Fred Norton (SBN 224725)
Bree Hann (SBN 215695)
Matt Turetzky (SBN 280997)
THE NORTON LAW FIRM PC
299 Third Street, Ste 106
Oakland, California 94607
Telephone: (510) 906-4900
Fax: (510) 906-4910
fnorton@nortonlaw.com
bhann@nortonlaw.com
mturetzky@nortonlaw.com

Attorneys for TESLA, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

TESLA, INC., a Delaware corporation,

Plaintiff,

v.

GUANGZHI CAO, an individual,

Defendant.

CASE NO.

COMPLAINT

JURY TRIAL DEMANDED

SUMMARY OF THE ACTION

1. Tesla, Inc. ("Tesla") leads the world in the design and production of all-electric vehicles, as well as clean energy generation and storage products. Defendant Guangzhi Cao was a member of Tesla's Autopilot team, an elite group of engineers developing Tesla's industry-leading Autopilot features, including its full self-driving technology – a crown jewel of Tesla's intellectual property portfolio. As part of the Autopilot team, Cao had access to crucially important, and highly confidential, Tesla trade secrets, including source code.

2. On January 3, 2019, Cao abruptly announced that he was quitting his job at Tesla, effective the very next day. Although he did not tell anyone at the time, Cao had accepted a job doing the same work for Xiaopeng Motors Technology Company Ltd. ("XMotors"), a Tesla imitator also pursuing self-driving and electric vehicle technology.

3. As Tesla has now learned, Cao began searching for a new job by November 2018. Long before he left, Cao began uploading complete copies of Tesla's Autopilot-related source code to his personal iCloud account – more than 300,000 files and directories, in violation of Tesla's policies and its agreements with Cao. Then, as he was looking to leave Tesla, Cao created .zip files of Tesla's complete Autopilot-related source code repositories, making them smaller and easier to move.

4. Unbeknownst to Tesla, Cao had at least a verbal offer from XMotors by November 26, 2018. Cao then traveled to China (the home of XMotors) between December 5 and 9, without telling his manager where he was going or why. He received a written employment offer from XMotors on December 12.

5. Tesla does not know when Cao accepted his job offer. However, as Tesla now knows, Cao deleted over 120,000 files in the month of December and disconnected his iCloud account from his Tesla-issued computer on December 26. Between December 27 and January 1, Cao repeatedly logged into Tesla's secure networks, and he cleared his browser history by January 4, his last day at Tesla.

6. When he left, Cao did not return Tesla's highly confidential information, nor disclose that he had made copies. Tesla thus believes that Cao still has, can access at will, and may be using

all the source code needed to replicate Tesla's proprietary Autopilot technology, none of which he has a legal right to possess.

7. Needless to say, Tesla's confidential information is not safe in the hands of XMotors or its employees. Inspired by and on a mission to beat Tesla, XMotors reportedly designed its vehicles around Tesla's open-source patents and has transparently imitated Tesla's design, technology, and even its business model. XMotors has also introduced reportedly "Autopilot-like" features (called X-Pilot), and now employs at least five of Tesla's former Autopilot employees, including Cao. And, as discussed below, this would not be the first time that a new XMotors recruit tried to bring his former employer's trade secrets to XMotors.

8. Tesla has spent hundreds of millions of dollars and more than five years developing Autopilot. Now that investment is at risk. Tesla must learn what Cao has done with Tesla's IP, to whom he has given it, and the extent to which Tesla has been harmed. Tesla files this lawsuit to compel the return of its valuable IP and protect it from further exploitation, and for all other relief as the facts may warrant.

THE PARTIES

9. Tesla is a Delaware corporation with its headquarters and principal place of business in Palo Alto, California.

10. Defendant Guangzhi Cao is an individual who, on information and belief, resides in Cupertino, California. From April 24, 2017 until January 4, 2019, Cao worked for Tesla in Palo Alto, California.

