

DMP:AAS/RMT/DKK/ICR
F. #2020R00535

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- against -

XINJIANG JIN,
also known as "Julien Jin,"

Defendant.

----- 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 January 2019 and the present, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant XINJIANG JIN, also known as "Julien Jin," 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 BE FILED UNDER SEAL

COMPLAINT AND
AFFIDAVIT IN SUPPORT
OF APPLICATION FOR AN
ARREST WARRANT

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

No. 20-MJ-1103

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 the present, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant XINJIANG JIN, also known as “Julien Jin,” 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 seven 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)

¹ Because the purpose of this 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.

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 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. The Defendant and 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.

5. The defendant XINJIANG JIN, also known as “Julien Jin” (hereafter “JIN”), is a 39-year-old citizen of the PRC employed by Company-1 as the “Security Technical Leader.” In his capacity as “Security Technical Leader,” JIN is 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”). JIN, who resides in, and works from Company-1’s offices in, Zhejiang Province in the PRC, has been employed by Company-1 since 2016.

B. The PRC Government’s Suppression of Political Dissent and Religious Speech

6. The PRC is a one-party state, whose government is entirely controlled by the Chinese Communist Party (“CCP”).² 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

² 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.

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.

7. 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.

8. 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 Cyberspace Administration of China ("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.

9. 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 "*Guoan*," 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 Security Police or “*Guobao*,” routinely monitor, among others, Chinese political dissidents who live in the United States and in other locations outside the PRC. The PRC government, the MSS, and the First Bureau of 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.

10. 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.

11. 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.

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

II. The Criminal Scheme

13. As set forth below in detail, the investigation has revealed that JIN has conspired with others 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 at the direction and under the control of officials of the PRC government. Among other actions taken at the direction of the PRC government, JIN and others terminated at least four video meetings hosted on Company-1’s networks commemorating the thirty-first anniversary of the Tiananmen Square massacre, most of which were organized and attended by U.S.-based participants, such as dissidents who had participated in and survived the 1989 Tiananmen Square protests. Some of the participants who were unable to attend these meetings 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.

14. As described below, JIN, officials from the PRC government, 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 Company-1's users themselves. In particular, in May and June 2020, JIN, together with others, including others located in the PRC, acted to disrupt meetings held on the Company-1 platform to discuss politically sensitive topics unacceptable to the PRC government by infiltrating the meetings to gather evidence about purported misconduct occurring in those meetings. In fact, there was no misconduct; JIN and his co-conspirators fabricated evidence of TOS violations to provide pretextual justification for terminating the meetings, as well as certain participants' accounts. JIN then 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

15. 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,

16. 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')."

17. 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>>.

B. The PRC Government Blocks Company-1's Services in China

18. As set forth below, beginning at least as early as June 4, 2019, JIN and others led Company-1's efforts to comply with and implement PRC government censorship directives.

19. On or about June 4, 2019, JIN exchanged electronic messages with a group of individuals who are Company-1 employees, including Employee-1, notifying them of his efforts to collect information from social media to identify and block a group of Company-1's users who were planning video chat meetings to commemorate the thirtieth anniversary of the June 4, 1989 Tiananmen Square massacre.

20. Similarly, on or about August 22, 2019, JIN, Employee-1, and other individuals who are Company-1 employees exchanged electronic messages discussing a video meeting hosted by a Company-1 user on what one of the employees identified as a Company-1 server in the United States. In sum and substance, JIN stated that the host organization was a Chinese cult that frequently made use of Company-1's services and stated that the user account should be blocked due to the religious (specifically, Christian) nature of the content. JIN asked Employee-1 for instructions about how to handle the situation and whether the account needed to be deleted. Based upon electronic information gathered during the investigation, Employee-1 was located in the United States at the time. In response, Employee-1 directed JIN to place the account in a "quarantine" status, or to create a separate meeting region for the account with the apparent purpose of limiting the features

and capabilities of Company-1's services that were available to the user, and expressed the hope that doing so would cause the user to stop using Company-1's platform.

21. Based upon publicly available information, despite JIN's, Employee-1's, and Company-1's proactive efforts to censor political and religious discussions disfavored by the PRC government and the CCP, on or about September 8, 2019, the PRC government blocked PRC-based Internet users from connecting to Company-1's service. 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 of disrupting the ability of Company-1's fee-paying corporate customers (whose fees comprise the bulk of Company-1's revenue) to use Company-1's services to communicate with their employees and business partners in the PRC.

22. Based on electronic communications I have reviewed between JIN and other Company-1 employees between October 2019 and June 2020, over the course of multiple meetings between PRC government officials and Company-1 employees, PRC government officials indicated that Company-1 could resume operations in the PRC once Company-1 complied with PRC laws and regulations. The officials also directed Company-1 to prepare and submit to various PRC government agencies, including the Hangzhou office of the PRC's MPS, Network Security, "rectification" plans and reports to describe how Company-1 would do so.

23. Based on electronic communications I have reviewed between JIN and other Company-1 employees between October 2019 and June 2020, as well as documents located on the personal mobile devices of JIN and Employee-1, JIN, Employee-1, and other Company-1 employees in the United States and the PRC collaborated to prepare Company-

1's "rectification" plan. As part of the rectification plans submitted, Company-1 agreed to, among other measures, proactively monitor communications for content that included the expression of political views unacceptable to the PRC government, and to make JIN the primary liaison with PRC authorities for all requests. The rectification plans submitted to PRC authorities included JIN's work email address as the primary point of contact. Also as part of the submitted rectification plans, Company-1 pledged to migrate the data storage of the accounts of approximately one million "Chinese users" from the United States to the PRC, thereby subjecting these accounts to PRC law and process. It is not clear how Company-1 and the PRC authorities ultimately defined "Chinese users."

24. Company-1 also agreed to provide PRC law enforcement and national security authorities with special access to Company-1's systems. For example, on or about October 25, 2019, JIN, Employee-1, Company-1's CEO ("CEO-1") and others exchanged electronic messages to discuss a meeting that JIN had attended at the Hangzhou office of the MPS, Network Security. JIN explained that Company-1 had discussed with the MPS "the supervision of hot illegal incidents" and had committed to "proactively report and give them early warning on a regular basis." According to JIN, MPS officers had advised that they would also "convey hot spots to [Company-1]" and had asked Company-1 "to report how much resources and budget the company plans to invest in safety supervision." JIN further explained:

[T]hey also want me to provide them with some detailed lists of our daily monitoring; such as Hong Kong demonstrations, illegal religions, fund-raising, pyramid schemes, etc.; I also communicated with them. Before, there were some things that we were difficult to determine whether they were legal or illegal, and they would help determine them; In the future, I will often run to their unit, [provide] live demonstration and [engage in] various communication[s].

25. In the same series of communications, JIN advised the group that he would create five Company-1 accounts for officers of the MPS's Hangzhou Public Security Bureau, Cybersecurity Department to use on Company-1's PRC-based network, and explained that JIN and CEO-1 had agreed with the MPS to use a combination of Company-1's employee messaging system and WeChat (a PRC-based Internet messaging application) to communicate with PRC government officials and to exchange classified information. JIN emphasized that "[a]ll activities will be classified as secret internally and externally."

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

27. Based on my review of electronic communications between JIN, Employee-1, and other individuals who are Company-1 employees, even after the PRC government unblocked Company-1's service in the PRC, those individuals discussed continuing their work to comply with the PRC government's demands, and JIN stated that he met and communicated frequently with PRC government officials from several agencies in an effort to demonstrate Company-1's compliance with their requirements. For example,

on or about November 20, 2019, JIN, Employee-1, and the head of Company-1's Hangzhou office—to whom JIN reported—exchanged electronic messages to discuss blocking the account of the niece of a PRC national who is a vocal critic of the CCP on social media and who had fled from the PRC to the United States.

C. The PRC Government Demands Greater Control Over Company-1's Operations Worldwide

28. As set forth below, as demand for Company-1's video meeting services skyrocketed during the COVID-19 pandemic, 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.

29. In electronic messages from on or about April 3, 2020 that included JIN and Employee-1, JIN stated that MSS's preference was for Company-1 not to terminate meetings of target users immediately. Based upon my training and experience, having Company-1 keep certain meetings open would allow the MSS to obtain additional details on meeting participants, monitor the content of a meeting, and gain actionable intelligence on the pro-democracy movement.

30. On or about April 8, 2020, JIN sent an electronic message to Employee-1 stating that JIN had been summoned to a meeting with PRC government officials to discuss recent security and privacy issues. Later that day, JIN advised Employee-1 that the PRC government had directed Company-1 to develop the capability to respond to a PRC government demand to terminate an illegal meeting, account or recording within one minute, which JIN referred to as the one-minute processing requirement.

31. In his electronic communications with Employee-1 on or about April 8, 2020, JIN provided the example of shutting down political meetings that were in progress and noted he was still working on several investigations for MSS. In response, Employee-1 suggested that another U.S.-based employee of Company-1 (“Employee-2”) could provide 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 had previously sent a message to Employee-2 directing Employee-2 to cooperate with JIN.) Based on my training and experience, I assess that Employee-1 endeavored to get JIN access to such a machine in order to give JIN direct access to Company-1’s U.S.-based systems, so that JIN could comply with instructions from the PRC government. JIN replied that the matter needed to be handled confidentially, separate from Company-1’s regular support function and stated that he would not be able to document his actions in a report. Employee-1 replied, “i see.”

32. On or about April 15, 2020, JIN exchanged electronic messages with Employee-2, the U.S.-based employee that Employee-1 had directed to cooperate with JIN’s work. JIN wrote: “Yesterday, [MSS] asked me to track down a bad organization overseas.” Employee-2 asked JIN, “Is there someone applying for an account here and doing bad things in China? Otherwise, it has nothing to do with [MSS].” JIN replied “Almost. But even abroad, political attacks on leaders are not allowed.” He further stated, “If you need approval, you can talk to [Employee-1] in person.” Employee-2 responded with a smiley face emoji. JIN then clarified, “Don’t write mail.” Employee-2 responded, “Just ask for instructions.” Employee-2 then continued, “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.” JIN responded, “We have so many people and multinational companies in China, we have to take care of both sides😊.”

33. On or about April 29, 2020, JIN and Employee-1 exchanged electronic messages regarding a conversation JIN had had with Company-1’s U.S.-based Chief Operating Officer (“COO”) and General Counsel about the PRC government’s one-minute processing requirement. JIN explained that his “workaround permissions” could meet most of his needs, but stated that Company-1’s COO and General Counsel, as well as Company-1’s head of compliance, had stated that Company-1 was obliged to report the PRC government’s one-minute processing requirement to Company-1’s U.S.-based compliance team. JIN commented that this did “not comply with the principle of confidential processing required by the powerful CN agency,” using “CN” as an apparent shorthand for China. JIN further explained, “The CN department I contacted allowed me to check their documents, but would not leave any proofs/photos and other things that might be exposed.” Employee-1 advised JIN, “All your access rights on us clusters will be taken away. But will retain the permissions of cn cluster”—referring to the U.S.-based and PRC-based server clusters that Company-1 used to store user data and provide Company-1’s service to users. JIN replied, “Many things cannot be done, and Net Security”—referring to the PRC’s MPS, Net Security—“will not agree. Unless we also voluntarily block the international version of [Company-1] on the mainland.” Employee-1 then asked JIN, “What is your current workaround?” JIN responded, “tos admin, superadmin is no longer needed.” Based upon information gathered during this investigation and the foregoing, I believe “tos admin” is a

reference to administrative privileges assigned to certain Company-1 employees to use in enforcing Company-1's TOS.

34. In the same exchange of electronic communications, after Employee-1 asked "Can this access user data," JIN replied "Can deal with illegal accounts." Employee-1 explained that "The current requirement"—apparently referring to Company-1's internal restrictions—"is that domestic engineers cannot access the data of us clusters"—indicating that PRC-based software engineers were not permitted to access user data stored on U.S.-based servers. JIN responded, "Net Security's requirement is that [the employee] must have the authority to directly handle it, and it must be handled within one minute. For example, including U.S. users, if the issue of June 4th is being discussed in a meeting, it must be handled within one minute of [the meeting being reported], otherwise will be [rate] as security non-compliant." Based upon information gathered in this case, my experience investigating cases involving the PRC, and publicly available information, the example of "the issue of June 4th" refers to discussions of the June 4, 1989 Tiananmen Square massacre, and JIN's statement reflects the PRC government's demand that Company-1 terminate meetings discussing the Tiananmen Square massacre, including meetings involving U.S.-based users.

35. On or about May 7, 2020, JIN wrote an electronic message to other individuals who are Company-1 employees stating that, even if other U.S. social media and search companies had no business in the PRC, they still terminated accounts and posts at the request of the "CN zf." Based on open source information and my training and experience, the "CN" in "CN zf" refers to "China" (the PRC) and "zf" is shorthand for *zhengfu*, a Chinese word for government. JIN continued that the CCP infiltrated the United States,

and, even if Company-1 withdrew entirely from the PRC, Company-1 would still need to deal with “CN zf” requests in order to avoid future attacks.

36. On or about May 7, 2020 and May 8, 2020, JIN, Employee-1 and Employee-2 exchanged electronic messages about the PRC government’s one-minute processing requirement. In those communications, JIN explained that he was unable to obtain billing information for a large customer as JIN could no longer access Company-1’s U.S.-based servers. JIN asked Employee-2 to restore JIN’s access, so that JIN could use Employee-2’s remote computer for emergency troubleshooting. Employee-2 agreed and indicated that he/she would meet with JIN later. JIN thanked Employee-2.

37. On or about May 19, 2020, JIN and Employee-1 exchanged instant messages. JIN warned Employee-1 that “6.4”—the June 4th anniversary of the Tiananmen Square massacre—was coming soon, and that the PRC “Internet Police“ were tracking all “cn users” on Company-1’s U.S.-based server cluster. Employee-1 responded, “[U]nderstood.”

38. 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:

JIN: Recently the MSS, Net Security and Net Police have been coming to our company frequently, and we are handling things carefully. The MSS requests that we sign the NDA and that we cannot disclose their request. In it, related to U.S. data, we are asking for instructions from the U.S., we need to discuss and determine a standard.

E-1: Ok. Did the Shanghai side reach out?

JIN: What the MSS is asking for are mostly politics related, therefore they request that we cannot disclose it, otherwise it will greatly impact our country's reputation.

JIN: It was the Shanghai Security Agency that sent those people.

E-1: Understood.

JIN: CN [China] has implemented real-name registration/verification, so there are not many that do bad things anymore. All are from the U.S., if we don't handle them well, net security will ban all [Company-1] overseas servers, so I respectfully ask you to take this seriously.

...

E-1: We will hurry and ban all the free accounts from US04 [a Company-1 server].

E-1: Our reputation is already bad regardless. 😊

JIN: We found out today that up until now, [Company-1's U.S. internet domain] still allows CN free registration...

E-1: Will release a web package to fix it tomorrow.

JIN: From net security's perspective, as long as it is a CN user, we need to handle it no matter where it is; if we don't handle it, they will initiate gfw or other methods to ban it.

In this context, based upon my experience investigating cases involving the PRC and this matter, I believe "NDA" refers to a "non-disclosure agreement," the "Shanghai Security Agency" refers to the Shanghai State Security Bureau, a regional office of the MSS, and "gfw" refers to the Great Firewall of China. In addition, JIN's statement "as long as it is a cn user, it will be processed no matter where it is" indicates that the MPS's definition of "Chinese users" includes persons of Chinese descent physically located in the United States.

