Seagate Technology and the Case of the Missing Huawei FDPR Enforcement

James Mulvenon[1]

Key Findings

- Restricting transactions involving certain products or technology through export controls helps to protect U.S. national security, promote U.S. foreign policy objectives, and mitigate against military expansion by foreign adversaries.
- In 2020, the Department of Commerce Bureau of Industry and Security (BIS) adopted new controls, such as the expansion of the Foreign Direct Product Rule (FDPR), that target the Chinese government and Chinese entities such as Huawei. BIS devoted significant resources to making these complicated rules clear, through outreach to the regulated community and through FAQs.
- Many companies indicated that they would follow the FDPR and apply for licenses to ship to Huawei shortly before the rule went into effect.[2] While there are reports of non-compliance, to date, BIS has penalized no company from its investigative efforts related to those these rules.
- BIS should be adopting a strategy of aggressive enforcement in the area of illegal diversion of exports to Huawei and China, as it has previously done with illegal diversion of exports to Iran, and that the Department of Justice is doing with regard to Russia export controls and sanctions.[3]
- The lack of investigations and prosecutions of FDPR violations related to Huawei demonstrates enforcement of the FDPR has not matched that of enforcement of other rules like export controls and sanctions aimed at Iran.[4] This lack of enforcement signals that the threat of Huawei acquiring U.S. technology does not appear to be taken as seriously as other national security risks.
- Seagate Technology, an American company based in California, is a leading global supplier of hard disk drives (HDD), which contain multiple semiconductors. A Senate Committee of Commerce, Science, and Transportation minority committee report in October 2021 confirmed that Seagate, unlike the rest of the HDD industry, continued to ship HDDs to Huawei without a license after the 14 September 2020 cutoff date set by the new FDPR.
- Several industry reports indicate that Seagate profited significantly from its sales to Huawei, and at the expense of its competitors who abided by the rules. By shipping these prohibited products to Huawei, Seagate potentially undermined U.S. national security.
- The Department of Commerce has yet to take any sort of enforcement action against Seagate, despite the evidence in the October 2021 report on Seagate's shipment of prohibited products for almost a year. It also sent the message to other companies that the FDPR will not be enforced.

---

[1] James Mulvenon is Scientific Research/Analysis Director at Peraton Labs, where he is helping to customize their world-class technology for great power competition with China, Russia, Iran, and North Korea. A Chinese linguist by training, he is a leading international expert on Chinese cyber, technology transfer, espionage, and military issues. Dr. Mulvenon's latest article, "A World Divided: The Conflict with Chinese Techno-Nationalism Isn't Coming – It's Already Here," appeared in *War on the Rocks* in early 2021.

[2] https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-enters-a-new-world-How-the-US-ban-will-affect-global-tech

[3] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture

[4] There are recent reports that the Department of Commerce is examining potential violations of the EAR by Synopsys for unlicensed sales to Huawei and SMIC. The Department of Commerce has not acknowledged any investigation into Seagate's publicly known unlicensed sales to Huawei for more than a year.

- Commerce's failure to consistently enforce export controls and to impose meaningful penalties for violations undermine U.S. national security and foreign policy objectives by allowing foreign adversaries to obtain U.S. technology and products, access to which the U.S. should control, and incentivizing businesses to choose revenue over U.S. national security.

The Context: The Role of Export Control Laws

Restricting transactions involving certain products or technology through export controls and sanctions help to protect U.S. national security, promote U.S. foreign policy objectives, and mitigate against military expansion by foreign adversaries. The U.S. export control system is complex and involves several departments, laws, and regulations. The three primary sets of regulations that control the export controls system and sanctions are the Department of State's Directorate of Defense Trade Controls (DDTC) International Traffic in Arms Regulations (ITAR) and the U.S. Munitions List (USML), which controls the distribution of defense and space-related articles and services; the Treasury Department's Office of Foreign Asset Control (OFAC) and Specially Designated Nationals (SDN) list, which enforces economic and trade sanctions; and the Department of Commerce Bureau of Industry and Security (BIS) Export Administration Regulations (EAR) and Commerce Control List (CCL), which controls the regulation of dual-use exports that have both military and civilian applications. The enforcement of export controls is a key part of fulfilling the U.S.'s foreign policy goals and national security objectives. Without adequate and consistent enforcement of these regulations, adversaries of the U.S. will acquire key technologies and weaponry.

BIS is responsible for the administration and enforcement of dual-use export controls and chairs an interagency process that includes the Departments of Defense (DOD), State, and Energy. BIS administers these controls through the EAR, which includes the Commerce Control List (CCL).

A critical function of the export control laws is to prevent adverse actors from obtaining sensitive technology in areas where the United States has a strong technological advantage over other countries. In recent years, these regulations have increasingly been directed at Chinese entities as the Chinese government continues to expand its military-civilian fusion strategy, wherein technology used in private industry is co-opted by China's military in furtherance of the country's goal of developing the most technologically advanced military in the world. Chinese policies such as the Made in China 2025 Plan create competitive advantages for China partly through the acquisition of emerging technologies from U.S. and other foreign firms. With the invasion of Ukraine, Russian firms now also face stricter controls under the EAR.

Enforcement

There is strict liability for violation of export control regulations, meaning that an entity is liable regardless of whether it intended to violate the law or did so unintentionally. This is because great harm can arise from such violations, regardless of intent. Larger criminal penalties can also be imposed for willful violations. Civil monetary penalties for violating the EAR can be approximately $300,000 per violation or twice the value of the underlying transaction, whichever is greater. Criminal penalties can include up to 20 years imprisonment or $1 million per violation, or both.

Export controls can be effective in curbing the transmission of technology and arms to adverse actors, but only when they are strictly enforced. Without an effective export controls system that enacts strict penalties, more violations occur, which damage U.S. interests. Violations of export controls also create an

uneven playing field between companies that follow the law and those that bend the rules. For publicly traded companies that have the obligation to maximize shareholder value, this uneven playing field means that companies that comply are at a competitive disadvantage vis-à-vis non-compliant competitors and will lose revenue that helps to pay for R&D and product development, and can lead to job losses. For some, non-compliance may be considered to be good business as violating the export control may result in penalties that will be a fraction of the revenue it gained by violating the law.

Exporters Obligations and BIS Outreach

Companies that export, re-export or transfer goods subject to U.S. export control laws have a legal duty to keep themselves apprised of export control regulations and to understand their applicability to specific technologies and product lines. BIS regulations can be complex; recognizing that fact, BIS systematically engages in a variety of activities to clarify its regulations and their applicability. For example, BIS publishes FAQs on its website and engages in outreach efforts, such as site visits with companies, meetings with trade associations and individual exporters, and hotline advice. BIS also updates its rules to refine areas of particular complexity. Though companies typically do not seek to violate export control regulations, there have been instances where a company choses to interpret export control regulations in a way that benefits the company, while not maintaining adherence to the spirit of the rules, despite the plethora of resources made available by BIS to enhance understanding of the rules. The responsibility of following and understanding the applicability of regulations lies with regulated entities. Exporters must pay attention to changes in regulatory framework and seek guidance from BIS if they do not understand new rules.

BIS is aware that there is under-compliance with some of the rules it has implemented and has taken steps to address patterns of non-compliance. Most notably, BIS has focused on foreign parties that, when dealing with U.S. goods, are subject to the same rules as U.S. companies. Indeed, the single largest BIS enforcement fine arose from a settlement with a non-U.S. company. In 2017, ZTE Corporation, a Chinese partially state-owned technology company, agreed to pay over $1.19 billion in both criminal and civil penalties for conspiring to violate the International Emergency Economic Power Act (IEEPA) by illegally shipping U.S.-origin items to Iran, obstructing justice, and making a false statement. Over the course of six years, ZTE Corporation had shipped over $32 million of U.S.-origin items to Iran without obtaining export licenses and took steps to conceal the shipments. The criminal fine (over $286 million) is the largest criminal fine for an IEEPA violation. ZTE Corporation also reached settlement agreements with BIS ($661 million, with $300 million of that suspended) and OFAC. ZTE was punished not only for selling the items to Iran but also for masking its involvement in the exports and continuing illegal shipments during investigation. ZTE Corporation's plea agreement also required the company to submit to three years of corporate probation and corporate compliance monitoring.[5,]

Other foreign companies have been similarly penalized for illegally exporting controlled items to Iran. Other significant examples include an August 2020 $31.4 million civil monetary penalty on the Singapore-based Nordic Maritime Pte. Ltd. and its chairman, Morten Innhaug, for using subsea survey equipment in

[5] https://www.justice.gov/opa/pr/zte-corporation-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions-sending

Iranian waters, in violation of a BIS-issued re-export license.[6] As well, in April 2021 SAP SE, a German software company, agreed to pay more than $8 million to resolve charges with the Departments of Justice, Commerce, and Treasury for violating the EAR and the Iranian Transactions and Sanctions Regulations. The company admitted to thousands of export violations spanning six years.[7]

Huawei and the Entity List

A key regulatory tool in the EAR for imposing targeted controls on malign actors is the Entity List, which includes entities believed to be involved in, or to pose a significant risk of being or becoming involved in, activities contrary to the national security or foreign policy interests of the United States. In May 2019, BIS added Huawei Technologies Co., Ltd. and many of its affiliates to the Entity List. Information that led to Huawei's addition to the Entity List included alleged violations of the IEEPA and conspiracy to violate IEEPA by providing prohibited financial services to Iran in addition to obstruction of justice in connection with the related investigation regarding those charges.[8] In addition to flouting sanctions against Iran, Huawei was added to the list because under China's Military-Civilian Fusion (MCF) policy and Belt and Road Initiative (BRI), "private" telecommunications companies such as Huawei were acting as a tool used by the Chinese Communist Party (CCP) for influence and access. BIS anticipated that adding Huawei and its affiliates to the Entity List may also further obstruct Huawei's goal of large-scale deployment of surveillance technologies through its "Safe Cities" project, which is funded by the BRI. This project aids governments in monitoring their own citizens and restricting Huawei's import of U.S. technology has complicated Huawei's global launch of its telecommunications infrastructure.

The addition of Huawei and its affiliates to the Entity List created a license requirement on the listed entities that supplemented those found elsewhere in the EAR. This means that under most circumstances the export, re-export, or transfer (in-country) of any item subject to the EAR to Huawei or any of its listed affiliates now requires a license.[9] At the end of 2020 Huawei and its affiliates accounted for 153 entities on the Entity List.[10]

Huawei's CEO, Ren Zhengfei, told his staff in a memo to "dare to lead the world" in software to counter the financial hit the company has taken due to U.S. sanctions. Ren went on to say that the company needed to shift focus to software because the industry is "outside of U.S. control and we will have greater independence and autonomy." The company has decided to invest more in businesses that do not use advance process techniques, such as the company's intelligent driving business.[11]

Case Study: Foreign Direct Product Rule

---

[6] https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/2596-nordic-maritime-press-release-final-08-24-20/file

[7] https://www.justice.gov/usao-ma/pr/sap-admits-thousands-illegal-exports-its-software-products-iran-and-enters-non

[8] https://www.bis.doc.gov/index.php/documents/pdfs/2447-huawei-entity-listing-faqs/file

[9] https://www.bis.doc.gov/index.php/documents/pdfs/2447-huawei-entity-listing-faqs/file

[10] https://www.bis.doc.gov/index.php/documents/pdfs/2711-2020-bis-annual-report-final/file

[11] https://www reuters.com/world/china/huawei-reduce-reliance-advanced-process-techniques-2021-04-12/

Under the FDPR, the EAR controls *foreign-produced* items that are a (1) direct product of certain U.S.-origin technology or software controlled for national security reasons or (2) are produced by plants, or major components of plants, that are a direct product of U.S.-origin technology. The FDPR further restricts the receipt of certain foreign-produced items (i.e., those incorporating U.S. technology or software or produced by plants or major components of plants) by designated entities on the Commerce Department's Entity List.

In May 2020, BIS amended the Foreign Direct Product Rule to "target Huawei's acquisition of semiconductors that are the direct product of certain U.S. software and technology."[12] Specifically, this targeted rule change made the following foreign-produced items subject to the EAR:

- Items, such as semiconductor designs, when produced by Huawei and its affiliates on the Entity List (e.g., HiSilicon), that are the direct product of certain CCL software and technology; and
- Items, such as chipsets, when produced from the design specifications of Huawei or an affiliate on the Entity List (e.g., HiSilicon), that are the direct product of certain CCL semiconductor manufacturing equipment located outside the United States. Such foreign-produced items will only require a license when there is knowledge that they are destined for reexport, export from abroad, or transfer (in-country) to Huawei or any of its affiliates on the Entity List. BIS removed uncertainty by clarifying that any foreign-produced wafer is unequivocally a foreign-produced item, whether the wafer is finished or unfinished.

An August 2020 amendment to this specially applied FDPR also clarifies that the restrictions apply not only where Huawei is the end user of the item, but also to *any* transaction where Huawei is the purchaser or otherwise serves as an intermediate consignee. While the previous version of the rule only restricted the transfer to Huawei of items in which Huawei had some input as to the design or specifications of the final item, the revision eliminates that proviso and places restrictions on *any* transactions involving the items identified where Huawei is involved in *any way* as an end user, purchase, or intermediate or ultimate consignee, absent a license from BIS (the application for which is generally subject to a policy of denial).

The rule even prohibits "commercial off the shelf" (COTS) products from being delivered to Huawei if they are either the direct product of specified software or technology or produced by a plant or major component of a plant that is, itself, the direct product of specified U.S.-origin software or technology. This amendment effectively bars the sale of most high-tech devices to Huawei, as all high-tech devices use chips and most modern chips are designed using software developed in the US and are fabricated using equipment partly made in the U.S.

The rule also clarified issues of intent for individuals involved in transactions. If a person has "knowledge" that such an item will be incorporated into or will be used in the "production" or "development of any "part," "component," or "equipment" produced, purchased, or ordered by Huawei, then a person cannot export, re-export, or transfer such an item to Huawei. Further, if a person has "knowledge" that Huawei is acting as a purchaser or intermediate consignee in a transaction—regardless of the ultimate end user of the

[12] https://2017-2021.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts html

item—the transfer of any such item is also prohibited. The BIS standard of "knowledge" includes not only actual positive knowledge, but also reason to know, reason to believe, or "awareness of a high probability" that a circumstance is likely to occur.

This change to the FDPR as applied to Huawei had a substantial impact on the high-tech sector and Huawei, was the source of significant publicity both inside and outside of the industry and forced dramatic changes to trade flows. Despite that fact, there have been no regulatory actions against companies violating the expanded Huawei FDPR, and only one relatively minor penalty of $80,000 against SP Industries Inc., a small company in Pennsylvania that committed four violations of the Export Administration Regulations by exporting controlled items to Huawei and its subsidiaries.[13] Moreover, the SP Industries Inc. settlement arose from a *voluntary disclosure*, rather than BIS investigative work. Also striking about the SP Industries settlement (which involved only four shipments) was the length of time it took to resolve the matter. Though the violations occurred in mid-2019, it wasn't until the end of 2021 that a civil penalty against the company was enforced.[14]

BIS should be adopting a strategy of aggressive and consistent enforcement in the area of illegal diversion of exports to Huawei and China, as it has previously done with illegal diversion of exports to Iran. Many companies, including Taiwan Semiconductor Manufacturing Co., Samsung Electronics, Samsung Display, and SK Hynix, indicated that they would follow the FDPR and apply for licenses to ship to Huawei shortly before the rule went into effect.[15] However, as evidenced by the lack of investigations and prosecutions of FDPR violations in the two years since it was implemented against Huawei, the enthusiasm for enforcing the FDPR has not matched that of enforcement of other rules like export controls and sanctions aimed at Iran.[16]

This lack of enforcement signals that the threat of Huawei acquiring U.S. technology does not appear to be taken as seriously as other national security risks. The Seagate story is consistent with that signaling.

Seagate Continued Sales to Huawei

Seagate Technology, an American company based in California, is a leading global supplier of hard disk drives (HDD), which contain multiple semiconductors. The company has increased its market share in recent years and controlled around 43 percent of the world market as of mid-2021. Although HDDs use semiconductors, including DRAM, and as such fall squarely within the scope of the FDPR, at the Deutsche Bank 2020 Virtual Technology Conference Seagate's CFO, Gianluca Romano, stated that Seagate did not believe that the company needed a license to continue to sell to Huawei and other Chinese customers and that he didn't believe that Seagate should be restricted in its shipments to Huawei. This was in direct contradiction to the stance of Western Digital, another U.S.-based HDD and solid state drive

---

[13] https://efoia.bis.doc.gov/index.php/documents/export-violations/export-violations-2021/1336-e2688/file

[14] https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/2869-press-release-sp-industries-settlement/file

[15] https://asia nikkei.com/Spotlight/Huawei-crackdown/Huawei-enters-a-new-world-How-the-US-ban-will-affect-global-tech

[16] There are recent reports that the Department of Commerce is examining potential violations of the EAR by Synopsys for unlicensed sales to Huawei and SMIC. The Department of Commerce has not acknowledged any investigation into Seagate's publicly known unlicensed sales to Huawei for more than a year.

(SSD) supplier to Huawei, and Toshiba, a Japan-based HDD supplier, both of which ceased shipments to Huawei after the rule went into effect. Western Digital's then CEO, Bob Eulau, further stated that the company was not shipping anything to Huawei at the time of the conference and would pause shipping HDDs to ensure compliance with regulations.[17]

Evidence suggests that Seagate continued to ship hard drives to Huawei after the FDPR went into effect and after the 14 September 2020 cutoff date set by the new FDPR. Wedbush Securities, an investment firm, stated that it "believe[s] it has been common knowledge within the storage industry that [Seagate] continued shipping parts to Huawei post the U.S. restrictions implemented in August…[Seagate's] legal team likely interpreted U.S. restrictions differently than its peers." Seagate's recent filings with the Securities and Exchange Commission (SEC) acknowledged that some of the company's "products and services are subject to export control laws and other laws affecting the countries in which our products and services may be sold, distributed, or delivered." The company also acknowledged that it could not ensure that its own interpretation of regulations would be accepted by regulatory and enforcement authorities, which further reflects that Seagate was not confident about its former interpretation of the FDPR. Seagate officials also told the Senate Committee of Commerce, Science, and Transportation minority committee staff in October 2021 that the company does not have a valid license to continue shipping hard disk drives to Huawei.[18]

In Seagate's case, several industry reports indicate that the company profited significantly from its sales to Huawei, and at the expense of its competitors. In February 2021 Deutsche Bank reported that Seagate held 51 percent of the HDD market share in the fourth quarter of 2020, which was up five points from the previous quarter and attributed the increase in market share to Seagate's decision to not cease shipping products to Huawei. Wells Fargo also indicated that Huawei was an eleven percent customer of Seagate's high-cap HDDs. By shipping these prohibited products to Huawei, Seagate appears to have profited at the expense of its competitors who abided by the rules, and thereby potentially undermined U.S. national security. The Senate Committee Report concluded that "Seagate likely made the strategic calculation to continue violating national security regulations based on the prospect of earning significantly greater profits through market monopolization than the potential cost of regulatory penalties."[19]

The Department of Commerce has yet to publicly take any sort of enforcement action against Seagate, despite the evidence outlined in the October 2021 investigation into Seagate's compliance with the FDPR. Publicly available information, such as Seagate CEO's comments at the 2020 Deutsche Bank conference and the bank studies previously mentioned, indicated that Seagate continued to sell controlled items to Huawei after the FDPR into effect. BIS' inaction not only allowed Seagate to continue shipping prohibited products for almost a year but also sent the message to other companies that the FDPR will not be enforced or may not be enforced consistently. This lack of effective and consistent enforcement and investigation in the face of ample evidence in effect incentivizes companies to continue to ship controlled exports to Huawei. Failure to enforce export controls and to do so aggressively with meaningful penalties undermines U.S. national security and foreign policy objectives by allowing foreign adversaries to obtain U.S. technology and products, access to which

[17] https://www.tomshardware.com/news/the-curious-case-of-storage-devices-and-huawei
[18] https://www.commerce.senate.gov/services/files/2C03C95D-6D36-49FA-8066-52DD1A98A1FE
[19] https://www.commerce.senate.gov/services/files/2C03C95D-6D36-49FA-8066-52DD1A98A1FE

the U.S. should and may be obligated to control, and incentivizing businesses to choose revenue over U.S. national security.