- "Country of concern" means a foreign adversary who "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."[6] Currently, the designated countries of concern are China, including Hong Kong and Macau; Cuba; Iran; North Korea; Russia; and Venezuela.[7]

- "Covered person" includes, among other things, (1) a foreign entity that is organized under the laws of a country of concern or has its principal place of business there, (2) a foreign entity that is 50% or more owned by a country of concern, (3) a foreign individual who is an employee of either such entity, or (4) a foreign individual who primarily resides in a country of concern.[8]

- "Bulk U.S. sensitive personal data" means "a collection or set of sensitive personal data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted," where the volume of the data meets or exceeds certain threshold requirements.[9]

- "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."[10]

The DSP prohibits certain covered data transactions — in particular, those involving data brokerage — and restricts others.[11] For example, the DSP prohibits U.S. persons from (1) "knowingly engag[ing] in a covered data transaction involving data brokerage with a country of concern or a covered person," or (2) knowingly engaging in any transaction involving data brokerage where a foreign, noncovered person gains access to bulk sensitive U.S. data, unless there is a binding contractual provision prohibiting the foreign person from

reselling the data to others.[12] Attempts to evade or cause violations of the DSP are also prohibited.[13]

On the other hand, the DSP imposes restrictions on U.S. persons who knowingly engage in a covered data transaction involving a vendor agreement, employment agreement or investment agreement with a country of concern or covered person.[14] U.S. persons can engage in these transactions, but only if they meet certain security and compliance requirements outlined in the regulations.[15]

Potential Pitfalls

As with any complicated regulatory enforcement framework, the DSP contains numerous potential pitfalls that may not be immediately obvious without a close reading of the rules. Helpfully, the DSP regulations provide numerous illustrative examples that attempt to clarify which types of transactions fall, and do not fall, within the scope of the DSP. But the regulations cannot, and do not, answer every question or address every potential factual scenario, and their broad sweep could potentially ensnare unwary U.S. companies.

For example, a U.S. company might think that it could contract with a Chinese cloud computing company to store its customers' financial information as long as the data was fully encrypted. However, the DSP regulations make clear that it is irrelevant whether sensitive personal data "is anonymized, pseudonymized, de-identified, or encrypted,"[16] and that such a vendor agreement would still be a restricted transaction.

Similarly, a U.S. company that collects bulk geolocation data from its customers might think that a covered foreign company could purchase a minority stake in the U.S. company as long as the investment agreement specifically prohibited the covered foreign company from accessing the sensitive data. But the DSP regulations explain that, unless the investment is purely passive, the investment agreement would still be a restricted transaction regardless of the contractual provision forbidding access.[17]

U.S. companies may also get tripped up by the level of knowledge required to meet the threshold for a DSP violation. Criminal prosecutions will be reserved for U.S. persons who acted willfully — i.e., who knew their conduct was unlawful. But civil enforcement actions under the DSP have a far more permissive threshold. The DOJ can bring a civil enforcement action against a U.S. person who "knowingly" violated the DSP, which means that the U.S. person "ha[d] actual knowledge, or reasonably should have known, of the conduct [or] circumstances" that gave rise to the violation.[18]

The DSP regulations highlight the potential for these sorts of civil violations with AI algorithms. The regulations offer an example of a U.S. company that trains the algorithm for an AI chatbot with bulk U.S. sensitive personal data and then licenses access to the chatbot worldwide, including to covered persons, even though the U.S. company has reason to know that the chatbot may disclose the sensitive data used to train it when responding to queries.

According to the regulations, even though the chatbot license itself did not give covered persons access to the underlying sensitive data, the U.S. company still violated the DSP because it "reasonably should have known" that "the license [could] be used to obtain access to the U.S. persons' bulk sensitive personal training data if prompted."[19]

This is more than a hypothetical concern. For example, when issuing the final version of the DSP regulations, the DOJ noted that journalists were able to create movement profiles identifying where tens of thousands of military and national security officials lived, as well

as their hobbies, by using lawfully purchased geolocation data.[20]

If this type of data were used to train an AI algorithm, users of the AI could potentially learn sensitive information by asking the AI questions designed to elicit that information. For example, users could ask the AI to list places outside of city limits where known military personnel repeatedly gather in an effort to find hidden bases.

Even an inadvertent disclosure of such sensitive information would likely cause the DOJ to scrutinize the conduct of the U.S. persons who controlled and licensed the AI.

Conclusion

As enforcement of the DSP shifts from anticipation to action, counsel should take steps now to mitigate risk and buttress their data collection and handling practices, such as conducting a DSP-specific data audit, and reviewing and revising contracts that involve data sharing with foreign counterparties.

The DSP introduces broad, complex and significant compliance obligations that deeply affect the operational mechanics of data handling, contracting and cross-border engagement. Even well-intentioned data strategies — if not carefully structured — can now trigger potential civil liability or criminal scrutiny.

And with the 90-day grace period for enforcement actions ending on July 8, we can expect the DOJ to begin looking for test cases to enforce the DSP against U.S. persons who improperly engage in prohibited and restricted data transactions.

Christian R. Everdell is a partner, and head of the U.S. privacy and data security group, at Cohen & Gresser LLP. He previously served as an assistant U.S. attorney in the U.S. Attorney's Office for the Southern District of New York.

Marvin J. Lowenthal is counsel at Cohen & Gresser.

[1] Executive Order 14117: Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern (February 28, 2024) ("EO 14117").

[2] EO 14117, preamble.

[3] Id., Section 2(a)-(c).

[4] 28 C.F.R. § 202.256.

[5] 28 C.F.R. § 202.210.

[6] 28 C.F.R. § 202.209.

[7] 28 C.F.R. § 202.601(a).

[8] 28 C.F.R. § 202.211.

[9] 28 C.F.R. §§ 202.205-06.

[10] 28 C.F.R. § 202.214.

[11] The DSP regulations also list several types of data transactions that are exempt from these prohibitions and restrictions. See 28 C.F.R. §§ 202.501-11. We do not address these here.

[12] 28 C.F.R. §§ 202.301-02.

[13] 28 C.F.R. §§ 202.304-05.

[14] 28 C.F.R. § 202.401.

[15] 28 C.F.R. §§ 202.248, 202.1001-02, 202.1101-04.

[16] 28 C.F.R. § 202.206.

[17] 28 C.F.R. § 202.228(c)(3).

[18] 28 C.F.R. § 202.230(a).

[19] 28 C.F.R. § 202.301(b)(1).

[20] 90 FR 1638.