UNITED STATES DISTRICT COURT

for the

Northern District of California

United States of America
v.
XIAOLANG ZHANG

Defendant(s)

Case No. CR 18 70919 MAG

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of April 30, 2018 in the county of Santa Clara in the Northern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1832(a)(1)	Theft of Trade Secrets

This criminal complaint is based on these facts:

See attached affidavit of S/A Eric Proudfoot
PENALTIES: 10 years imprisonment, $250,000 fine, $100 special assessment, and 3 years' supervised release

☑ Continued on the attached sheet.

Complainant's signature

Eric M. Proudfoot, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: July 9, 2018

Virginia K. DeMarchi
Judge's signature

City and state: San Jose, California

Virginia K. DeMarchi, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT PRESENTED IN SUPPORT FOR A CRIMINAL COMPLAINT

I, Eric M. Proudfoot, Special Agent of the Federal Bureau of Investigation ("FBI"), being duly sworn, hereby declare as follows:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit is presented in support of a criminal complaint charging **Xiaolang Zhang** ("**Zhang**") with the crime of theft of trade secrets, in violation of Title 18, United States Code, Section 1832, Theft of Trade Secrets.

2. I am an "investigative or law enforcement officer of the United States" within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 1832.

3. I have been employed as a Special Agent of the Federal Bureau of Investigation since March 2, 2008, and am currently assigned to the San Francisco Division. While employed by the Federal Bureau of Investigation, I have investigated federal criminal violations related to high technology/cybercrime, child exploitation, child pornography, foreign counterintelligence, and intellectual property crime. I have gained experience through training at the Federal Bureau of Investigation and everyday work relating to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

4. As an FBI agent, I am authorized to investigate violations of United States law and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. During my career as a Special Agent of the FBI, I have received training and possess actual experience relating to Federal criminal procedures and Federal statutes. I have

also received specialized training and instruction in the field of investigation in computer-related crimes. I have had the opportunity to conduct, coordinate, and participate in numerous investigations relating to computer-related crimes. I have participated in the execution of numerous search warrants conducted by the FBI and have participated in the seizure of email accounts and computer systems.

5. The facts in this affidavit are based on my personal participation in this investigation, my training and experience, and documents, records, emails, and other types of information obtained during the investigation from other sources and witnesses. The FBI has, thus far conducted interviews and reviewed documentation provided by the victim company, Apple, ("Apple"), which included file listings, closed circuit television images, physical access badge history, and employee agreements. The FBI has also conducted a physical search of ZHANG's residence, authorized on June 22, 2018, by the Honorable Susan van Keulen, Magistrate Judge, United States District Court, Northern District of California, San Jose Disivison. Because this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of U.S. law occurred. Also, where I refer to conversations and events, I often refer to them in substance and in relevant part rather than in their entirety or verbatim, and figures and calculations set forth in this complaint are approximate, unless otherwise noted.A

APPLICABLE STATUTES

6. The FBI is investigating alleged violations of Title 18, United States Code, Section 1832, which states in part:

> (a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the

> economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—
>
> (1) Steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
>
> (2) Without authorization copies, duplicates, . . . downloads, uploads, . . . replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) Receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) Attempts to commit any offense described in paragraphs (1) through (3) . . .
>
> (5) Conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,
>
> shall . . . be fined under this title or imprisoned not more than 10 years, or both.

ENTITIES

7. Apple, Inc. "Apple" is a technology company headquartered in Cupertino, California with an annual revenue (in 2017) of $229 billion.

8. Xiaopeng Motors, aka Xpeng Motors, ("XMotors") is an intelligent electric vehicle company with headquarters in Guangzhou, China, and North American offices located in Palo Alto, California.

INDIVIDUALS

9. **Xiaolang Zhang** ("ZHANG") is a former Apple employee, working as a hardware engineer on their autonomous vehicle development team.

ZHANG BACKGROUND

10. **ZHANG** was hired at Apple starting on December 7, 2015, to work on a project to develop software and hardware for use in autonomous vehicles (the Project). Although Apple has made general statements to the press about being interested in autonomous vehicle development, the details of Apple's research and development for the Project is a closely

guarded secret that has never been publicly revealed. Most recently, **ZHANG** worked on the Compute Team, where he designed and tested circuit boards to analyze sensor data within the Project. Because of his role on the team, **ZHANG** was granted broad access to secure and confidential internal databases containing trade secrets and intellectual property for the Project. Among these are multiple confidential databases whose names and categories are known to the government (the "Databases").

11. **ZHANG** took paternity (new parent) leave following the birth of his child from April 1 to April 28, 2018, pursuant to Apple's employee leave policy. While on paternity leave, **ZHANG** traveled with his family to China. On April 30, 2018, shortly after returning from China, **ZHANG** met with his immediate supervisor at Apple, and explained that **ZHANG** would be resigning to move back to China in order to be closer to his mother who he stated was in poor health. As the meeting progressed, **ZHANG** disclosed that he intended to work for XMOTORS – a Chinese start-up company focused on electric automobiles and autonomous vehicle technology.

12. After hearing **ZHANG's** intentions and feeling that he had been evasive during their meeting, **ZHANG's** supervisor asked a representative from Apple's New Product Security Division to join the meeting with **ZHANG**. At the conclusion of their meeting, **ZHANG** was asked to turn in all Apple-owned devices, and **ZHANG** was advised he would then be walked off the campus. **ZHANG** turned over to Apple two (2) Apple iPhones and one (1) MacBook laptop computer. Apple security then immediately disabled **ZHANG's** remote network access, badge privileges, network access, and other employee accesses. **ZHANG** was also reminded about Apple's intellectual property policy, and **ZHANG** acknowledged that he understood and would comply.

13. On May 1, 2018, Apple New Product Security asked that the internal Apple team overseeing the confidential Databases where Apple's materials, including proprietary and confidential materials, are stored began reviewing **ZHANG's** historical network user activity. At the same time, an Apple Global Security attorney began a physical security review of **ZHANG**'s building access and activities on the Apple campus. The Apple security attorney also requested forensic analysis of **ZHANG**'s Apple-owned devices from Apple Information Security.

14. Apple's database security team found that in the days just prior to April 30, 2018, **ZHANG's** Apple network activity increased exponentially compared to the prior two years of his employment. The majority of his activity consisted of both bulk searches and targeted downloading copious pages of information from the various confidential database applications. The information contained within the downloading contained trade secret intellectual property, based on the level of **ZHANG's** access within Apple's autonomous vehicle team.

15. Historical analysis of **ZHANG's** network activity by Apple Information Security (AIS) show that with the confidential database A (the name of which is known to the affiant), **ZHANG** generated 581 rows of user activity on April 28, 2018 alone. On April 30, 2018, **ZHANG** generated 28 rows of user activity. By comparison, **ZHANG** generated 610 rows of user activity during the entire previous month. The amount of activity is unusual for **ZHANG** given that he announced his resignation on April 30, 2018.

16. AIS historical network activity of **ZHANG** from confidential database B (database containing technical documents for the Project) reflect 3,390 rows of user activity generated on April 28 and April 29, 2018. By comparison, **ZHANG** generated 1,484 rows of user activity over the time period of July 2017 through March 2018. Some of the technical .pdf documents

downloaded on April 28 and April 29, 2018 include confidential topics such as Prototypes and Prototype Requirements (power requirements, low voltage requirements, battery system, drivetrain suspension mounts, etc.) As noted above, this amount of downloading activity is unusual for **ZHANG** given his resignation on April 30, 2018.

17. Apple Security's review of swipe badge access and close circuit television footage revealed that **ZHANG** had been on Apple's campus at or around 9:14 p.m. on the evening of Saturday, April 28, 2018. CCTV footage showed that **ZHANG** entered both the autonomous vehicle software and hardware labs, and left the building less than an hour later carrying a computer keyboard, some cables, and a large box. **ZHANG's** network activity, physical presence on campus, and removal of Apple property all occurred during **ZHANG**'s paternity leave - contrary to Apple corporate policy. **ZHANG's** activity was particularly alarming to several groups within Apple's hierarchy: the New Product Security Division, Apple's Research and Development team overseeing the Autonomy Project, and Apple's Global Security Investigations Group since it occurred in the few days prior to **ZHANG's** resignation from Apple.

18. The Apple security attorney then contacted Apple Employee Relations on May 1, 2018, to discuss bringing **ZHANG** back to Apple for a follow-up interview. **ZHANG** was contacted and replied later in the evening of May 1, agreeing to be re-interviewed by Apple.

19. On May 2, 2018, **ZHANG** was interviewed a second time by the Apple security attorney and an Apple employee relations representative whose identity is known. During the interview, **ZHANG** admitted to pursuing employment with X-Motors while still employed at Apple. **ZHANG** initially denied coming onto the Apple campus during his paternity leave and denied removing items that were Apple property. As the interview progressed, Apple security

personnel confronted **ZHANG** verbally, stating that Apple was aware that **ZHANG** was, in fact, on the Apple campus during the evening of April 28, 2018. After being confronted with this information, **ZHANG** recanted his earlier denials and admitted to being present on the Apple campus while still on paternity leave. **ZHANG** further admitted to taking the online data from "the Databases" while on paternity leave. **ZHANG** also admitted removing items from the laboratories prior to his paternity leave (including two circuit boards and a Linux server from the hardware lab). **ZHANG's** reason for these actions were that he took the hardware because he thought the hardware might benefit him in a new position within Apple. (Prior to taking paternity leave, **ZHANG** had begun negotiations to transfer to a separate proprietary research program at Apple, but the transfer had never taken place.) **ZHANG** further explained that he had compiled and downloaded the data because **ZHANG** has an interest in platforms and wanted to study the data on his own.

20. **ZHANG** admitted to being shown a proprietary chip by colleagues while on campus during the evening of Saturday, April 28, 2018. Further, **ZHANG** admitted "air-dropping" the data he had taken from Apple's system onto a personally-owned device (a device not owned by Apple), which **ZHANG** identified as his wife's laptop computer. **ZHANG** provided the Apple interviewers consent to search **ZHANG's** wife's laptop for any Apple intellectual property. **ZHANG** also offered to return the Linux server and circuit boards he had taken from the hardware lab.

21. **ZHANG** departed the Apple campus during the May 1 interview and returned in less than an hour with the computer **ZHANG** identified as his wife's laptop computer (Subject Computer), along with a Linux server and the two circuit boards **ZHANG** had admitted to taking from Apple. The Apple security attorney and the employee relations representative performed a

cursory review of the Subject Computer in **ZHANG**'s presence for any intellectual property and noted several folders of concern, particularly a folder entitled "RECENT" that contained approximately 40GB worth of data. Additionally, the laptop's system event logs reflected "Air Drop" activity on both April 29, 2018 and April 30, 2018.

22. Apple security personnel asked **ZHANG** if he further ex-filtrated or forwarded any of the data on his wife's laptop, which **ZHANG** denied. **ZHANG** was advised that the Apple team would need to keep the Subject Computer in order to perform a more in-depth search for Apple intellectual property, to which **ZHANG** consented.

23. Apple security personnel has advised the FBI that at the present time, the Apple Digital Forensic Investigations team has discovered that approximately 60 percent of the data on the Subject Computer was "highly problematic;" the complete evaluation remains ongoing.

24. **ZHANG** was voluntarily terminated from Apple effective May 5, 2018 (though his accesses and permissions had been de-activated since April 30, 2018), and now claims to be working for XMotors out of their Mountain View, California location. **ZHANG** also advised the Apple investigators that he is planning to move his family to Guangzhou, China in the near future.

FILES RECOVERED FROM SUBJECT COMPUTER

25. Apple Information Security provided the FBI with a sample set of files Apple identified as belonging to Apple and recovered from the Subject Computer along with technical descriptions of each file. The information contained in each file is largely technical in nature, including engineering schematics, technical reference manuals, and technical reports.

26. One of these files was identified as by its specific file name (known to the affiant), and it is a 25-page pdf document containing electrical schematics for one of the circuit boards that

form Apple's proprietary infrastructure technology for the Project. An excerpt of the schematic showing the Intellectual Property caveat is included below:

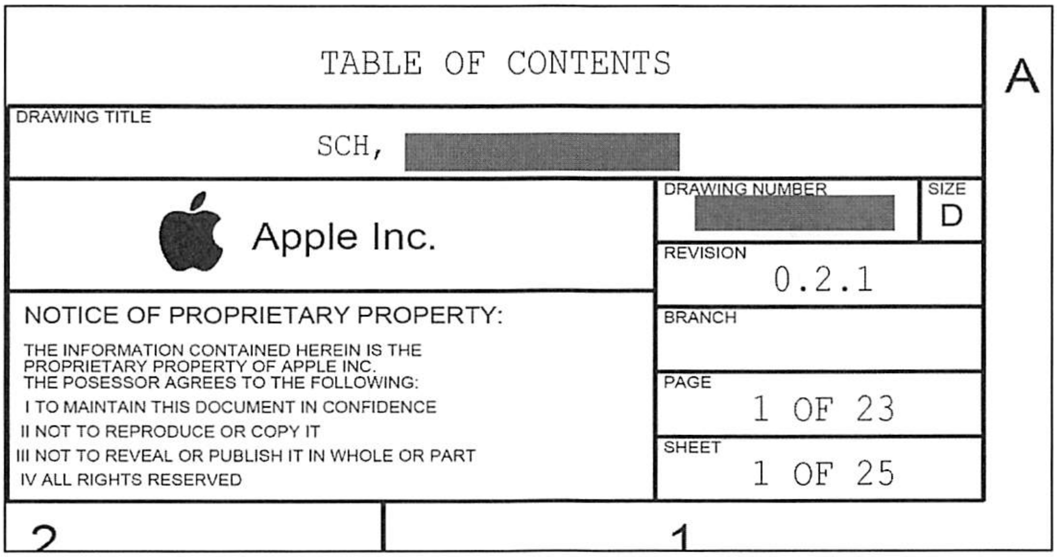

TABLE OF CONTENTS

A

DRAWING TITLE

SCH, [redacted]

Apple Inc.

DRAWING NUMBER [redacted]

SIZE D

REVISION 0.2.1

BRANCH

PAGE 1 OF 23

SHEET 1 OF 25

NOTICE OF PROPRIETARY PROPERTY:

THE INFORMATION CONTAINED HEREIN IS THE PROPRIETARY PROPERTY OF APPLE INC.
THE POSESSOR AGREES TO THE FOLLOWING:
I TO MAINTAIN THIS DOCUMENT IN CONFIDENCE
II NOT TO REPRODUCE OR COPY IT
III NOT TO REVEAL OR PUBLISH IT IN WHOLE OR PART
IV ALL RIGHTS RESERVED

2

1

27. The file was only accessible to certain Apple employees that were disclosed on the Project as described below. This single file serves as the basis for the instant criminal charge. The Subject Computer is currently in the possession of the FBI, having been seized from Apple pursuant to a search warrant issued by U.S. Magistrate Judge Susan van Keulen on June 22, 2018.

APPLE'S STEPS TO PROTECT ITS INTELLECTUAL PROPERTY

28. Apple goes to great lengths to protect data and intellectual property for the Project. The Databases are protected by several layers of access control. First, an employee must be logged into Apple's virtual private network (VPN). Accounts for VPN are provisioned during the onboarding process for new hires and controlled via an internal tool. The employee must then download an internal application and install the VPN. Next, the employee must be granted "disclosure" for the Project. Disclosure status allows an employee to receive information for the Project.

29. Apple uses an internal software tool to manage requests for project disclosure and maintains a record of all disclosures. An employee has to be "sponsored" for disclosure on the Project by someone who is already disclosed. The sponsor will submit a disclosure request on behalf of the employee through the disclosure tool. The request must include a business justification for the employee to be granted access. An administrator reviews the request and approves or denies it. Approximately 5,000 of Apple's over 135,000 full time employees are disclosed on the Project.

30. Not all employees disclosed on the Project are granted access to the Databases. After receiving disclosure, an employee must also separately request database access, unless they are designated as a "core employee" for the Project.

31. **ZHANG** had core employee status and access to the Databases because he was working full time on the Project under the Research and Development organization. Approximately 2,700 employees have access to one or more of the Databases.

32. Apple also goes to great lengths to communicate the importance of secrecy to its employees. Before starting at Apple, corporate employees must sign an Intellectual Property Agreement (IPA). The IPA specifies that an employee may not use Apple's intellectual property except as authorized by Apple, including a prohibition against transfer and transmission of intellectual property without Apple's consent.

33. **ZHANG** signed an IPA on October 28, 2015. In addition, **ZHANG** took an annual Business Conduct course which discussed appropriate handling of confidential material. The training explained that confidential material includes unannounced product designs and features, project or product timelines and staffing, project code names and marketing and financial information, among other things.

34. The annual Business Conduct training also explained that once an employee is formally disclosed on a project, an employee has authorized awareness of a confidential project, can discuss project details with people disclosed on the project, and may be given access to specific confidential information or documents. The training stated that being disclosed does not mean an employee can disclose other people at will.

35. Employees disclosed on the Project must also attend an in-person secrecy training for the Project. **ZHANG** attended the secrecy training on December 9, 2015. The training covered the importance of keeping the nature and the details of the Project secret and avoiding intentional or unintentional information leaks. The training reviewed methods for ensuring information about the project is only provided to individuals disclosed on the project, the fact that family members should not have access to information about the Project, as well as possible consequences for providing information or confirmation of information to non-disclosed individuals, including employment termination. The training also covered Apple's policy prohibiting employees from storing IP on devices over which they do not have personal control, and requirements for storing and transmitting Project documents using secure mechanisms.

INTERVIEW OF ZHANG BY FBI AGENTS

36. **ZHANG** was interviewed by Agents from the FBI on June 27, 2018, at the time of an execution of a Federal search warrant at his residence. **ZHANG** admitted to taking files from the Project, and further admitted to transferring these files to a non-Apple digital device, described by **ZHANG** as his wife's laptop computer (Subject Computer). **ZHANG** told the Agents that because he needed to turn-in his Apple-owned laptop upon resignation, he transferred the files to Subject Computer for access in the future.

ZHANG'S INTERNATIONAL TRAVEL PLANS

37. On July 7, 2018, FBI Agents learned that **ZHANG** purchased a last-minute round-trip airline ticket with no co-travelers, departing San Jose, California on July 7, 2018 traveling to Beijing, China with a final destination of Hangzhou, China aboard Hainan Airlines. Agents intercepted **ZHANG** at the San Jose International Airport after he had passed through the security checkpoint of Terminal B, where he was arrested by federal agents without incident based on probable cause to believe that he had committed theft of trade secrets in violation of 18 U.S.C. § 1832.

CONCLUSION

38. Through my training and experience as an FBI Agent, I believe that **ZHANG** used his employment as an Apple employee, working on a secretive program, to obtain intellectual property and trade secrets from Apple prior to resigning from Apple. **ZHANG** admitted both to Apple and to the FBI to taking Apple's data and admitted "air-dropping" this information onto Subject Computer. Subject had received initial Intellectual Property training and annual training thereafter which would have prohibited such behavior. Further, **ZHANG** signed an Intellectual Property Agreement on October 28, 2015, indicating that **ZHANG** understood his responsibilities and would abide by Apple's policies.

39. Based upon the foregoing, my training and experience, and the training and experience of agents and investigators involved in this investigation, I believe that there is probable cause to believe that **ZHANG** has committed the crime of theft of trade secrets in violation of Title 18, United States Code Section 1832.

ERIC M. PROUDFOOT
Special Agent
Federal Bureau of Investigation

Sworn to before me this 9th day of July, 2018

Virginia K. DeMarchi
HONORABLE VIRGINIA K. DeMARCHI
United States Magistrate Judge

AO 257 (Rev. 6/78)

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☒ COMPLAINT ☐ INFORMATION ☐ INDICTMENT ☐ SUPERSEDING

OFFENSE CHARGED

Count One: 18 U.S.C. § 1832(a)(1) – Theft of Trade Secrets

☐ Petty
☐ Minor
☐ Misde-meanor
☒ Felony

PENALTY: 10 years imprisonment, $250,000 fine, $100 special assessment, 3 years' supervised release

Name of District Court, and/or Judge/Magistrate Location
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

DEFENDANT - U.S

XIAOLANG ZHANG

DISTRICT COURT NUMBER

MAG

CR 18 70919

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)

Eric M. Proudfoot, FBI

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:
☐ U.S. ATTORNEY ☐ DEFENSE

SHOW DOCKET NO.

☐ this prosecution relates to a pending case involving this same defendant

MAGISTRATE CASE NO.

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

Name and Office of Person Furnishing Information on this form ALEX G. TSE, Acting

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) Amie D. Rooney

DEFENDANT

IS *NOT* IN CUSTODY

1) ☐ Has not been arrested, pending outcome this proceeding. If not detained give date any prior summons was served on above charges

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

FILED
JUL 09 2018
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

IS IN CUSTODY

4) ☒ On this charge

5) ☐ On another conviction } ☐ Federal ☐ State

6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

Has detainer been filed? ☐ Yes ☐ No } If "Yes" give date filed

DATE OF ARREST Month/Day/Year July 7, 2018

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY Month/Day/Year

☐ This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

☐ SUMMONS ☒ NO PROCESS* ☐ WARRANT

Bail Amount:

If Summons, complete following:
☐ Arraignment ☐ Initial Appearance

Defendant Address:

** Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment*

Date/Time: Before Judge:

Comments: