

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

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

**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:** USA v. LINWEI DING a.k.a. LEON DING      **CASE NUMBER:** 3:24-cr-00141 VC  
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:**

# United States District Court

FOR THE  
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

**FILED**

Mar 05 2024

Mark B. Busby  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
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

\_\_\_\_\_  
*Clara Kurland*  
Clerk

\_\_\_\_\_  
*WBC*

\_\_\_\_\_  
Bail, \$ Arrest Warrant

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

ISMAIL J. RAMSEY (CABN 189820)  
United States Attorney

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

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

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

INDICTMENT

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

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

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

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

27 Google’s Proprietary Information Protection Policies

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

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

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

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

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

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

- 26 a) To hold all Google Confidential Information, which includes Google trade  
27 secrets, "in strict confidence;"
- 28 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

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

6 16. Beginning on or about June 13, 2022, less than one month after DING's unauthorized and  
7 secret upload activity started, DING received several emails from the Chief Executive Officer (CEO) of  
8 Beijing Rongshu Lianzhi Technology Co., Ltd. ("Rongshu"), an early-stage technology company based  
9 in the People's Republic of China (PRC). The emails indicated that the CEO had offered DING the  
10 position of Chief Technology Officer (CTO), with a monthly salary of 100,000 RMB (approximately  
11 \$14,800 in June 2022), plus an annual bonus and company stock. Rongshu's business objectives  
12 included the development of acceleration software designed for machine learning on GPU chips.  
13 Rongshu touted its development of AI federated learning platforms, which were systems for training AI  
14 models using decentralized data sources for greater data privacy.

15 17. DING traveled to the PRC on October 29, 2022, and remained there until March 25,  
16 2023. Beginning in or about December 2022, while in the PRC, DING participated in investor meetings  
17 to raise capital for Rongshu. Rongshu's CEO informed potential investors during an April 17, 2023  
18 meeting that DING was Rongshu's CTO.

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

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

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

1 Beijing on or about November 24, 2023. A Zhisuan document, which DING circulated on November  
2 29, 2023 to the members of a Zhisuan WeChat group, stated in part, “we have experience with Google’s  
3 ten-thousand-card computational power platform; we just need to replicate and upgrade it – and then  
4 further develop a computational power platform suited to China’s national conditions.”

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

6 Google Detects DING’s Exfiltration of Google Confidential Information

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

13 I have searched my personal possessions, including all devices, accounts,  
14 and documents in my custody or control for any non-public information  
15 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.

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

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

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

23 25. On or about December 29, 2023, Google learned that DING had presented as the CEO of  
24 Zhisuan at the MiraclePlus investor conference in Beijing on November 24, 2023. Google then  
25 suspended DING’s network access and remotely locked his Google laptop. Google searched DING’s  
26 network activity history and discovered DING’s unauthorized uploads from May 2022 through May  
27 2023.

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



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

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

8 FBI Investigation of DING

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

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

14 General Description of Stolen Trade Secrets

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

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

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

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

26 LINWEI DING,

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

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

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

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

8 c. knowingly and without authorization received, bought, and possessed trade secrets  
9 belonging to Google, and attempted to do so, knowing the same to have been stolen and  
10 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

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

27 //

28 //

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

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

6 LINWEI DING,

7 shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections  
8 981(a)(1)(C), 1834, and 2323, and Title 28, United States Code, Section 2461(c), any property used, or  
9 intended to be used, in any manner or part to commit or facilitate the commission of the offenses, and  
10 any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses,  
11 including, but not limited to, a sum of money equal to the total amount of proceeds defendant obtained  
12 or derived, directly or indirectly, from the violations, or the value of the property used to commit or to  
13 facilitate the commission of said violations.

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

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

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

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

18 d. has been substantially diminished in value; or

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

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

22 //

23 //

24 //

25 //

26 //

27 //

28 //



**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
- Misdemeanor
- 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.

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

**PROCEEDING**

Name of Complainant 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 re prosecution 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 **ISMAIL J. RAMSEY**

U.S. Attorney  Other U.S. Agency

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

**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

If Summons, complete following:

Arraignment  Initial Appearance

Defendant Address: \_\_\_\_\_

Bail Amount: \_\_\_\_\_

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

Date/Time: \_\_\_\_\_ Before Judge: \_\_\_\_\_

Comments: