DMP:AAS/ICR/NJM/JKW
F. #2020R00535

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X

UNITED STATES OF AMERICA

- against -

JIN XINJIANG (金新江),
also known as "Julien Jin,"
CHEN YUANYUAN (陈媛媛),
FU YIBIN (傅一彬),
HUANG YIWEN (黄奕雯),
also known as "Nicole Huang,"
JIN TAO (金涛),
LIU ZHIYANG (刘智洋),
SHEN ZHENHUA (沈振华),
SONG GUORONG (宋国荣),
TIAN XINNING (田心宁) and
XU WEI (徐威),

Defendants.

AMENDED COMPLAINT AND AFFIDAVIT IN SUPPORT OF APPLICATION FOR ARREST WARRANTS

(T. 18, U.S.C., §§ 371, 1028(a)(7) and 1028(f))

No. 20-MJ-1103 (SJB)

- X

EASTERN DISTRICT OF NEW YORK, SS:

JOSEPH HUGDAHL, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such.

COUNT ONE
(Conspiracy to Commit Interstate Harassment)

In or about and between 2017 and 2020, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants JIN XINJIANG (金新江), also known as "Julien Jin," CHEN YUANYUAN (陈媛媛), FU YIBIN (傅一彬), HUANG YIWEN (黄奕雯), also known as "Nicole Huang," JIN TAO (金涛), LIU ZHIYANG (刘智洋), SHEN ZHENHUA (沈振华), SONG GUORONG (宋国荣), TIAN XINNING (田心宁) and XU WEI (徐威), together with others, did knowingly, and with the intent to harass and intimidate, and place under surveillance with the intent to harass and intimidate one or more persons, conspire to use one or more interactive computer services and electronic communication systems of interstate commerce, and one or more facilities of interstate and foreign commerce to engage in a course of conduct that caused, attempted to cause and would be reasonably expected to cause substantial emotional distress to one or more persons and their immediate family members, contrary to Title 18, United States Code, Section 2261A(2)(B).

(Title 18, United States Code, Section 371)

COUNT TWO
(Unlawful Conspiracy to Transfer Means of Identification)

In or about and between January 2019 and June 2020, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants JIN XINJIANG (金新江), also known as "Julien Jin," HUANG YIWEN (黄奕雯), also known as "Nicole Huang" and JIN TAO (金涛), together with others, did knowingly conspire to transfer, possess and use, without lawful authority, and attempt to

transfer, possess and use, without lawful authority, one or more means of identification of another person, to wit: one or more email and online videotelephony accounts in the names of one or more victims, with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law, to wit: the Conspiracy to Commit Interstate Harassment charged in Count One.

(Title 18, United States Code, Sections 1028(a)(7) and 1028(f))

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I have been employed as a Special Agent by the Federal Bureau of Investigation ("FBI") for over ten years. During my tenure with the FBI, I have participated in numerous investigations, during the course of which I have, among other things: (a) conducted physical and electronic surveillance, (b) executed search warrants, (c) reviewed and analyzed recorded conversations and records, and (d) debriefed cooperating witnesses. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file; and from reports of other law enforcement officers involved in the investigation.

2. The statements attributed to individuals in this Affidavit are set forth in sum, substance and in part unless otherwise indicated. Many of the statements attributed to individuals were originally made in Chinese and are summarized or quoted in this Affidavit based on draft translations, which are subject to change. I have personally reviewed each of

---

[1] Because the purpose of this Amended Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

the electronic communications, including emails and chat messages, described in this affidavit, and participated personally in some of the interviews discussed herein. My knowledge of other interviews is based upon my review of reports and conversations with other law enforcement officers.

I. Background

A. Company-1

3. Company-1 is a U.S. communications technology company with headquarters in San Jose, California, but with operations around the world. Company-1 provides videotelephony and online chat ("video chat") services through a cloud-based peer-to-peer software platform and is used for teleconferencing, telecommuting, distance education, and social relations. Company-1's users can host or participate in video chat "meetings" that allow as many as hundreds or thousands of users to see, hear, and speak with each other from locations around the world.

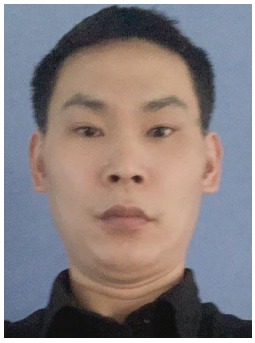
4. Company-1 has significant operations in the People's Republic of China ("PRC"), where it employs hundreds of workers who focus primarily on research and development. Company-1 has multiple subsidiaries in the PRC, including one in Hangzhou, Zhejiang Province.

B. The Defendants

5. The defendant JIN XINJIANG (金新江), also known as "Julien Jin" (hereafter "JULIEN JIN"), is a 42-year-old citizen of the PRC who was employed by Company-1 from 2016 until approximately December 2020 as the "Security Technical Leader." In this capacity, JULIEN JIN was responsible for, among other things, serving as

primary liaison with PRC authorities, including law enforcement and intelligence services, and for preventing Company-1's users from using Company-1's communications platforms and services to commit violations of law or to engage in activities that otherwise violate Company-1's Terms of Service ("TOS"). JULIEN JIN led a team of Company-1 employees in the PRC.

Photo of JULIEN JIN



6. The other defendants, as detailed further below, conspired with JULIEN JIN in censoring, or directed JULIEN JIN to censor, speech disfavored by the PRC government and the Chinese Communist Party ("CCP") occurring on the Company-1 communications platform.

7. Defendant CHEN YUANYUAN (陈媛媛) is a female and a citizen of the PRC. CHEN is an official in the Cyberspace Administration of China ("CAC") in Hangzhou's Xihu District since at least in or about June 2020. CHEN provided guidance and directives to JULIEN JIN about removing content associated with a U.S.-based critic of the CCP and sought to have employees of Company-1 terminate video chat meetings during which U.S.-based dissidents intended to commemorate the Tiananmen Square massacre in Beijing, PRC (discussed in further detail below), an issue sensitive to PRC government and the CCP.

8. Defendant FU YIBIN (傅一彬) is a 39-year-old male and a citizen of the PRC. Since at least in or about 2005, FU has been a Ministry of Public Security ("MPS") officer, badge number 000832, stationed in Zhejiang Province as part of the Network Security Corps. FU provided guidance and directives to JULIEN JIN that led to the termination of video chat meetings on Company-1's platform that were organized by U.S.-based Chinese nationals to commemorate the 1989 Tiananmen Square massacre.

Photo of FU YIBIN

9. Defendant HUANG YIWEN (黄奕雯), also known as "Nicole Huang," is a 25-year-old female and a citizen of the PRC from Zhejiang Province. HUANG is believed to reside in either Indonesia or the PRC. HUANG worked with JULIEN JIN to create pretextual violations of the Company-1's TOS to terminate video chat meetings on Company-1's platform that were organized by U.S.-based Chinese nationals to commemorate the 1989 Tiananmen Square massacre.

Photo of HUANG YIWEN

10. Defendant JIN TAO (金涛) is a male citizen of the PRC. Since at least in or about 2020, JIN TAO has been an MPS officer stationed in Hangzhou as part of the cyber/network police. Among other things, JIN TAO provided directives to JULIEN JIN that led to the termination of video chat meetings on Company-1's platform that were organized by U.S.-based Chinese nationals with Company-1 accounts provisioned in the United States to commemorate the 1989 Tiananmen Square massacre.[2]

11. Defendant LIU ZHIYANG (刘智洋) is a 43-year-old male citizen of the PRC. Since in or about July 2002, LIU has been stationed in Beijing as an officer with the MPS's First Bureau. LIU provided guidance and directives to JULIEN JIN that led to the termination of video chat meetings on Company-1's platform that were organized by U.S.-based Chinese nationals to commemorate the 1989 Tiananmen Square massacre.

[2] When users set up new paid Company-1 accounts in the United States, the accounts provision to one of Company-1's server "clusters" in the United States that enable the Company-1 meeting experience. Company-1's clusters are distinguished primarily based on location and the type of account (i.e., a paid account or a free account).

Photo of LIU ZHIYANG

12. Defendant SHEN ZHENHUA (沈振华) is a 41-year-old male and a citizen of the PRC. Since at least in or about 2018, SHEN has been stationed in Hangzhou as an officer with the MPS's Network Security Bureau. SHEN provided guidance and directives to JULIEN JIN that led to the termination of video chat meetings on Company-1's platform that were organized by U.S.-based Chinese nationals to discuss U.S. legislation pertaining to Hong Kong and to commemorate the 1989 Tiananmen Square massacre.

13. Defendant SONG GUORONG (宋国荣) is a 43-year-old male citizen of the PRC. Since at least in or about 2020, SONG has been an MPS officer stationed in Hangzhou with the Hangzhou Xihu District's cyber/network police, with badge number 014679. SONG provided guidance and directives to JULIEN JIN that led to the termination of video chat meetings on Company-1's platform that were organized by U.S.-based Chinese nationals to commemorate the 1989 Tiananmen Square massacre.

Photo of SONG GUORONG

14. Defendant TIAN XINNING (田心宁) is a male citizen of the PRC. Since at least in or about October 2019, TIAN has been stationed in Beijing as an officer with the MPS's Network Security Bureau. TIAN provided guidance and directives to JULIEN JIN that led to the removal of critics of the CCP from Company-1's communications platform and led to the termination of video chat meetings on Company-1's platform that were organized by U.S.-based Chinese nationals to commemorate the 1989 Tiananmen Square massacre.

15. Defendant XU WEI (徐威) is a 35-year-old male citizen of the PRC. Since in or about June 2011, XU has been an official in the CAC in the Xihu District's Network Propaganda Guidance Center. XU provided guidance and directives to JULIEN JIN that led to the removal of critics of the CCP from Company-1's communications platform and led to the termination of video chat meetings on Company-1's platform that were organized by U.S.-based Chinese nationals to commemorate the 1989 Tiananmen Square massacre.

Photo of XU WEI

C. The PRC Government's Suppression of Political Dissent and Religious Speech

16. The PRC is a one-party state, whose government is controlled by the CCP.[3] While the constitution and laws of the PRC government purport to guarantee PRC citizens the freedom of speech, the CCP regards any political dissent as a threat not only to its own political interests, but also to the PRC's one-party system of government itself. Thus, the PRC government's national security and law enforcement agencies regard political dissent as a national security threat and routinely monitor and actively censor political speech inconsistent with CCP-approved political viewpoints, as well as speech that threatens to damage the reputation of the PRC government or the CCP or threatens to undermine the PRC's CCP-dominated social order.

17. The CCP's "unapproved" topics include discussions about the overthrow of the CCP's control of the PRC government and the statuses of the Hong Kong Special Administrative Region and the Republic of China—commonly referred to as Taiwan—to remarks on CCP General Secretary Xi Jinping's apparent resemblance to the fictional cartoon character Winnie the Pooh. The modern "Five Poisons" of the CCP—

[3] The information set forth in this section is based on my review of publicly available information and my experience investigating numerous cases involving the PRC.

namely Uighurs, Tibetans, adherents of Falun Gong spiritual practice, pro-democracy dissidents, and advocates for the independence of the island of Taiwan—are especially sensitive to the CCP.

18. To effectuate this censorship scheme, the PRC government requires electronic communications service providers that operate in the PRC, such as Company-1, to proactively monitor users' activities on their networks and to terminate discussions of politically sensitive topics. The PRC government similarly requires service providers to respond immediately when a PRC national security or law enforcement agency demands that the service provider terminate a discussion of a politically sensitive topic. Beginning in 2017, the PRC government expanded its control over electronic communications service providers by requiring them to store data for Chinese users within the national borders of the PRC.

19. Service providers who fail to adhere to the PRC government's censorship requirements risk being excluded from the PRC's market. The PRC government, through the CAC, the primary operator of the system informally known as the "Great Firewall of China," has the capability to block Internet access within China to particular servers and applications, and uses that capability to prevent PRC citizens from accessing the networks of electronic communications service providers that fail to comply with the PRC government's censorship demands.

20. The PRC government's efforts to censor political dissent do not end at the PRC's national borders. The PRC government, and in particular the Ministry of State Security ("MSS"), colloquially known as "*guo an*," which is the foreign intelligence and secret police agency of the PRC government responsible for counterintelligence, espionage

and political security, and the First Bureau of the Ministry of Public Security ("MPS")—colloquially known as the Domestic/National Security Police or "*guo bao*," and more recently as the Political Security Protection Bureau or "*zheng bao*"—routinely monitor, among others, Chinese political dissidents who live in the United States and in other locations outside the PRC. The MPS's First Bureau is the PRC's "secret" police, with a mandate that includes the suppression and censorship of political dissent, criticism and other potential threats to the PRC government and CCP. The MPS's Eleventh Bureau, colloquially known as "*wang an*," is the MPS's Network/Internet Security Bureau, that among other responsibilities, aids in the enforcement of the PRC government's online censorship directives. The PRC government, the MSS, and the MPS regularly use cooperative contacts both inside the PRC and around the world in an effort to influence, threaten and coerce political dissidents abroad. Indeed, I am aware that the PRC government has threatened or coerced Chinese political dissidents living in the United States in an effort to silence them.

21. The June 4, 1989 Tiananmen Square massacre is one of the politically sensitive topics of discussion that is routinely censored by the PRC government. On the night of June 3, 1989, into the morning of June 4, 1989, following weeks of large student-led protests advocating greater democratic representation for the people in the PRC's CCP-controlled system of governance, the People's Liberation Army ("PLA") violently crushed the protesters at Tiananmen Square and surrounding areas in Beijing, PRC during a state of

martial law. The PLA's crackdown led to the deaths of hundreds of PRC citizens and was widely condemned as a massacre.

22. The Tiananmen Square massacre has been, and continues to be, the subject of discussion throughout the world, including both in the United States and in the PRC, and PRC political dissidents around the world regularly commemorate the anniversary of the Tiananmen Square massacre and discuss the CCP's control over the PRC government. The PRC government has attempted to prevent such dialogue within the PRC, including by banning discussions and by using the PRC government's control over the Internet within the PRC to shut down such discussions on various electronic communications platforms.[4]

23. The PRC government also prohibits unauthorized religious activities, including online religious discussions. The PRC government requires religious groups to register with government authorities and restricts religious activities by both registered and unregistered religious groups. Collective or large-scale religious activities held outside of registered religious facilities, for example, are strictly restricted, and religious activities by unauthorized religious groups are likewise prohibited. The PRC government also imposes criminal penalties on religious groups it deems to be "cults" and uses these laws to persecute

---

[4] Based on a review of the defendants' internal discussions, the investigation has revealed that certain defendants, most notably SHEN ZHENHUA, appear to hold beliefs about the student protests leading to the Tiananmen Square massacre consistent with the official explanation of Chen Xitong, who was mayor of Beijing at the time of the incident. In sum and substance, according to Chen Xitong's summary of the events, the student movement and protests beginning in April of 1989 were used by a small number of people to seize power from "legitimate" student unions that were democratically elected to cause planned, organized, and premediated political turmoil, which developed into a counter-revolutionary riot in Beijing to overthrow the leadership of the CCP and the socialist PRC itself. This "struggle"—which Chen blamed on Western influences—was only quelled by the work of senior CCP leaders, the PLA, and MPS officers.

and suppress the free exercise of religious expression by members of religious groups opposed by the CCP.

II. The Criminal Scheme

24. As set forth below in detail, JULIEN JIN, CHEN YUANYUAN, FU YIBIN, HUANG YIWEN, JIN TAO, LIU ZHIYANG, SHEN ZHENHUA, SONG GUORONG, TIAN XINNING, XU WEI and others conspired to use Company-1's systems in the United States to censor the political and religious speech of individuals located in the United States and around the world pursuant to the directives of the PRC government. Following the termination of JULIEN JIN's employment with Company-1 in or about December 2020, other PRC officers, including XU and CHEN, have continued to attempt to use Company-1's systems in the United States to similarly censor the political and religious speech of individuals located in the United States and elsewhere.

25. Among other actions taken at the direction of the PRC government, JULIEN JIN and certain other Company-1 employees repeatedly sought to terminate video chat meetings organized by a prominent, U.S.-based critic of the CCP and the PRC government, beginning in or about 2017 and continuing into June 2020. Further, JULIEN JIN and others also deplatformed U.S.-based users seeking to commemorate the 30th anniversary of the Tiananmen Square massacre in 2019 and terminated at least four video chat meetings hosted in 2020 on Company-1's networks commemorating the 31st anniversary of the Tiananmen Square massacre, most of which were organized and attended by U.S.-based participants. Some of the participants who were unable to attend the meetings in 2020—including dissidents who had participated in and survived the 1989 Tiananmen Square protests—were Company-1 customers in Queens and Long Island, New

York who had purchased subscriptions to Company-1's services, and therefore entered into service agreements with Company-1 governed by the TOS.

26. In May and June 2020, JULIEN JIN, FU YIBIN, HUANG YIWEN, JIN TAO, LIU ZHIYANG, SHEN ZHENHUA, SONG GUORONG, TIAN XINNING, XU WEI, CHEN YUANYUAN and others collaborated to identify meeting participants and to disrupt some of the meetings hosted on Company-1's U.S. servers, at times creating pretextual reasons to justify their actions to other employees and executives of Company-1, as well as to Company-1's users. In particular, while working under the direction of FU, JIN TAO, LIU, SHEN, SONG, TIAN and XU—among other PRC governmental officials—JULIEN JIN, HUANG and other co-conspirators acted to disrupt meetings held on the Company-1 platform during which participants intended to discuss topics considered politically sensitive by the PRC government, by infiltrating the meetings to gather evidence about purported misconduct occurring in those meetings or by gathering intelligence about the planned agenda of the meetings before the meetings even occurred.

27. In fact, there was no misconduct; JULIEN JIN, HUANG YIWEN and their co-conspirators fabricated evidence of TOS violations to provide pretextual justification for terminating the meetings, as well as certain participants' accounts. On the basis of these fabrications, JULIEN JIN tasked a high-ranking employee of Company-1 in the United States ("Employee-1") to effect the termination of meetings and the suspension and cancellation of user accounts.

A. Company-1's TOS

28. Based upon my review of Company-1's TOS, Company-1's TOS represent to Company-1's users that "[Company-1] will provide the Services, and you may

access and use the Services, in accordance with this Agreement." As relevant, Company-1's TOS represent that:

> [Company-1] will maintain reasonable physical and technical safeguards to prevent unauthorized disclosure of or access to Content, in accordance with industry standards. [Company-1] will notify You if it becomes aware of unauthorized access to Content. [Company-1] will not access, view or process Content except (a) as provided for in this Agreement and in [Company-1]'s Privacy Policy; (b) as authorized or instructed by You, (c) as required to perform its obligations under this Agreement; or (d) as required by Law. [Company-1] has no other obligations with respect to Content.

Under Company-1's TOS, users agree, among other things, that they will not use Company-1's services in a prohibited fashion, including to:

> (iii) engage in activity that is illegal, fraudulent, false, or misleading, (iv) transmit through the Services any material that may infringe the intellectual property or other rights of third parties; . . . or (vi) use the Services to communicate any message or material that is harassing, libelous, threatening, obscene, indecent, would violate the intellectual property rights of any party or is otherwise unlawful, that would give rise to civil liability, or that constitutes or encourages conduct that could constitute a criminal offense, under any applicable law or regulation; . . . (ix) use the Services in violation of any [Company-1] policy or in a manner that violates applicable law, including but not limited to anti-spam, export control, privacy, and anti-terrorism laws and regulations and laws requiring the consent of subjects of audio and video recordings, ...

29. The TOS also reference Company-1's Privacy Policy, which states in relevant part that Company-1 will use "Operation Data," meaning "technical information from [Company-1]'s software or systems hosting the Services, and from the systems, applications and devices that are used to access the Services" to, among other items, "Detect, investigate and stop fraudulent, harmful, unauthorized or illegal activity ('fraud and abuse detection')."

30. The TOS in place at the time of the events detailed below was updated on or about April 13, 2020, and Section 3d(ix) of the TOS prohibits use of Company-1's

platform in violation of any Company-1 policy or in a manner that violates applicable law, including but not limited to anti-terrorism laws. The TOS stated that users could notify Company-1 of violations of the TOS agreement by contacting the email address <<violation@[Company-1].us>>.

31. According to Company-1 TOS, customers were subject to the local laws of the jurisdiction in which they used Company-1's platform. In other words, U.S.-based users of Company-1's platform in the United States would be subject to laws in the United States and not to the extraterritorial application of laws in the PRC.

B. JULIEN JIN and Others Follow Directives of the PRC Government to Censor Certain Political and Religious Speech

32. Beginning at least as early as November 2017, JULIEN JIN and certain other Company-1 employees in the United States and the PRC sought to comply with and globally implement the PRC government's censorship directives, even with respect to Company-1 users based in the United States. These censorship efforts continued through at least in or about June 2020 for JULIEN JIN, FU YIBIN, HUANG YIWEN, JIN TAO, LIU ZHIYANG, SHEN ZHENHUA, SONG GUORONG and TIAN XINNING; through at least in or about March 2021 for XU WEI; and through at least in or about June 2021 for CHEN YUANYUAN.

33. In or about November and December 2017, JULIEN JIN, Employee-1 and certain other Company-1 employees in the PRC and the United States exchanged emails related to alleged abuses of Company-1's platform for discussion of topics considered sensitive by the PRC government. In a Chinese-language email sent on or about November 30, 2017, JULIEN JIN described some "illegal" uses of the platform and noted examples that

included "Beijing * June * fourth activities and other political activities, Falun Gong, ISIS and other religious superstitions."[5] JULIEN JIN noted that "these" needed to be alerted and dealt with in real time as the cases might have a great impact on Company-1's operations and maintenance. JULIEN JIN described how Employee-1 had already pulled statistics on "Buddhist" accounts—which accounts held religious meetings impermissible under PRC law—and referenced behavioral analysis conducted on the accounts and meetings associated with these users. On or about December 1, 2017, Employee-1 replied in Chinese, "Totally agree. All abusing needs to be caught, the sooner the better."

34. In or about May 2018, JULIEN JIN and certain other Company-1 employees began to target a U.S.-based critic of the PRC government and the CCP who had fled from the PRC and resides in New York ("Victim-1").[6] In early May 2018, officials

---

[5] Citations to electronic communications include original spelling, punctuation, and grammar. All translations of Chinese language into English are in draft form and subject to revision.

[6] [redacted]

from the CAC notified employees based in Company-1's office in Jiangsu Province about Victim-1's use of Company-1's platform and requested that Company-1 terminate Victim-1's meetings. Similarly, on or about May 15, 2018, the Propaganda Department of the Suzhou Municipal Party Committee[7] and the director of the CCP Propaganda Department in Suzhou, PRC interviewed the head of Company-1's office in Suzhou and others to learn the details of Victim-1's allegedly improper use of Company-1's platform.

35. Thereafter, PRC-based Company-1 employees identified Victim-1's accounts and notified JULIEN JIN, Employee-1 and Company-1's chief executive officer ("CEO-1") of their findings. In response, Employee-1 instructed Company-1 employees, "Check all related accounts." Accordingly, JULIEN JIN and others in the PRC identified additional accounts affiliated with Victim-1 and provided their findings to Employee-1 and CEO-1.

36. In the ensuing months, JULIEN JIN and certain other Company-1 employees engaged in a multifaceted effort to eliminate Victim-1 from the platform, including by using a "quarantine zone" on a server operated by a different Internet Service Provider ("ISP") with known latency issues—causing continued disruptions to service—to cause Victim-1 and his/her associates to abandon the platform, and by deleting stored video recordings that Victim-1's associates had made of their meetings on the platform. On or about May 7, 2018, Employee-1 accessed an account related to a U.S.-based associate of Victim-1 ("Victim-2"), determined that Victim-2's account had three stored video

---

[7] The Publicity Department of the Central Committee of the CCP is often referred to as the "Propaganda Department" and is responsible for ideology-related work, including enforcement of media censorship.

recordings, and deleted these three recordings without Victim-2's knowledge or consent and based on his/her affiliation with Victim-1.

37. The decision to move Victim-1's meetings to the quarantine zone was based not only on the desire to negatively impact the quality of Company-1 services provided to Victim-1 and his/her associates, but also to prevent Company-1's platform itself from being targeted by a distributed denial-of-service ("DDoS") attack by the PRC government, which Company-1 employees believed was possible based on information that the PRC government had previously attacked a competitor of Company-1 through a DDoS attack for not censoring disfavored content.

38. Meetings pertaining to Victim-1 were not the only candidates for relegation to the Company-1 quarantine zone. For example, on or about May 3, 2018, Employee-1 instructed JULIEN JIN and certain other Company-1 employees to "closely monitor 6/4 related meeting lately. Once found, put the account into" the quarantine zone. When a PRC-based employee asked what was meant by a "6/4 related meeting," Employee-1 replied "June 4th," a reference to the June 4th anniversary of the Tiananmen Square massacre.[8]

39. On or about June 2, 2018, a Company-1 employee in Suzhou sent an email to JULIEN JIN and Employee-1 indicating receipt of a call from the MPS about live broadcast meetings related to Victim-1 originating in Australia—with the meeting hosted in Company-1's Australian data center—and involving content related to "6/4." Over the next

[8] The PRC government and the CCP prevent teachings and discussions within the PRC about the events of the student protests that culminated in the Tiananmen Square massacre on June 3, 1989 and June 4, 1989. I am aware that, as a result, many PRC citizens are unfamiliar with the details of the event or the significance of any reference to June 4.

two days, JULIEN JIN and certain other Company-1 employees in the PRC moved multiple accounts they assessed to be related to Victim-1 to the quarantine zone based on what appears to have been an analysis of social media activity and Company-1 metadata on the devices and IP addresses used in the accounts that overlapped with the devices and IP addresses known to be used by Victim-1.

40. In or about June 2018, the issue of Victim-1's continued use of Company-1's platform surfaced again. Officials from the Propaganda Department of the CAC visited Company-1's office in Suzhou and asked Company-1 to block several accounts the CAC claimed to be associated with Victim-1 and to provide information on the registration of these accounts. Whereas the initial solution devised in May 2018 allowed for Victim-1 and his/her associates to use the platform with reduced quality of service in the quarantine zone, Company-1 employees began to take more aggressive action to remove Victim-1 from the platform. On or about June 27, 2018, Employee-1 sent an email to JULIEN JIN, CEO-1 and certain other Company-1 employees that effectively changed Company-1's policy on responding to Victim-1, advising that, going forward, Victim-1 and his/her supporters would now be deplatformed. According to Company-1 logs, on or about June 27, 2018, JULIEN JIN terminated approximately 15 accounts of U.S.-based users he assessed to be associated with Victim-1 based on what appears to have been an analysis of social media activity and Company-1 metadata on the devices and IP addresses used in the accounts that overlapped with the devices and IP addresses known to be used by Victim-1.

41. Despite Company-1's efforts to deplatform Victim-1, the PRC government flagged the company for its failure to act more quickly. On or about July 10, 2018, Employee-1 received a message from a Company-1 employee in Suzhou indicating

that Company-1 had received a "rectification" notice from the CAC with issues of concern. Primary among these was the presence of "harmful political information" on the platform—an apparent reference to Victim-1's use of the platform.[9]

C. JULIEN JIN and Others Continue to Perpetrate Harassment of PRC Dissidents

42. In the fall of 2018, Company-1 hired a general counsel, who was later given the title Chief Legal Officer (hereinafter "CLO-1"). CLO-1's responsibilities included, among other duties, the supervision of Company-1's response to law enforcement requests, including the eventual supervision of JULIEN JIN. However, the investigation has not revealed any evidence from 2018 or 2019 suggesting that Employee-1, JULIEN JIN or any other Company-1 employee who participated in suppressing the speech of users who allegedly violated PRC laws relating to political and religious expression consulted with CLO-1 before doing so, notwithstanding Company-1's official policies to the contrary (as detailed further below). Indeed, the investigation has revealed that certain Company-1 employees continued to monitor the platform for any use of the platform relating to Victim-1, commemorations of the Tiananmen Square massacre and other issues considered sensitive by the PRC government, and to act to suppress the speech of U.S.-based users and meetings hosted on U.S.-based servers.

43. For example, on or about September 21, 2018, after PRC government authorities contacted Company-1's Shanghai office concerning allegedly unlawful religious content on the platform, a PRC-based Company-1 employee emailed CEO-1, Employee-1,

---

[9] Based on my training and experience, I understand that an entity in the PRC is generally required to submit a rectification report to the PRC authorities that explains the specifics of incidents that run afoul of PRC regulations, laws or expectations and describes the measures that will be put in place to prevent any future infraction.

and the site leaders of Company-1's offices in Suzhou and Hefei, PRC. The employee asked if Company-1 should provide account information for the user hosting the meeting to the Shanghai authorities, if the host account should be moved to the quarantine zone or directly disabled, and how to flag the issue under the TOS for possible future occurrences of similar conduct. JULIEN JIN and the site leader of Company-1's office in Hangzhou, PRC were subsequently added to the email chain. Employee-1 responded by delegating responsibility to JULIEN JIN and instructing him to move the account to the quarantine zone. A few days later, JULIEN JIN responded via email and asked Employee-1 in a mix of English and Chinese, "As of now, our US General Counsel is already onboard. Can you provide us more guide line from the US side? If so, please share with us?" The investigation has not uncovered evidence that JULIEN JIN or any of his work colleagues, in fact, consulted with CLO-1 ("our US General Counsel") on this matter.

44. Similarly, JULIEN JIN and others caused the blocking of an account tangentially related to Victim-1 in early 2019, without consulting CLO-1. On or about January 4, 2019, Victim-1 asked one of his/her employees, who was a United States person residing in Jericho, New York ("Victim-3"), to come to Victim-1's residence and assist with a video chat meeting. In an interview with the FBI, Victim-3 noted that Victim-1 had been encountering trouble connecting to the Company-1 platform. Accordingly, Victim-3 allowed Victim-1 to use Victim-3's personal Company-1 account for the meeting. Victim-3 reported to the FBI that, shortly after the meeting commenced, his/her device screen went "black" and the meeting was ended prematurely. Records from Company-1 indicate that, on or about January 4, 2019, Victim-1 used Victim-3's account from an IP address and ISP

in New York in a meeting that contained only one other participant, who joined from an IP address resolving to an ISP in Toronto, Canada.

45. Not realizing his/her account had been blocked, Victim-3 repeatedly contacted Company-1 customer service. On or about January 8, 2019, JULIEN JIN added an entry to the internal Company-1 ticket tracking the request and stated he had checked Victim-3's ID, "which was banned in [Victim-1] events earlier time. (TOS-NSA). Maybe we'd better pretend not to know this ticket." By using the phrase "TOS-NSA," I believe that JULIEN JIN intended to convey that Victim-3's account was banned at the request of the MSS, which is sometimes referred to by PRC citizens as the "National Security Agency" or "NSA," for purported violations of Company-1's TOS.[10] Indeed, on or about January 9, 2019, JULIEN JIN added another entry to the tracking ticket: "In [Victim-1's] events in 2018.06, we disabled a lot of Victim-1's/ Victim-1's fan's account and devices."

46. In internal emails exchanged on or about January 9, 2019, Employee-1, JULIEN JIN and two other Company-1 employees discussed the status of Victim-3's account that had been banned for its affiliation with Victim-1. Employee-1 replied in a January 9, 2019 email to JULIEN JIN, among others, that the "current strategy is to block as many as possible, not leaving any opportunities for [Victim-1] to use" Company-1's platform. JULIEN JIN then wrote on the tracking ticket, "We got confirmation from [Employee-1] that

---

[10] In correspondence with English speakers, JULIEN JIN refers to the MSS as the "National Security Agency" or "NSA;" in his correspondence with Chinese speakers and with MSS officers themselves, JULIEN JIN refers to the same organization as either "*guo an*" or "国安," the pinyin and Chinese characters respectively that are commonly translated as either "state security" or "national security" and used by Chinese speakers to refer to the MSS.

we should continue blocking [Victim-1]. We have to keep [Victim-1's] events away from [Company-1]."

47. At the same time, JULIEN JIN and Employee-1 assisted the PRC government's efforts to track meetings regarding the Tiananmen Square massacre—without consulting with CLO-1. For example, on or about May 21, 2019, Employee-1 sent JULIEN JIN notice that "we will strengthen the monitoring of meetings" as "6, 4" was very close—a reference to the upcoming June 4th commemorations of the Tiananmen Square massacre. JULIEN JIN acknowledged receipt of the instruction and thanked Employee-1 for the reminder. Shortly thereafter, on or about June 3, 2019, JULIEN JIN requested assistance from Employee-1 on a matter ostensibly related to the June 4, 2019 commemorations of the Tiananmen Square massacre. Employee-1 instructed JULIEN JIN to "pay special attention today."

48. According to log activity for June 4, 2019, JULIEN JIN blocked five Company-1 accounts to disrupt commemorations of the Tiananmen Square massacre. On or about June 6, 2019, JULIEN JIN emailed Employee-1 and CEO-1, among others, regarding his work with the local MSS to "force bidden" five user accounts because of "illegal" commemorations of the 30th anniversary of the Tiananmen Square massacre. By "force bidden," JULIEN JIN appears to have meant "force forbidding"—or blocking—the accounts. Notably, Company-1 records reveal that the five accounts were provisioned in the United States and appear to be used by U.S.-based customers.

49. On or about August 22, 2019, JULIEN JIN, Employee-1 and certain other Company-1 employees again acted—without coordinating with CLO-1—to disrupt a video meeting hosted by a Company-1 user on what appears to be a Company-1 server in the

United States. In electronic messages, JULIEN JIN claimed that the host was a "Chinese cult organization" with "very frequent" use of Company-1's services and stated that the user account should be blocked due to the religious content of the meeting. JULIEN JIN asked Employee-1 for instructions about how to handle the situation and whether the account needed to be disabled and the account's recordings deleted. In response, Employee-1—who was in the United States at the time—directed JULIEN JIN to place the account in a quarantine status. Employee-1 further expressed the hope that doing so would cause the user to stop using Company-1's platform.

50. Ultimately, JULIEN JIN succeeded in suppressing the speech of users in the United States and in other jurisdictions outside of the PRC by implementing separate protocols for Company-1's responses to PRC-related law enforcement requests as compared to law enforcement requests from other governments. Company-1 created a formal system and applied a written policy, the "Subpoena Intake and Processing Policy October 2018," that included a process for involving Company-1's legal function for questions on whether the requests were issued by legitimate agencies and were for "standard data." The policy required governments to submit written legal process to Company-1 and were handled by a Company-1 compliance function called the "Trust and Safety Team" staffed with personnel supervised by Company-1's head of global tech support. However, in practice, this team had no role in responding to requests from the PRC government. As to requests from the PRC government, JULIEN JIN and his team received requests directly from PRC authorities and worked with Employee-1, and certain other Company-1 employees, to respond, all without oversight from Company-1's legal function, including CLO-1.

51. JULIEN JIN outlined these disparate approaches in a September 3, 2019 email. He indicated that requests from the "US/EU/../Excluding China" were addressed through the support team headed by a high-level U.S.-based employee, and detailed the processes by which JULIEN JIN assisted such requests. In contrast, Company-1 handled special requests by law enforcement received from "Local China" without involvement of the Company-1 legal function. As to such requests, "Local NSA [MSS] and Cyber police prefer reach us directly—by phone call and meetings . . . we have to follow local law. No other team but we will [be] involve[d] in this case."

52. As a result of this dichotomy, JULIEN JIN, working with certain other Company-1 employees, successfully deplatformed users outside of the PRC for conduct occurring outside of the PRC, including users based in the United States or using Company-1 servers contained in the United States, thus subjecting these users to the extraterritorial application of the PRC government's censorship regime.

D. JULIEN JIN Works to Unblock Company-1's Services in the PRC

53. Beginning in September 2019, notwithstanding the proactive measures taken by JULIEN JIN, and certain other Company-1 employees, to censor political and religious discussions disfavored by the PRC government and the CCP, the PRC government blocked PRC-based internet users from connecting to Company-1's platform due to, among other things, its purported failures in executing PRC censorship directives. The blockage had the effect of disrupting service not only to individual users who had registered free accounts to use Company-1's service, but also to Company-1's fee-paying corporate customers who sought to communicate with employees and business partners located in the

PRC. The blockage of Company-1's service in the PRC began on or about September 8, 2019 and concluded on or about November 17, 2019.

54. As reflected by internal Company-1 correspondence, PRC government officials informed JULIEN JIN and certain other Company-1 employees that Company-1 could resume operations in the PRC once Company-1 complied with PRC laws and regulations.[11] The officials directed Company-1 to prepare and submit rectification plans and reports to various PRC government agencies, including the Hangzhou offices of the MPS's Network Security Bureau, to describe how Company-1 would comply with PRC laws and regulations.

55. As part of the proposed plans submitted in the rectification report, Company-1 indicated an intention to, among other measures, proactively monitor users' communications for content that included the expression of political and religious views unacceptable to the PRC government, June 4 commemorations (a reference to commemorations of the Tiananmen Square massacre), the Hong Kong "riots," Falun Gong, and the Dalai Lama in Tibet, among others. Company-1 also indicated its intention to monitor communications for content that spread "rumors" to smear Chinese leaders. The

---

[11] In or about late October 2019, CEO-1 flew to the PRC, where he/she and JULIEN JIN met with the MPS's Network Security Bureau and other PRC government officials to address the blockage. While in Beijing, JULIEN JIN and CEO-1 first met TIAN XINNING of the MPS's Network Security Bureau. On or about October 23, 2019, JULIEN JIN and TIAN began communicating directly, and JULIEN JIN requested that TIAN provide guidance. After returning to Hangzhou on or about October 24, 2019, JULIEN JIN contacted TIAN about Company-1's intention to implement what they had discussed in Beijing and asked for assistance with introductions to the MPS in Hangzhou. TIAN noted that he would relay the relevant requirements to the MPS in Hangzhou and subsequently arranged for the MPS Network Security Bureau in Hangzhou, including SHEN ZHENHUA, to contact JULIEN JIN.

rectification report specifically referenced Victim-1 and the actions Company-1 had already taken against Victim-1 and his/her assistants, fans, and some users of Victim-1's sponsors. To formalize JULIEN JIN's role as the primary liaison with PRC authorities for all requests, the final rectification report included JULIEN JIN's work email address and telephone number as a point of contact for PRC authorities.[12]

56. On or about October 25, 2019, JULIEN JIN, Employee-1, CEO-1 and certain other Company-1 employees exchanged electronic messages to discuss a meeting that JULIEN JIN had attended at the Hangzhou office of the MPS's Network Security Bureau. JULIEN JIN explained that Company-1 had discussed with the MPS "illegal event regulation hotspots" and would "take the initiative to regularly report to and alert them." According to JULIEN JIN, MPS officers had advised that they would also "send us the hotspots." JULIEN JIN further explained:

> [T]hey also want me to provide a list of some details on our routine monitoring; such as Hong Kong protests, illegal religions, fundraising and multi-level marketing, etc. . . . I have also communicated with them and they will help with the determination of issues that we find difficult to determine whether they are illegal; I will go to their unit often in [the] future to give live demonstrations and communicate various issues.

---

[12] Despite JULIEN JIN's role as Company-1's primary liaison with PRC authorities, evidence uncovered in the investigation indicates multiple defendants possessed contact information for certain other Company-1 employees. For example, whereas SONG GUORONG created and maintained only a contact at Company-1 for JULIEN JIN, SHEN ZHENHUA created and maintained contacts for JULIEN JIN and the site leader of Company-1's office in Hangzhou to whom JULIEN JIN reported. Additionally, after JULIEN JIN's termination from Company-1 in or about December 2020, FU YIBIN created a new contact for a different Company-1 employee in the PRC. Moreover, MPS officers continued to engage directly with Company-1 employees in the PRC and the United States other than JULIEN JIN. For example, as detailed below, in or about June 2020, the MPS's First Bureau in Beijing directed a request to both JULIEN JIN and the site leader of Company-1's office in Hefei, PRC.

57. In the same series of communications, JULIEN JIN advised that he would create five Company-1 accounts for officers of the MPS's Network Security Bureau in Hangzhou to use on Company-1's PRC-based network. Internal Company-1 communications reflect that, from October 2019 through May 2020, JULIEN JIN created Company-1 accounts for several PRC officials, including FU YIBIN, JIN TAO, SHEN ZHENHUA and SONG GUORONG. JULIEN JIN further explained that the MPS had agreed to use a combination of Company-1's commercial messaging system and a PRC-based Internet messaging application to communicate with Company-1. JULIEN JIN emphasized that "[a]ll activities should be confidential internally and externally."

58. On or about November 4, 2019, CEO-1, JULIEN JIN and one other Company-1 employees based in the PRC exchanged electronic messages about translating the rectification report from the Chinese language into English. JULIEN JIN noted that in communications with the MPS's Network Security Bureau, the MPS had advised that the information in the rectification report needed to remain confidential and was not suitable for the "US" [the United States] to see. CEO-1 disagreed and emphasized the need for transparency; he/she indicated that CLO-1 and Company-1's board would need to review the report. JULIEN JIN replied that he would adjust the language in the report about addressing Company-1 users who supported activities disfavored by the CCP and PRC government. JULIEN JIN noted he would also delete language in the draft rectification report about Company-1's monitoring being "global, not limited to China."

59. In the same exchange, JULIEN JIN noted that there were some boundaries that were not obvious, such as "illegal political activities," "spreading rumors to

smear Chinese state leaders" and "illegal religions." JULIEN JIN indicated he would specify on the document "China ONLY."

60. On or about November 5 and 6, 2019, JULIEN JIN and SHEN ZHENHUA communicated about the progress of implementing Company-1's rectification plans.[13] SHEN requested materials and data regarding, among other things, Company-1's network security management mechanism, technical security measures for Company-1's network security and Company-1's network security emergency response protocol. SHEN requested updates on whether points identified in the inspection—including on content security and data security—had been completed.

61. On or about November 17, 2019—the day Company-1's service was finally unblocked in the PRC—JULIEN JIN thanked TIAN XINNING and the MPS's Network Security Bureau for their guidance and assistance in removing the blockage. JULIEN JIN commented that rectification work was progressing as scheduled. TIAN responded that the key was to enforce "KYC"— know your customer—and to regulate the content security and user behavior, safeguard system security, timely respond to supervision and regulation compliance, and establish an emergency response mechanism with the local PRC authority. JULIEN JIN replied that a competitor of Company-1 had been blocked by MPS's Network Security Bureau because of "June 4th" commemorative meetings. JULIEN JIN claimed that Company-1 had strict supervision and regulation over political-related activities but had failed to handle religious activity or illegal fundraising in the past because

[13] SHEN and MPS officers under his direction appear to have also visited JULIEN JIN at Company-1's office in Hangzhou on multiple occasions to provide guidance on fulfilling the measures listed in the rectification report.

of the difficulty in assessing the legality of such conduct. JULIEN JIN indicated that Company-1 would strictly follow the rectification report.

62. In an exchange of electronic messages with a U.S.-based Company-1 employee on or about November 18, 2019, JULIEN JIN wrote, "As you know, local we're working with China Government on Cybersecurity recently (Top 1 by CEO). And here's good news – [Company-1's Internet domain] has been unblocked in China since yesterday." JULIEN JIN continued, "We doesn't make an official announcement on this, becuase there're a few rectification work we're still working on." JULIEN JIN further explained, "By the way, the direct reason local government blocked [Company-1's Internet domain] this time is because those illegal activies on [Company-1's platform] in China. I think somehow it's realted with TOS."

63. Following the unblocking of Company-1 in the PRC, JULIEN JIN spearheaded monitoring of user content disfavored by the PRC government and the CCP across Company-1's service globally. On or about November 19 and 20, 2019, JULIEN JIN and a TOS analyst at Company-1's office in Hefei exchanged chats about a new account associated with a user described in their messages as the "niece" of Victim-1, who resided in the United States. The TOS analyst stated a meeting in the account seemed to be related to "Hong Kong independence." JULIEN JIN responded, "Polical must be strictly controlled. But for political issues, don't tell customers." When the TOS analyst asked if Company-1 should directly block the account, JULIEN JIN responded affirmatively. The TOS analyst reported that he/she used an alias email account to join the meeting hosted by the "niece," indicated that the meeting was about a U.S. congressional bill related to Hong Kong, and reported that he/she had subsequently blocked the accounts of all the meeting's participants.

Similarly, on or about November 20, 2019, JULIEN JIN, Employee-1 and the site leader of Company-1's Hangzhou office exchanged electronic messages to discuss blocking the account of the same "niece."

64. On or about November 21, 2019, JULIEN JIN reported to SHEN ZHENHUA regarding the actions taken to block some foreign accounts and devices of "Hong Kong independence" and Victim-1's "niece." JULIEN JIN claimed that Company-1 was improving content monitoring as Victim-1 had recently become active again. After SHEN requested that JULIEN JIN prepare a report on these matters, JULIEN JIN agreed and thanked SHEN for his guidance. On or about November 29, 2019, JULIEN JIN electronically submitted to SHEN the report on the actions taken against "Hong Kong independence" and Victim-1's "niece."

E. JULIEN JIN Works to Continue Censorship Activities on Behalf of the PRC Government

65. In early 2020, as demand for Company-1's video meeting services climbed sharply during the COVID-19 pandemic, Company-1 sought to restructure and expand its operations in the PRC. Throughout the expansion process, the PRC government imposed additional controls over Company-1's operations and demanded a policy of immediate remediation of any illegal conduct on the Company-1 platform. In internal discussions, certain Company-1 employees, including JULIEN JIN, stressed that failure to comply with these growing requirements could result in another blockage of Company-1's platform in the PRC. Indeed, internal communications between JULIEN JIN, Employee-1 and certain other Company-1 employees in the United States and the PRC reflect a decision

to monitor for content disfavored by the PRC government and the CCP in a manner that extended to users outside of the PRC, including in the United States.[14]

66. In early 2020, JULIEN JIN communicated with MPS and CAC representatives regarding any necessary changes to network security requirements and to indicate Company-1's intention to comply with the CAC's directives. On or about February 19 and 20, 2020, JULIEN JIN requested MPS Officer SHEN ZHENHUA's assistance to pass PRC security reviews, as usage of the Company-1 platform had increased with the onset of the COVID-19 pandemic. JULIEN JIN noted that, through the counseling from senior Chinese legal counsel over the past period, Company-1 China had been refining network security and other compliances. SHEN indicated that he had instructed "Officer Song" of the Xihu District to contact JULIEN JIN. JULIEN JIN thanked SHEN for his guidance and later indicated that he had spoken with "Officer Song" over the phone. Based on the investigation, I believe that "Officer Song" is MPS Officer and defendant SONG GUORONG. JULIEN JIN added that Company-1 was constantly addressing "network security" issues, including during the Chinese New Year, regarding what he characterized as "rumors and nonsense" about the pandemic in China that had surfaced on a U.S. social media platform.

67. On or about February 20, 2020, JULIEN JIN contacted SONG GUORONG, thanking him for his support of Company-1 and indicating that he had created

---

[14] Based on my review of communications and my experience conducting counterintelligence investigations relating to the PRC, the PRC government's definition of what constitutes "domestic" or "Chinese" users extends beyond PRC nationals located in the PRC; the definition also includes "overseas" Chinese, Chinese expatriates, and often, anyone with Chinese ancestry, regardless of nationality.

two Company-1 "VIP" accounts—or paid accounts—for SONG's use. Similarly, on or about February 21, 2020, JULIEN JIN notified SHEN ZHENHUA he had created additional VIP accounts for the MPS in Hangzhou.

68. On or about April 3, 2020, JULIEN JIN asked TIAN XINNING about queries from the MPS's Network Security Bureau in Shanghai, as Company-1 had already been in contact with the MPS's Network Security Bureau in Hangzhou. TIAN advised that local public security offices were responsible for day-to-day work interface, security supervision and regulation, and other important matters. TIAN noted it was the responsibility of Company-1 to assist the MPS in cooperating with the investigations and law enforcement regardless of the location. TIAN further advised Company-1 to cooperate as much as it could.

69. On or about April 3, 2020, JULIEN JIN wrote to certain other Company-1 employees, including Employee-1, that the MSS's preference was for Company-1 not to terminate meetings of target users immediately. I assess that, by keeping open meetings of investigative interest to the MSS, Company-1 would allow the MSS to obtain additional details on meeting participants, monitor the content of a meeting and gain actionable intelligence.

70. In May 2020, JULIEN JIN continued soliciting guidance from the MPS and CAC on network security requirements. On or about May 13, 2020, JULIEN JIN discussed Company-1's platform with FU YIBIN. After providing information on some of Company-1's features, JULIEN JIN invited FU to visit Company-1's office in Hangzhou to share guidance and to help with Company-1's "healthy growth."

71. At the same time JULIEN JIN was collaborating with various PRC authorities regarding compliance with changing PRC network security requirements, CLO-1 began to institute policies and controls that diminished JULIEN JIN's ability to carry out the global monitoring and censorship of content on Company-1's platform required by the PRC government. While Company-1 moved to consolidate a global compliance program for law enforcement requests, various media reports emerged questioning Company-1's security protocols, as well as the company's exposure to the PRC government. Around this time, CLO-1 announced a policy to revoke the access of Company-1's PRC-based employees—including JULIEN JIN—to Company-1's customer data stored in the United States. These policy changes progressively restricted the authorized methods available to JULIEN JIN and others to comply with the new requirements imposed by the PRC government. For example, JULIEN JIN lost access to the Company-1 system through which he could access user data, account information, and meeting information for the accounts of users based in the United States.

72. On or about April 7 and 8, 2020, JULIEN JIN wrote Employee-1 that JULIEN JIN had been summoned to a meeting with PRC government officials to discuss recent security and privacy issues. JULIEN JIN reported that the PRC government had directed Company-1 to develop the capability to respond within one minute to a PRC government demand to terminate an illegal meeting, account or recording, which JULIEN JIN referred to as the "one-minute processing requirement."

73. In these communications with Employee-1, JULIEN JIN noted that he was still working on several investigations for the MSS pertaining to users on the Company-1 platform. In response, Employee-1 suggested that another U.S.-based employee of

Company-1 ("Employee-2") could provide JULIEN JIN with access to a "remote" machine in the United States connected to Company-1's U.S.-based servers and internal systems. Employee-1 contemporaneously sent a message to Employee-2 directing Employee-2 to cooperate with JULIEN JIN. JULIEN JIN replied that the matter needed to be handled confidentially—apart from Company-1's regular support function—and stated that he would not be able to document his actions in a report. Employee-1 responded, "[I] see." Considering the previously announced policy change instituted by CLO-1 of terminating PRC employees' access to U.S.-based data, I assess that the use of a "remote" machine constituted an effort to circumvent the new, more restrictive, access control policies announced by CLO-1.

74. On or about April 15, 2020, JULIEN JIN and Employee-2 engaged in the following electronic communications:

> JULIEN JIN: Yesterday, [the MSS] asked me to track down a bad organization overseas.
>
> Employee-2: Is there someone applying for an account here [in the United States] and doing bad things in China? Otherwise, it has nothing to do with [the MSS]."
>
> JULIEN JIN: Almost. But even abroad, political attacks on leaders are not allowed. If you need approval, you can talk to [Employee-1] in person.
>
> Employee-2: 😀
>
> JULIEN JIN: Don't write mail.
>
> Employee-2: Just ask for instructions. To be honest, the United States has freedom of speech, and there is everything that you like to say, you really don't care. It only matters if you do bad things in the country.
>
> JULIEN JIN: We have so many people and multinational companies in China, we have to take care of both sides 😂.

75. On or about April 29, 2020, JULIEN JIN and Employee-1 exchanged electronic messages regarding a prior conversation between JULIEN JIN, CLO-1 and Company-1's new Chief Compliance Officer ("CCO-1") about the PRC government's one-minute processing requirement. JULIEN JIN explained that his "workaround permissions" could meet most of his needs but complained that CLO-1 and CCO-1 had insisted that Company-1 was obliged to report the PRC government's requests to Company-1's U.S.-based compliance team, which "is not compliance with powerful CN authorities' confidentiality principles"—using "CN" as shorthand for the PRC. JULIEN JIN further explained, "The CN departments I came into contact with allowed me to check their identification but will not leave any identification/photographs and anything else that may be exposed."

76. In the same conversation, Employee-1 explained that all of JULIEN JIN's access permissions in Company-1's "us clusters will be revoked, but cn cluster permissions will be retained"—referring to U.S.-based and PRC-based server clusters where Company-1 stored user data and provided Company-1's service to users, respectively. JULIEN JIN replied, "If so, I cannot do a lot of things. [The MPS's] Network Security [Bureau] will not agree to this either. Unless we also actively block China from the international version of [Company-1]." After Employee-1 inquired "What is your current workaround," JULIEN JIN responded that his permissions allowed him to "deal with violating accounts."

77. In the same exchange, Employee-1 advised, "The current requirement"—referring to Company-1's internal access control policies—"is that domestic

engineers cannot access us clusters data"—indicating that PRC-based software engineers were not permitted to access user data stored on U.S.-based servers. JULIEN JIN responded, "Network Security's requirements are that we must have direct disposition permissions for one-minute handling. For example, if US users have meetings that discuss the June 4th incident, it must be handled within one minute after reporting. Otherwise, security is not qualified."

78. After Employee-1 asked what JULIEN JIN had discussed previously with CLO-1 and CCO-1 and if they allowed him to access the data, JULIEN JIN pasted into the exchange with Employee-1 the image of a screenshot of an earlier chat with CCO-1, in which CCO-1 instructed JULIEN JIN, "What I do want notice of are China government and law enforcement requests for information on accounts." JULIEN JIN then advised Employee-1:

> If [Company-1] has a harmonious relationship with CN, the international version of our [Company-1 domain] may be used in China. If we have a poor relationship, our international version cannot be used in China. We only have very few cn users on cn cluster. A large number of multinational companies have branches, partners and business partners, etc. in cn. I personally feel that we still need to enhance cooperation with cn.

79. On or about May 7, 2020, JULIEN JIN wrote to three other Company-1 employees about an upcoming report to senior Company-1 executives in which he wanted to emphasize that Company-1 needed to pay attention and maintain the relationship with "cn zf" and how even those U.S. social media companies that conducted no business in the PRCstill deleted specific accounts and posts at the request of the "CN zf." In context, "cn" and "CN" appear to refer to the PRC ("China"); I am aware that in other chats, JULIEN JIN explained that "zf" is shorthand for *zhengfu*, the Chinese phrase for government. One of

JULIEN JIN's subordinates advised that they not talk about this subject as it made it seem as if the United States was infiltrated by the CCP.[15] JULIEN JIN replied that he only wanted to highlight that, even if Company-1 withdrew from the PRC, Company-1 would still need to deal with "CN zf" requests to avoid future attacks.

80. On or about May 7 and May 8, 2020, JULIEN JIN, Employee-1 and Employee-2 wrote each other about the PRC government's one-minute processing requirement. JULIEN JIN explained that he was unable to obtain billing information for a large customer, as JULIEN JIN could no longer access Company-1's U.S.-based servers. JULIEN JIN asked Employee-2 to restore JULIEN JIN's access privileges, so that JULIEN JIN could use Employee-2's remote computer for emergency troubleshooting. Employee-2 agreed and indicated that he/she would meet with JULIEN JIN later.

81. In May 2020, JULIEN JIN corresponded with FU YIBIN about the PRC government's expectations for Company-1 with respect to the forthcoming anniversary of the Tiananmen Square massacre. On or about May 19, 2020, in response to a query from FU, JULIEN JIN provided details about the use of the Company-1 platform in the PRC and asked FU about the status of the Hangzhou CAC review of Company-1's app—approval of which was necessary for Company-1 to continue plans for expansion in the PRC. JULIEN JIN commented that the CAC was reviewing, among other items, Company-1's content moderation, human review teams and law enforcement support, and described the differences in the registration processes at Company-1 for overseas users and PRC-based users. JULIEN JIN also noted that "6.4 is approaching and those of us who are doing control and

---

[15] The original complaint mistakenly attributed this comment to JULIEN JIN rather than to one of JULIEN JIN's colleagues.

supervision works are under great pressure." As to "6-4," FU advised, "please fortify the content control and supervision. Any situation spotted needs to be prompted reported to the local region. Avoid passivity." JULIEN JIN replied, "We will take the 6.4 issue very seriously; the company will conduct control and supervision both internally and externally where social networking and public opinions are monitored."

82. On or about May 19, 2020, JULIEN JIN and Employee-1 exchanged instant messages about the forthcoming anniversary of the Tiananmen Square massacre. JULIEN JIN warned Employee-1 that "6.4" was coming soon, and that the "cn users" whom the PRC "Internet Police"—another name for the MPS's Network Security Bureau in Hangzhou—were tracking were on a Company-1 server cluster based in the United States. Employee-1 responded, "[U]nderstood."

83. The messages set forth below, sent as part of that aforementioned exchange of electronic messages, show that JIN emphasized the increased pressure and scrutiny that the MSS, MPS and "net police" were placing on Company-1, the need to keep secret the MSS's demands to censor political content, and the fact that the PRC government demanded that Company-1 censor the political speech of Chinese users no matter where they were located:

JULIEN JIN: …06/04 is close by, and the CN users that cyber police have been chasing recently are all on US04 [a Company-1 server].

Employee-1 ("E-1"): Understood.

JULIEN JIN: MSS, Network Security and Net Police have been making many trips to the company and we are handling this carefully. MSS is requesting us to sign a NDA agreement that prevents us from disclosing their request;

	where it involves US data, we are awaiting instructions from the US side and we need to formulate a standard.
E-1:	Ok. Did the Shanghai side look for us?
JULIEN JIN:	Whatever the MSS wants basically involves politics, so they are requesting us not to disclose it. Otherwise, it will have a great impact on China's reputation.
JULIEN JIN:	It was Shanghai's Department of State Security that sent people over.
E-1:	Understood.
JULIEN JIN:	Those using their real name in CN to do bad things are actually not that many; they are mostly from the U.S. If we do not handle this well, Network Security will block [Company-1's] overseas server, so please place importance on this.
. . .	
E-1:	Please block all the US04 free accounts as soon as possible
E-1:	Anyway, the reputation is already bad. 😃
JULIEN JIN:	We discovered today [Company-1's U.S. internet domain] still allows free registration in cn…
E-1:	Fix the we errors tomorrow.
JULIEN JIN:	From the Network Security perspective, we have to handle it no matter where the cn users are; if we do not handle it, they block us by enabling gfw or through other means.

84. In this context, based upon my experience investigating this case and others involving the PRC, I believe "NDA" refers to a "non-disclosure agreement," "Shanghai's Department of State Security" refers to the Shanghai State Security Bureau ("SSSB"), which is a regional office of the MSS, and "gfw" refers to the Great Firewall of China. In addition, JIN's statement "we have to handle it no matter where the cn users are"

indicates JULIEN JIN's understanding that the MPS's definition of "Chinese users" included persons of Chinese descent physically located in the United States. JULIEN JIN indicated noncompliance could have ramifications for Company-1.

85. Moreover, in the minutes from one of his meetings with "National security"—in this case the SSSB—about "Law enforcement support," JULIEN JIN wrote among other things, that companies are required to report situations involving data from abroad, and the MSS—likely a reference in this instance to the SSSB—will decide whether to obtain such data.

86. JULIEN JIN also provided warnings to a wider audience at Company-1 about the approaching June 4, 1989 anniversary. On or about May 19, 2020, JULIEN JIN wrote CEO-1, CLO-1, CCO-1, and Employee-1, among others, "June 4th is coming, which is a sensitive date for China Cybersecurity. They're very strict on this period—'Zero Abuse report.'" I assess that JULIEN JIN meant that the PRC government would not tolerate any "abuse" on Company-1's platform related to commemorations of the Tiananmen Square massacre.

87. Between on or about May 21, 2020 and May 25, 2020, TIAN XINNING notified JULIEN JIN of the request of the MPS's Network Security Bureau to meet with CEO-1 in Beijing. It is not clear how TIAN expected CEO-1 to travel to Beijing given the limited flight availability between the United States and the PRC and the PRC government's lengthy quarantine requirements for foreign arrivals in place at the time. JULIEN JIN conveyed to TIAN that he had been speaking recently with FU YIBIN and other MPS Network Security officers in Hangzhou on securing approvals necessary for Company-1's expanded operations in the PRC.

88. On or about May 22, 2020, JULIEN JIN wrote CEO-1 that "China centre cybersecurity"—a reference to the MPS's Network Security Bureau in Beijing and TIAN XINNING—"want to have a meeting you next week." CEO-1 replied that he/she needed to consult with CLO-1 first. Later that day, CLO-1 wrote JULIEN JIN that he/she had heard about the need to meet with "China Center Cybersecurity." Although CEO-1 could not travel to Beijing, CLO-1 indicated that Company-1 would agree to a meeting on Company-1 platform and asked JULIEN JIN to determine the purpose of the meeting. CLO-1 speculated as to possible topics including, among others: "June 4th—we understand this is a sensitive time. We will follow local Chinese law on this. But, we need to log it. If this is the sensitivity, maybe we can figure out in advance how to prepare."

F. JULIEN JIN and Others Censor the Political and Religious Speech of Company-1 Users Located Outside the PRC at the Direction of JIN TAO, SONG GUORONG, XU WEI and Others

89. As set forth below, JULIEN JIN collaborated with PRC government officials to proactively identify meetings that the PRC officials might deem objectionable. In the spring of 2020, despite being deprived of privileged access to Company-1's U.S.-based servers, JULIEN JIN caused Company-1 employees based in the United States to assist in disclosing U.S.-based user data to the PRC government and to censor political and religious speech. By June 2020, his efforts to comply with the PRC government's demands culminated in JULIEN JIN's participation in a scheme to fabricate pretextual violations of Company-1's TOS, which caused U.S.-based employees of Company-1 to terminate the accounts and meetings involving individuals located outside the PRC, including in the United States.

90. In late May 2020, and because of his inability to directly access customer information in the United States, JULIEN JIN brought several requests received from the PRC authorities concerning political and religious speech on Company-1's platform to the attention of CLO-1 and CCO-1. As shown below, the focus for CLO-1 and CCO-1 was determining whether the users in these meetings were based in the PRC, and thereby subject to the jurisdiction of the PRC authorities making the requests. Notably, JULIEN JIN appeared to intentionally deceive CLO-1, CCO-1 and others about whether the users were based in the PRC. At the time, Company-1 lacked a precise means to determine where users were physically located and often relied on analyses of the users' billing addresses, the location of IP addresses, as well as other indicators.

91. On or about May 21, 2020, JULIEN JIN provided to JIN TAO a unique identifier for a meeting hosted on Company-1's U.S.-based servers, as well as the password for a Company-1 meeting scheduled to take place on or about May 22, 2020 about the PRC's then proposed national security law in Hong Kong and to commemorate the anniversary of the Tiananmen Square massacre. JULIEN JIN informed JIN TAO that the meeting contained "non-China users (US, HK regions)." Indeed, based on the FBI's interviews with various individuals in the United States, I believe the meeting would have included prominent U.S.-based dissidents, including some residing in the Eastern District of New York, had it been allowed to take place. JIN TAO asked for JULIEN JIN to check on the commemoration's meeting host and asked if Company-1 discovered "it by yourselves." JULIEN JIN replied, "Yes, we conducted self-examination, it is the most sensitive period lately." JIN TAO replied, "Yes, there are more sensitive content recently." JIN TAO

instructed JULIEN JIN, "If these are discovered through examination, send them to me immediately."

92. Later in the same discussion, JULIEN JIN continued, "Since these meetings are in the U.S., we can't directly check. I have to request the information from the U.S. colleagues. We have now separated the data management. Chinese data can only be visited by Chinese companies, the U.S. data can only be visited by Americans." JIN TAO asked if JULIEN JIN could prioritize the matter. JULIEN JIN replied, "I have kept emphasizing how important we are; we will keep quarrelling and communicating with the big U.S. legal counsel" and stated he would block the account of the meeting's host, who was a prominent PRC dissident based in Hong Kong ("Victim-4"). After JIN TAO inquired if JULIEN JIN could block the account from his end, JULIEN JIN replied that "as of now, the U.S. accounts can only be blocked when we make a request to the U.S. side." Based upon publicly available information, I know that Victim-4 provided support to the Tiananmen Square protesters in 1989 and has participated in Hong Kong politics as a pro-democracy activist. Victim-4 has subsequently been incarcerated on political charges following Hong Kong's July 2020 passage of a national security law favored by the PRC government.

93. After notifying JIN TAO of Victim-4's forthcoming meeting, JULIEN JIN sent an electronic message on or about May 22, 2020 to a group of Company-1 employees, including Employee-1, another U.S.-based employee ("Employee-3"), CLO-1, Company-1's country manager in the PRC and CCO-1 (collectively, the "Compliance Group"), and urged them to take action against the meeting and the meeting's organizer so as to prevent the PRC's "cybersecurity org" from blocking all of Company-1 servers in the

PRC. I assess that "cybersecurity org" refers to the CAC and/or the MPS. Notably, whereas JULIEN JIN informed JIN TAO that the meeting contained "non-China users," JULIEN JIN claimed to the Compliance Group the requested action would prevent "CN users" from joining—a seeming reference to PRC-based users.

94. CCO-1 asked CLO-1 and Employee-3 to determine "whether the host account [is] owned by [U.S. Persons]/US-based Chinese nationals-OR-operated by China-based users via proxy[.] If the latter, Julien [JIN] said we have suspended such meetings before." The investigation has not uncovered any evidence suggesting that JULIEN JIN relayed to the Compliance Group the insight he conveyed to JIN TAO about the meeting containing "non-China users." Employee-1, CCO-1 and Employee-3 eventually determined Victim-4's account was provisioned in Hong Kong. CCO-1 commented in the Compliance Group chat, "We found multiple meetings scheduled" in Victim-4's account "that appear to be political so we suspended the account for now."

95. After Company-1's suspension of Victim-4's account, JULIEN JIN informed JIN TAO that "the 6.4 meeting yesterday has been addressed" and noted that Company-1 "will address this religion [meeting] today," apparently referring to a separate meeting that the PRC authorities found objectionable.

96. On or about May 22 and 23, 2020, JULIEN JIN wrote the Compliance Group that Company-1 was at risk because its users were hosting meetings with religious themes absent the requisite "religious service license" in the PRC. JULIEN JIN advised the Compliance Group that, before Company-1 could apply for a "religious service license" in the PRC, Company-1 must immediately terminate a "religious" meeting hosted on its

platform and provide user account information regarding the meeting participants located on U.S. clusters to the PRC government.

97. In the same chat, CLO-1 instructed Employee-1 to terminate the account. CLO-1 instructed CCO-1 to track how Company-1 responded to "this stuff"—referring to Chinese law enforcement requests—to improve transparency. JULIEN JIN then asked Employee-1 for information on the meeting's presenters. In response, Employee-1 provided JULIEN JIN with Chinese characters identifying what appears to be one of the presenters, together with an IP address resolving to ChinaNet Yunnan Province Network in Yunnan Province, PRC, noting this metadata was for a participant rather than the host. Employee-1 then terminated the meeting host's account, citing a purported TOS violation as the justification, and instructed JULIEN JIN to keep an eye on the topic. Based on electronic messages exchanged with certain other Company-1 employees, Employee-1 cited a TOS violation committed by the meeting participants as the justification for terminating the account. JULIEN JIN noted the account owner would still have access to Company-1's free service and requested forced termination of that access as well. The Compliance Group complied with JULIEN JIN's request.

98. On or about May 23, 2020, JULIEN JIN contacted SONG GUORONG with information on the host of the religious meeting received from Company-1 employees in the United States. JULIEN JIN noted the accounts were "force forbidden" from using Company-1's platform. SONG acknowledged receipt of the information.

99. Following the termination of the religious meeting, JULIEN JIN prepared a rectification report on the incident for the MPS and the CAC. On or about May 25, 2020, JULIEN JIN submitted this rectification report to the MPS's JIN TAO and SONG

GUORONG. That same day, JULIEN JIN submitted the same rectification report to XU WEI, an official with the CAC in the Xihu District of Hangzhou.

100. In an electronic conversation between JULIEN JIN and JIN TAO on or about May 26, 2020, JIN TAO asked JULIEN JIN for the account information for the individual hosting a meeting on Company-1's U.S. cluster. JULIEN JIN explained that Company-1 employees based in the PRC could not access data in the United States. JULIEN JIN then asked for and received the information from Employee-2, before sending the information to JIN TAO.

101. JULIEN JIN also sent electronic messages to task three Company-1's U.S.-based employees, including Employee-1, with providing him with user account information requested by the MSS and the MPS's First Bureau. On or about June 1, 2020, JULIEN JIN forwarded to Employee-1 and other U.S. employees what appeared to be feedback from the MSS describing their need for user information regarding any "cn" participants in a Company-1 meeting organized by a prominent U.S.-based dissident ("Victim-5") and hosted on Company-1's platform on or about May 31, 2020. I assess that, by using the phrase "cn" participants, JULIEN JIN likely meant Chinese participants.

102. Based upon publicly available information and witness interviews, Victim-5 was a student leader in the 1989 Tiananmen Square protests and has been an outspoken advocate for human rights and democracy in the PRC. Victim-5, who is based in the United States, used the Company-1 account of a U.S.-based associate ("Victim-6") to host the May 31, 2020 meeting commemorating the Tiananmen Square massacre.

103. Employee-2 agreed to provide JULIEN JIN with data responsive to the MSS request for information regarding Victim-5's May 31, 2020 meeting by disclosing

Victim-6's account information, including the account holder name, the user ID, account ID, and account number. Employee-2 asked for Employee-1's assistance in terminating the account. Employee-1 then terminated Victim-6's account and provided JULIEN JIN with confirmation of the termination; this communication included Victim-6's true name and email account. On or about June 1, 2020 and in a separate chat involving JULIEN JIN and Employee-2, Employee-2 sent JULIEN JIN numerous records regarding Victim-6's account, including documents with details on all of Victim-6's prior meeting history on Company-1's platform, as well as the IP addresses from which Victim-6 joined the meetings. Employee-2 also provided JULIEN JIN with multiple documents containing what appears from my review to be the names, IP addresses and devices used by all participants in Victim-5's May 31, 2020 meeting. The participant data pertained to several users who joined from IP addresses in the United States, as well as from Taiwan, Hong Kong and the PRC.

104. Victim-5 has informed the FBI, in sum and substance, that, leading up to the May 31, 2020 meeting, Victim-5 held several practice meetings in preparation. Initially, Victim-5 intended to use a pre-existing Company-1 account of an associate with experience using Company-1's platform. However, after users in the PRC encountered difficulties in joining the practice meetings, Victim-5 formed the view that PRC authorities were already surveilling the participants. As a result of this security concern, Victim-5 directed Victim-6 to upgrade from a free account to a paid account that would maximize service and the number of users allowed to participate in a Company-1 meeting.

105. Victim-5 further informed the FBI, in sum and substance, that PRC authorities pressured several potential meeting speakers in the PRC not to attend Victim-5's meeting on the Company-1 platform. According to Victim-5, PRC police officers arrived at

the residence of a potential speaker on the morning of May 31, 2020 and prevented him/her from using any electronics (and thereby attending the meeting). The PRC government similarly pressured another participant who had provided Victim-5 with a pre-recorded video to be played during the meeting on the Company-1 platform; Victim-5 reported to the FBI that this potential speaker was detained by PRC authorities two hours before the meeting started on May 31, 2020 and held until after June 4, 2020. He/she was released with the warning that he/she would be incarcerated if the video that he/she had provided to Victim-5 was seen by more than 500 viewers.

106. In addition, based upon witness interviews and review of open-source information, another anti-CCP demonstrator who currently resides in Australia ("Victim-7") received a call from his/her father in the PRC in April 2020. During the call, an MPS officer who was with the participant's father stated, in sum and substance, that the participant needed to stop anti-CCP activities, provide the officer with the passwords to the participant's social media accounts and return to the PRC. Victim-7 refused and recorded the call. During the May 31, 2020 meeting on Company-1's platform discussed above, Victim-7 discussed that call involving the MPS. On or about June 1, 2020, Victim-7's parents received an electronic message from the MPS, which message contained a screenshot showing Victim-7 in the May 31, 2020 meeting on Company-1's platform. Victim-7's father then sent the participant an electronic message asking whether the participant wanted his/her parents "dead." Victim-7 has stated, in sum and substance, that he/she was distressed by the pressure exerted by PRC officials on Victim-7 and Victim-7's family, particularly after the May 31, 2020 meeting on Company-1's platform.

107. On or about June 1, 2020, the site leader of Company-1's office in Hefei exchanged messages with JULIEN JIN and provided JULIEN JIN with the contact information for LIU ZHIYANG. At about this same time, JULIEN JIN began communicating with an individual who appears to be another MPS officer. The MPS officer provided JULIEN JIN with the same contact information for LIU and instructed JULIEN JIN to call the MPS directly. JULIEN JIN subsequently contacted LIU and later reported in a chat communication with the MPS officer that LIU said he was very satisfied.

108. Following his contact with LIU ZHIYANG, JULIEN JIN sent an update to the head of Company-1's office in Hefei. JULIEN JIN noted that he had just communicated with "*guo bao*," that is, the First Bureau of the MPS, and stated that "he"—referring to LIU—was "very satisfied with my answer." JULIEN JIN summarized that LIU's concern "about [Company-1] was mainly from the security perspective," "including intercommunication at home and abroad, how do we ensure security – the infiltration of pornography, religion, and political-related activities." JULIEN JIN had told LIU that "we [Company-1] do have a powerful security team as well as all kinds of supervisory and regulatory measures in place." JULIEN JIN further noted that LIU's only outstanding concern was with the number of Company-1 users in "Xinjiang." Based upon my training and experience and publicly available information, "Xinjiang" refers to the Xinjiang Province of the PRC, which has been the focus of international scrutiny because of the PRC government's alleged wholesale detention of the local Muslim population, including the Uighur ethnic minority group.

109. On or about June 1, 2020, JULIEN JIN sent an electronic message advising Employee-1 and two other U.S.-based employees of Company-1 that the MPS's

First Bureau had requested "Xinjiang users' data, user category, the number of the registered, and number of participants, etc." According to JULIEN JIN, the MPS further requested that the data be provided no later than "8:30 (China time)" the following day.

110. In the same series of communications, JULIEN JIN stated that, with respect to the data request from the PRC government, "[f]or global [accounts] it can either include or exclude cn01." Based upon my training and experience and the information gathered in the investigation, JULIEN JIN's reference to "global" accounts meant that he wanted to provide the PRC government with information related to accounts located anywhere in the world, not just in the PRC. Moreover, JULIEN JIN's reference to including or excluding "cn01" meant that the data could, but did not need to, include data about users whose data was stored on a Company-1 server in the PRC.

111. As discussed above, JULIEN JIN himself, located in the PRC, did not have access to data stored on Company-1's U.S. servers. Based upon publicly available records and communications I have reviewed, the Company-1 employees whom JULIEN JIN asked for help with the PRC government's data request related to Xinjiang Province, including Employee-1, were located in the United States.

112. On or about June 1, 2020, in response to JULIEN JIN's request, Employee-2 sent JULIEN JIN an electronic communication containing a spreadsheet with approximately 23,000 account IDs and user IDs for Company-1 accounts. The investigation has not revealed if JULIEN JIN provided some or all of this information to LIU ZHIYANG and the MPS.

113. On or about June 2, 2020, XU WEI began including JULIEN JIN on directives and notifications from the CAC on content from online platforms that was subject

to censorship that appears to have included several PRC nationals employed with other companies that monitored content on their respective platforms.[16] In the directive from on or about June 2, 2020, XU advised JULIEN JIN and the others to perform self-examination and self-correction soon, comprehensively investigate stored information, strictly control newly added information, firmly implement information content examination review mechanisms and fortify information content security firewalls. In addition, XU advised JULIEN JIN and the others to "toughen user management," "promptly and strictly take actions on non-compliance and harmful content or accounts that publish non-compliance and harmful contents," and "toughen the public review of content information, including replies, comments, pop-up advertisements and such." JULIEN JIN indicated that he understood XU's directive.

114. On or about June 3, 2020, SONG GUORONG issued a directive to JULIEN JIN and other PRC-based employees of technology companies responsible for monitoring content on their platforms. SONG instructed that "tomorrow"—June 4, 2020, the 31st anniversary of the Tiananmen Square massacre—"is a sensitive day" and that JULIEN JIN and others in the PRC should "enhance control over content and initiate prompt actions on issues." On or about June 4, 2020, JULIEN JIN indicated to SONG that he understood SONG's directive.

---

[16] JULIEN JIN continued to receive similar censorship instructions from the CAC through at least July 2020, including from one directive from YUANYUAN CHEN to remove all content related to a well-known individual in the PRC ("Victim-8"). At the time, Victim-8 was advocating support for ideas put forth by Victim-1 disfavored by the CCP.

G. JULIEN JIN, HUANG YIWEN, Employee-1 and Certain Other Company-1 Employees Terminate June 3, 2020 and June 4, 2020 Meetings Commemorating the Tiananmen Square Massacre

115. By June 2020, JULIEN JIN's efforts to comply with the PRC government's network security demands culminated in JULIEN JIN and HUANG YIWEN's participation in a scheme to fabricate pretextual violations of Company-1's TOS, which caused U.S.-based employees of Company-1 to terminate the accounts and meetings involving individuals located outside the PRC, including in the United States. The investigation has revealed the Company-1 employees in the PRC, including JULIEN JIN, spoke with the PRC authorities about what constituted acceptable use of Company-1's platform and Company-1's TOS. Specifically, JULIEN JIN engaged in repeated conversations with PRC officials about what content violated Company-1's TOS, meaning the PRC authorities knew the exact types of pretextual complaints to submit to get commemorations of the Tiananmen Square massacre on Company-1's platform shut down.

116. As discussed below, JULIEN JIN and HUANG YIWEN spearheaded efforts to terminate or otherwise disrupt a series of meetings on the Company-1 platform on or about June 3, 2020 and June 4, 2020 related to the Tiananmen Square massacre. These efforts represented an active and deliberate process involving collaboration between JULIEN JIN, HUANG, Company-1 employees and others based in the PRC, to identify participants in and to disrupt these meetings for pretextual reasons.

117. The scheme involved, among other things, a coordinated attempt to trigger the suspension and/or termination of Company-1 accounts belonging to meeting organizers by fabricating evidence—some of which was manufactured in the names of PRC dissidents themselves—and otherwise falsely reporting that the June 3, 2020 and June 4,

2020 meetings involved discussions related to terrorism or pornography, and thus were in violation of Company-1's TOS. In fact, no such discussions or violations of the TOS were occurring. Through their scheme, JULIEN JIN, HUANG YIWEN and other members of the conspiracy sought to further efforts by the PRC government to prevent discussions of the Tiananmen Square massacre that the PRC government deemed subversive.

118. In furtherance of the scheme, the co-conspirators created a series of alias email accounts (the "Alias Email Accounts"), which they deployed in several ways to undermine the June 3, 2020 and June 4, 2020 meetings. First, members of the conspiracy used the Alias Email Accounts to create Company-1 accounts, to set the profile picture of some of those accounts to images associated with terrorism or pornography, and to enter some of the meetings using those accounts. Second, the co-conspirators used the Alias Email Accounts to submit purported false reports of TOS violations to JULIEN JIN and Company-1. The false reports included screenshots from the meetings of the images associated with terrorism or pornography that were generated by the conspirators themselves.

The June 3, 2020 Meeting

119. Based upon interviews conducted in the course of this investigation, as well as a review of screenshots of meetings and electronic communications, on or about June 2, 2020 and June 3, 2020, individuals associated with a student leader and participant in the 1989 student protests at Tiananmen Square ("Victim-9") organized a meeting on Company-1's platform to commemorate the anniversary of the Tiananmen Square massacre (the "June 3 Meeting"). Victim-9 is a resident of the Eastern District of New York and participated in the June 3 Meeting from his residence. The meeting was invitation-only, and social media postings about the meeting did not include the specific location of the meeting on Company-

1's platform. Throughout the course of several hours, the June 3 Meeting was shut down by Company-1, and then restarted by the organizers in a different meeting room on Company-1's platform. Based upon law enforcement interviews, the June 3 Meeting was configured so that only certain individuals, chosen to speak by the meeting host, could speak during the meeting. Moreover, participants in the June 3 Meeting informed the FBI that the meetings did not include discussions of child abuse or exploitation, terrorism, racism or incitements to violence.

120. Based upon law enforcement interviews and my review of electronic communications, including meeting invitations, early on or about June 3, 2020, I assess that Victim-9 inadvertently initiated the June 3 Meeting in a Company-1 meeting room using an incorrect meeting number (the "Incorrect June 3 Meeting") that had not been circulated to any of the invited participants.

121. Information obtained from Company-1 indicates that Victim-9 created the meeting room and meeting number for the Incorrect June 3 Meeting on or about June 2, 2020 at approximately 7:53 PM EDT. On or about June 3, 2020, JULIEN JIN exchanged electronic messages with a Company-1 employee based in San Jose ("Employee-4") who had previously aided JULIEN JIN after JULIEN JIN lost access privileges to, among other things, customer data in the United States. JULIEN JIN had also previously discussed with Employee-4 JULIEN JIN's work on the risk management of political issues for Company-1 with the PRC authorities.

122. On or about June 3, 2020, at approximately 4:19:22 AM EDT, JULIEN JIN asked if he could have a meeting [with Employee-4] for a few minutes about a "6.4" issue. At approximately 4:19:41 AM EDT, Employee-4 started a Company-1 meeting with

JULIEN JIN that lasted until approximately 4:26:14 AM EDT. During this meeting, from approximately 4:19:59 AM EDT until approximately 4:22:09 AM EDT, Employee-4 used the "screen share" feature in the Company-1 meeting with JULIEN JIN, allowing JULIEN JIN to see the content on the monitor of the device Employee-4 was using in the meeting.

123. On or about June 3, 2020, at approximately 4:20:45 AM EDT, JULIEN JIN sent Employee-4 a message that included the email address associated with Victim-9's Company-1 account. Company-1's network logs indicated that at approximately 4:21 AM EDT, Employee-4 used his/her access privileges to log into and access Victim-9's Company-1 account. Through the screen share feature, the information visible to JULIEN JIN in the PRC from Employee-4's monitor in the United States would have included the meeting information and meeting link to the meeting number created by Victim-9 for the Incorrect June 3 Meeting that had not been circulated to anyone outside of Company-1.

124. In an interview with the FBI, Employee-4 noted that during his/her meeting with JULIEN JIN on June 3, 2020, JULIEN JIN stated that he had received a request from the PRC government that Victim-9's account was suspicious. JULIEN JIN asked Employee-4 to check on the account. Employee-4 told the FBI that he/she checked Victim-9's account but did not find any indicators of fraud or any signs of abnormal behavior associated with the account. Further, since Victim-9's account was in Company-1's U.S. cluster, Employee-4 stated as much to JULIEN JIN and directed him to Company-1's legal department.

125. On or about June 3, 2020, at approximately 6:25 AM EDT, JULIEN JIN sent an electronic message to the Compliance Group, stating that PRC law enforcement officials had notified him of an upcoming "political" meeting on Company-1's platform and

provided the meeting number for the Incorrect June 3 Meeting. JULIEN JIN's notification included the information that the meeting would occur at "7:00 AM New York" and referenced the meeting number for the Incorrect June 3 Meeting. JULIEN JIN recounted that the PRC officials requested that the meeting not be shut down immediately, as PRC law enforcement officials intended to use a public link to monitor the content of the meeting for evidentiary purposes. According to the instructions, after 20 to 30 minutes, the meeting could be terminated.

126. Based upon information obtained from email service providers, shortly before the aforementioned 7:00 AM EDT start time for the June 3 Meeting, HUANG YIWEN conducted internet searches related to reporting TOS violations to Company-1:

a. On or about June 3, 2020, between approximately 6:41 AM and 6:45 AM EDT, an individual logged in to an account created on or about May 23, 2020 (the "QAA Account) conducted searches in English for "violence," "violence picture," and "gambling website," and in Chinese for "bloody violence picture," "violence picture," and "big breasts."

b. Between approximately 6:48 AM and 6:50 AM EDT that same day, an individual logged into a second account (the "HUH Account") conducted internet searches in Mandarin Chinese for reporting a violation of the terms of use to the Company-1 help center and Company-1 support.

127. Based on witness interviews and metadata obtained from Company-1, Victim-9 started the Incorrect June 3 Meeting at approximately 7:04 AM EDT from Victim-9's Company-1 account. Since none of the invited participants had received the details of the meeting room for the Incorrect June 3 Meeting, none participated in the Incorrect June 3 Meeting. However, there were other participants besides Victim-9 in the Incorrect June 3 Meeting who appear to have used Company-1 profiles associated with nonexistent email

accounts or email accounts that appear to have been created by co-conspirators for the purpose of disrupting the meeting.

128. By approximately 7:30 AM EDT, and due in part to confusion with the meeting numbers, the June 3 Meeting had moved from the Incorrect June 3 Meeting room to a room hosted by another individual who had participated in the 1989 Tiananmen Square protests, which individual was located in the Washington, D.C. area ("Victim-10"). Other participants in the meeting included residents of the Eastern District of New York. The decision to switch the host from Victim-9 to Victim-10 was a spontaneous decision and had not been planned prior to June 3, 2020.

129. On or about June 3, 2020, between approximately 7:33 AM and 7:41 AM EDT, four electronic complaints in English were submitted to Company-1's automated, internet-based system for reporting the contents of a Company-1 meeting. The complaints identified the host account for the June 3 Meeting and referred to "disgusting pics," "child abuse" and "inciting violence." Notably, all four complaints referenced the email address associated with Victim-9's Company-1 account, rather than the Company-1 account of the Victim-10 who was actually hosting the meeting at the time. Additionally, the four complaints referenced specific times of the alleged abuses (7:00 PM or 7:30 PM), yet these times do not correlate with the timing of the Incorrect June 3 Meeting and also appear to reflect a PRC time zone. Notably, at approximately 7:38 AM EDT and 7:45 AM EDT, two complaints from email accounts discussed further below (the "Foreign Accounts") were sent to the Company-1 email address established for reporting possible violations of the TOS. These complaints stated that Victim-9's Company-1 account was being used to incite racial division, violence and resistance. Moreover, although the June 3 Meeting was conducted in

Chinese—except for a prayer that was given in German but translated into Chinese—all of these complaints were made in English.

130. Based upon information obtained from email service providers, two of the aforementioned complaints were associated with an email address created in the name of an individual who resides in Japan and is a vice-president of a group established in 1989 to promote democracy in the PRC ("Victim-11"). The email account in the name of Victim-11 was created on or about June 3, 2020 at approximately 6:32 AM EDT, shortly before the complaints were filed. The email account in the name of Victim-11 is also associated with a Company-1 account in the name of Victim-11, which account attended some iterations of the June 3 Meeting.

131. Based on my training, experience, and knowledge of the investigation to date, I assess that members of the conspiracy created a Company-1 account designed to make it look as if an individual critical of the PRC government was attending the June 3 Meeting. The other complaints described above in the preceding paragraph are also associated with email accounts created between approximately 4:23 AM and 6:32 AM EDT on or about June 3, 2020—shortly before the complaints were submitted. Victim-11 confirmed that he/she had not used Company-1's platform since approximately 2019 after an incident trying to use Company-1's platform led to Victim-11's suspicion the CCP might be watching him/her, and therefore Victim-11 did not attend the June 3 Meeting and did not submit the complaint referenced above

132. Based upon my review of information provided by email service providers, other electronic communications and my training and experience, HUANG

YIWEN created and used several different email accounts in furtherance of the conspiracy's activities on June 3, 2020, and June 4, 2020. Specifically:

a. HUANG YIWEN used an email account created in her own name (the "HYW Account"). The subscriber name for that account is in the name "Nicole Huang." The initials "HYW" are contained in the name of the email account, and "HYW" appears to be an abbreviation of name "Huang Yiwen." According to information from a social media company, HUANG attended a university in Shaoxing, Zhejiang Province, PRC. According to information provided by an email provider, between March 14, 2020 and May 12, 2020, the user of the HYW Account accessed the website for a university in Shaoxing approximately 14 times.

b. On or about May 23, 2020, two email addresses were created within approximately 22 minutes of each other. Each of those accounts was created from the same IP address, which, according to open-source information, is hosted by an ISP in Hong Kong that provides internet service for residential customers. The first such account (the "QAZ Account") was subsequently updated to include HUANG YIWEN's personal email account, the HYW Account, as the "recovery" address. In addition, the "Recovery SMS" number and "Signin Phone Numbers" for the QAZ Account are the same telephone number. The last eight digits of that number are also contained, in the same order, in the email address associated with the QAZ Account.

c. On or about June 4, 2020, during the conduct described below, the HYW Account was accessed from a specific IP address at approximately 9:01 AM EDT. The QAZ Account was accessed from that same IP address approximately 17 minutes later, and then approximately two hours after that.

d. Another other account created on or about May 23, 2020 (the QAA Account)—created approximately 22 minutes before the QAZ Account—also was used in furtherance of the scheme on June 3, 2020 and June 4, 2020, as described below.

e. The QAZ Account was accessed from a particular IP address at approximately 8:54 AM and 9:50 AM EDT on or about June 4, 2020, as it was engaged in conduct discussed below. A fourth email account, also involved in the conduct discussed below (the "HUH Account"), was accessed from that same IP address at

approximately 8:57 AM, 9:00 AM, and 9:52 AM EDT that same day.

f. On or about and between May 22, 2020, and May 23, 2020, the HYW Account accessed multiple chat threads about current affairs on a Hong Kong-based forum website that, based on open-source records and my training and experience, is known as one of the platforms used by protesters against the CCP (the "Forum Website"). During that same time frame, the HUH Account accessed different chat threads on the Forum Website. Notably, although access from the two accounts occurred close in time—including at approximately 9:03 PM EDT for the HUH Account, 9:05 PM EDT for the HYW Account, and 9:06 PM EDT again for the HUH Account—no access by one account occurred at exactly the same time as access by the other account. Based on my training and experience and the foregoing, HUANG YIWEN switched back and forth between the two accounts to simultaneously track two threads of interest or to appear as if two different users were participating in discussions at the same time.

133. Based upon information obtained from an email service provider, on or about June 3, 2020, between approximately 7:51 AM and 8:38 AM EDT, HUANG YIWEN conducted internet searches with the HUH Account for "[Victim-9] [Company-1] meeting," for the names of other political opponents of the CCP who had protested the Tiananmen Square massacre, for a web translation function and for the name of an individual in Germany who was helping to organize the meeting with Victim-9.

134. Between approximately 8:14 AM and 8:25 AM EDT, HUANG YIWEN and others sent six emails to the Company-1 email address established for reporting possible violations of the TOS. Those emails, written in English, complained that Victim-10's account, which was then hosting Victim-9's meeting, was inciting racial conflicts, violence and resistance:

a. At 8:14 and 8:15 AM EDT, HUANG YIWEN and others used the Foreign Accounts to write that Victim-10's account "incited, racial

conflicts, incited violence and resistance." The subjects and content of both emails were identical.

b. At 8:23 AM EDT, the QAA Account wrote that the host account for that meeting "is constantly inciting racial conflicts, inciting violence."

c. At 8:25 AM EDT, the HUH Account wrote: "I need to report that [the user of the host account] is a suspected organice of a meeting that incites racial discrimination."

d. The other two emails, at 8:15 and 8:18 AM EDT, reported that the host account "is inciting racial conflicts, inciting violence and resistance" and "is constantly inciting racial conflicts, inciting everyone to fight violently." Those two emails were sent from the same account (the "WB Account").

The WB Account was created on or about June 3, 2020 using an IP address hosted by a company in Singapore. IP addresses hosted by that company were also used to create three other email accounts on or about June 3, 2020, each of which accounts was used in an apparent attempt to trigger Company-1 TOS violations on June 4, 2020, as discussed below.

135. Notwithstanding the complaint emails from the QAA Account and the HUH Account, based upon interviews with meeting participants and my review of electronic data gathered in the investigation, no user associated with either email address attended the June 3 Meeting on Company-1's platform.

136. Between approximately 7:53 and 7:56 AM EDT, JULIEN JIN sent electronic messages to the Compliance Group containing two images, the first of which included Victim-9's name, the name of Company-1 and "2020/6/3"—a reference to the June 3 Meeting. The second image contained a screenshot from the June 3 Meeting. JULIEN JIN wrote "meeting!" and asked the U.S.-based employees to suspend the relevant account. It is not clear how JULIEN JIN was aware that the June 3 Meeting hosted by Victim-10 was

taking place. Nonetheless, JULIEN JIN urged the Compliance Group to shut down the account hosting the June 3 Meeting—which, at that time, JULIEN JIN appeared to still believe was being hosted by Victim-9 rather than Victim-10—telling them that the meeting was in progress and warning them that the "cyberspace people" were waiting for Company-1's response. In the context of the investigation, and based on the foregoing, "cyberspace people" refers to officers of the MSS and/or the MPS.

137. At approximately 8:13:10 AM EDT, JULIEN JIN sent messages to the Compliance Group with a link to the June 3 Meeting room and the meeting room number for the meeting hosted by Victim 9. It is not clear how JULIEN JIN obtained this information as his access to U.S.-based customer data had been revoked. Notably, JULIEN JIN requested suspension of the meeting host's account before Company-1 had received any complaints specific to Victim-10 (which first arrived at 8:14 AM EDT). In the Compliance Group chats, Employee-3 reported that he/she had terminated the meeting at approximately 8:16:58 AM EDT and "locked" Victim-10's account.

138. Though JULIEN JIN successfully caused termination of the meeting by claiming that Company-1 had received complaints of purported TOS violations, the complaints emailed on or about June 3, 2020 were not sent to JULIEN JIN's email address, but rather to a generic U.S.-based email mailbox (violation@[Company-1].us) and a Company-1 complaint desk. Notably, the same group of accounts that emailed complaints directly to JULIEN JIN's personal Company-1 email address on or about June 4, 2020 (discussed below) were similarly responsible for the June 3, 2020 complaints sent to <<violation@[Company-1].us>>.

139. Although JULIEN JIN brought the June 3, 2020 complaints to the attention of other Company-1 employees, none of those complaints appear to have been sent to his work account, and the investigation has not identified any way he would have had reason to know of the existence of the complaints if he were not involved in or aware of the scheme of manufacturing pretextual complaints to cause terminations of meetings and accounts.

140. After learning that the June 3 Meeting had been shut down, JULIEN JIN thanked the other employees and noted at approximately 8:23 AM EDT—nine minutes after the complaints were first lodged against Victim-10—"We reported several abuse for this meeting. So we may refer to this they against tos."

141. As the June 3 Meeting hosted by Victim-10 restarted again in a new meeting room hosted by Victim-9's Company-1 account, CLO-1 asked JULIEN JIN if there was proof the PRC authorities asked JULIEN JIN to shut the meeting down. JULIEN JIN responded by pasting the same open-source information he pasted earlier with Victim-9's email address and stated, "Authorities want use to make sure no more such anti-CN political public meetings." CLO-1 asked how JULIEN JIN knew this was out of the PRC since the analysis of IP activity, billing and other indicators showed Victim-9's account was for a U.S.-based user. JULIEN JIN replied, "I think they're fake. They speak chinese, not english." CLO-1 responded that they could not shut down a U.S.-based account based on a Chinese law enforcement request. JULIEN JIN warned that the "cyber people here," which likely included MPS officers and CAC officials such as FU YIBIN, JIN TAO, SHEN ZHENHUA, SONG GUORONG, TIAN XINNING and XU WEI, believed that Company-1 should take "all measures to terminate illegal activities by ourselves."

142. In the same message, CLO-1 replied that was not possible since Company-1 could not apply "Chinese law to other countries," even though the Compliance Group had just applied PRC law to shut down the meeting hosted by Victim-10. Though JULIEN JIN had no way of knowing any of the details of the June 3 Meeting participants, JULIEN JIN made the unsubstantiated claim, "That kind meetings has lots of Chinese participants, with China ip." CLO-1 responded that Employee-3's analysis of the meeting participants indicated they were all from the United States and countries other than the PRC. Indeed, to the extent there was any participation from the PRC in an iteration of the June 3 Meeting, it appeared to have been from JULIEN JIN's co-conspirators. JULIEN JIN continued, advising that "Yesterday's similar political meeting," which may have been a reference to the May 31, 2020 meeting hosted by Victim-6 for Victim-5, "has more than 1000 participants and some are China ip," information JULIEN JIN would not have known absent Employee-1, Employee-2 and other Company-1 employees in the United States.

143. One of JULIEN JIN's subordinates in the PRC later sent an electronic message to JULIEN JIN and other employees assigned to the Company-1 group responsible for monitoring the use of Company-1's platforms for the expression of political views unacceptable to the PRC government, asking if the PRC "internet police," a reference to the MPS, was satisfied with the group's measures on June 3, 2020.

The June 4, 2020 Meeting

144. As set forth in this section, on or about June 4, 2020, individuals associated with another participant in the 1989 student protests at Tiananmen Square ("Victim-12") organized a meeting on Company-1's platform to commemorate the event. Throughout the course of several hours on or about June 4, 2020, the meeting was shut down

twice by Company-1, and then restarted by the organizers in a series of different meeting rooms on Company-1's platform. The June 4 meeting or meetings are collectively referred to as the "June 4 Meeting." The meeting or meetings were all hosted by individuals located in the Eastern District of New York, who had gathered in a single residence for purposes of participating in and hosting the June 4 Meeting. Victim-12 was participating in the June 4 Meeting from his/her residence in the Washington, D.C. area.

145. Based upon interviews conducted during this investigation, the first host of the June 4 Meeting ("Victim-13") was him/herself a protester during the Tiananmen Square massacre. On or about May 29, 2020, Victim-13 upgraded his/her paid Company-1 account for an additional fee for enhanced functionality to accommodate a request by a prominent non-governmental organization to simultaneously broadcast the June 4 Meeting. Based upon interviews conducted during this investigation, Victim-13 was not aware of Company-1's actions to shut down the June 3 Meeting and would not have hosted the June 4 Meeting on Company-1's platform had he/she been aware of those actions.

146. In addition, the June 4 Meeting was publicly advertised and organized to occur on the Company-1 platform specifically to encourage participation by PRC individuals. Moreover, based upon interviews conducted during this investigation, organizers of the June 4 Meeting created a list of designated speakers, and instituted settings for the meeting that would prevent non-designated speakers from disrupting the meeting with verbal outbursts—a common way PRC authorities disrupted dissident political speech during past commemorations of the Tiananmen Square massacre. Organizers also instituted settings within the Company-1 platform to screen out potentially suspicious usernames that could be PRC government representatives seeking to infiltrate the meeting.

147. As described below, HUANG YIWEN used at least three email accounts—the HUH Account, QAZ Account and QAA Account—in an effort to disrupt the June 4 Meeting. Each of those accounts emailed JULIEN JIN's work address to report purported violations of Company-1's TOS related to the June 4 Meeting. Notably, JULIEN JIN's work email address is not listed by Company-1 in any publicly available website as an email address to which to direct concerns about TOS violations, but, as discussed above, JULIEN JIN's email had been provided as a primary contact to the PRC government as part of Company-1's rectification following the block in 2019. Indeed, as discussed above, Company-1 has established a specific and well-publicized email account for reporting such concerns. Additionally, based on the investigation to date, JULIEN JIN does not appear to have had any other direct communication with the accounts used to send the false reports. Accordingly, it appears that HUANG and other possible co-conspirators obtained JULIEN JIN's email address directly from the rectification report, from other PRC government official(s) communicating with JULIEN JIN or from JULIEN JIN himself through some other means of communication.

148. On or about June 4, 2020, at approximately 3:53 AM EDT, JULIEN JIN notified the Compliance Group in an electronic message of another "serious June 4th meeting by [Victim-12] (Today)," noted that Victim-12 "is a lead of such illegal political activities," and asked, "Could we do something to prevent subsequent huge influence on us? Eg, Terminate or temply [temporarily] suspend that account for 24 hours until 06/05 as TOS violation?" JULIEN JIN included a social media post from Victim-12 with the details for the meeting hosted on Victim-13's account. CLO-1 replied, "Yes. Let me look at it."

149. At approximately 8:25 AM EDT, after Company-1 had not yet shut down the meeting, JULIEN JIN suggested: "Put them into QUAR [quarantine] is another approach, as if [Company-1] is having server issues . . . About 24 hours later you could recover that . . . It's a public meeting , so we could join and report to [Company-1 U.S.] as abuse meeting, then you US may have evidence to suspend it." Notably, metadata regarding the meeting suggests that one of JULIEN JIN's subordinates in the PRC attended iterations of the June 4 Meeting.

150. CLO-1 replied, "Ok. Calling team." In an interview with the FBI, CLO-1 described that the focus was on identifying where Victim-12 was located. CLO-1 was unfamiliar with Victim-12 and made a telephone call to Employee-1. During the call, CLO-1 asked Employee-1 if Victim-12 was "Chinese," by which CLO-1 meant located in the PRC, and if Victim-12 was famous. Employee-1 replied in the call that Victim-12 was "super famous."

151. However, Victim-12 was not the original host of the June 4 Meeting. Had CLO-1 and Employee-1 used the available tools to analyze the identifiers provided by JULIEN JIN associated with Victim-13's account, i.e., the account that actually hosted the June 4 Meeting, CLO-1 and Employee-1 would likely have reached the conclusion that Victim-13 was a U.S.-based user. Instead, after receiving JULIEN JIN's request to shut down the June 4 Meeting and fearing another shutdown of Company-1's services in the PRC, CLO-1 authorized Employee-1 to take action. Employee-1 subsequently terminated Victim-13's account before the actual commemoration of the Tiananmen Square massacre had begun.

152. Based upon interviews conducted in this investigation and my review of electronic data gathered during the investigation, after that iteration of the June 4 Meeting was terminated and Victim-13's account cancelled, the June 4 Meeting organizers upgraded a free Company-1 account to a paid one with different subscriber information in order to shield the account from scrutiny by the PRC government, and used the account to initiate a new meeting in a different meeting room on Company-1's platform. This tactic was unsuccessful—JULIEN JIN thereafter notified Employee-1 of the creation of the new meeting.

153. Again, based upon information provided by email service providers, HUANG YIWEN's search activity suggests that members of the conspiracy used false complaints to terminate the second iteration of the June 4 Meeting. That information also shows that, starting at approximately 8:41 AM EDT and while logged into the HUH Account, HUANG conducted an internet search for Company-1 video conferencing, followed approximately two minutes later with searches in Chinese for "naked girl" and "pornography" in an image database, and word searches for "naked girl," "naked girl images" and "IS pictures." There were also searches for "violence picture" and "gambling website." Based upon my training and experience, "IS" is a reference to the Islamic State of Iraq and al-Sham, or "ISIS," a foreign terrorist organization. Image searches were also conducted during the same time period for "naked girl" and "pornography."

154. At approximately 9:00:06 AM EDT and using the HYW Account, HUANG YIWEN searched for "Company-1." At 9:00:20 AM EDT and still using the HYW Account, HUANG visited Company-1's website.

155. Using the HUH Account, the QAA Account and the QAZ Account, HUANG YIWEN then emailed Company-1 about purported violations of Company-1's TOS related to the second June 4 Meeting:

a. At approximately 9:57 AM EDT, the HUH Account sent an email to JULIEN JIN's work email with the subject "Someone in this group incites terrorism and violence." The email stated that someone in the June 4 Meeting was inciting terrorism and violence. The email contained an image that appears from my review to be a screenshot of user profiles from three meetings stacked on top of each other. The screenshots included: (1) a Company-1 profile with the name "Kate Steve" and a picture including the motto and iconography of the Basque separatist group Euskadi Ta Askatasuna ("ETA");[17] (2) a Company-1 profile in the name of a real person who is known for authoring a book about the PRC government's censorship efforts ("Real Person-1") and a picture of what appeared to be a group of Islamic clerics standing in front of darkly clad and masked men holding weapons; and (3) a Company-1 profile with the name "Free man" and picture of a masked person holding a flag resembling that of the Islamic State terrorist group.

b. At approximately 9:59 AM EDT, the HUH Account sent two emails to JULIEN JIN with the same subject, "Someone in this group incites terrorism and violence." The first email also included the meeting number for the June 4 Meeting. The second email also contained what appears from my review to be the same images depicted in the email sent at 9:57 AM EDT.

c. Between approximately 9:30 AM and 10:16 AM EDT, a participant with the profile name "Kate Steve," using the QAA Account, entered the June 4 Meeting. The profile picture for "Kate Steve" was the picture associated with ETA discussed above.

d. At approximately 9:49 AM EDT, the QAA Account emailed the Company-1 email address for reporting TOS violations. The subject of the email was "[Victim-9 email account] this account is constantly inciting racial conflicts an violence and pornography." Significantly, although this email referred to Victim-9's email

[17] Based upon publicly available information, ETA has a history of conducting assassinations and kidnappings throughout Spain since 1968 that have resulted in the deaths of several hundred people.

account, Victim-9 did not attend the June 4 Meeting; instead, Victim-9 hosted the June 3 Meeting.

e. At approximately 9:57 AM EDT, the QAA Account emailed JULIEN JIN with a subject that identified Victim-9's email account and the sentence "This account is constantly inciting racial conflicts and violence." The email contained only an image of what appears from my review to be a screenshot of various users in a Company-1 meeting. The image included users identified as: the name of Real Person-1 with a profile picture of two naked women; "Free man," with a profile picture including an Islamic State flag; and another individual with a profile picture of an Islamic State flag. Again, although the email referred to Victim-9, Victim-9 did not attend the June 4 Meeting.

f. Between approximately 9:34 AM and 10:16 AM EDT, HUANG YIWEN used a Company-1 account associated with the QAZ Account and entered the June 4 Meeting.

g. At approximately 9:57 AM EDT, the QAZ Account emailed JULIEN JIN with the subject "report." The email indicated that an unidentified account "frequently incites violent and terrorist content." The email also provided what appears from my review to be a screenshot of a Company-1 meeting with profiles that included: a profile in the name of Real Person-1 with a picture of a card dealer, apparently to suggest some form of gambling; and several users, including "Free man," with images depicting the Islamic State flag.

h. Approximately four minutes later, the QAZ Account sent a second email to JULIEN JIN. The subject of the email was "the account frequent incites violent and terrorist content." The email included the same text as the earlier email and what appears from my review to be a similar screenshot of profiles in a Company-1 meeting.

i. As discussed above, during the June 4 Meeting, the QAZ Account and the HYW Account were accessed from the same specific IP address. During that same time period, the Company-1 profile associated with the QAZ Account was accessed from that same specific IP address. In addition, during that same time period, the QAZ Account and the HUH Account were accessed from another specific IP address. Another Company-1 account participating in the June 4 Meeting was also accessed from that same specific IP address.

156. Based upon information from email service providers, and the information set forth herein, some of the user accounts reported in the aforementioned email complaints were associated with email accounts created by members of the conspiracy. Most notably, the profile picture that was reported as inciting violence by the HUH Account was associated with the QAA Account. In other words, based upon my training and experience, HUANG YIWEN and members of the conspiracy introduced into the June 4 Meeting at least one image that purportedly incited violence and then reported the image they introduced. Moreover, the account for the user profile "Free man" associated with an email address (the "Free Man Account") created on or about June 3, 2020, from an IP address resolving to Singapore and hosted by the same company that hosted IP addresses used on or about June 3, 2020 to create other email addresses used by members of the conspiracy. In addition, based on information from email service providers and metadata from Company-1, the Free Man Account and two other accounts participated in the June 4 Meeting from the same electronic device; the Company-1 profiles associated with those two other accounts each showed a profile picture depicting an ISIS-related image.

157. In total, based upon my review of electronic communications obtained during the investigation, 14 email complaints related to the June 3 Meeting and the June 4 Meeting were sent to JULIEN JIN on or about June 4, 2020, between 9:54 AM and 10:16 AM EDT—a period of approximately 20 minutes. As set forth above, JULIEN JIN is not identified publicly by Company-1 as an individual to whom to email complaints about meetings, and his email address is not publicly displayed, although it was provided to PRC authorities. The emails to JULIEN JIN appeared to be from ten different complainants, but

based on the information set forth herein and my training and experience, I assess that they represented coordinated efforts by PRC-based co-conspirators including HUANG YIWEN.

158. Indeed, the complaints often used verbatim language, including identical spelling and grammatical mistakes and referencing the date June 4, 2019, rather than June 4, 2020, to complain about purported participants in the meetings who were promoting violence, pornography or Islamic terrorism, attached identical screenshots of user profiles with ISIS flags and used identical IP addresses. In addition, many of the complaints did not refer to a specific meeting on the Company-1 platform or included screenshots of meetings that had already lapsed; many of the screenshots had time stamps reflecting PRC time zones. Moreover, although the June 3 and June 4 Meetings were conducted in Chinese, all of the complaints were made in English. Based upon my review of publicly available information and the foregoing, I assess that these complaints were submitted in English because the individuals sending them knew that the likely decision-makers for terminating any meetings would be English speakers in the United States.

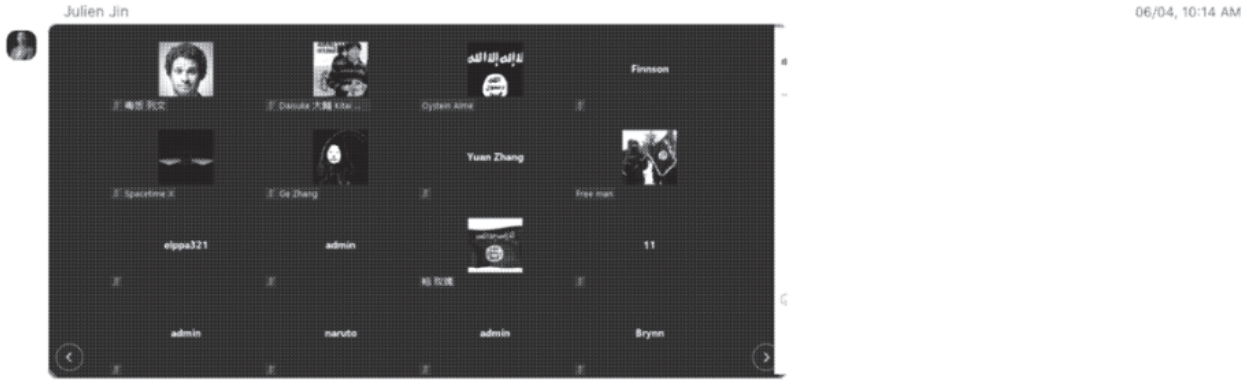
159. At approximately 9:42 AM EDT on or about June 4, 2020, JULIEN JIN sent a message to Company-1 employees monitoring content that included the expression of political views unacceptable to the PRC government, in which message JULIEN JIN told his subordinates that "there are so many of own people, friendlies." After one of JULIEN JIN's subordinates asked if the "friendlies" were from Company-1, JULIEN JIN replied that "Net Security," a reference to the MPS's Network Security Bureau, was "working overtime."

160. At approximately 10:05 AM EDT on or about June 4, 2020, shortly after some of the aforementioned email complaints had been sent, JULIEN JIN wrote to

various Company-1 employees: "We get report about Someone inside this group incites terrorism and violence . . . They also send such abuse info to [Company-1 U.S.] site, I think [a Company-1 employee's] tos team received that too." JULIEN JIN added, "there're IS [Islamic State] flag on someone's photo. Can you suspend that as terrorism and violence meetings ?"

161. After JULIEN JIN sent an electronic message with a screenshot of a user profile with the Islamic State flag as seen in Image 1 below, Employee-1 agreed to terminate the meeting as well as the paid account used to host Victim-12's meeting. Notably, based upon my familiarity with Company-1's platform, users of Company-1's platform appear to be able to change their profile pictures by selecting from images in the photo galleries of the users' devices; it is not clear if Company-1 allows users to store images in their Company-1 profiles. JULIEN JIN thanked Employee-1 and others for their immediate support. The image provided by JULIEN JIN appears from my review to be identical to images attached to two emails JULIEN JIN received at 9:54 AM and 10:00 AM EDT, from two different email addresses.

Image 1



162. JULIEN JIN later exchanged messages with his subordinates in the PRC monitoring content disfavored by the PRC government, notifying them of the ISIS flag in the June 4 Meeting. One of JULIEN JIN's subordinates, who was a participant in iterations of the June 4 Meeting, asked JULIEN JIN at approximately 11:42 AM EDT, "What the heck, ISIS?"—likely indicating the actual content had nothing to do with terrorism. The subordinate continued and asked JULIEN JIN, "So how was it, the Internet Police was satisfied with our measures yesterday?"

163. As noted above, the June 4 Meeting was configured so that only certain individuals, chosen to speak by the meeting host, could speak during the meeting. Moreover, participants in the June 4 Meeting have stated to FBI agents that the meetings did not include discussions of child abuse or exploitation, terrorism, racism or incitements to violence. The FBI also has reviewed a video of the meeting and observed that the only violence discussed in the meeting was the violence inflicted by the PLA on protesters at Tiananmen Square in 1989.

164. Based upon interviews conducted as part of this investigation, the termination of the June 4 Meeting has caused substantial emotional distress to participants in the meeting. For example, one of the speakers at the June 4 Meeting ("Victim-14") reported sending a chat message on or about June 3, 2020 to his/her father's account indicating that Victim-14 was going to participate in an event about the Tiananmen Square massacre. After sending the message, Victim-14 received a chat message on his/her account that Victim-14's account had violated the user agreement and was shut down. Additionally, approximately two weeks after the June 4 Meeting, the local MPS called the mobile telephone of Victim-14's father in the PRC. During the call, the MPS instructed

Victim-14's father to tell Victim-14 to stop speaking out against the CCP and to support socialism and the CCP. The MPS also inquired about Victim-14's life in the United States and asked when Victim-14 intended to return to the PRC.

165. As discussed above, other PRC government actions related to the pro-democracy discussions on the Company-1 platform in May and June 2020 also caused significant emotional distress to other participants, including to Victim-7. In interviews with the FBI, Victim-13 noted feeling helpless following the actions taken by Company-1 against meetings he/she organized. Victim-13 stated that these actions had taken place while he/she was in the United States using an American service. Victim-13 explained that he/she left the PRC to escape the PRC government's influence and persecution but was now experiencing it in the United States.

The Conspiracy's Use of the Names of Real Individuals

166. As alluded to above, members of the conspiracy used the names of real individuals to further their scheme. This aided their ability to infiltrate the June 3 Meeting and the June 4 Meeting, as the organizers of the meetings were screening for potential CCP representatives seeking to cause disruptions.

167. Information provided by the email service provider for the Free Man Account and Company-1 subscriber information shows that the account is linked to a Company-1 account used by the conspiracy to display images associated with ISIS and lists that the account was created in the name of Victim-5. Victim-5 has told the government that the email address is unfamiliar to him/her and that he/she never used the account. Based upon my familiarity with Company-1's platform, a Company-1 employee looking at

information associated with the Company-1 account, however, would have seen the name of the student leader in that email address as part of the information about the account.

168. The Company-1 account created in the name of Victim-11, associated with an email address in the name of Victim-11, similarly would have given the impression that an individual known to be critical of the PRC government was participating in the June 3 Meeting.

169. Finally, the Company-1 account associated with the name of Real Person-1 was used to display various images associated with terrorism and pornography. As noted above, based upon publicly available information, Real Person-1 is a writer known for publishing a book about PRC government censorship and is associated with a news publication regarding Tibet. As a result, upon information and belief, members of the conspiracy used Real Person-1's name in order to gain entry to the meeting—because meeting organizers who were screening participants would not have rejected the actual Real Person-1—and to give the impression that Real Person-1 was actually participating in the meeting when he/she was not.

Continued Efforts to Terminate Meetings and Accounts

170. On or about June 5, 2020, JULIEN JIN notified U.S.-based Company-1 employees of his receipt of a message from the "CN cybersecurity"—a reference to the CAC and/or the MPS—indicating that 48 communications platforms had failed to take instant action on illegal content in the "June 4th" period and were thereafter fined or forced offline by PRC authorities. Thereafter, Employee-1 terminated two of the accounts that hosted one

of the U.S.-based meetings commemorating the anniversary of the Tiananmen Square massacre, based on purported TOS violations.

171. In electronic messages sent to the Compliance Group, in response to CLO-1's and CCO-1's requests for JULIEN JIN to provide documentation detailing all the PRC law enforcement requests he had received in connection with the action taken against accounts hosting Tiananmen Square anniversary meetings, JULIEN JIN claimed that there was no legal documentation for the PRC government requests to terminate the "June 4th political accounts." Rather, JULIEN JIN wrote that Company-1 should indicate that "Incites terrorism and violence" was the basis for the termination of the accounts, meaning that the users committed TOS violations.

172. CCO-1 has informed the FBI that JULIEN JIN repeatedly ignored CCO-1's authority, as JULIEN JIN regularly bypassed CCO-1 and CLO-1 by engaging directly with Employee-1 and CEO-1 despite being admonished by CLO-1 against doing so. Additionally, following the events of June 3, 2020, and June 4, 2020, JULIEN JIN expressed to CCO-1 that he did not feel the need to respond to or report to CCO-1.

Continued CAC, MPS, and MSS Requests of Company-1

173. In approximately December 2020, Company-1 terminated JULIEN JIN's employment. However, XU WEI, CHEN YUANYUAN and other officials with the CAC, MPS and MSS continued to make requests of Company-1 related to "illegal" content, including commemorations of the 32nd anniversary of the Tiananmen Square massacre on or about June 4, 2021. There is no indication Company-1 acted on these requests.

174. On or about March 23, 2021, Company-1 received a call from an official with the CAC in Shanghai regarding "illegal," politically sensitive meetings

occurring on Company-1's platform. The Shanghai CAC official provided Company-1 with Twitter handles and key words associated with the launch of these meetings and requested Company-1 block users from within the PRC. Also on March 23, 2021, XU WEI and other officials with the CAC, MPS and MSS in Hangzhou asked for someone at Company-1 to be made "available" and inquired about Company-1's capabilities for handling "illegal" meetings.

175. On or about May 24, 2021, an official with CAC in Beijing contacted an employee of Company-1 and requested vigilance on "sensitive" upcoming meetings on Company-1's platform, a reference to the approaching anniversary of the Tiananmen Square massacre. The CAC official in Beijing made specific mention of an upcoming event in Hong Kong that would feature Victim-12.

176. On or about June 3, 2021, a Company-1 employee received a call from CHEN YUANYUAN and another CAC official in Hangzhou, who conveyed a request to terminate a meeting on Company-1's platform commemorating the Tiananmen Square massacre organized by Victim-5 and Victim-5's organization.

WHEREFORE, your deponent respectfully requests that arrest warrants issue so that the defendant JIN XINJIANG (金新江), also known as "Julien Jin," CHEN YUANYUAN (陈媛媛), FU YIBIN (傅一彬), HUANG YIWEN (黄奕雯), also known as "Nicole Huang," JIN TAO (金涛), LIU ZHIYANG (刘智洋), SHEN ZHENHUA (沈振华),

SONG GUORONG (宋国荣), TIAN XINNING (田心宁) and XU WEI (徐威), may be dealt with according to law.

Joseph Hugdahl

JOSEPH HUGDAHL
Special Agent
Federal Bureau of Investigation

Sworn to me through the transmission of this
Affidavit by reliable telephonic and electronic means
pursuant to Federal Rule of Criminal Procedure 4.1, this
6 th day of April, 2023

[redacted]

THE HONORABLE SANKET J. BULSARA
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK