UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CRIMINAL COVER SHEET

Instructions: *Effective November 1, 2016, this Criminal Cover Sheet must be completed and submitted, along with the Defendant Information Form, for each new criminal case.*

CASE NAME: **CASE NUMBER:** 3:24-cr-00141 VC

USA v. LINWEI DING a.k.a. LEON DING **CR**

Is This Case Under Seal?	**Yes** ✓	**No**	
Total Number of Defendants:	**1** ✓	**2-7**	**8 or more**
Does this case involve ONLY charges under 8 U.S.C. § 1325 and/or 1326?	**Yes**	**No** ✓	
Venue (Per Crim. L.R. 18-1):	**SF** ✓	**OAK**	**SJ**
Is this a potential high-cost case?	**Yes**	**No** ✓	
Is any defendant charged with a death-penalty-eligible crime?	**Yes**	**No** ✓	
Is this a RICO Act gang case?	**Yes**	**No** ✓	

Assigned AUSA (Lead Attorney): Casey Boome **Date Submitted:** 3/5/2024

Comments:

RESET FORM SAVE PDF

United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

UNITED STATES OF AMERICA,

V.

LINWEI DING a.k.a. LEON DING,

DEFENDANT(S).

INDICTMENT

18 U.S.C. § 1832(a)(1), (2) and (3) – Theft of Trade Secrets (4 Counts);

18 U.S.C. §§ 981(a)(1)(C), 1834, and 2323, and 28 U.S.C. § 2461(c) – Criminal Forfeiture.

A true bill.

/s/ Foreperson of the Grand Jury
Foreman

Filed in open court this 5th day of

March 2024.

Clerk

Bail, $ Arrest Warrant

ISMAIL J. RAMSEY (CABN 189820)
United States Attorney

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. LINWEI DING, a.k.a. Leon Ding, Defendant.	CASE NO. 3:24-cr-00141 VC VIOLATIONS: 18 U.S.C. § 1832(a)(1), (2) and (3) – Theft of Trade Secrets (4 Counts); 18 U.S.C. §§ 981(a)(1)(C), 1834, and 2323, and 28 U.S.C. § 2461(c) – Criminal Forfeiture. SAN FRANCISCO VENUE

INDICTMENT

The Grand Jury charges:

Introductory Allegations

At all times relevant to this Indictment:

Background on Google, LLC

1. Google, LLC ("Google") was a technology company headquartered in Mountain View, California. Google was a subsidiary of Alphabet Inc., the world's third-largest technology company by revenue with a market capitalization of approximately $1.75 trillion. Google's products and services included Google Search, Google Maps, YouTube, Android, Chrome, Google Play, and Google Cloud, among others.

2. Google was integrating artificial intelligence ("AI") into its products and services and

conducting research to develop next generation AI technology. Among Google's AI initiatives was the development of supercomputing data centers capable of supporting machine learning workloads used to train and host large AI models. Google used these data centers to train its proprietary large AI models, conduct research, and integrate AI applications into its products and services. Google Cloud also leased the supercomputing power of its data centers to other companies who used the infrastructure to train their own AI models and host AI applications.

3. Large AI models and the AI applications they supported could make predictions, find patterns, classify data, understand nuanced language, and generate intelligent responses to prompts, tasks, or queries. To achieve this capability, large AI models were "trained" through a computation-intensive process known as machine learning, which involved the analysis of an enormous volume of text, code, images, video, and other data.

4. The core hardware components of a Google supercomputing data center included, among others, Graphics Processing Units ("GPUs") and Tensor Processing Units ("TPUs") (collectively, "hardware infrastructure"). GPUs and TPUs were advanced computer chips with the extraordinary processing power required to facilitate machine learning and run AI applications. Google purchased the GPUs used in its data centers from another technology company. TPUs were developed in-house by Google to perform matrix processing for neural network machine learning. A neural network was an AI model trained to make decisions in a manner similar to the human brain. Multiple chips were combined onto a server, and a single data center contained thousands of servers.

5. The hardware infrastructure in Google's network of data centers was managed by several layers of software (the "software platform"). The software platform provided instructions, in the form of code, which communicated tasks to the hardware infrastructure for execution. One component of the software platform was the Cluster Management System ("CMS"), which functioned as the "brain" of Google's supercomputing data centers in that the CMS organized, prioritized, and assigned tasks to the hardware infrastructure, allowing the hardware to function efficiently when executing machine learning workloads or hosting AI applications.

Google's Proprietary Information Protection Policies

6. Google took reasonable measures to safeguard its proprietary technology, information,

and trade secrets. For instance, Google secured its physical space by deploying campus-wide security guards and installing cameras on most building entry points. Google restricted access to its buildings by requiring employees to badge in at front entrances. Certain floors or areas within buildings were further restricted to a subset of employees by badge access. Advance registration was required for guests, and Google employees were required to escort their guests at all times.

7. Google also took measures to secure its network. One method was a system of data loss prevention that monitored and logged certain data transfers to and from Google's network. Google also required each device to be uniquely identified and authenticated before accessing the Google corporate network. All Google employees were required to use two-factor authentication for their work-related Google accounts. Employee activity on Google's network was logged, including file transfers to platforms such as Google Drive or DropBox.

8. Google collected physical and network access information, including badge access times and locations, Internet Protocol (IP) addresses for employee logins, and two-factor authentication logs, and gathered this information in a database to analyze potential risks. This data was regularly assessed both by automated tools and human analysts to detect potential malicious activity. For example, if a Google employee's account were used to access the network through an IP address registered in a different location from a door access badge-in for the same employee, an "Impossible Location Signal" would be generated, and Google's security team would be notified. Google employees were instructed to report remote work from foreign locations, and Google automatically limited the network access of employees traveling to certain countries, such as China, North Korea, and Iran.

9. Within the Google network, access to certain sensitive information, including the trade secrets identified below in Counts One through Four, was further restricted to a subset of employees whose job duties related to the subject matter.

10. Every Google employee was required to sign an Employment Agreement through which the employee agreed:

a) To hold all Google Confidential Information, which includes Google trade secrets, "in strict confidence;"

b) Not to use Google Confidential Information "for any purpose other than for the

benefit of Google in the scope of [their] employment;"

c) Not to "retain any documents or materials or copies thereof containing any Google Confidential Information" upon termination from Google; and

d) Not to engage in other employment or business activity that "directly relates to the business in which Google is now involved, becomes involved, or has plans to become involved," or "otherwise conflicts with Google's business interest."

11. Every new Google employee was required to sign Google's Code of Conduct, which stated, in part, that every Google employee must "take steps to keep our trade secrets and other confidential intellectual property secret." Additional supplementary security training was often provided for employees working on sensitive technology projects.

12. All employees were trained on the importance of protecting Google's intellectual property. For instance, Google employees were required to complete "Privacy and Information Security" training while onboarding with Google and periodically thereafter. This training included modules about the importance of protecting Google's trade secrets.

Linwei DING's Employment with Google

13. Google hired Linwei DING as a software engineer in 2019. DING signed Google's Employment Agreement on February 20, 2019, and began working for Google on May 13, 2019. The following day, May 14, 2019, DING signed Google's Code of Conduct.

14. The focus of DING's work was the software platform deployed in Google's network of supercomputing data centers. DING's job responsibilities included development of software that allowed GPUs to function efficiently for machine learning, AI applications, or other purposes required by Google or Google Cloud clients. Due to DING's job responsibilities, he was authorized to access Google Confidential Information related to Google's supercomputing data centers, including the hardware infrastructure, the software platform, and the AI models and applications they supported.

Without Informing Google, DING Affiliated with PRC-Based Companies in the AI Industry While Transferring Google's Trade Secrets and Other Confidential Information

15. DING began uploading Google Confidential Information from Google's network into a personal Google Cloud account ("DING Account 1") on May 21, 2022, and continued periodic uploads

until May 2, 2023. In total, DING uploaded more than 500 unique files containing Google Confidential Information, including the trade secrets alleged in Counts One through Four. DING exfiltrated these files by copying data from the Google source files into the Apple Notes application on his Google-issued MacBook laptop. DING then converted the Apple Notes into PDF files and uploaded them from the Google network into DING Account 1. This method helped DING evade immediate detection.

16. Beginning on or about June 13, 2022, less than one month after DING's unauthorized and secret upload activity started, DING received several emails from the Chief Executive Officer (CEO) of Beijing Rongshu Lianzhi Technology Co., Ltd. ("Rongshu"), an early-stage technology company based in the People's Republic of China (PRC). The emails indicated that the CEO had offered DING the position of Chief Technology Officer (CTO), with a monthly salary of 100,000 RMB (approximately $14,800 in June 2022), plus an annual bonus and company stock. Rongshu's business objectives included the development of acceleration software designed for machine learning on GPU chips. Rongshu touted its development of AI federated learning platforms, which were systems for training AI models using decentralized data sources for greater data privacy.

17. DING traveled to the PRC on October 29, 2022, and remained there until March 25, 2023. Beginning in or about December 2022, while in the PRC, DING participated in investor meetings to raise capital for Rongshu. Rongshu's CEO informed potential investors during an April 17, 2023 meeting that DING was Rongshu's CTO.

18. DING never informed Google about his affiliation with Rongshu.

19. By no later than May 30, 2023, DING had founded Shanghai Zhisuan Technology Co. Ltd., ("Zhisuan") and was acting as its CEO. Zhisuan was a PRC-based startup company that proposed to develop a CMS that could accelerate machine learning workloads, including training large AI models powered by supercomputing chips.

20. On or about May 30, 2023, DING applied on behalf of Zhisuan to a PRC-based startup incubation program known as MiraclePlus. Zhisuan was accepted to the program, and on or about November 20, 2023, DING signed an agreement granting a seven percent ownership interest in Zhisuan to a MiraclePlus affiliated company in exchange for investment capital for Zhisuan. DING traveled to the PRC and pitched Zhisuan to investors at the MiraclePlus venture capital investor conference in

Beijing on or about November 24, 2023. A Zhisuan document, which DING circulated on November 29, 2023 to the members of a Zhisuan WeChat group, stated in part, "we have experience with Google's ten-thousand-card computational power platform; we just need to replicate and upgrade it – and then further develop a computational power platform suited to China's national conditions."

21. DING never informed Google about his affiliation with Zhisuan.

Google Detects DING's Exfiltration of Google Confidential Information

22. On or about December 2, 2023, DING uploaded additional files from the Google network to another personal Google Drive account ("DING Account 2") while DING was in the PRC. On December 8, 2023, after Google detected this activity, DING told a Google investigator that he had uploaded the files to his personal account to use the information as evidence of the work that he had conducted at Google. DING assured the investigator that he had no intention of leaving Google. DING signed a Self-Deletion Affidavit (SDA), dated December 8, 2023, that stated in part:

> I have searched my personal possessions, including all devices, accounts, and documents in my custody or control for any non-public information originating from my job at Google . . . I have permanently deleted and/or destroyed all copies of such information . . . As a result, I no longer have access to such information outside the scope of my employment.

DING did not tell Google that he had previously uploaded more than 500 confidential files, including Google trade secrets, between May 2022 and May 2023, nor that he was affiliated with Rongshu and Zhisuan.

23. Unbeknownst to Google, on December 14, 2023, DING booked a one-way ticket from San Francisco to Beijing on a China Southern Airlines flight scheduled to depart on January 7, 2024.

24. On December 26, 2023, DING sent an email to his manager resigning from Google and stating that his last day would be January 5, 2024.

25. On or about December 29, 2023, Google learned that DING had presented as the CEO of Zhisuan at the MiraclePlus investor conference in Beijing on November 24, 2023. Google then suspended DING's network access and remotely locked his Google laptop. Google searched DING's network activity history and discovered DING's unauthorized uploads from May 2022 through May 2023.

26. Also on or about December 29, 2023, Google investigators reviewed surveillance footage

from the entrance to the Google building where DING worked. Google observed another employee scan DING's access badge on December 4, 6, and 8, 2023, making it appear as though DING had been working from his U.S. Google office on those dates when in fact DING was in the PRC. The employee who scanned DING's badge stated to Google that DING had asked him/her to periodically scan his badge while he was traveling to make it appear as though he was working from his office.

27. On January 4, 2024, Google security personnel retrieved DING's Google laptop and mobile device from DING's residence.

FBI Investigation of DING

28. On January 6, 2024, the Federal Bureau of Investigation (FBI) executed a search warrant at DING's residence, seizing his electronic devices and other evidence.

29. On January 13, 2024, the FBI executed an additional search warrant for the contents of DING Accounts 1 and 2. DING Account 1 contained more than 500 unique files containing Google Confidential Information, including the trade secrets alleged in Counts One through Four.

General Description of Stolen Trade Secrets

30. In general, the trade secrets alleged in Counts One through Four pertain to the hardware infrastructure and software platform that allow Google's supercomputing data centers to train large AI models through machine learning. The trade secrets contain detailed information about the architecture and functionality of GPU and TPU chips and systems, the software that allows the chips to communicate and execute tasks, and the software that orchestrates thousands of chips into a supercomputer capable of executing at the cutting edge of machine learning and AI technology.

COUNTS ONE THROUGH FOUR: (18 U.S.C. § 1832(a)(1), (2), & (3) – Theft of Trade Secrets)

31. The allegations contained in Paragraphs 1 through 30 are realleged and incorporated as if fully set forth herein.

32. On or about the dates set forth in the separate counts below, in the Northern District of California and elsewhere, the defendant,

LINWEI DING,

intending to convert a trade secret that was related to a product and service used in and intended for use in interstate and foreign commerce to the economic benefit of anyone other than the owner of that trade

secret, and knowing and intending that the offense would injure the owner of that trade secret, as specifically alleged in each of Counts One through Four below:

a. knowingly stole, and without authorization appropriated, took, carried away, concealed, and by fraud, artifice, and deception obtained trade secrets belonging to Google;

b. knowingly and without authorization copied, duplicated, sketched, drew, downloaded, uploaded, altered, photocopied, replicated, transmitted, delivered, sent, communicated, and conveyed trade secrets belonging to Google; and

c. knowingly and without authorization received, bought, and possessed trade secrets belonging to Google, and attempted to do so, knowing the same to have been stolen and appropriated, obtained, and converted without authorization:

Count	Date	Item Description
One	On or about and between June 1, 2022 and April 17, 2023	Chip architecture and software design specifications for TPU version 4
Two	On or about and between June 1, 2022 and April 17, 2023	Chip architecture and software design specifications for TPU version 6
Three	On or about and between June 1, 2022 and April 17, 2023	Hardware, software, system management, and performance specifications for GPU chips deployed in Google's supercomputing data centers
Four	On or about June 1, 2022	Software design specifications for Google CMS that managed machine learning workloads on TPU and GPU chips in Google's supercomputing data centers

Each in violation of Title 18, United States Code, Sections 1832(a)(1), (2), and (3).

//

//

FORFEITURE ALLEGATION: (18 U.S.C. §§ 981(a)(1)(C), 1834, and 2323, and 28 U.S.C. § 2461(c) – Proceeds and Property Involved in Theft of Trade Secrets)

33. The allegations contained in Counts One through Four of this Indictment are realleged and by this reference fully incorporated herein for the purposes of alleging forfeiture. Upon conviction of any of those offenses, the defendant,

LINWEI DING,

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 1834, and 2323, and Title 28, United States Code, Section 2461(c), any property used, or intended to be used, in any manner or part to commit or facilitate the commission of the offenses, and any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses, including, but not limited to, a sum of money equal to the total amount of proceeds defendant obtained or derived, directly or indirectly, from the violations, or the value of the property used to commit or to facilitate the commission of said violations.

34. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 2323(b).

//

//

//

//

//

//

//

All pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 1834, and 2323, Title 28, United States Code, Section 2461(c), and Federal Rule of Criminal Procedure 32.2.

DATED: March 5, 2024

A TRUE BILL.

/s/
FOREPERSON
San Francisco, California

ISMAIL J. RAMSEY
United States Attorney

/s/ Casey Boome
CASEY BOOME
LAURA VARTAIN
Assistant United States Attorneys

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

BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT ☐ SUPERSEDING

OFFENSE CHARGED

18 U.S.C. § 1832(a)(1), (2) and (3) – Theft of Trade Secrets (4 Counts)

☐ Petty ☐ Minor ☐ Misde-meanor ☒ Felony

PENALTY: For each count:
- 10 years' imprisonment;
- $250,000 fine, or twice the gross gain/loss;
- $100 special assessment; and
- 3 years' supervised release.

PROCEEDING

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

Federal Bureau of Investigation

☐ 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

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under
} MAGISTRATE CASE NO. _____

Name and Office of Person Furnishing Information on this form: ISMAIL J. RAMSEY

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned): Casey Boome

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

DEFENDANT - U.S

LINWEI DING a.k.a. LEON DING

DISTRICT COURT NUMBER

3:24-cr-00141 VC

FILED
Mar 05 2024
Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

DEFENDANT

IS *NOT* IN CUSTODY

Has not been arrested, pending outcome this proceeding.

1) ☒ 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)

_____

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 _____

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

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

Defendant Address:

_____

Date/Time: _____ Before Judge: _____

Comments: