Davis Polk

New national security package extends statute of limitations for sanctions violations

May 2, 2024 | Client Update | 15-minute read

The U.S. Congress attached a range of unrelated measures to the recent military aid package to Taiwan, Ukraine, and Israel extending the statute of limitations for sanctions violations, requiring the divestiture of TikTok, tightening sanctions on Russia and Iran, and restricting data brokers.

On April 24, 2024, President Biden signed into law the 21st Century Peace through Strength Act (the Act) as part of a broader foreign aid package providing funding to Taiwan, Ukraine, and Israel. The Act combines a series of unrelated national security provisions that, among other things:

- Extend the statute of limitations for violations of U.S. sanctions laws to 10 years;
- Require the President to identify individuals and entities that are targeted under the Russia-related sanctions programs of the European Union (EU) and United Kingdom (UK) but are not currently the subject of U.S. sanctions, in order to encourage "harmonization" of U.S. sanctions with those of the EU and UK;
- Prohibit OFAC from issuing licenses for transactions involving frozen Russian sovereign assets and authorizes the President to seize and repurpose certain Russian sovereign assets to fund Ukrainian war compensation or reconstruction efforts in Ukraine;
- Expand secondary sanctions targeting dealings with Iran and Hamas, along with other modest expansions of existing sanctions programs;
- Impose a deadline prohibiting the provision of services to distribute, maintain, or update TikTok for U.S. users unless it is divested by its parent company and provides a mechanism for banning other Chinese- or Russian-owned mobile applications (apps); and
- Prohibit data brokers from transferring personal data of U.S. persons to entities 20% or more owned by Chinese or Russian interests (among others) or based in those countries.

Because of the means by which they were adopted, the individual measures were not extensively debated or subject to amendment, and, while broadly consistent with recent themes in U.S. national security policy, may create some tensions or implementation challenges. We provide below a summary of some of the key elements of the Act and their implications.

Amendments to U.S. sanctions

Doubling statute of limitations for sanctions violations

The Act extends the statute of limitations for violations of the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA) – the two principal statutory authorities for U.S. sanctions – from 5 years to 10

years. Based on Supreme Court precedent, the extended statute of limitations will not apply to criminal prosecution of sanctions violations that have already become time-barred, but the effect on potential civil liability is less clear. The same analysis applies to violations of export control rules prior to the adoption of the Export Control Reform Act of 2018, which were governed by IEEPA (subsequent violations are governed by a five-year statute of limitations which remains unchanged).

As we have noted in prior client updates, the Office of Foreign Assets Control (OFAC) and the Department of Justice (DOJ) have increasingly adopted an aggressive enforcement posture for sanctions violations. In the long term, the extended statute of limitations is likely to significantly increase the number of enforcement cases brought by OFAC and DOJ, as well as the size of potential penalties. It is also likely to increase the burden on buyers in the merger and acquisition context, as the acquired liabilities now stretch back for a ten-year period.[1] Similarly, the scope of investigations of potential sanctions violations (often incorporating a five-year "lookback" period) may expand significantly. It is also likely that OFAC will amend its recordkeeping requirements under 31 CFR § 501.601 to extend the required retention period from 5 to 10 years.

The amendment of the IEEPA statute of limitations has wider implications, as IEEPA is a broad and flexible authority used for other measures related to national security. Recent executive orders underpinning proposed mechanisms to restrict outbound U.S. investment in China (discussed in our client update here), transfers of sensitive personal data regarding U.S. persons (discussed here), and controls on information and communications technology and services posing national security risks (discussed here and here) are all issued under authority of IEEPA as well.

Potential expansion of Russian sanctions lists

While the United States, EU, and UK have generally coordinated their sanctions response to Russia's invasion of Ukraine closely, their respective sanctions programs do not completely align. The biggest—though not the only—divergence has been the designation of individual Russian oligarchs and, to a lesser extent, financial institutions. The Act requires the President to identify and submit a report on any foreign persons that are targeted under EU and UK Russia-related sanctions and eligible for designation for United States blocking sanctions under specified Russia-related executive orders or the Global Magnitsky Human Rights Accountability Act, but that are not in fact designated. After submitting the report, the President "may impose sanctions" on any persons identified that are not currently the subject of U.S. sanctions.

While the Act does not require the President to impose sanctions on all the persons identified, nor is it likely that the areas of divergence among the lists are not already known, the requirement of a report is clearly meant to increase pressure on OFAC to expand (or, in the Act's terms, "harmonize") its designation of Russian oligarchs and others. Furthermore, while most potential sanctions targets have probably already been analyzed by OFAC, the process of preparing a formal analysis of whether each person and entity not listed is eligible for listing is likely to be a significant burden on OFAC's targeting staff. It remains to be seen how OFAC will respond to the report and if the agency will meaningfully expand the number of existing designations. The agency's more cautious approach to the designation of Russian oligarchs was surely a deliberate decision, likely taken in light of the extensive multinational commercial holdings of many oligarchs and the companies they control and the potential for disruption of markets outside Russia.

Freezing and potentially seizing Russian assets

Following the sweeping sanctions imposed on the Russian government, hundreds of billions of dollars of Russia's sovereign assets have been frozen by financial institutions in the EU, UK, United States, and other U.S. allies. According to the Act, approximately $300 billion in Russian sovereign assets have been immobilized worldwide, with approximately $4 to $5 billion of those assets subject to the jurisdiction of the United States.[2] Over the past year, there have been increasing calls to make those assets available to Ukraine to support its reconstruction and recovery efforts. To that end, the Act a) prohibits OFAC from releasing any frozen Russian sovereign assets by license and b) establishes a mechanism for the President to seize and repurpose Russian sovereign assets and make them available to Ukraine through a "Ukraine Support Fund."

The provisions apply broadly to "Russian sovereign assets," which include assets of any agency or instrumentality of the Russian government as well as any property or funds of the Russian government, including the Central Bank, Ministry of Finance and National Wealth Fund. The Act prohibits OFAC from releasing any Russian sovereign asset that is "blocked or effectively immobilized" by the United States before a) the President has certified that the hostilities between Russia and Ukraine have ceased, and Ukraine's claims against Russia have either been satisfied or are being resolved by a bona fide international mechanism, and b) Congress is given 30 days' advance notice and an opportunity to pass a resolution of disapproval. In effect, no transactions involving Russian sovereign assets may be licensed, and (though OFAC's interpretation of the provision is not yet certain) the reference to assets "effectively immobilized" in addition to

those blocked could be read to prohibit licensing of transfers of U.S.-linked assets held outside the United States that would clear through the U.S. financial system. Such an interpretation, if relied on by OFAC, would effectively prohibit these assets from being released in satisfaction of other claims against the Russian Federation.

Second, the Act authorizes (but does not require) the President to seize any such assets within U.S. jurisdiction for the purpose of transferring those funds to the Ukraine Support Fund, which will be used to fund humanitarian efforts in Ukraine and Ukraine's reconstruction and rebuilding efforts. The Act directs the President to coordinate with other G7 leaders prior to taking action to seize assets. Finally, the Act permits the seizure of sovereign assets of Belarus as well, if the President determines that Belarus has engaged in an act of war against Ukraine.

Expansion of secondary sanctions targeting Iran and other changes

Although U.S. sanctions against Iran are already quite broad, the Act expands so-called "secondary sanctions" further. Secondary sanctions target transactions conducted by non-U.S. persons outside U.S. jurisdiction (and therefore not in violation of U.S. direct sanctions) by threatening that persons engaging in such transactions may themselves be placed on U.S. sanctions lists. Although secondary sanctions are sometimes phrased in mandatory terms (i.e., persons found to have engaged in targeted conduct "shall" be designated for the specified sanctions), in fact the making of such a finding requires further action by the Executive Branch and is in fact discretionary. In other words, acts targeted by secondary sanctions create the possibility that U.S. sanctions will be imposed, but that consequence is not automatic.

With respect to Iran, the Act further expands secondary sanctions authority at the margins for a number of activities, most notably 1) knowingly providing port services to any sanctioned Iranian vessel or any vessel that in turn knowingly transported or dealt in Iranian-origin petroleum products; 2) for refineries, knowingly engaging in a significant transaction to process, refine, or otherwise deal in any Iranian-origin petroleum product; 3) specifically for Chinese financial institutions, knowingly engaging in any transaction involving a purchase of Iranian petroleum products (regardless of size or frequency); and 4) for any financial institution, knowingly engaging in any transaction involving Iranian UAVs or their parts, again regardless of size or frequency. The Act also calls for the creation of secondary sanctions regimes targeting financial institutions maintaining accounts for senior leaders of Iran and Hamas (and certain other terrorist organizations).

Other provisions target human rights abuses and drug trafficking but have less impact on existing law.

Divestiture of TikTok (and others?)

The Act sets a hard deadline for the divestiture of TikTok in the United States by making it unlawful for an entity to provide 1) services to distribute, maintain or update a "foreign adversary controlled application" by means of a marketplace or 2) internet hosting services, within the United States that enable U.S. users to access, maintain or update such an application on or after a date that is 270 days after the designation of the application (in the case of TikTok, January 19, 2025), unless a "qualified divestiture" has taken place prior to that deadline. The Act does not prohibit individual U.S. persons from obtaining or using the applications, but the prohibitions on infrastructure and support services (borrowed from prior regulations targeting applications posing a national security threat) are designed to make it extremely difficult as a practical matter for U.S. persons to access and use the application. The 270-day deadline is subject to a single 90-day extension at the discretion of the President to permit closing of a binding agreement to divest. Enforcement is against those providing the prohibited support services and could result in a fine of up to $5,000 per U.S. user of the targeted application supported by the service provider. Finally, the owner of the foreign adversary controlled application is required to make all account data of U.S. persons hosted in the application available for download by the user before any prohibition takes effect so that the user can transfer data and content to other platforms. If the foreign adversary controlled application is not divested by the deadline, the owner is subject to a $500 per user fine if it has not complied with this requirement.

The Act specifically defines a "foreign adversary controlled application" to include an application operated directly or indirectly by ByteDance (or ByteDance affiliates such as TikTok). However, the application also creates authority for the President to designate any other application that is "controlled by a foreign adversary" for a ban, following publication of a finding that the application poses a significant threat to U.S. national security. "Controlled by a foreign adversary" includes any person or entity that is, or is directly or indirectly controlled or owned 20% or more by, one or more persons or entities organized or domiciled in China, Russia, Iran, or North Korea. Relevant applications are those permitting the sharing of text, image, video, or similar content with more than one million U.S. users. These authorities are similar to those already established by executive order and the Department of Commerce's Information and Communication Technology Services (ICTS) regulations; the primary difference is that, with respect to TikTok, the relevant findings and deadlines have been taken out of the hands of the Executive Branch.[3]

The “qualified divestiture” must be to an entity that, in turn, is not “controlled by a foreign adversary.” Moreover, ByteDance is still subject to an order from the President following a review of its previous acquisition of U.S. company Musical.ly by the Committee on Foreign Investment in the United States (CFIUS) requiring it to divest TikTok.[4] The resolution of that order has been under negotiation for years and is the subject of a pending (but suspended) judicial challenge; as a practical matter, the concurrence of CFIUS is also very likely necessary.

TikTok and its users successfully enjoined the application of a separate, third attempt to exclude TikTok from the United States via an executive order issued by then-President Trump under the authority of IEEPA, on both statutory and First Amendment grounds.[5] The Biden administration withdrew the order and chose not to pursue an appeal. Given these prior challenges, further litigation over this new provision is likely, and the outcome of such litigation is uncertain.

Restrictions on data transfers by data brokers to “foreign adversary countries”

Finally, the Act broadly prohibits “data brokers” from providing access to “personally identifiable sensitive data of a United States individual” to any “foreign adversary country” (which currently include China, Russia, Iran, and North Korea) or any entity “controlled” by those countries (which is broadly defined). The Federal Trade Commission (FTC) is assigned enforcement authority for these provisions, and a violation will be treated as “an unfair or a deceptive act or practice” under the FTC Act. The prohibition goes into effect 60 days after adoption, on June 23.

As discussed in our client update, in February 2024, President Biden issued Executive Order (E.O.) 14117, which directs the DOJ and other relevant U.S. government agencies to develop a regulatory framework to restrict access by countries of concern (including China) to Americans’ bulk sensitive personal data and government-related data. The DOJ concurrently issued an Advanced Notice of Proposed Rulemaking (ANPRM) establishing a framework of restrictions, prohibitions, and conditions on bulk data transfer focusing on cybersecurity requirements for an allowable category of transactions and an outright prohibition for categories (including data brokerage) viewed as more problematic. The restriction to “data brokers” is a significant reduction in scope from the ANPRM but, as described below, it covers a wider range of data. By assigning enforcement authority to the FTC rather than the DOJ, however, the Act also brings a new enforcement agency into scope and creates potential tension between rules.

Who is covered?

The restrictions apply to a “data broker,” which is defined as:

– An entity that, for valuable consideration “sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available data of United States individuals that the entity did not collect directly from such individuals to another entity that is not acting as a service provider.”

The rule is thus aimed at “brokers” in the common usage of the word and explicitly excludes entities providing, maintaining, or offering a product or service with respect to which personally identifiable sensitive data is not itself the product or service, service providers, entities transmitting information at the request of the subject, and entities reporting, publishing, or otherwise making available news or information that is available to the general public.[6] Merely processing or hosting data in a covered country is not acting as a “data broker.”

What is restricted?

The Act prohibits the sale, licensing, rent, trade, transfer, release, disclosure, provision of access to, or otherwise making available personally identifiable sensitive data by data brokers to either a foreign adversary country, or to an entity that is “controlled” by a foreign adversary, which as above includes any person or entity that is, or is directly or indirectly controlled or owned 20% or more by, one or more persons or entities organized or domiciled in China, Russia, Iran, or North Korea.

What data is covered?

The brokering restriction applies to personally identifiable “sensitive data.” The term “sensitive data” covers 16 categories of data, including government identifiers; health data;[7] financial data;[8] biometric information; genetic information; precise geolocation information; private communications; device log-in credentials; information identifying the sexual behavior of an individual; calendar or address book information, phone or text logs, photos, audio recordings, or videos for private

use; nude or revealing photographs or videos; information revealing video content requested by an individual; any information about an individual under the age of 17; an individual's race, color, ethnicity, or religion; information revealing an individual's online activities over time; an individual's status in the Armed Forces; or other data that is used to identify the foregoing information.

Although this definition overlaps in part with the proposed definition of "sensitive personal data" under the ANPRM, the Act's definition is notably broader, covering data such as an individual's communications, online activities, and private photos or videos. Whether and how DOJ alters the approach proposed in the ANPRM in response to the new statute, and whether and how the DOJ and FTC will coordinate interpretation and enforcement, remain unclear. It is clear, however, that international transfers of sensitive personal data will remain a national security focus for the foreseeable future.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Kendall Howell
+1 202 962 7068
kendall.howell@davispolk.com

Paul Marquardt
+1 202 962 7156
paul.marquardt@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com

Patrick Q. Sullivan
+1 202 962 7179
patrick.sullivan@davispolk.com

Charles Marshall Wilson
+1 202 962 7130
charles.wilson@davispolk.com

1 As noted in our recent client update, the DOJ has increasingly emphasized the importance of sanctions-related due diligence in the M&A context.

2 Notably, approximately $190 billion of Russian assets are immobilized in Belgium.

3 See our prior client updates regarding the Department of Commerce's Information and Communication Technology Services regulations here and here.

4 Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51297 (Aug. 19, 2020).

5 *See* Executive Order 13942 of Aug. 6, 2020, 85 Fed. Reg. 48637 (Aug. 11, 2020); *TikTok v. Trump*, 507 F. Supp. 3d 92 (D.D.C. 2020); *Marland v. Trump*, 498 F. Supp. 3d 624 (E.D. Pa. 2020).

6 A "service provider" means an entity that (A) collects, processes, or transfers data on behalf of, and at the direction of that (i) is not a foreign adversary country or (ii) a Federal, State, Tribal, territorial, or local government entity; and (B) receives data from or on behalf of an individual or entity described in subparagraph (A)(i) or a Federal, State, Tribal, territorial, or local government entity.

7 Any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual.

8 A financial account number, debit card number, credit card number, or information that describes or reveals the income level or bank account balances of an individual.