JURISDICTION AND VENUE

11. This Court has jurisdiction pursuant to 28 U.S.C. § 1331 because this matter involves claims under the Defend Trade Secrets Act ("DTSA"), 18 U.S.C. §§ 1836 *et seq*. This Court has supplemental jurisdiction over the remaining claims pursuant to 28 U.S.C. § 1367, as the remaining claims form part of the same case or controversy: Cao's access to, taking of, and use of Tesla's intellectual property and confidential information.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to the claims occurred in this District. For example, Tesla

employed Cao in Palo Alto, which is within the Northern District; Cao downloaded Tesla's source code while physically present at or connected to his Tesla workplace.

FACTUAL BACKGROUND

A. Tesla's Industry-Leading Autopilot Technology And Autopilot Source Code

13. Tesla's Autopilot technology is widely regarded as the most advanced, safest, and most reliable technology of any consumer advanced driver-assistance system solution. Today, Autopilot is an advanced driver assistance system that augments drivers' perception, improves their decision-making, and assists in controlling their vehicles. Autopilot offers advanced driver assistance features including lane-keeping, adaptive cruise control, and automatic parking. More recently, Tesla introduced Navigate on Autopilot, which guides a car from a highway's on-ramp to off-ramp, including suggesting and making lane changes, navigating highway interchanges, and taking exits (in each case under the driver's supervision). Tomorrow's Autopilot will make Tesla's vehicles fully autonomous, capable of driving short and long distances without driver involvement.

14. Tesla has a global fleet of more than 500,000 cars, which have driven more than a billion collective miles with Autopilot activated. Every day, thousands of Autopilot-enabled Tesla vehicles provide real-time feedback to Tesla's servers, yielding voluminous data that Tesla uses to continually improve the Autopilot system. This fleet gives Tesla exponentially more data than its autonomous vehicle competitors, who generally have only small fleets of prototype vehicles, and has allowed Tesla to accelerate its autonomy technology in a way no other company can.

15. Tesla uses multiple, highly confidential kinds of source code for its Autopilot features, including the firmware, Autopilot, and neural net source code repositories (the "Autopilot Trade Secrets"). Firmware source code executes core tasks on Tesla's vehicles, such as motor controls, steering, and infotainment functions. Autopilot source code executes Autopilot-related functions, such as semi-autonomous driving, in response to environmental and driver-supplied inputs, and uses the neural net to process (and "see") information from onboard cameras to make decisions. The neural net source code does not run on Tesla's vehicles directly but is used to "train" the neural net using a massive dataset via machine-learning processes. Each of these source code repositories is highly valuable in its own right. Taken together, the Autopilot Trade Secrets would

give a competitor an enormous advantage in attempting to replicate Tesla's current self-driving technology, and in anticipating future developments.

16. Tesla derives independent value from maintaining the secrecy of its source code and other proprietary information related to Autopilot and the functioning of its vehicles. Tesla's source code reveals how Tesla has approached and solved problems in vehicle autonomy, and disclosure of that source code could give competitors an unfair, and unearned, advantage.

17. For example, unlike many of Tesla's competitors, Tesla's self-driving functionality is primarily based on cameras and radar, without the use of another expensive sensor, LIDAR. The source code reveals in great detail how Tesla has used camera and radar to solve problems in autonomous driving.

18. As another example, the source code also reflects and contains improvements that are built on Tesla's massive volume of fleet telemetry data. If disclosed to a competitor, that competitor could use Tesla's source code to copy Tesla's work, compete with Tesla, or otherwise accelerate the development of its own vehicle autonomy technology.

19. Similarly, across all of its source code (including firmware, Autopilot, and neural net source code), Tesla has invested enormous time and expense to write and incrementally improve its source code over time. Disclosure of this source code to Tesla's competitors could give them access to off-the-shelf code that they could use in operating their own vehicles or vehicle autonomy software. If Tesla's source code is disclosed to competitors, those competitors will unfairly receive, for free, the fruit of Tesla's labor and investment over many years to develop, improve, and refine its various kinds of source code.

B. Tesla Vigorously Protects The Confidentiality Of Its Confidential Information

20. Tesla's policies and practices robustly protect confidential and proprietary information, including the Autopilot Trade Secrets. For example, Tesla requires all its employees to enter into agreements that obligate them to safeguard the company's confidential information, including trade secrets and source code. Employees must sign confidentiality agreements as a condition of their employment, such as Tesla's Employee Non-Disclosure and Inventions

Assignment Agreement ("NDA"), and must periodically re-sign as the company revises and updates its agreements.

21. Tesla secures its physical facilities by restricting access to authorized personnel, and then monitoring actual access with security guards and cameras. Visitors to Tesla's headquarters in Palo Alto ("Deer Creek"), where the Autopilot team is located, must check in with a receptionist or security guard, sign a nondisclosure agreement, and submit to a photograph. While at Deer Creek, they must be escorted by a Tesla employee at all times.

22. Tesla also protects its confidential information with stringent information security policies and practices. Tesla's network and servers are themselves password-protected and firewall-protected and are accessible only to current Tesla employees with proper credentials. And after an employee resigns or is terminated, Tesla promptly deactivates that user's network, active directory, and email permissions, which cuts off access to Tesla's source code repositories. In addition, Tesla prohibits employees from storing confidential Tesla information on unsecured systems, such as iCloud, Google Drive, or DropBox – which Cao violated here.

C. Tesla Guards The Autopilot Source Code Even More Strictly

23. The Autopilot Trade Secrets are extremely valuable, and Tesla takes extreme care to keep them secret. Each of Tesla's 200 Autopilot team members must sign Tesla's NDA, which requires employees to keep confidential all of Tesla's confidential and proprietary information, including technical data, trade secrets, source code, and other business information. The Autopilot team members are also subject to Tesla's general policies and practices, as described above. In addition, the Autopilot team is physically separated from the other employees at Deer Creek. Employees with approved access rights to the Autopilot team area must badge into the area and pass through a turnstile, which prevents "tailgating" by other people who are not authorized to enter the restricted area. This physical separation ensures that other Tesla employees, or authorized guests, cannot see or learn what the Autopilot team is doing. The Autopilot team's work is top secret, even within Tesla.

24. Tesla stores the Autopilot Trade Secrets on a Tesla-owned server, protected behind Tesla's firewall. Of Tesla's approximately 45,000 employees worldwide, only about 800 have

access to the firmware source code, while only about 200 have access to any portion of the Autopilot source code. Access to both firmware and Autopilot source code is granted and monitored by high-level managers in the Autopilot group. Tesla restricts the neural network source code most stringently: currently, only about 40 people have access to this source code, which is granted on a strict "need-to-know" basis and only by the head of Artificial Intelligence at Tesla. As noted above, by virtue of his position and responsibilities, Cao had access to all three types of source code.

D. XMotors Copies Tesla To Catch Up

25. Given Tesla's success with its electric and autonomous cars, numerous companies are trying to catch up. One such company is XMotors.[1] XMotors is one of many Tesla-inspired startups, and its copying of Tesla is well documented.[2] For example, XMotors' first vehicle, the G3, has been called a "Tesla clone" based on visual similarities in the vehicles' styling, touchscreen, user interface, instrument cluster, headlights, and more. XMotors has also announced that it will operate a broad "super charging" network (Tesla's global fast-charging network is called the "Supercharger" network), and will operate a direct sales and service network, like Tesla has done since its inception.

26. XMotors has also pursued Tesla's employees. In 2017, XMotors hired a former Tesla Autopilot team member as its Vice President of Autonomous Driving. Tesla is informed and believes that this employee is now responsible for the self-driving research and development team for XMotors. At least five former Autopilot team members have now gone to XMotors, including Cao.

27. XMotors has previously gained notoriety in connection with competitors' trade secrets. In July 2018, a former Apple employee was arrested at the San Jose International Airport

---

[1] On information and belief, the parent company, based in China, is Xiaopeng Motors Technology Company Ltd., often referred to as Xpeng Motors. According the website www.xmotors.ai,, "XMotors is a fully-owned subsidiary of XPENG Motors." On information and belief, the XMotors entity that hired Cao is formally known as XMotors.ai, Inc.

[2] https://interestingengineering.com/is-xpeng-set-to-be-the-tesla-of-china; https://qz.com/1362926/chinese-ev-unicorn-xpeng-motors-wouldnt-exist-without-tesla/; https://electrek.co/2018/12/13/tesla-inspired-ev-startup-xiaopeng-all-electric-suv/; https://electrek.co/2018/04/10/ev-startup-tesla-clone-alibaba-foxconn-xiaopeng/.

for stealing self-driving intellectual property from Apple.[3] Like Cao, that individual had accepted a job with XMotors and left his old job with valuable trade secrets he had no right to possess.

E. Cao Agreed to Protect Tesla's Confidential Information

28. Cao was subject to confidentiality agreements throughout his employment at Tesla. Even before he was hired, he expressly assented to a non-disclosure agreement as part of his pre-employment interview process. The day before his first day as an employee, on April 23, 2017, he agreed to a Tesla Motors, Inc. Employee Proprietary Information and Inventions Agreement, which included restrictions on his use of Tesla's confidential information. *See* **Exhibit A** (the "First NDA"). On June 4, 2018, Cao agreed to an updated agreement with substantially similar provisions. *See* **Exhibit B** ("Second NDA," and together with Exhibit A, the "NDAs").

29. The NDAs cover all of Tesla's technical data, trade secrets, source code, and other business information, and require employees to keep that information confidential. *See* Exhibit A at § 1, Exhibit B at § 1. Both NDAs explicitly require an employee, upon termination, to "immediately" return to Tesla all Tesla hard copy and electronic documents and materials. *See* Exhibit A at § 4, Exhibit B at § 4. Both prohibit current and former employees from soliciting Tesla employees on behalf of another company for 12 months after they leave Tesla. *See* Exhibit A at § 8.2; Exhibit B at §§ 9.2.1, 9.2.2.

F. Cao Misappropriates The Autopilot Trade Secrets

30. Cao started as a full-time employee at Tesla on April 24, 2017, as a Staff Computer Vision Scientist, working as part of the team building the neural net that is the foundation for Tesla's self-driving technologies. Because of his position and job duties, Cao had extensive access to Tesla's confidential information, including all of the Autopilot Trade Secrets. While at Tesla, Cao worked on Autopilot with the former Tesla employee who later left to become XMotors' current Vice President of Autonomous Driving.

31. As Tesla now knows, Cao violated Tesla's policies and his agreements with Tesla from the beginning. Cao used his personal iCloud account from 2017 to 2018 to create backup

[3] https://www.reuters.com/article/us-apple-theft/ex-apple-worker-charged-with-stealing-self-driving-car-trade-secrets-idUSKBN1K02RR.

copies of Tesla's highly confidential information, including the Autopilot Trade Secrets. For example, a forensic analysis shows that, between March 25, 2018 and December 26, 2018, he backed up entire repositories for the firmware, Autopilot, and neural net source code repositories – apparently all of the source code to which he had access – including more than 300,000 individual files and directories. Tesla believes that all of this information remains accessible to Cao in his personal iCloud account, in violation of Tesla's policies, Cao's agreements, and his legal obligations.

32. Between November 2 and November 13, 2018, Cao created .zip files of all of the Autopilot source code. At the same time, he was looking to leave Tesla for another job. Although Tesla does not know when Cao began talking to XMotors about employment, Cao's wife referred to an offer from Xiaopeng in a November 26, 2018 iMessage to Cao. On December 1, Cao began deleting files from his laptop. And from December 5 through 9, 2018, Cao quietly traveled to China, where XMotors is located, without telling his Tesla supervisor where he was going or why.

33. Three days later, on December 12, Cao received his formal XMotors offer letter, for the position of "Senior Director of Engineering, heading the camera perception team."

34. Tesla does not know when Cao accepted his offer at XMotors, but he gave notice on January 3, 2019. On December 26, 2018, he logged out of his personal iCloud account, disconnecting that account from his Tesla-issued computer. Between December 27 and January 1, Cao repeatedly logged into Tesla's secure networks; between December 1 and his last day, he deleted more than 120,000 files from his Tesla computer. He cleared his browser history on January 4, 2019, his last day at Tesla. No one at Tesla instructed Cao to take these steps, and no one at Tesla was aware he did so until late February 2019 when his misconduct was discovered as a result of Tesla's investigative efforts.

35. Cao did not disclose to Tesla that he had copied thousands of files, including the Autopilot Trade Secrets, to his iCloud account. He did not return the electronic copies of those documents when he left the company, as required by the NDAs. There is every reason to believe the Autopilot Trade Secrets remain in Cao's personal iCloud folder today.

36. Since Cao's departure from Tesla, at least one other Tesla employee has accepted an offer at XMotors. On January 26, 2019, that other Tesla employee sent texts about how Cao solicited him to join XMotors, including "Guangzhi [Cao] wants me to be their manager," and "I went to eat with Xiaopeng at noon on Monday." The employee received an offer letter from XMotors.ai, Inc. on February 20, 2019 and left Tesla on February 26, 2019.

37. According to his current LinkedIn profile, at XMotors Cao is now "[d]eveloping and delivering autonomous driving technologies for production cars," precisely what he was doing for Tesla.

G. Tesla Faces The Threat Of Immediate And Irreparable Harm

38. Absent immediate relief, Tesla believes Cao and his new employer, XMotors, will continue to have unfettered access to Tesla's marquee technology, the product of more than five years' work and over hundreds of millions of dollars of investment, which they have no legal right to possess. Tesla has been damaged by the misappropriation of its confidential information, including because it has incurred substantial investigatory costs, and will suffer immeasurable harm if its confidential information, including the Autopilot Trade Secrets, are subject to further disclosure or misuse.

FIRST CLAIM FOR RELIEF

Misappropriation of Trade Secrets in Violation of the Defend Trade Secrets Act

39. Tesla incorporates by reference all of the preceding paragraphs as if fully set forth herein.

40. Tesla's confidential, proprietary, and trade secret information, including the Autopilot Trade Secrets, are protected under the DTSA, 18 U.S.C. § 1836 *et seq.*

41. Tesla's confidential, proprietary, and trade secret information relates to products and services used, sold, shipped and/or ordered in, or intended to be used, sold, shipped and/or ordered in, interstate or foreign commerce.

42. The information derives independent economic value by not being accessible, through proper means, to competitors like XMotors. The information is also not readily available to the public or to Tesla's other competitors.

43. Tesla takes reasonable measures to keep this information secret and confidential, as described above. Tesla derives significant economic benefit from maintaining the secrecy and confidentiality of this information.

44. Cao's conduct constitutes a misappropriation and misuse of Tesla's confidential information in violation of the DTSA because Cao used and/or disclosed the information without Tesla's consent. Further, Cao acquired the information under circumstances giving rise to a duty to maintain the information's secrecy and limit its use. Cao owed that duty to Tesla as an agent, employee, and representative of Tesla.

45. Cao has not returned the information that he took from Tesla. Upon information and belief, Cao is retaining and using Tesla's trade secret and confidential information.

46. Cao's conduct constitutes a willful and malicious misappropriation of Tesla's confidential information.

47. Tesla has suffered and will continue to suffer damage and irreparable harm, absent immediate injunctive relief. Because Tesla's remedy at law is inadequate, Tesla seeks preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and the competitive and other benefits that information confers.

48. Thus, Tesla is entitled to preliminary injunctive relief, restitution, compensatory and exemplary damages, and reasonable attorneys' fees pursuant to 18 U.S.C. § 1836.

SECOND CLAIM FOR RELIEF

Misappropriation of Trade Secrets in Violation of the California Uniform Trade Secrets Act

49. Tesla incorporates by reference all of the preceding paragraphs as if fully set forth herein.

50. At all times relevant to this Complaint, the California Uniform Trade Secrets Act, California Civil Code §§ 3426-3426.11 ("CUTSA") was in effect.

51. Tesla developed and owns trade secrets as defined by CUTSA, as described above.

52. The information derives independent economic value by not being accessible, through proper means, to competitors like XMotors. The information is also not readily available to the public or to Tesla's other competitors.

53. Tesla derives significant economic benefit from maintaining the secrecy and confidentiality of this information.

54. Tesla takes reasonable measures to maintain its trade secrets, as described above.

55. Cao's conduct constitutes a misappropriation and misuse of Tesla's confidential information in violation of CUTSA because Cao used and/or disclosed the information without Tesla's consent. Further, Cao acquired the information under circumstances giving rise to a duty to maintain the information's secrecy and limit its use. Cao owed that duty to Tesla as an agent, employee, and representative of Tesla.

56. Cao has not returned the information that he took from Tesla. Upon information and belief, Cao is retaining and using Tesla's trade secret and confidential information

57. Cao's conduct constitutes a willful and malicious misappropriation of Tesla's trade secrets and confidential information.

58. As a consequence of the foregoing, Tesla has suffered and will continue to suffer damages and irreparable harm.

59. Unless Cao is preliminarily and permanently enjoined from the foregoing conduct, Tesla faces the threat of irreparable harm as described above. Tesla has also suffered damages. Additionally, Tesla is entitled to an award of punitive damages and attorneys' fees pursuant to CUTSA based on Cao's willful and malicious misappropriation of Tesla's trade secrets.

THIRD CLAIM FOR RELIEF

Breach of Contract

60. Tesla incorporates by reference all of the preceding paragraphs as if fully set forth herein.

61. The NDAs are valid, enforceable contracts and Tesla and Cao are parties to both contracts.

62. Tesla did all, or substantially all, of the significant things that the NDAs required of Tesla.

63. Through his conduct described herein, Cao breached his contractual obligations to Tesla, including the confidentiality obligations and non-solicit restrictions in the NDA §§ 1, 4, 9.2 and Second NDA §§ 1, 4, and 8.

64. As a direct and proximate result of the foregoing breaches, Tesla has suffered, and will continue to suffer, damages in an amount to be proven at trial.

FOURTH CLAIM FOR RELIEF

Breach of Employee's Duty of Loyalty

65. Tesla realleges and incorporates by reference each of the foregoing paragraphs as though fully set forth herein.

66. By virtue of his position as an employee of Tesla, Cao owed a duty of loyalty to Tesla, at least insofar as he was entrusted with Tesla's highly sensitive, valuable confidential information, including the Autopilot Trade Secrets.

67. Through his conduct described herein, Cao breached his duty to Tesla.

68. As a direct and proximate result of the foregoing breaches, Tesla has suffered, and will continue to suffer, damages in an amount to be proven at trial.

69. In doing the things herein alleged, Cao acted willfully, maliciously, oppressively, and with full knowledge of the adverse effects on Tesla, and with willful and deliberate disregard of the consequences to Tesla, so as to constitute oppression, fraud, and malice. Tesla is therefore entitled to exemplary and punitive damages.

PRAYER FOR RELIEF

WHEREFORE, Tesla respectfully prays for relief as follows:

A. For preliminary and permanent injunctive relief enjoining Cao and all persons or entities acting in concert or participation therewith, from:

(1) retaining, disclosing, or using any Tesla confidential and proprietary information in any manner, such as the Autopilot Trade Secrets, including without limitation to design, develop, or offer products or services in the autonomous driving industry;

(2) directly or indirectly soliciting any employee or contractor of Tesla to terminate their employment with, or otherwise cease their relationship with, Tesla for a period of one year following the termination of Cao's employment with Tesla; and

B. For preliminary and permanent injunctive relief requiring Cao to submit to ongoing auditing of his personal and work-related systems and accounts to monitor for unlawful retention or use of Tesla's confidential and proprietary information;

C. For compensatory damages in an amount to be proven at trial;

D. For prejudgment interest according to law;

E. For recovery of attorneys' fees, costs, and expenses incurred in this action; and

F. For such other and further relief as the Court may deem just and proper.

Dated: March 20, 2019

THE NORTON LAW FIRM PC

By: */s/ Fred Norton*
Fred Norton
Attorneys for Plaintiff
Tesla, Inc.

DEMAND FOR JURY TRIAL

Plaintiff Tesla, Inc. hereby demands a trial by jury of all issues so triable.

Dated: March 20, 2019

THE NORTON LAW FIRM PC

By: */s/ Fred Norton*
Fred Norton
Attorneys for Plaintiff
Tesla, Inc.