D. JIN and Employee-1 Censor the Political and Religious Speech of Company-1 Users Located Outside the PRC at the Direction of the PRC Government

39. As set forth below, JIN collaborated with PRC government officials to proactively identify meetings that the officials might deem objectionable. In the spring of 2020, despite being deprived of access to Company-1's U.S.-based servers, JIN caused Company-1 employees based in the United States to assist him with disclosing U.S.-based user data to the PRC government and censor political and religious speech. By June 2020, his efforts to comply with the PRC government's demands culminated in 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.

40. On or about May 21, 2020, JIN sent an electronic message to a PRC law enforcement officer he referred to as "Officer Jin," which message contained unique identifiers for meetings hosted on Company-1's U.S.-based servers, as well as the passwords for a Company-1 meeting scheduled to take place on or about May 22, 2020. Based upon publicly available information, this meeting was organized to commemorate the forthcoming anniversary of the Tiananmen Square massacre. After notifying "Officer Jin" of the meetings that would be hosted on Company-1's U.S.-based servers with content that JIN characterized as in violation of PRC law, JIN sent an electronic message to a group of Company-1 employees, including Employee-1, 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. Based on the investigation and my training and experience, "cybersecurity org" refers to the CAC and/or MPS.

41. On or about May 22, 2020, JIN notified Company-1 compliance employees in the United States, including Employee-1, that, on or about May 15, 2020, a prominent PRC dissident based in Hong Kong (“Dissident-1”) had hosted a meeting using Company-1’s service using Company-1’s U.S. clusters. Based upon publicly available information, I know that Dissident-1 provided support to the Tiananmen Square protesters in 1989 and has participated in Hong Kong politics as a pro-democracy activist. After JIN sent his message, several Company-1 employees, including Employee-1, exchanged electronic messages in which they identified several scheduled meetings that they described as “political” and that were associated with Dissident-1’s Company-1 account.

42. On or about May 22, 2020, JIN received a message indicating that Company-1 suspended and terminated Dissident-1’s account prior to these planned “political” meetings. JIN thanked the U.S.-based team for the prompt action that safeguarded Company-1’s business in the PRC.

43. Also on or about May 22, 2020, JIN used an electronic message to advise a U.S.-based group of Company-1 employees, including Employee-1, that Company-1 was at risk because its users were hosting meetings with religious themes absent the requisite “religious service license” in the PRC. JIN advised Employee-1 and others 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. In response, Employee-1 provided JIN with Chinese characters identifying what appears to be a U.S.-based Company-1 account holder, together with an IP address resolving to ChinaNet Yunnan Province Network in Yunnan, PRC. Employee-1

subsequently terminated the associated user account on the basis of a purported TOS violation and provided JIN with user account metadata. Based on electronic messages exchanged with other Company-1 employees, Employee-1 cited a TOS violation committed by the meeting participants as the justification for terminating the account. JIN noted the account owner would still have access to Company-1's free service and requested forced termination of that access as well. Company-1's U.S. team complied with JIN's request.

44. Similarly, in an exchange of electronic messages between JIN and a PRC law enforcement official on or about May 26, 2020, the official asked JIN for the account information for the individual hosting a meeting room in Company-1's U.S. data cluster. JIN explained that Company-1 employees like JIN who were based in the PRC could not access data in the United States. JIN then exchanged electronic messages with Employee-2, who provided the information to JIN. JIN then passed the information electronically to the PRC law enforcement official.

45. JIN also sent electronic messages to task Company-1's U.S.-based employees, including Employee-1, with providing him with user account information requested by the MSS and MPS's Domestic Security Police. On or about June 1, 2020, 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 "Chinese" participants in a Company-1 meeting organized by a prominent U.S.-based dissident ("Dissident-2") and hosted on Company-1's platform on or about May 31, 2020.

46. Based upon publicly available information and interviews conducted in this case, Dissident-2 was a student leader in the 1989 Tiananmen Square protests and has been an outspoken advocate for human rights and the advance of democracy in the PRC.

Dissident-2, who is based in the United States, used the Company-1 account of an associate (“Associate-1”) to host the May 31, 2020 meeting commemorating the Tiananmen Square massacre.

47. Employee-2 agreed to provide JIN with responsive data to the MSS request for information on Dissident-2’s May 31, 2020 meeting by disclosing Associate-1’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 Associate-1’s account and provided JIN with confirmation of the termination; this communication included Associate-1’s true name and email account. On or about June 1, 2020 and in a separate chat involving JIN and Employee-2, Employee-2 sent JIN numerous records regarding Associate-1’s account, including documents with details on all of Associate-1’s prior meeting history on Company-1’s platform, as well as the IP addresses from which Associate-1 joined the meetings. Employee-2 also provided JIN with multiple documents containing what appears from my review to be the names and IP addresses used by all participants in Dissident-2’s May 31, 2020 meeting. The participant data pertained to several users who joined from IP addresses in the U.S.

48. Dissident-2 has informed the FBI, in sum and substance, that, leading up to the May 31, 2020 meeting, Dissident-2 held several practice meetings in preparation. Initially, Dissident-2 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, Dissident-2 formed the view that PRC authorities were already surveilling the participants. As a result of this security concern,

Dissident-2 directed Associate-1 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.

