U.S. Department of
JUSTICE

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. 24-cr-00141 VC VIOLATIONS: 18 U.S.C. § 1832(a)(1), (2) and (3) – Theft of Trade Secrets; 18 U.S.C § 1831(a)(1).(2), and (3) – Economic Espionage 18 U.S.C. §§ 981(a)(1)(C), 1834, and 2323, and 28 U.S.C. § 2461(c) – Criminal Forfeiture. SAN FRANCISCO VENUE

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

The Grand Jury charges:

Introductory Allegations

At all times relevant to this Superseding 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. Google was integrating artificial intelligence ("AI") and machine learning ("ML") 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 training and serving state of the art proprietary AI models, conducting AI research, and integrating AI into Google's core products and services. Google Cloud also leased part of its supercomputing data centers to other companies who used the infrastructure to train their own AI models and host AI applications.

2. 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 created through a computation-intensive process called "training," which involved processing an enormous volume of text, code, images, video, and other data.

3. Google offered a range of products designed to accelerate ML tasks, including Graphics Processing Unit ("GPU") and Tensor Processing Unit ("TPU") based products. GPUs and TPUs were advanced computer chips with the extraordinary processing power required to train and serve large AI models. Google's customers could access and use TPUs and GPUs for their own machine learning workloads via Google Cloud. Google also used the chips for its own purposes, for example to train and serve its own AI models, such as Gemini.

4. TPUs were developed in-house by Google to accelerate deep learning workloads. Deep learning uses neural networks, a type of AI model trained to make decisions in a manner similar to the human brain. Google built complex systems that combined thousands of interconnected TPU chips to achieve high performance and support large AI models. Google designed its TPUs to contain four primary components: (1) TensorCore; (2) BarnaCore/SparseCore; (3) high bandwidth memory (HBM) access interface; and (4) inter-chip-interconnect (ICI). The TensorCore component was the main processing component of the chip and was responsible for most of the acceleration. The BarnaCore/SparseCore component was responsible for sparse computation, which provided substantial acceleration on certain types of deep learning workloads. The HBM access provided a way for the chip to access memory. ICI was a Google-developed technology that allowed TPU chips to communicate. Google created custom designed machines to house multiple TPUs and to scale the processing power for ML workloads. Each TPU machine had multiple components designed to optimize value, cost, and

efficiency. Multiple TPU machines were installed on a rack, and machines across multiple racks were then connected. This large-scale proprietary system allowed Google to create a supercomputer and accelerate ML tasks at scale. The hardware infrastructure for Google's TPUs was managed by several layers of software. Google used custom designed software to manage the hardware and resources within a TPU, to facilitate communication between TPUs, and to allocate and manage collections of interconnected TPUs to complete different workloads.

5. GPUs were accelerators that could be also used for machine learning. Google purchased the GPUs used in its data centers from another technology company. Google designed custom machines intended to hold multiple GPUs, as a well as a system designed to connect thousands of GPUs and to provide the necessary power, cooling, and networking for high-performance computing. Google's GPU hardware infrastructure was managed by several layers of software. Google used custom designed software to facilitate communication between GPUs and to allocate and manage collections of interconnected GPUs.

6. To enhance the functions of its GPU products, Google used a custom designed SmartNIC, a type of network interface card. A SmartNIC was a hardware device that offloaded networking functions from a server's Central Processing Unit (CPU). Google's SmartNIC incorporated a proprietary chip component designed to deliver low-latency and high-bandwidth transfers of data over large-scale networks. Google also developed software and used its custom designed SmartNIC to enhance its high performance and cloud networking products.

7. 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

8. 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.

9. Google also took measures to secure its network. One method was a data loss prevention system 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.

10. 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 the People's Republic of China (PRC), the Democratic People's Republic of Korea (DPRK), and Iran.

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

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

a) To hold all Google Confidential Information, which included 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."

13. 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.

14. 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

15. 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.

16. 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 Secretly Exfiltrating Google's Trade Secrets and Other Confidential Information

17. 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 1,000 unique files containing Google Confidential Information, including the trade secrets alleged in Trade Secret Categories One through Seven. 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 by Google.

18. 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 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 ML 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.

19. 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.

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

21. 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 Cluster Management System (CMS) that could accelerate ML workloads, including training large AI models powered by supercomputing chips.

22. 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."

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

DING Intended to Benefit the PRC Government and Instrumentalities

24. On or about November 17, 2023, Ding circulated a PowerPoint presentation to other Zhisuan employees citing PRC national policies encouraging the development of the domestic AI industry. The presentation, which was circulated to potential Zhisuan investors, pointed to the State Council's 2017 "Notice on the Development of the New Generation of Artificial Intelligence," which called for the development of high-performance computing infrastructure. The PRC State Council is the chief administrative authority in the PRC, and it functions as the executive branch of the central government. The presentation also cited a policy document titled "Interim Measures for the Management of Generative AI Services," which was published and sponsored by seven PRC government agencies, including the Cyberspace Administration of China (CAC). The CAC, also known as the State Internet Information Office, is a PRC government agency responsible for regulating and managing the PRC's internet and cyberspace. The presentation quoted Article 6 of the Interim Measures document, which seeks to "Encourage independent innovation in basic technologies such as generative ratification intelligence algorithms, chips, and supporting software platforms . . . ."

25. In or about December 2023, Ding created a PowerPoint presentation containing an application to a PRC talent program based in Shanghai. Talent programs are sponsored by the PRC to incentivize individuals engaged in research and development outside of the PRC to transmit that knowledge and research to the PRC in exchange for salaries, research funds, lab space, or other incentives. Ding's application stated that his product "will help China to have computing power infrastructure capabilities that are on par with the international level."

26. An internal Zhisuan memo dated December 14, 2023, indicates that Zhisuan intended to

market itself to and provide services to multiple PRC-controlled entities, including government agencies and universities.

Google Detects DING's Exfiltration of Google Confidential Information

27. On or about December 2, 2023, DING uploaded additional files from the Google network to another personal Google Drive account controlled by DING ("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 1,000 confidential files, including Google trade secrets, between May 2022 and May 2023, nor that he was affiliated with Rongshu and Zhisuan.

28. 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.

29. 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.

30. 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.

31. 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.

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

FBI Investigation of DING

33. 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.

34. 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 1,000 unique files containing Google Confidential Information, including the trade secrets in Trade Secret Categories One through Seven.

General Description of Stolen Trade Secrets

35. In general, the trade secrets described in Trade Secret Categories One through Seven pertain to the hardware infrastructure and software platform that allowed Google's supercomputing data centers to train and serve large AI models. The trade secrets contain detailed information about the architecture and functionality of TPU chips and systems and GPU systems, the software that allowed the chips to communicate and execute tasks, and the software that orchestrated thousands of chips into a supercomputer capable of training and executing cutting-edge AI workloads. The trade secrets also pertain to Google's custom designed SmartNIC and related software.

Trade Secret Category 1:

36. Instruction sets, protocols, internal specifications, and implementation level details related to the four primary components of Google's custom designed TPU chip: (1) TensorCore; (2) BarnaCore/SparseCore; (3) high bandwidth memory (HBM) access interface; and (4) inter-chip-interconnect (ICI).

Trade Secret Category 2:

37. Documents including details of the design, performance, and operation of Google's custom designed TPU chips, TPU machines, and TPU systems.

Trade Secret Category 3:

38. Design documents for Google's TPU software that managed the hardware and resources

within a TPU, facilitated communication between TPUs, and allocated and managed collections of interconnected TPUs to different workloads.

Trade Secret Category 4:

39. Documents including details of the design, performance, and operation of Google's custom GPU machines and GPU systems.

Trade Secret Category 5:

40. Design documents for Google's GPU software that facilitated communication between GPUs and allocated and managed collections of interconnected GPUs to different workloads.

Trade Secret Category 6:

41. Design specifications to implement Google's proprietary chip component designed to deliver low-latency and high-bandwidth transfers of data over large-scale networks on Google's SmartNIC.

Trade Secret Category 7:

42. Design documents for Google's software to implement its high performance and cloud networking on its SmartNIC.

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

43. The allegations contained in Paragraphs 1 through 42 are realleged and incorporated as if fully set forth herein.

44. 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 Seven 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	Trade Secret Category One
Two	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Two
Three	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Three
Four	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Four
Five	On or about and between June 3, 2022 and April 17, 2023	Trade Secret Category Five
Six	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Six
Seven	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Seven

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

COUNTS EIGHT THROUGH FOURTEEN: (18 U.S.C. § 1831(a)(1), (2), & (3) – Economic Espionage

45. The allegations contained in Paragraphs 1 through 42 are realleged and incorporated as if fully set forth herein.

46. 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 or knowing that the offense would benefit any foreign government, foreign instrumentality, or foreign agent:

a. knowingly stole, and without authorization appropriated, took, carried away, concealed, and by fraud, artifice, and deception obtained trade secrets alleged in each of Counts Eight through Fourteen below 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 alleged in each of Counts Eight through Fourteen below belonging to Google; and

c. knowingly and without authorization received, bought, and possessed trade secrets alleged in each of Counts Eight through Fourteen below 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
Eight	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category One
Nine	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Two

Ten	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Three
Eleven	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Four
Twelve	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Five
Thirteen	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Six
Fourteen	On or about and between June 1, 2022 and April 17, 2023	Trade Secret Category Seven

Each in violation of Title 18, United States Code, Sections 1831(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)

47. The factual allegations contained in Paragraphs 1 through 46 of this Superseding 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.

48. 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: February 4, 2025

A TRUE BILL.

/s/ Foreperson

FOREPERSON
San Francisco, California

ISMAIL J. RAMSEY
United States Attorney

/s/
CASEY BOOME
MOLLY K. PRIEDEMAN
Assistant United States Attorneys

STEPHEN MARZEN
YIFEI ZHENG
Trial Attorneys
National Security Division