Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Feds Put Heat On Foreign Data Transfers With Sweeping Rules

By **Allison Grande**

Law360 (May 9, 2025, 9:43 PM EDT) -- The U.S. Department of Justice's unexpected guidance and brief enforcement reprieve on a national data security program intended to curb foreign access to Americans' sensitive data has handed companies some welcome breathing room, but the strong interest that federal enforcers have shown in the topic means that businesses can't afford to delay compliance efforts.

In one of the few holdovers from the Biden administration, the DOJ's National Security Division confirmed last month that it's forging ahead with a new data security program that requires companies to take steps to prevent the large-scale transfer of Americans' genomic, biometric, personal health, geolocation, financial and other kinds of sensitive data to China, Russia and other foreign adversaries, while issuing a "best practices" guide featuring a list of more than 100 frequently asked questions to aid compliance.

"While the guidance wasn't a radical departure from anything that the government has said previously, it did provide helpful details and put more meat on the bone about companies' due diligence, contracting and auditing obligations," Gary Kibel, a data privacy and security partner at Davis+Gilbert LLP, told Law360.

Aside from fleshing out the sweeping bulk data transfer rules, the National Security Division also informed the public that it would "not be prioritizing" civil enforcement actions against covered companies and individuals for violations that occur between the program's April 8 effective date and July 8, as long as those entities are "engaging in good faith efforts to comply with or come into compliance with" the framework.

In instituting this three-month delay, the NSD acknowledged that covered entities may need to take time-consuming steps such as conducting internal reviews of data flows to determine whether the program's prohibitions and restrictions on certain commercial transactions apply to their activities and drafting or revising policies and contracts with third parties, a recognition that experts say is vital.

"The rule is very dense and complicated, and while it's not clear how an investigation might take place, the NSD's guidance provides enough illustrious examples for companies to make the necessary adjustments to take reasonable steps and act in good faith, which, if they can do that, should put them well ahead of any enforcement action or inquiry," said Artie McConnell, the co-leader of the national security investigations and litigation task force at BakerHostetler and a former assistant U.S. attorney in the Eastern District of New York.

He added that while these type of export controls and restrictions may be familiar to defense contractors that regularly work with the government, the rule significantly "expands that regime to the industry writ large" by broadly applying to businesses across industry sectors that amass large quantities of sensitive data such as biometrics, health and financial information.

Even though the NSD has indicated it won't jump straight to enforcement, companies shouldn't waste any time heeding the rules and the division's accompanying guidance, especially given the caveat that only entities that are engaged in "good faith" compliance efforts are eligible to avoid immediate regulatory scrutiny.

"It's an area for everyone to take seriously and make sure they're at least doing an assessment of their systems," said Loyaan Egal, a Morgan Lewis & Bockius LLP partner who formerly served as deputy chief in the foreign investment review section in the NSD. "This has definitely been set up in a way where companies need to ask for permission [for data transfers] on the front end and don't want to be asking for forgiveness later."

When enforcement does start to heat up, the NSD — which has the power to impose both civil penalties of up to $368,136 per violation or twice the amount of the infringing transaction, whichever is greater, and criminal penalties that can include a fine up to $1 million or up to 20 years imprisonment — is expected to pay close attention to this issue in light of its apparent significant to the current administration, as evidenced by officials electing to carry on with the data security program despite its creation having been mandated through an executive order signed by former President Joe Biden last year, attorneys say.

"This is a regulation focused on national security, and anything involving national security is going to have heightened scrutiny," said Egal, noting that the final rule highlights the consistency between administrations on national security and foreign data transfer issues. "But at the same time, there are still a lot of gray areas that require more specificity and the government has to appreciate that having companies make this significant dedication of resources to a completely new regime is going to take time."

While the NSD is likely to want to vigorously enforce the rule and has deep experience dealing with national security matters like countering terrorism and export control, the division also has limited resources that are being further constricted by the current administration's push to make cuts across the government, which is likely to "put a lot of strain on the division's ability to do monitoring and enforcement as needed" and lead to more targeted enforcement, Egal said.

"What we're likely to see will be a strategic effort where the NSD will pursue enforcement where it can get the most return on its investment, where the action can have not only a significant deterrent effect on a specific entity but also general deterrence," Egal said.

The DOJ unit could, however, receive an enforcement assist from a somewhat unexpected source: the Federal Trade Commission.

During a keynote address at the International Association of Privacy Professionals' Global Privacy Summit in Washington, D.C., last month, FTC Commissioner Melissa Holyoak flagged as one of her top priorities the need to bring "stronger enforcement against companies that sell, transfer and disclose Americans' sensitive personal data, like precise geolocation data," in bulk to foreign adversaries who can

use this information for nefarious activities such as surveillance and blackmail.

Holyoak, who is one of the three commissioners at the currently all Republican-led agency, said that she expected the FTC to not only continue to use its abilities to police unfair and deceptive practices to clamp down on foreign adversaries gaining access to this data by tricking consumes with misleading privacy disclosures or by hacking companies that hold this information, but also to pay closer attention to the "often overlooked way" that foreign adversaries are moving to purchase data in bulk from data brokers and others that gather data from "unwitting" individuals.

In order to address the latter scenario, Holyoak teased that the commission could use its new enforcement powers under the Protecting Americans' Data from Foreign Adversaries Act, which was enacted last April and **prohibits data brokers** from transferring, selling or providing access to Americans' sensitive personal data to China and other foreign adversaries.

Holyoak, who previously served as the solicitor general of Utah, also revealed that, "in the future, there may be opportunities to partner with the Department of Justice as it enforces its recently-enacted rule that restricts the transfer of Americans' sensitive personal data from countries of concern."

With regulators squarely focused on this issue, companies that could get swept up by the regulation need to get to work building a "fulsome" data compliance program, noted Christian Auty, U.S. lead of the global data privacy and security practice at Bryan Cave Leighton Paisner LLP, adding that the NSD's new compliance guide can provide "a good roadmap" for the creation of such a framework to support continuing permissible transactions to foreign entities.

Additionally, "the compliance guide indicates that U.S. persons should ensure that compliance with the final rule is supervised by senior-level employees and that such employees participate in and execute annual certifications required by the rule," Auty noted, further ramping up pressure on organizations to get their affairs in order.

One of the first steps that companies should take is understanding what data they hold, where it's going and if these transmissions are covered by the broad restrictions in the bulk data transfer rule.

"The final rule unquestionably creates a new class of sensitive data going forward," Auty said. "What I mean by this is that data that qualifies as sensitive data will need to be accounted for by every organization to ensure compliance with the final rule. This means it will need to be located, mapped, counted and tracked."

This analysis also applies to the U.S. subsidiary of a foreign corporation, noted Christopher Kavanaugh, a partner at Cleary Gottlieb Steen & Hamilton LLP and former federal prosecutor.

"Those [U.S.] companies could come within the rule's scope, and they will need to consider whether the foreign parent has access to covered data, and how they are using or sharing it," Kavanaugh said.

While most companies should be able to use existing learning, procurement and contract management resources, the final rule creates a definition of sensitive data not found in any other existing data privacy or transfer regime — including in the way it sweeps up transactions that involve de-identified and anonymized data — and includes no thresholds or exemptions, meaning that it "may be new territory for some," Auty said.

The guidance also identifies classes of prohibited and restricted transactions, auditing and due diligence requirements for restricted transfers, and the process for applying for general or specific licenses to permit prohibited transfers that companies should become familiar with, even though the NSD has said it won't be issuing specific licenses during the 90-day transition period, attorneys say.

"Companies should be focused on doing inventory of their data and who has access to that in order to determine whether those findings require compliance with these rules, and if they do, ramping up their auditing, reporting and other compliance capabilities in order to meet the good faith effort that the DOJ says it's looking for," said Morgan Lewis' Egal.

The new rule will also require companies to look beyond their own systems in order to review and potentially renegotiate their vendor contracts to ensure that these transactions are compliant and information isn't being passed along to any blacklisted entities, attorneys noted. While the guidance helpfully includes model contractual language for these agreements, companies will also need to regularly monitor these interactions and screen vendors against covered persons list, which the NSD is still preparing, that identifies and designates those subject to the control and direction of foreign adversaries.

"There's no grandfathering in of older contracts, so if companies are dealing with any data at all that could meet the definition of bulk U.S. sensitive personal data and are engaged in international data transfers, then they need to revisit their contracts, because it's likely this issue wasn't addressed in older form agreements," said Davis+GIlbert's Kibel.

As the regulations continue to get ironed out, companies may want to consider taking advantage of opportunities that the NSD pushes in its guidance for companies to voluntarily disclose inadvertent breaches of the data transfer rules and to submit additional unresolved questions for the division to address, attorneys said.

According to its guidance, the NSD "may consider a qualifying voluntary self-disclosure as a mitigating factor in any enforcement action, which may result in a reduction in the base amount of any proposed civil penalty" and that it would "use its best efforts to respond consistent with available resources" to any informal inquiries, which it may use to "develop and refine future guidance."

"Even if companies don't get a response, just putting those questions out there shows that they're thinking about these issues and trying to comply," said BakerHostetler's McConnell. "And that can be something that they can point to later on if the government comes knocking."

--Editing by Jay Jackson Jr. and Emily Kokoll.