49. Dissident-2 further informed the FBI, in sum and substance, that PRC authorities pressured several potential meeting speakers in the PRC not to attend Dissident-2's meeting on the Company-1 platform. According to Dissident-2, 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 Dissident-2 with a pre-recorded video to be played during the meeting on the Company-1 platform; Dissident-2 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 Dissident-2 was seen by more than 500 viewers.

50. In addition, based upon interviews conducted during the investigation and review of open source information, another anti-CCP demonstrator who currently resides in Australia (the "Australian participant") received a WeChat 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. The Australian participant refused and recorded the call. During the May 31, 2020 meeting on Company-1's platform discussed above, the Australian participant discussed that call involving the MPS. On or about June 1, 2020, the Australian participant's parents received an electronic message from the MPS, which message contained a screenshot

showing the Australian participant in the May 31, 2020 meeting on Company-1's platform. The Australian participant's father then sent the participant an electronic message asking whether the participant wanted his/her parents "dead." The Australian participant has stated, in sum and substance, that he/she was distressed by the pressure exerted by PRC officials on the participant and the participant's family, particularly after the May 31, 2020 meeting on Company-1's platform.

51. On or about June 1, 2020, JIN sent an electronic message advising Employee-1 and other U.S.-based employees of Company-1 that the MPS, Domestic Security Police, had requested "Xinjiang users' data, user category, the number of the registered, and number of participants, etc." According to JIN, the MPS further requested that the data be provided no later than "8:30 (China time)" the following day. 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.

52. In the same series of communications, 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, 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, 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.

53. As discussed above, 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 JIN asked for help with the PRC government's data request related to Xinjiang, including Employee-1, were located in the United States.

54. On or about June 1, 2020, in response to JIN's request, a Company-1 employee in the United States sent JIN an electronic communication containing a spreadsheet with approximately 23,000 account IDs and user IDs for Company-1 accounts.

E. JIN and Other Company-1 Employees Terminate June 3, 2020 and 4, 2020 Meetings Commemorating the Tiananmen Square Massacre

55. As discussed below, JIN 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 JIN, Company-1 employees, and others based in the PRC, to identify participants in and to disrupt these meetings for pretextual reasons. 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 the TOS. In fact, no such discussions or violations of the TOS were occurring. Through their scheme, JIN 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.

56. 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. 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

57. 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 (“Dissident-3”) organized a meeting on Company-1’s platform to commemorate the anniversary of the Tiananmen Square massacre (the “June 3 Meeting”). 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. Dissident-3 is a resident of the Eastern District of New York and participated in the June 3 Meeting from his residence. 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.

58. Based upon law enforcement interviews and my review of electronic communications, including meeting invitations, I assess that Dissident-3 initiated the June 3 Meeting using an incorrect meeting number (the “Incorrect June 3 Meeting”) that had not been circulated.

59. On or about June 3, 2020, at approximately 6:25 AM EDT, JIN sent a message to several individuals who work at Company-1, 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. It is not clear how JIN or PRC law enforcement obtained this nonpublic information. JIN’s notification included the information that the meeting would occur at “7:00 AM New York” and referenced a meeting number. As noted above, the meeting number was not publicly available. 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.

60. Based on witness interviews and metadata regarding the Incorrect June 3 Meeting, that meeting began at approximately 7:04 AM EDT, hosted by a Company-1 account linked to Dissident-3. None of the invited participants participated in the Incorrect June 3 Meeting; the only participants appear to have used Company-1 profiles associated

with nonexistent email accounts or email accounts that appear to have been created for the purpose of disrupting the meeting.

61. By approximately 7:30 AM EDT, 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 (the “Assistant”). Other participants in the meeting included residents of the Eastern District of New York.

62. 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 Dissident-3’s Company-1 account, rather than the Company-1 account of the Assistant who was actually hosting the meeting. 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 Dissident-3’s Company-1 account was being used to incite racial division, violence and resistance. Moreover, although the June 3 Meeting was conducted in Mandarin—except for a prayer that was given in German but translated into Mandarin—all of these complaints were made in English.

63. 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, based upon publicly available information, resides in Japan and is a vice-president of a group established in 1989 to promote democracy in the PRC (the “Dissident-4”). The email account in the name of Dissident-4 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 Dissident-4 is also associated with a Company-1 account in the name of Dissident-4, which account attended some of the June 3 Meeting. 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. Notably, the investigation has found no evidence showing that Dissident-4 attended the June 3 Meeting.

64. Based upon my review of information provided by email service providers, other electronic communications, and my training and experience, one of JIN’s co-conspirators (“CC-1”) created and used several different email accounts in furtherance of the conspiracy’s activities on June 3, 2020, and June 4, 2020. Specifically:

- a. CC-1 used an email account created in his/her own name (the “HYW ACCOUNT”). The subscriber name for that account is CC-1’s name.
- 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 internet service provider in Hong Kong that provides internet service for residential customers. The first such account (the “QAZ ACCOUNT”) was subsequently updated to include CC-1’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. The 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, an individual who was logged in to the HYW ACCOUNT accessed multiple chat threads about current affairs on 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, an individual using 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 exactly the same time as access by the other account. Based on my training and experience and the foregoing, CC-1 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.

65. 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, an individual logged in to the HUH ACCOUNT conducted internet searches for “[Dissident-3] [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 Dissident-3.

66. Between approximately 8:14 AM and 8:25 AM EDT, CC-1 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 the Assistant’s account, which was then hosting Dissident-3’s meeting, was inciting racial conflicts, violence, and resistance:

- a. At 8:14 AM and 8:15 EDT, CC-1 and others used the FOREIGN ACCOUNTS to write that the Assistant’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 [sic] of a meeting that incites racial discrimination.”
- d. The other two emails, at 8:15 AM 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 were used in an apparent attempt to trigger Company-1 TOS violations on June 4, 2020, as discussed below.

67. 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 address attended the June 3 Meeting on Company-1's platform.

68. Between approximately 7:53 and 7:56 AM EDT, JIN sent via electronic messages to other Company-1 employees located in the U.S. two images, the first of which included Dissident-3's name, the name of Company-1, and "2020/6/3"—a reference to the June 3 Meeting. The second image contained what appeared to be a screenshot of a Company-1 meeting. JIN wrote "meeting!" and asked the U.S.-based employees to suspend the relevant account. JIN urged other Company-1 employees located in the United States to shut down the account hosting the June 3 Meeting—which, at that time, was the Assistant and not Dissident-3—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. After a request from Company-1 employees located in the United States, JIN provided the meeting details at approximately 8:13:10 AM EDT. Notably, JIN requested suspension of the Assistant's account before Company-1 had received any complaints specific to the Assistant (which first arrived at 8:14 AM EDT). In the communications, a Company-1 employee reported that he/she had terminated the meeting at

approximately 8:16:58 AM EDT and also reported that he/she had terminated the Assistant's account, after noting that account was a "free" account rather than a paid one.

69. Though 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 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 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>>.

70. Although 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.

71. After learning that the June 3 Meeting had been shut down, JIN thanked the other employees and noted at approximately 8:23 AM EDT—nine minutes after the complaints were first lodged against the Assistant—"We reported several abuse for this meeting. So we may refer to this they against tos." JIN also warned the U.S.-based Company-1 employees that the "cyber people here" believed that Company-1 should take "all measures to terminate illegal activities by ourselves," as PRC authorities expected Company-1 to ensure there were no more political and anti-PRC public meetings. Based upon the investigation and my training and experience, "cyber people here" refers to officers of the MSS and/or the MPS. One of JIN's subordinates later sent an electronic message to

JIN and other employees assigned to the Company-1 group monitoring the use of Company-1's systems for the expression of political views unacceptable to the PRC government, asking if the PRC "internet police," which, as discussed, is a reference to the MPS, were satisfied with the group's measures on June 3, 2020.

The June 4, 2020 Meeting

72. 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 ("Dissident-5") 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.

73. Based upon interviews conducted during this investigation, the lead organizer of Dissident-5's meeting ("Organizer 1") was him/herself a protester during the Tiananmen Square massacre. On or about May 29, 2020, Organizer 1 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, Organizer 1 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.

74. 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 meeting created a list of designated speakers, and set the meeting to settings 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 user names that could be PRC government representatives seeking to infiltrate the meeting.

75. As described below, CC-1 used at least three email accounts in an effort to disrupt the June 4 Meeting. Each of those accounts emailed JIN's work address to report purported violations of Company-1's TOS related to the June 4 Meeting. Notably, 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 JIN's email was provided as a primary contact to the PRC government as part of Company-1's written "rectification" proposals. 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, JIN does not appear to have had any other direct communication with the accounts used to send the false reports. Accordingly, it appears that CC-1 and other possible co-conspirators obtained JIN's email address directly from the rectification report, from other PRC government official(s) communicating with JIN on Company-1's rectification plans, or from JIN himself through some other means of communication.

76. On or about June 4, 2020, at approximately 3:53 AM EDT, JIN notified U.S.-based Company-1 employees of “[a]nother serious June 4th meeting by [Dissident-5] (Today),” noted that Dissident-5 “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?”

77. At approximately 8:25 AM EDT, after Company-1 had not yet shut down the meeting, 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] us as abuse meeting, then you US may have evidence to suspend it.” Notably, metadata regarding the meeting suggests that one of JIN’s associates at Company-1, located in the PRC, attended all iterations of the June 4 Meeting. After receiving JIN’s request, Employee-1 terminated the account used to host Dissident-5’s meeting before the actual commemoration of the Tiananmen Square massacre had begun, as well as the host account.

78. Based upon interviews conducted in this investigation and my review of electronic data gathered during the investigation, after that meeting was terminated and the 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 room on Company-1’s platform.

79. Again, based upon information provided by email service providers, CC-1’s search activity suggests that members of the conspiracy used false complaints to terminate Dissident-5’s second meeting on June 4, 2020. That information also shows that,

starting at approximately 8:41 AM EDT, CC-1 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 [ISIS] 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.”

80. The HUH ACCOUNT, the QAA ACCOUNT, and the QAZ ACCOUNT, all associated with CC-1 as discussed above, 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 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”);³ (2) a Company-1 profile with the name “Oystein Alme” 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 JIN with the same subject, “Someone in this group incites

³ 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.

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 “[Dissident-3 email account] this account is constantly inciting racial conflicts an [sic] violence and pornography.” Significantly, although this email referred to Dissident-3’s email account, Dissident-3 did not attend the June 4 Meeting; instead, Dissident-3 hosted the June 3 Meeting.
- e. At approximately 9:57 AM EDT, the QAA ACCOUNT emailed JIN with a subject that identified Dissident-3’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: “Oystein Alme,” 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 Dissident-3, Dissident-3 did not attend the June 4 Meeting.
- f. Between approximately 9:34 AM and 10:16 AM EDT, a Company-1 user whose account was associated with the QAZ ACCOUNT entered the June 4 Meeting.
- g. At approximately 9:57 AM EDT, the QAZ ACCOUNT emailed 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: “Oystein Alme,” 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 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 in paragraph 19, 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.

81. 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 notable, 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, members of the conspiracy introduced at least one image that purportedly incited violence and then reported the image they introduced. Moreover, the account for the user profile “Free man” was 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 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.

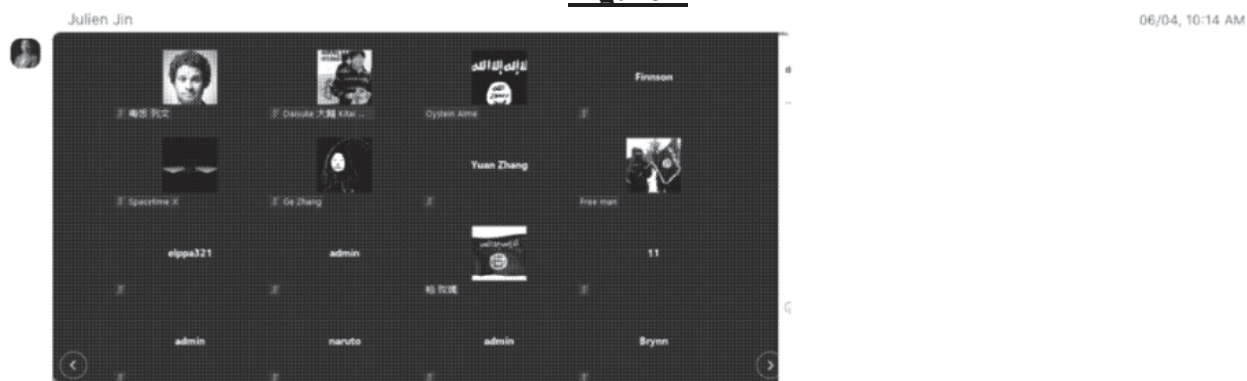
82. In total, based upon my review of electronic communications obtained during the investigation, 14 email complaints related to the June 3 Meeting and the June 4 Meeting were sent to JIN on or about June 4, 2020, between 9:54 AM and 10:16 AM EDT—a period of approximately 20 minutes. As set forth above, 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 JIN appeared to be from ten different complainants, but, based on the information set forth herein and my training and experience, I believe that they represented coordinated efforts by PRC-based co-conspirators including CC-1. 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 4 Meeting was conducted in Mandarin, 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 Company-1 is based in the United States and that the likely decision-makers for terminating any meetings would be English speakers.

83. At approximately 9:42 AM EDT on or about June 4, 2020, JIN sent an message to Company-1 employees monitoring content that included the expression of

political views unacceptable to the PRC government, in which message JIN told his subordinates that “there are so many of own people, friendlies.” After one of JIN’s subordinates asked if the “friendlies” were from Company-1, JIN replied that MPS’s “Net Security” was “working overtime.”

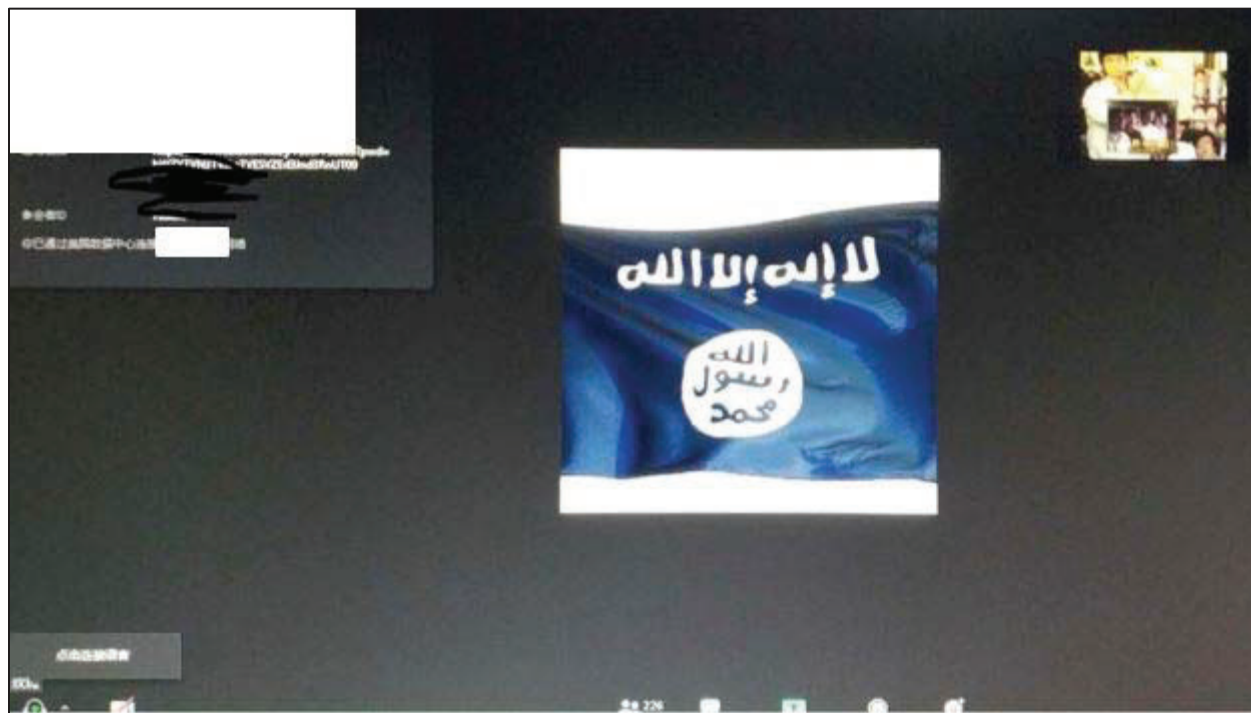
84. At approximately 10:05 AM EDT on or about June 4, 2020, shortly after some of the aforementioned email complaints had been sent, JIN wrote to various Company-1 employees: “We get report about Someone inside this group incites terrorism and violence . . . They also send such abuse info to [Company-1] us site, I think [a Company-1 employee’s] tos team received that too.” JIN added, “there’re [sic] IS [Islamic State] flag on someone’s photo. Can you suspend that as terrorism and violence meetings ?”

85. After JIN sent an electronic message with a screenshot of a user profile with the Islamic State flag (see Figure 1), Employee-1 agreed to terminate the meeting as well as the paid account used to host the Dissident-5’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. JIN thanked Employee-1 and others for their immediate support. The image provided by JIN appears from my review to be identical to images attached to two emails JIN received at 9:54 AM and 10:00 AM EDT, from two different email addresses.

Figure 1

86. In an exchange of electronic messages among JIN and other individuals who were the Company-1 employees monitoring content that included the expression of political views unacceptable to the PRC government, one of JIN's subordinates asked JIN at approximately 11:42 AM EDT, "What the heck, ISIS?" The subordinate continued, "I also changed my profile picture, joined in to take a look." He then asked JIN, "So how was it, the Internet Police was satisfied with our measures yesterday?" Notably, one of the complaints sent to Company-1 (see redacted Figure 2 below) included a screen capture of a user profile from the meeting containing the image of an ISIS flag. That screen capture contained a Company-1 identification intentionally marked out with what appeared to be a computer-generated black marker. Based upon my training and experience, the blacking out of information was designed to disguise the sender's identity in order to conceal that the sender of the complaint was the user displaying the ISIS flag or another individual working with the complainant.

Figure 2



87. 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.

88. 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 (“Speaker-1”) reported sending a message on or about June 3, 2020 via WeChat to his/her father’s WeChat account indicating that Speaker-1 was going to participate in an event about the Tiananmen

Square massacre. After sending the message, Speaker-1 received a message on his/her WeChat account that Speaker-1'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 Speaker-1's father in the PRC. During the call, the MPS instructed Speaker-1's father to tell Speaker-1 to stop speaking out against the CCP and to support socialism and the CCP. The MPS also inquired about Speaker-1's life in the U.S. and asked when Speaker-1 intended to return to the PRC.

89. 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 the Australian participant.

The Conspiracy's Use of the Names of Real Individuals

90. As discussed 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.

91. 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 contains the name of an individual who is a student leader and participant in the 1989 student protests at Tiananmen Square. That individual 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.

92. The Company-1 account created in the name of Dissident-4, associated with an email address in the name of Dissident-4, similarly would have given the impression that an individual known to be critical of the PRC government was participating in the June 3 Meeting.

93. Finally, the Company-1 account associated with the name “Øystein Alme” was used to display various images associated with terrorism and pornography. Based upon publicly available information, Øystein Alme is a Norwegian writer known for the 2006 publication of the book titled “Silenced – China’s Great Wall of Censorship” and is associated with a news publication regarding Tibet. As a result, upon information and belief, members of the conspiracy used Alme’s name in order to gain entry to the meeting—because meeting organizers who were screening participants would not have rejected the real Alme—and to give the impression that Alme was participating in the meeting when he was not.


Continued Efforts to Shut Down Meetings

94. Based upon my review of electronic communications between JIN and other individuals who are Company-1 employees, on or about June 5, 2020, JIN notified Company-1 employees in the United States of his receipt of a message from the “CN cybersecurity”—as discussed, a reference to officers of the MSS and/or the MPS—indicating that 48 communications platforms did not 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 on the basis of purported TOS violations.

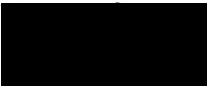
95. Based upon my review of electronic communications between JIN and other individuals who are Company-1 employees, when senior Company-1 executives asked JIN to provide documentation detailing all of the PRC law enforcement requests he had received in connection with the action taken against accounts hosting Tiananmen Square anniversary meetings, JIN stated that there was no legal documentation for the PRC government requests to terminate the “June 4th political accounts.” Instead, 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.

WHEREFORE, your deponent respectfully requests that an arrest warrant issue so that the defendant XINJIANG JIN, also known as “Julien Jin,” may be dealt with according to law.



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
19th day of November, 2020



THE HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK