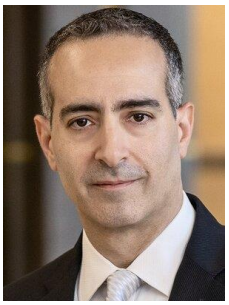
LAW360

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

Cos. Should Prepare For Foreign Data Transfer Regulations

By **David Plotinsky and Jiazhen Guo** (April 9, 2024, 5:11 PM EDT)


David Plotinsky


Jiazhen Guo

In the relatively near future, companies will be faced with a new regulatory regime designed to protect U.S. sensitive data from countries of concern.

This development has potentially far-reaching effects on a variety of companies — including companies that may not think of themselves as data companies — but with careful preparation, such companies can endeavor to minimize the effect on their business operations, and to put processes in place to ensure regulatory compliance.

On Feb. 28, President Joe Biden issued an executive order on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern."

Concurrent with the executive order, the U.S. Department of Justice published a draft advance notice of proposed rulemaking, or ANPRM, to establish a program to implement the executive order and to solicit public comments.

The program aims to safeguard an array of sensitive data that could otherwise be transferred through data aggregators, vendor agreements, employment agreements, or investment agreements to China, Cuba, Iran, North Korea, Russia and Venezuela.

Background

Although the program is designed to fill a gap in current legal authorities, it draws heavily from other national security regulatory processes, including the Committee on Foreign Investment in the United States, or CFIUS, export controls, and financial sanctions.

For the industry, therefore, compliance with those other regulatory regimes can provide at least a partial playbook to plan for the forthcoming regulations.

The executive order defines sensitive personal data to cover six categories: (1) covered personal identifiers; (2) geolocation and related sensor data; (3) biometric identifiers; (4) human 'omic data; (5) personal health data; and (6) personal financial data.

The program will regulate such data only in bulk if a dataset surpasses a threshold number of U.S. persons or devices. However, the bulk thresholds will not apply to transactions involving government-

related data, which includes (1) sensitive personal data linked to current or recent government employees and (2) precise geolocation data for any location within an area enumerated on a list of geofenced areas.

As proposed by the ANPRM, a "covered data transaction" involves bulk U.S. sensitive personal data or government-related data and involves a data brokerage, vendor agreement, employment agreement or investment agreement.

The ANPRM contemplates outright prohibitions of (1) data-brokerage transactions involving the transfer of bulk sensitive personal data or government-related data and (2) transactions involving the transfer of bulk human genomic data or biospecimens from which such data can be derived.

However, the program will permit data transactions involving (1) vendor agreements that contain the provision of goods and services, including cloud service agreements, (2) employment agreements and (3) investment agreements, but only if these three types of transactions comply with to-be-developed security requirements.

How Companies Can Prepare

In order to prepare for the new regulatory regime, there are steps that the industry can begin taking even while the government continues to develop the regulations.

Public Comment

Issuance of the executive order was preceded by industry outreach conducted by executive branch agencies, in the course of which the general contours of the new authority were previewed.

There is a 45-day public comment period that ends on April 19, and stakeholders should seriously consider filing comments to potentially influence how exactly the government scopes the new program. For instance, information about specific unintended consequences may be helpful.

Companies will also want to track comments submitted by others, and then stand by for a subsequent notice of proposed rulemaking that will contain proposed regulatory text. The NPRM will likely spur a second round of public comments, which will give stakeholders a final chance to provide input prior to the final rules being promulgated.

In addition, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency will conduct a separate rulemaking to develop security requirements that can make permissible an otherwise prohibited sensitive data transfer pursuant to a vendor agreement, employment agreement or investor agreement, as discussed above. Companies should therefore closely track that rulemaking process as well.

Timing

The executive order requires the DOJ to issue proposed rules within 180 days, which means the NPRM should be issued no later than Aug. 26.

Although the DOJ will need time to review additional comments received on the NPRM, we believe the government will attempt to issue final rules by the end of the year. That is a very ambitious goal,

however — especially if the November elections result in a presidential transition and the rulemaking therefore occurs during a lame-duck period.

We note that a separate executive order on regulating outbound investment in China and its accompanying ANPRM were issued in early August, and more than six months later, the U.S. Department of the Treasury has gathered public comments but has not yet issued a subsequent NPRM.

However, the Treasury is likely not as motivated to issue outbound investment regulations as the DOJ is to issue sensitive data transfer regulations, so companies should certainly be prepared for at least the possibility of regulations before the end of the year.

Exclusions and Exemptions

The ANPRM proposes to exclude certain types of passive investment from the scope of covered data transactions, similar to what was proposed in the ANPRM issued by the Treasury with respect to outbound investment regulations. Examples of proposed exclusions are investments in publicly traded securities, passive investment by limited partners, and investments below a de minimis threshold.

The program also proposes certain exemptions, mirroring those found in the government's approach to sanctions.

For example, proposed exemptions include transactions involving personal communications and informational materials; activities conducted for official government business; transactions integral to financial services or required for regulatory compliance, including banking and payment processing; and data exchanges between a U.S. person and its foreign subsidiary or affiliate.

Companies should carefully evaluate the potential exclusions and exemptions noted above, as well as others described in the ANPRM, and assess the extent to which the exemptions may enable them to continue their business operations unabated.

Due Diligence

As with many other regulatory regimes, the new rules governing sensitive data transfers will likely require that companies undertake new types of due diligence.

Many data transfers will certainly wind up outside the scope of the regulations, either because they are not covered in the first place or because they fall under one of the anticipated exemptions. However, the new regulations will require many companies to conduct new types of due diligence — both internal and with respect to planned transactions — to determine whether data transfers trigger the regulations.

In addition, the record of that diligence can help companies defend themselves from enforcement actions. Ideally, the diligence record will demonstrate to inquisitive regulators that a data transfer was permissible. However, even if the government determines otherwise, a record of thorough and rigorous diligence may help challenge a government determination or serve as a mitigating factor.

As the regulations continue to be developed, affected companies may want to start drafting new diligence checklists to address sensitive data transfers. Companies and their counsel will also need to decide the extent to which they are comfortable relying on checklists, versus doing deeper dives to obtain a higher degree of confidence that responses to diligence questions will be able to withstand any

future scrutiny by regulators.

Contractual Language

Companies will also likely devise new contractual language, similar to what is done to address other regulatory regimes.

For example, to address CFIUS risk it is common for foreign investors to request representations and warranties from U.S. companies that they are not so-called TID U.S. businesses — i.e., businesses involved in critical technology, critical infrastructure, or sensitive personal data, any of which can result in CFIUS jurisdiction or increased scrutiny.

As another example, it is standard for many investment funds to include provisions in limited partnership agreements that prevent foreign limited partners from obtaining certain rights that could trigger CFIUS jurisdiction.

Looking ahead to new regulations on sensitive data transfers, it seems likely that deal documents will start to include new language to protect U.S. investors, vendors, employers and other affected companies.

Such language could include representations that a company receiving data is not owned or controlled by, or subject to the jurisdiction or direction of, a country of concern. Additionally, on the part of the party transferring the data, it could include representations that the data is not sensitive data as defined by the regulations, or if it is, that the data is compliant with government-mandated security requirements that make certain otherwise prohibited transfers permissible.

Compliance and Enforcement

The program will require a risk-based compliance program, similar to the risk-based approach to sanctions compliance programs recommended by the Treasury's Office of Foreign Assets Control.

The new program does not aim to establish broad and uniform due diligence, recordkeeping or reporting standards, but rather the executive order directs the DOJ to adopt a compliance framework akin to OFAC's sanctions programs, under which companies and individuals are expected to design and implement compliance measures tailored to their specific risk profiles.

In the event of a violation, the DOJ would evaluate the adequacy of the compliance program as part of any enforcement action.

Companies should start thinking about standing up new compliance programs in anticipation of the new regulations. For companies that already have export control compliance programs, or sanctions compliance programs, those programs can be used as a starting point to work with counsel to put in place new compliance programs tailored to sensitive data transfers.

Advisory Opinions and Licenses

The ANPRM provides that transactions will not be reviewed by the government on a case-by-case basis. Rather, the regulations will establish generally applicable rules for engaging in specific categories of data transactions, and companies will be responsible for deciding on their own whether transactions are

covered — and will be subject to enforcement actions if they decide incorrectly.

This element of the new regime is similar to the executive order mentioned above that will result in new restrictions on outbound investment in China. Although those regulations remain pending with the Treasury, one potential concern is the compliance jeopardy for companies.

Perhaps in recognition of those concerns, the executive order and its accompanying ANPRM indicate that there will be mechanisms for companies to seek advisory opinions in advance of engaging in a transaction. Companies should start to think, therefore, about any of their activities that may not lend themselves to clear interpretation of the regulations.

The program will also involve a process for issuing both general and specific licenses. General licenses will provide the DOJ with flexibility to exempt certain types of transactions from regulation, modify the conditions of these transactions, or allow for phased terminations.

Specific licenses will enable companies and individuals to seek exemptions for engaging in particular data transactions. Companies may also therefore want to start thinking about data transfers that are likely to be within the scope of the new regulations but might be amenable to a license.

Overlap With Other Authorities

Companies and their counsel should also be prepared for the possibility that the new regulations on sensitive data transfers will overlap with other regulatory regimes. There is particular potential for overlap with CFIUS jurisdiction, and the ANPRM proposes to regulate foreign investments as restricted covered data transactions independently, until and unless CFIUS intervenes with mitigation measures to address national security risks.

Conclusion

The executive order adds another brick to the wall the government has been gradually building to keep certain data from getting transferred to China and other countries of concern.

For both U.S. companies and companies located in countries of concern, this new development adds yet another challenge to their efforts to carefully navigate an intricate geopolitical and regulatory landscape.

As those companies seek to continue their business operations while also remaining compliant with this increasingly complicated environment, it will be important to take proactive steps to understand and respond to the new executive order and the resulting regulations.

David Plotinsky is a partner at Morgan Lewis & Bockius LLP. He is former acting chief of the U.S. Department of Justice's Foreign Investment Review Section.

Jiazhen Guo is an associate at the firm.