Skadden

Enforcement Focus on China: What Companies Should Do to Be Prepared

Warren Feldman
Partner / New York
212.735.2420
warren.feldman@skadden.com

Eytan J. Fisch
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

Steve Kwok
Partner / Hong Kong
852.3740.4788
steve.kwok@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Jocelyn E. Strauber
Partner / New York
212.735.2995
jocelyn.strauber@skadden.com

Four Times Square
New York, NY 10036
212.735.3000

On January 29-30, 2019, Skadden and Han Kun Law Offices co-hosted two seminars — first in New York, then in Washington, D.C. — titled "Enforcement Focus on China: What Companies Should Do to Be Prepared." Topics included the U.S. Department of Justice's (DOJ) recent China Initiative (Initiative), China's potential response to the Initiative, and an intersection between U.S. and Chinese law that may put companies in the challenging position of having to comply with conflicting demands.

Both seminars included Han Kun partners Chen Ma and Xiaoming Li, along with Steve Kwok, a Skadden partner in Litigation, Government Enforcement and White Collar Crime, and Cross-Border Investigations. The panelists for the New York session included Skadden Government Enforcement and White Collar Crime partners Jocelyn Strauber and Warren Feldman. The panelists for the D.C. session included Eytan Fisch, a Skadden Banking/Regulatory partner, and Michael Leiter, a Skadden partner in National Security, CFIUS, Cybersecurity and Privacy, and Congressional Investigations and Government Policy.

The DOJ's China Initiative

Ms. Strauber began the discussion in New York by providing an overview of the DOJ's China Initiative. She noted that the Initiative is unusual in that it expressly singles out a specific country and, with respect to enforcement under the Foreign Corrupt Practices Act (FCPA), targets "Chinese companies that compete with American businesses." Ms. Strauber expressed the view that the Initiative appears to be more than just a "paper policy" with no real expectation that the defendants will be brought to the U.S. to face charges, but instead seems to signal a new determination by DOJ to bring Chinese defendants into U.S. courts through extradition and other means and to obtain judgments against them through parallel civil enforcement actions.

Mr. Feldman noted that the Initiative's explicit focus on Chinese individuals and Chinese companies might invite claims of selective prosecution, although the legal hurdle for bringing such challenges is high. One also can expect defense counsel to oppose extradition requests by arguing that cases brought under the China Initiative are "political offense" cases.

Although the China Initiative was announced against the backdrop of ongoing trade negotiations between the U.S. and China, the panel was of the view that, even if a mutual satisfactory trade deal could be reached, it would be unrealistic to expect the

Initiative to fall by the wayside. Mr. Feldman provided an overview of the concerns, some of them persisting for years within the U.S. government, that the Initiative is designed to address.

The panel proceeded to discuss several recent cases involving Chinese companies and individuals, including *United States v. Chi Ping Patrick Ho*, *United States. v. United Microelectronics Corp*. and *United States v. Huawei*. The panel observed that these cases all demonstrated the DOJ's willingness — and, in some cases, success — in employing aggressive tactics in prosecuting Chinese entities and individuals. Based on recent cases, we do not expect trial juries to be receptive to defendants' jurisdictional arguments. Ms. Strauber noted that, under the amended Federal Rule of Criminal Procedure 4, service on foreign companies has been made easier, as evidenced in the *Microelectronics* case, where both companies voluntarily appeared at the arraignment through counsel.

Mr. Kwok noted that, given the active plaintiffs' bar in the U.S., the Initiative might also lead to an increase in civil suits against Chinese companies, as plaintiff's counsel piggyback on the work of the criminal authorities. Mr. Feldman agreed, noting that cases that begin as civil litigation between private litigants might also pique the interest of prosecutors and lead eventually to a criminal investigation and even prosecution. Ms. Strauber mentioned the DOJ's anti-"piling on" policy, which discourages duplicative enforcement actions for the same conduct. She added, though, that it remains to be seen how this policy will be applied to cases brought under the Initiative.

The panelists in Washington, D.C., covered many of the same points. Mr. Leiter discussed the national security concerns that the U.S. Congress and intelligence community have had for many years about certain practices — such as trade secrets theft, economic espionage, cyber intrusions, etc. — allegedly engaged in by Chinese businesses in certain sectors. Mr. Fisch echoed this observation. He explained that the penalties imposed in the ZTE case, for example, were predicated on conduct from years ago. The panel noted, however, that U.S. authorities are not always sufficiently sensitive to the second- and third-order effects of their actions. The ban on ZTE from doing business with U.S. companies, to cite one example, turned out to have widespread unintended negative ripple effects on U.S. businesses.

China's Potential Responses to the Initiative

Mr. Kwok then asked the Han Kun panelists for their views on how DOJ's China Initiative is generally perceived by Chinese legal commentators and how China might respond to it. Mr. Li explained that many commentators in China view the Initiative as an attempt by the U.S. to thwart China's economic and technological growth. Prior to the financial crisis of 2007-2008, China was on a path to reform its business and regulatory practices, though that reformation has since stalled. The silver lining in this very difficult moment in the bilateral relationship is that it might provide further impetus for implementing the reforms that certain Chinese policymakers, including its top leadership, have been advocating for quite some time.

Just as the China Initiative should cause Chinese companies to beef up their compliance infrastructure, Ma noted that American businesses operating in China also should ensure their compliance with Chinese law. Anticorruption, for example, remains an area where both Chinese and American companies should maintain continued vigilance. Employees should be reminded that, even if certain improper practices are engaged in by one's competitors in China — such as improper payments to government officials to speed customs clearance or expedite license approvals — "everyone does it" does not provide a license to engage in the same conduct and offers no protection to multinational companies from criminal prosecution by the Chinese authorities. Such conduct may violate both Chinese and U.S. laws and lead to substantial criminal penalties.

The panelists then discussed the China Cybersecurity Law, which imposes new requirements on data localization and data export, and reminded the audience to ensure that their companies' IT professionals are aware of this new legislation and making adjustments, where necessary, to comply with it. Mr. Ma noted that the implementing regulations are still in draft form, and companies should pay close attention to what the final regulations say when they become available.

The panel discussed whether companies have amended their travel policies in the wake of the arrest of Huawei's CFO, Sabrina Meng. Mr. Li observed that certain Chinese companies have enacted policies to allow for only essential travel to the U.S. Mr. Kwok noted that the U.S. State Department has a travel advisory in place for travel to China. Mr. Ma observed that multinational companies should pay attention to who they list as their "legal representatives" in the company registry, as there have been cases involving such representatives being barred from leaving China while civil disputes involving their companies remain pending in Chinese courts.

The Interaction of Chinese and U.S. Law

The panel discussed a number of illustrative areas where multinational companies may be caught between competing demands by U.S. and Chinese authorities. The first area involves

the attorney-client privilege, which is not recognized in China, at least not in the same form applicable to the work of U.S. practitioners. In addition to local law implications, this difference also has significant U.S. law implications. Noting that the privilege does not exist in China, a number of U.S. courts have upheld subpoenas that called for the production of documents involving communications between Chinese counsel and their clients. Hence, in cases where U.S. law advice also is being sought (for example, conducting a China-based internal review that may present FCPA issues), U.S. companies would be well-advised to structure the engagement relationship to make clear that the work (including work done by Chinese counsel and other professional advisers) is overseen by U.S. counsel to safeguard the attorney-client privilege and any resulting work product under U.S. law.

The panelists then discussed the potential issues that may arise from the interaction between the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act in the U.S. and the Chinese Cybersecurity Law. Under the CLOUD Act, U.S. companies are now obligated to respond to lawful requests for information by the U.S. authorities even if the requested information is located overseas, if the information is within a U.S. company's custody and control. The Chinese Cybersecurity Law requires data generated in the regular course of business in China to be localized in China and restricts what data can be exported and how. Issues may arise if the information requested by the U.S. authorities resides in a server in China and is subject to production under the Cloud Act but cannot be lawfully exported from China consistent with the requirements in the Chinese Cybersecurity Law.

Ms. Strauber offered some potential workarounds, including providing summaries of documents and making redactions. Mr. Feldman suggested offering assistance to the U.S. authorities in the drafting of Mutual Legal Assistance requests. Mr. Kwok noted that in cases where both governments have made clear they have commenced separate investigations, it may be possible to provide the information requested by the U.S. authorities to the Chinese authorities and let the governments sort out what can be shared. In this connection, Mr. Leiter noted that companies need to be very thoughtful when they interact with authorities from multiple jurisdictions. In addition to the substance of the communications, the timing and sequencing of such communications also can raise sensitive issues that require close coordination by lawyers in different countries.

Similar issues to those described above may arise under the Chinese Criminal Judicial Assistance Law, which is intended explicitly to counteract the extraterritorial application of foreign law in China. Before any information may be provided to foreign *criminal* authorities, this Chinese law requires that the information must first be provided to the Chinese authorities. While the terms of the law refer to only requests for information by foreign criminal authorities, the line between a civil and a criminal matter in the U.S. can be blurry at times and also may shift over the course of an investigation. Companies therefore need to be vigilant even if they appear to be dealing at the moment only with a civil inquiry in the U.S. There is no one-size-fits-all solution, but some of the accommodations discussed above may also be applicable here.

The seminars concluded with a discussion on the use of WeChat in China. Mr. Kwok observed that WeChat has all but replaced the use of corporate e-mail in China, but WeChat generally does not have the same security features as corporate email systems. Moreover, communications that take place over WeChat are not subject to company oversight and preservation. Mr. Feldman noted that the U.S. Attorney's Manual conditions the award of cooperation credit on the company having a document retention policy that "prohibit[s] employees from using software that generates but does not appropriately retain business records or communications." The panelists suggested that companies should examine how their employees are using WeChat and devise policies that both comply with legal requirements and take into account the realities of modern electronic communications in China. Ms. Strauber noted that various big data metrics may be useful to companies' IT departments in spotting unusual patterns in email usage and stressed the importance of creating a culture of compliance in the workplace to reduce instances of employees using WeChat intentionally to circumvent company controls.