Huawei indictments: economic sanctions and export controls risks for US and multinational companies

China's telecom giant Huawei has long been in the sights of the US lawmakers who suspect the privately-owned company of possibly being involved in Chinese espionage activities – and sanctions violations. Recent indictments (and the arrest in Vancouver of CFO Meng Wanzhou) raises the heat for companies in the Huawei supply chain, as Timothy O'Toole, Brian Fleming, Collman Griffin and Caroline Watson explain.

Longstanding tensions between the United States government and Huawei Technologies Co., Ltd. ('Huawei'), came to a head in late January 2019, when the acting US Attorney General announced two separate indictments against the Chinese telecoms equipment giant.

In one indictment in Eastern District of New York ('EDNY'), Huawei was charged[1] with violations of the International Emergency Economic Powers Act ('IEEPA') and the Iranian Transactions and Sanctions Regulations ('ITSR'), along with related bank fraud, wire fraud, money-laundering, and obstruction-of-justice charges, both for alleged substantive and conspiracy violations. The EDNY charges arise out of Huawei's alleged scheme to surreptitiously conduct business in Iran, in part by deceiving US financial institutions and regulatory authorities. Co-defendants in the EDNY indictment include Huawei's US subsidiary Huawei Device USA, Inc. ('Huawei USA'); the Hong Kong company Skycom Tech Co., Ltd. ('Skycom'), an (alleged) Huawei subsidiary; and Huawei CFO Meng Wanzhou, along with individuals whose names have been redacted from the indictment as published.

In a second indictment in the Western District of Washington ('WDWA'), Huawei subsidiaries Huawei USA and Huawei Device Co., Ltd. were charged[2] with conspiring to steal trade secrets from T-Mobile USA, Inc. ('T-Mobile'), as well as related wire fraud and obstruction-of-justice charges. The WDWA charges arise out of Huawei's alleged attempts to steal an innovative smartphone-testing robot technology known as 'Tappy', in order to improve and develop Huawei's own robotic technology known as 'xDeviceRobot'.

Since at least 2008, the Committee on Foreign Investment in the United States ('CFIUS') has prevented or severely limited several Huawei investments in the United States – and even investments in the United States by companies doing business with Huawei. (CFIUS is an inter-agency government committee that can prevent foreign investment in the United States on national security grounds.) The US intelligence community and several prominent senators and members of the House of Representatives have warned that Huawei may use investments in the United States to gain access to critical infrastructure, such as telecommunications network routing equipment, and then eavesdrop on US domestic communications on behalf of the Chinese government.

Now, however, economic sanctions and export controls appear to be the most prominent national security risk in US authorities' minds when dealing with Huawei. Furthermore, the Huawei indictments appear to be part of a larger trend of China-focused economic sanctions and export control enforcement. Notably, in the year leading up to the Huawei indictments, the US Department of Justice ('DOJ') secured criminal convictions of numerous individuals for wilfully providing sensitive integrated circuit technologies to China; the US Department of Treasury, Office of Foreign Assets Control ('OFAC') announced its first enforcement action against a Chinese company in connection with apparent Iran sanctions violations; and the US Department of Commerce, Bureau of Industry and Security ('BIS') increased the number of Chinese and Hong Kong companies on the Entity List to more than 180, surpassed by only Russia in terms of the total number of Entity List companies.

The Huawei indictments and increased enforcement do not only

create risk for Chinese companies; US and multinational partners of Chinese companies may now face heightened enforcement risk, as well. Of course, even before the Huawei indictments, US and multinational companies faced legal risks for any conduct that US authorities might deem supportive of a Chinese partner's alleged efforts to violate US economic sanctions or export control law – as any company seeking to navigate BIS's deemed export rule or Entity List in China can attest. After the Huawei indictments, however, it seems clear US authorities are focusing even more of their attention on China, creating greater risk even for unwitting involvement in China-related conduct that the US government may deem malign.

Accordingly, we see the Huawei indictments as a useful illustration of the kinds of economic sanctions and export controls risks that US and multinational companies should consider when doing business in China or with Chinese partners. Specifically, we offer four take-aways for legal and compliance practitioners, set forth below.

1) Use the Huawei indictments to fine-tune existing compliance programmes – especially since you may now be on notice about economic sanctions and export controls risk in China.

According to the EDNY indictment, Huawei, its subsidiaries, and its CFO Meng Wanzhou allegedly lied to US financial institutions about the company's dealings with Iran and relationship with Skycom, the alleged subsidiary based in Hong Kong that was at the centre of the alleged scheme to re-export US-origin items to Iran. Similarly, according to the WDWA indictment, two Huawei subsidiaries sought to steal technology for the 'Tappy' robot from T-Mobile, the US subsidiary of the German telecommunications company Deutsche Telekom AG.

Both indictments characterise the US persons involved as victims of Huawei's alleged fraud and unfair technology acquisition strategy. Furthermore, we are not aware of any US persons who have faced enforcement actions in connection with the Huawei indictments thus far, although the case is ongoing.

However, US or multinational companies caught up in the next big China-focused enforcement action may not be so fortunate.

Witting involvement in Huawei's alleged misconduct would almost certainly give rise to significant enforcement risk. For example, as a point of comparison, in January 2018, an investigation into Chinese and Russian attempts to gain access to US controlled radiation hardened integrated circuits ('RHICs') resulted in a criminal conviction for a US citizen in Texas who helped fulfil purchase orders for foreign purchasers while certifying his company was the end-user for the products.[3]

Simple list-based screening for OFAC specially designated nationals ('SDNs') or BIS denied parties may no longer be enough.

Furthermore, even unwitting involvement in Huawei's alleged misconduct could give rise to legal risk if US authorities determine that a Huawei partner had failed to conduct reasonable due diligence. This risk is only exacerbated by the Huawei enforcement actions, which may give US authorities grounds to argue that US and multinational companies should be on notice for misconduct similar to that in which Huawei is alleged to have engaged. Specifically, US authorities may now argue that a US or multinational bank or supplier should know to take extra precautions when dealing with companies similar to Huawei, potentially resulting in civil liability if an enforcement action is later launched. Furthermore, while T-Mobile's 'Tappy' robot may not have been export-controlled at the time of the alleged attempted trade secret theft from T-Mobile, the enactment of The Export Control Reform Act of 2018 ('ECRA') will likely soon expand the list of technologies subject to US export controls, potentially creating liability in similar situations in the future.

Accordingly, we recommend that US and multinational companies take advantage of the Huawei indictments to fine-tune their economic sanctions and export control compliance programmes, in particular in connection with China. Simple list-based screening for OFAC specially designated nationals ('SDNs') or BIS denied parties may no longer be enough. Companies may need to be on the lookout for potential evasive behaviour as well, even by Chinese partners that are as well-established as Huawei. Compliance programmes should thus be able to spot and resolve 'red flags' that a Chinese partner may be engaged in misconduct similar to the alleged scheme to re-export US items to Iran at the center of the EDNY indictment. Failure to take sufficient care may empower US authorities to argue that a company knew or should have known about a potential violation of US law, increasing legal risk.

2) Consider auditing past dealings with Huawei

The two Huawei indictments cover a narrow sliver of the telecommunications giant's global business and may, potentially, implicate only a small portion of the company's economic sanctions and export control-related misconduct. Notably, in the 2016 subpoena that first indicated a serious US government investigation into Huawei's alleged export control violations, BIS reportedly requested information on Huawei's dealings in other embargoed countries such as Cuba, Iran, North Korea, Sudan, and Syria – all countries where the Chinese telecoms company is known to do business. Accordingly, in addition to the EDNY indictment announced already, Huawei may face additional enforcement actions in connection with dealings in Cuba,

North Korea, Sudan, and Syria in the future.

In addition, the WDWA indictment suggests that attempted technology theft was part of Huawei's way of doing business. In one telling detail, the indictment alleged that one Huawei Chinese subsidiary had a formal policy offering bonuses to employees who stole confidential information from competitors. If this allegation is true, Huawei may have sought to steal other technologies as well, including US export-controlled technologies, potentially giving rise to additional enforcement actions. Such actions may create risk for other US and multinational companies that have done business with the company in the past five years.

Accordingly, financial institutions may want to consider auditing their past dealings with Huawei, in particular when financing was provided in US dollars or services were provided by US persons or from the United States. Similarly, Huawei suppliers may want to consider auditing any transactions with Huawei where a US export licence was required, or where US goods, services, or technology were otherwise exported, re-exported, or transferred to the Chinese company.

The focus of these audits should be to search for red flags, perhaps unnoticed at the time, indicating that Huawei may have used US financing, goods, services, or technology in unauthorised ways, for example in support of the export or re-export of US items to Cuba, Iran, North Korea, Sudan, and Syria. If any red flags are uncovered, a company should confer with US counsel to determine the best approach to remediate the issues, which could potentially involve voluntarily self-disclosing the information to US authorities. Under the right circumstances, a voluntary self-disclosure can help frame the narrative in the company's favour and earn credit with US authorities for cooperation.

Links and notes

1 https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial

2 https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade

3 https://www.justice.gov/usao-edtx/pr/texas-man-sentenced-conspiring-illegally-export-radiation-hardened-integrated-circuits

3) Develop contingency plans for a Huawei entity listing or denial order

Despite the DOJ's two criminal indictments against Huawei, neither the Chinese company nor any of its subsidiaries are currently on the Entity List or subject to a BIS denial order,

Huawei's current suppliers should consider contingency plans in case an entity listing or denial order occurs and all exports or re-exports of US items to the company are prohibited.

which would prevent the supply of almost all US items to the company, including entirely civilian items designated as EAR99. However, the Huawei indictments significantly increase the risk of such action.

Notably, the DOJ criminal indictment of ZTE Corporation – another Chinese telecommunications company alleged to have engaged in similar export control violations in connection with Iran – was preceded by ZTE's inclusion on the Entity List. A similar fate could await Huawei. Such a penalty would give the US government significant leverage over the Chinese telecommunications equipment provider, which could ultimately lead to a guilty plea, much in the same way it did with ZTE.

Accordingly, Huawei's current suppliers should consider contingency plans in case an entity listing or denial order occurs and all exports or re-exports of US items to the company are prohibited. For example, suppliers should consider how to mitigate any losses that may arise from contracts with Huawei that may be cancelled, legal strategies for terminating any contracts with Huawei if export restrictions are imposed while minimising potential liability, and closely monitoring the Huawei enforcement action to ensure that any shipments to the Chinese company can be stopped, if necessary.

In addition, although the time has likely passed to insert sanctions and export control compliance and termination language into ongoing contracts with Huawei, companies doing business in China can still use the Huawei indictments to revisit their current compliance language for the relevant contracts – and insist on strong contractual language in future dealings with partners that may present similar risks.

4) Assess the impact of the Huawei indictments on other US government dealings

Finally, the Huawei indictments are likely to have several follow-on effects for other dealings with the US government, which companies should fully assess before deciding whether to continue dealings with the company.

In the CFIUS context, US authorities have long taken a hard line regarding Huawei and have insisted on severing ties with the company as a condition for approval of sensitive investments in the United States. One notable example is the agreement by Germany's Deutsche Telekom AG and Japan's SoftBank Group Ltd to stop using Huawei equipment so as to obtain CFIUS approval for the merger of their two US subsidiaries, T-Mobile and Sprint Corp. In light of the Huawei indictments and the newly enacted Foreign Investment Risk Review Modernization Act of 2018 ('FIRRMA'), companies should expect CFIUS to scrutinise Huawei connections even more closely in connection with any foreign direct investment in the United States.

Similarly, in the US government contracts context, the National Defense Authorization Act for Fiscal Year 2019 now prohibits US government agencies from procuring or obtaining any equipment, systems, or services, that use Huawei components as substantial or essential components. Companies doing significant business with the US government may therefore also wish to assess their relationship with Huawei going forward.

Timothy O'Toole (member), Brian Fleming (member), Collman Griffin (associate) and Caroline Watson (associate) are attorneys at Washington, DC law firm Miller & Chevalier Chartered.

www.millerchevalier.com