[redacted]

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X

UNITED STATES OF AMERICA

- against -

HUAWEI TECHNOLOGIES CO., LTD.,
HUAWEI DEVICE CO., LTD.,
HUAWEI DEVICE USA INC.,
FUTUREWEI TECHNOLOGIES, INC.,
SKYCOM TECH CO., LTD.,
WANZHOU MENG,
also known as "Cathy Meng" and
"Sabrina Meng,"
[redacted]

Defendants.

- X

S U P E R S E D I N G
I N D I C T M E N T

Cr. No. 18-457 (S-3) (AMD)
(T. 18, U.S.C., §§ 371, 981(a)(1)(C), 982(a)(1), 982(a)(2), 982(b)(1), 1343, 1344, 1349, 1512(k), 1832(a)(5), 1832(b), 1956(h), 1962(d), 1963(a), 1963(m), 2323(b)(1), 2323(b)(2), 2 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c); T. 50, U.S.C., §§ 1702, 1705(a) and 1705(c))

THE GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this Superseding Indictment, unless otherwise indicated:

I. The Defendants

1. The defendant HUAWEI TECHNOLOGIES CO., LTD. ("HUAWEI") was a global networking, telecommunications and services company headquartered in Shenzhen, Guangdong, in the People's Republic of China ("PRC"). As of the date of the filing of this Superseding Indictment, HUAWEI was the largest telecommunications

equipment manufacturer in the world. HUAWEI was owned by its parent company, Huawei Investment & Holdings Co., Ltd. ("Huawei Holdings"), which was registered in Shenzhen, Guangdong, PRC, and predecessor entities of that company.

2. The defendant HUAWEI DEVICE CO., LTD. ("HUAWEI DEVICE") was a company in the PRC that designed and manufactured wireless phones. HUAWEI DEVICE was a subsidiary of HUAWEI.

3. The defendant HUAWEI DEVICE USA INC. ("HUAWEI DEVICE USA"), a manufacturer of communication products whose headquarters was in the United States, and the defendant FUTUREWEI TECHNOLOGIES, INC. ("FUTUREWEI"), a research and development company whose headquarters was in the United States, were both subsidiaries of HUAWEI and Huawei Holdings.

4. The defendant SKYCOM TECH CO., LTD. ("SKYCOM") was a corporation registered in Hong Kong whose primary operations were in Iran. SKYCOM functioned as HUAWEI's Iran-based subsidiary. As of 2007, Huawei Holdings owned SKYCOM through a subsidiary ("Huawei Subsidiary 1"), an entity the identity of which is known to the Grand Jury. In or about November 2007, Huawei Subsidiary 1 transferred its shares of SKYCOM to another entity ("Huawei Subsidiary 2"), an entity the identity of which is known to the Grand Jury, which was purportedly a third party in the transaction but was actually controlled by HUAWEI. Following this transfer of SKYCOM shares from Huawei Subsidiary 1 to Huawei Subsidiary 2, HUAWEI falsely claimed that SKYCOM was one of HUAWEI's local business partners in Iran, as opposed to one of HUAWEI's subsidiaries or affiliates.

5. The defendant WANZHOU MENG, also known as "Cathy Meng" and "Sabrina Meng," was a citizen of the PRC. From at least in or about 2010, MENG served as Chief Financial Officer of HUAWEI. Between approximately February 2008 and April 2009, MENG served on the SKYCOM Board of Directors. More recently, MENG also served as Deputy Chairwoman of the Board of Directors for HUAWEI.

[redacted]

II. The Scheme to Misappropriate Intellectual Property

8. Since at least in or about 2000 through the date of this Superseding Indictment, the defendants HUAWEI, FUTUREWEI, HUAWEI DEVICE and HUAWEI DEVICE USA (the "IP Defendants") and others executed a scheme to operate and grow the worldwide business of HUAWEI and its parents, global affiliates and subsidiaries through the deliberate and repeated misappropriation of intellectual property of companies headquartered or with offices in the United States (the "Victim Companies") for commercial use. By misappropriating the intellectual property of the Victim Companies, the IP Defendants received income directly and indirectly, including by benefitting from the sale of products containing stolen intellectual property and saving on research and development costs, which income the IP Defendants agreed to use to establish and operate the worldwide

business of Huawei and its parents, global affiliates and subsidiaries, including in the United States.

9. The misappropriated intellectual property of the Victim Companies comprised or included trade secret information, as defined by Title 18, United States Code, Section 1839(3), and other confidential and nonpublic intellectual property. To protect trade secret information and other intellectual property from disclosure, the Victim Companies each employed reasonable measures, including but not limited to physical, electronic and network security, company policy and training, and legal agreements and contracts. The IP Defendants believed that the misappropriated intellectual property comprised or contained trade secret information, and knew and intended that such misappropriation would injure the Victim Companies.

10. The misappropriated intellectual property of Victim Companies consisted of 10 or more copies of copyrighted works with a value greater than $2,500 within a period of 180 days, as defined and described within Title 18, United States Code, Section 2319. The IP Defendants knew and intended that the misappropriation of copyrighted works would injure the Victim Companies.

11. To obtain the intellectual property of the Victim Companies, the IP Defendants sometimes entered into confidentiality agreements with the owners of the intellectual property and then violated the terms of the confidentiality agreements by misappropriating the intellectual property for the IP Defendants' own commercial use. The IP Defendants also tried to recruit employees of the Victim Companies in order to gain access to intellectual property of their former employers, and the IP Defendants directed and incentivized their own employees to steal intellectual property from other companies.

12. On other occasions, the IP Defendants used proxies such as professors working at research institutions or third party companies, purporting not to be working on behalf of the IP Defendants, to gain access to the Victim Companies' nonpublic intellectual property. Those proxies then impermissibly provided the Victim Companies' nonpublic proprietary information to the IP Defendants.

13. In another effort to gain access to the nonpublic intellectual property of the Victim Companies, in 2013, HUAWEI launched a formal policy instituting a bonus program to reward employees who obtained confidential information from competitors. Under the policy, HUAWEI established a formal rewards schedule to pay employees of HUAWEI affiliates for stealing information from competitors based upon the value of the information obtained. Employees were directed to post confidential information obtained from other companies on an internal HUAWEI website, or, in the case of especially sensitive information, to send an encrypted email to a special huawei.com email mailbox. A "competition management group" was tasked with reviewing the submissions and awarding monthly bonuses to the employees who provided the most valuable stolen information. Biannual awards also were made available to the top "Huawei Regional Divisions" that provided the most valuable information. A memorandum describing this program was sent to employees in the United States.

14. To avoid and minimize the costs of potential civil and criminal liability in the United States, and therefore more easily establish and operate HUAWEI's U.S. business, the IP Defendants engaged in a pattern of obstruction. In advance of and during civil proceedings regarding the IP Defendants' alleged misappropriation of intellectual property, the IP Defendants provided false information in the form of affidavits or reports of

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.