

EXHIBIT 38

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

IN THE MATTER OF THE SEARCH OF:

Redacted

DEVICES FOUND WITHIN THE
PREMISES OR ON THE PERSON OF TAO;
AND INFORMATION ASSOCIATED
WITH AN EMAIL ADDRESS STORED AT
GOOGLE

Case No. 19-mj-8187-JPO

Filed Under Seal

**APPLICATION AND AFFIDAVIT IN
SUPPORT OF A SEARCH WARRANT**

I, Stephen Lampe, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search three premises: (1) **Redacted**; (2) **Redacted**; (3) **Redacted** (hereafter "PREMISES"); along with (4) any computer and computer media located therein; and, finally, (5) information associated with certain accounts that are stored at premises controlled by Google LLC, an email provider headquartered at **Redacted** California, 94043, in the Northern District of California ("Google," also "the Provider"). The PREMESIS and other locations to be searched are described in the following paragraphs and in Attachment A. The items and evidence for which to be searched are described in Section I of Attachment B. The request to search for item (5), the information stored by Google, is made pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), requiring Google to disclose to the government copies of information (including the content of communications) further described in Section II of Attachment B. Upon receipt of the information described in

Section II of Attachment B, government-authorized persons will review that information to locate the items described in Section III of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since December, 2014. I am presently assigned to the Kansas City Division Counter-intelligence Squad, which investigates, among other things, matters related to 18 U.S.C. § 666 and 18 U.S.C. § 1343 violations (the Subject Offenses). Further, I have received basic training in cyber-based investigative techniques pertaining to the use of the internet and email in the furtherance of crimes.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711.

LEGAL BACKGROUND

5. Title 18, United States Code, Section 666 provides that “[w]hoever, if the circumstances described in section (b) of this section exists . . . being an agent of an organization, or of a State, local, or Indian tribal government, or any agency thereof . . . corruptly solicits or demand for the benefit of any person or accepts or agrees to accept, anything of value from any person, intending to be influenced or rewarded in connection with any business, transaction, or

series of transactions of such organization, government, or agency involving any thing of value of \$5,000 or more” is a violation of federal law.

6. The circumstances described in section (b) “is that the organization, government, or agency receives, in any one-year period, benefits in excess of \$10,000 under a Federal program involving a grant, contract, subsidy, loan, guarantee, insurance, or other form of Federal assistance.” The term “agent” means “a person authorized to act on behalf of another person or a government and, in the case of an organization or government, includes a servant or employee, and a partner, director, officer, manager, and representative. The term “government agency” means “a subdivision of the executive, legislative, judicial, or other branch of government, including a department, independent establishment, commission, administration, authority, board, and bureau, and a corporation or other legal entity established, and subject to control, by a government or governments for the execution of a governmental or intergovernmental program.”

7. Title 18, United States Code, Section 1343 provides that transmitting “by means of wire, radio, or television communication” any “writing, signs, signals, pictures or sounds” (or causing any such false statements to be transmitted), in interstate or foreign commerce, for the purpose of executing “any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises” is a violation of federal law.

PROBABLE CAUSE

Overview

8. Feng “Franklin” Tao (Tao) is an associate professor and researcher at the University of Kansas (KU) Center for Environmentally Beneficial Catalysis (CEBC) located at the [REDACTED] Redacted

CEBC's research focuses on sustainable technology to conserve natural resources and energy. The CEBC performs proprietary research as well as United States Government (USG) funded research. As explained in detail below, Tao maintained his employment at KU despite holding another position at a Chinese university, in violation of KU policy. As also explained below, Tao made false statements and failed to report his outside employment to KU, which enabled Tao to keep his KU job as well as to work on USG-funded research.

9. Tao, as of May 16, 2019, as a KU employee, worked on research funded by two U.S. Department of Energy contracts, and four U.S. National Science Foundation contracts. Of note, Tao’s research included studies utilizing Ambient-Pressure X-ray Photoelectron Spectroscopy (AP-XPS), a surface chemical analysis technique, funded by the Department of Energy.

10. Kansas Board of Regents policy requires faculty and staff of Regents institutions to file a conflict of interest report upon employment and at least annually thereafter. A KU online identification (ID) was and is required to access the online reporting system. The policy indicated that outside employment can result in real or apparent conflicts regarding commitment of time or effort. As an employee of KU, Tao was required to file these reports. Since

December 9, 2014, Tao has filed five conflict of interest reports via the online reporting system, potentially violating Title 18, United States Code, Section 1343. The most recent report filed by Tao was on September 25, 2018. Tao did not disclose outside employment on any of these reports. As such, Tao was able to maintain employment with KU, which provided him access to USG research funds through the KU Center for Research (KUCR). Portions of Tao's salary were paid through USG research funds, potentially violating Title 18, United States Code, Section 666. KU maintains that if Tao had disclosed full-time employment with an entity other than KU, Tao would not be authorized to maintain employment with both entities at the same time.

Tao Held Outside Employment in China
in Violation of KU Policy

11. While working as a professor at KU, Tao also held a position in China without reporting it. Between approximately April 2019 and the time of this filing, both KU and the FBI have received a series of complaints regarding Tao, both anonymously and from an individual claiming to be a former post-doctoral student sponsored by Tao to study in the United States (Student #1). The sum and substance of the complaints were that Tao had taken a Changjiang Professor position in China, which Student #1 explained was a talent program¹ sponsored by the Chinese government. According to Student #1, Tao took that position in May

¹ The term "Chinese Talent Plans" refers collectively to hundreds of diverse plans designed by the Chinese government to recruit, cultivate, and attract high-level scientific talent in furtherance of China's scientific development, economic prosperity, and national security.

of 2018. Student #1 stated that the position required a five-year contract with the Chinese university as well as a requirement to be physically present in China for approximately 9 months a year. Student #1 also provided what purports to be an unsigned contract between Tao and Fuzhou University (FU) in China.² The contract is titled “Changjiang Scholar Distinguished Professor Employment Contract.” The appointment of the contract was from May 1, 2018, to April 30, 2023. Notably, the start date listed in this contract is *before* Tao’s September 2018 statement to KU that he did not have any outside employment. Pursuant to the contract, Tao is to be a full-time employee of FU, and is to be provided a job incentive of 550,000 Chinese Yuan (approximately \$80,070 USD)³ per year to include the Ministry of Education’s Distinguished Professor award of 200,000 yuan (approximately \$29,116 USD), plus base salary, basic performance salary, and a housing allowance. Fuzhou University, pursuant to the terms of the contract, shall provide Tao research labs, equipment (including a certain class of equipment valued at approximately 10 million yuan (approximately \$1,455,816 USD), and research funds worth 20 million yuan (approximately \$2,911,632 USD). In return, the contract

² Student #1 has given conflicting statements about how she obtained the unsigned contract. She told agents in person that Tao’s secretary had given it to her. In an email to agents later that same day, she said she hadn’t been truthful earlier and that she had downloaded the contract from Tao’s email account after Tao gave her the password for another account and asked her to assist him in writing grant submissions – she used the same password to access Tao’s email. At this time I am unsure how she obtained the contract, but I suspect she obtained it by hacking into Tao’s email account (prior to any contact with agents). She also stated that she provided the contract to KU and to the FBI because she was angry with Tao over not crediting her on a published research article, which I have no reason to doubt.

³ Conversion of Chinese Yuan and US Dollar based on US Federal Reserve Bank exchange rate for June 30, 2019 of 6.869 RMB to 1 USD.

specifies that Tao will train talent (which involves teaching one physical chemistry class every academic year), recruit and advise at least two or three doctoral students and at least three to four master's students per year, and develop internationally cooperative research programs and academic programs with international peers. Pursuant to the contract Tao is required to apply for the nation's major scientific research projects and publish more than 60 research articles. The contract stipulates that all Tao's achievements in education and scientific research obtained during the term of appointment shall be considered achievements of the position itself as enforced by national intellectual property rights, laws, statutes and regulations.

12. Open source reporting, some of which was provided by Student #1 as well as anonymously, corroborates many of the above-described complaints. For example, text from the website, gaokeyan.com, titled "Fuzhou University: Outstanding Talent Programs," lists Tao as the most recent recipient of the Changjiang Scholar award in the year 2017. An online news article dated in or around June 2018, from fuzhou.xuexiaodaquan.com, is titled "Secretary Chen Yongzheng Pays a Visit to the School of Chemistry's 'Changjiang Scholar [of the Ministry of Education] and Distinguished Professor Tao Feng." In this article, Secretary Chen is pictured with a person who appears to be Tao. The final sentence in the article reads, "Professor Tao Feng is the first Changjiang Scholar Distinguished Professor that Fuzhou University has brought in directly from overseas." A webpage from sohu.com, titled "Salute to Our Teachers | You are the Brightest Stars in the Night Sky" dated on or about September 11, 2018, records that FU held an award ceremony for Teacher's Day on September 10th. Page three of this article reports FU has hired two Changjiang Scholars. Page four of the article lists Tao Feng as a

“Changjiang Scholar” Distinguished Professor for FU. Page eleven of the article summarizes the concluding and ideological remarks provided by Chen Yongzheng, University Party Secretary.⁴ I have no information or knowledge concerning the accuracy of these websites or articles beyond the fact that they were discovered during open source searches of the internet.

13. FBI review of KU e-mails further corroborates the complaints.⁵ For example, a series of emails sent and received by Tao corroborates that Tao was interested in and applied for a Changjiang professorship. In or about March 2016, Tao sent an email to an official at Xiamen University (XU), expressing his interest in applying to XU in conjunction with the Changjiang professorship. In or about June 2016, the XU official emailed Tao to inform him that the application process for the Changjiang professorship was starting. In or about July 2016, Tao requested login account information for the Changjiang Scholarship from a Human Resources Department at Xiamen University.

⁴ Open source research reveals that the University Party Secretary is a position roughly equivalent to the President of a university, however the role is different. One article suggests the Party Secretary acts as “decision maker, administrator, coordinator, and political power representative.” Further, the position “is appointed by the Party committee of the government that provides funding to the institution.”

⁵ The University of Kansas Electronic Mail Policy states “KU email accounts remain the property of the State of Kansas.” The following warning banner is displayed prior to accessing KU computer systems:

Access to electronic resources at the University of Kansas is restricted to employees, students, or other individuals authorized by the University or its affiliates. Use of this system is subject to all policies and procedures set forth by the University located at www.policy.ku.edu.

Unauthorized use is prohibited and may result in administrative or legal action. The University may monitor the use of this system for purposes related to security management, system operations, and intellectual property compliance.

14. Tao's interest in a Changjiang professorship continued into 2017 and 2018. For example, in or about July 2017, Tao sent an email asking for assistance in formatting his Changjiang professorship form and received a response containing a link to the Changjiang Professor application website. Similarly, in or about January 2018, Tao received an email from a Chinese professor congratulating Tao as the Changjiang scholar.

15. Tao appears to have engaged in activities consistent with the duties described in the unsigned contract provided by Student #1. For example, in or about June 2018, Tao used his KU email address to send a message to a Japanese professor requesting that the Japanese professor send an advertisement to all STM⁶ groups in Japan about an opening for a faculty position of STM in China. The included advertisement offered faculty positions with a group in China led by a Changjiang Professor, which is consistent with Tao recruiting talent and attempting to form relationships outside of China. The group had an ambient pressure XPS (AP-XPS) and other characterization tools of surface science. Similarly, in June and July of 2018, Tao corresponded with other professors, who appeared to work outside of China, about positions working for FU. The University of Kansas did not have any authorized collaborative agreements with FU.

⁶ I am unsure whether STM here refers to "Science, Technology and Medicine," "Science, Technology and Math," or "Scanning Tunneling Microscope," but the context seems to support either of the former interpretations. Regardless, I don't believe the interpretation of this abbreviation is critical to the determination of probable cause to support the requested search warrant.

16. Indeed, Tao describes himself as working for FU. For example, in or about October 2018, in an email to ELSEVIER | STM Journals, Tao states he received “a joint appointment at Fuzhou University (China) other than the current one.” Similarly, on or about January 29, 2019, Tao received an email from a person accepting a position with FU. In that email, the person asked, “Which is the name of the team or the professor I will work with at Fuzhou University?” Tao responded on or about February 25, 2019, with only “Franklin (Feng) Tao” in the body of the email.⁷ A contact card in [Redacted [X.Z.]] KU email account lists the Chinese characters for Feng Tao with a corresponding email address of “taofeng@fzu.edu.cn”. This is a Fuzhou University email address.

17. Based on the analysis of KU email accounts, it appears that Tao has had full-time employment with FU in China since or before May 1, 2018, as a Changjiang Scholar. Tao actively recruited researchers for FU and established international collaboration between FU and Kansai University in Japan. This activity was required of Tao by his FU contract and suggests that the unsigned version of the contract viewed by the FBI is substantially similar to a contract signed by Tao and FU. On September 25, 2018, Tao certified he had no employment outside of KU, via an electronic online reporting system, potentially violating Title 18, United States Code, Section 1343. As such, Tao maintained employment with the KU, which provided

⁷ Tao did not in fact reply to the person accepting the position at FU, rather Tao forwarded the email to a contact at FU. I incorrectly stated in a prior affidavit that Tao had responded to the email.

him continued access USG research funds from which Tao's salary was paid, potentially violating Title 18, United States Code, Section 666.

Gmail Results Support Initial Complaint

18. On or about November 7, 2017, Tao created the Gmail account franklin.tao.2017@gmail.com (hereafter "Gmail account"). On the same day, Tao configured his Gmail account to send emails as his KU email address. Additionally, Tao made a request to KU to forward his KU email account to his Gmail account. This allowed Tao to monitor emails to, and send emails from, his KU email account remotely. Security alerts from Google show Tao accessed his Gmail accounts from more than one computer and more than one phone. Google provided recent logins for the Gmail account that revealed Tao accessed his Gmail account from IP addresses belonging to KU, Sprint, and Cogent Inc. Account subscriber information from Sprint revealed Tao maintained an active account as of August 7, 2019, at the address **Redacted**

19. Tao's emails show his effort and subsequent success in becoming a Changjiang Scholar at FU. On or about November 11, 2017, Tao sent an email to the Consulate General of the People's Republic of China in Chicago (hereafter "Consulate General") with the subject, "Urgently need Passport." In that email, Tao provided documents from FU and stated he "must attend the preparation of materials for the defense of a talent plan of the Department of Education of China." The attachments included were labeled "An Announcement about Matters Concerning the Panel of Peer Expert Reviewers for the 2017 "Changjiang Scholars Award Program"" and "Fujian Province-Fuzhou University". In the latter, titled "Panel of Peer

Expert Reviewers for the 2017 Changjiang Scholars Arard Program: List of Candidates Participating in Oral Defense and Acknowledgement of Receipt,” Tao is listed as Distinguished Scholar in Chemical Science Group. Tao’s wife, **Redacted** later provided Tao official documentation from FU, scans of Tao’s Legal Permanent Resident card, and a Word document addressed to the Consulate General requesting travel credentials for November 17, 2017, for the Changjiang Scholar defense. **Redacted** also provided Tao with a Travelocity itinerary for a flight from Kansas City, Missouri, to Fuzhou, China, on November 17, 2017. On or about November 17, 2017, Tao received an email from a qq.com account which stated, “Hello Teacher Tao. Please see the attached Changjiang Oral Defense PowerPoint that Teacher Wang edited for you. Thanks!” The first slide of that Powerpoint was titled “2017 “Changjiang Scholars Arard (sic) Program” Distinguished Professor Candidates – Presentation of Oral Defenses” and listed Feng Tao as the presenter.

20. On or about January 11, 2018, Tao received an email from an FU email account congratulating Tao on being chosen for the Changjiang Scholarship. On or about February 5, 2018, Tao received two attachments via two emails from the same qq.com account. The first attachment was named, “Hiring Contract for Changjiang Scholar Distinguished Professor Tao Feng – Template”. The second attachment was titled ““Changjiang Scholar” Distinguished Professor - Addendum to Employment Contract” was an agreement dated February 5, 2018, between FU and Tao where FU agreed to pay Tao 50 million yuan (approx. \$7,279,080 USD) for research costs.

21. As part of his contract, Tao was required to recruit post-doctoral, doctoral, and masters students to FU. On or about November 30, 2018, Tao sent an email to Huang Yuli at the National University of Singapore introducing himself, “This is Franklin from Fuzhou University and University of Kansas.” Tao inquired in the email whether Huang would consider a position at Fuzhou University. On or about January 29, 2019, Ruben Palacio of Universidad de Antioquia, Columbia, wrote Tao an email accepting a position at FU. Tao’s Gmail account contains numerous other such solicitations.

22. As part of his contract with FU, Tao was required to perform significant research in the field of Physical Chemistry. As such, FU would provide funding to purchase equipment for Tao’s lab at FU. On or about July 4, 2018, Tao forwarded from his FU email account (taofeng@fzu.edu.cn) a quote for laboratory equipment. One of the attached quotes noted the terms of delivery as “CIP Fuzhou.” Open source research suggests “CIP” means “Carriage and Insurance Paid to” a delivery location. Fuzhou University was listed in the “MSSRS” field of the quote. Tao’s Gmail account contains numerous other instances of Tao equipping his lab at FU to begin research as directed by his contract.

23. Tao’s contract stipulates that he must lead developments in the field of Physical Chemistry in applying for innovative research groups and seeking approval by the National Natural Science Foundation of China (hereafter “NSFC”). On or about March 17, 2019, Yu-Wen Chen forwarded an email from NSFC that had an attached text and image that appeared to be from a web page. In that text, there was a message addressed Chen Yuwen that read, “Professor Tao Feng has added you as a program participant when filling out the application

below. Please confirm.” The image below that message contained what appears to be a unique alphanumeric identifier, Tao’s name and Fuzhou University in Chinese characters, and Tao’s FU email address, taofeng@fzu.edu.cn.

24. Tao appears to have had full-time employment with FU in China since or before May 1, 2018, as a Changjiang Scholar based on the analysis of his KU and Gmail email accounts. Tao actively recruited researchers for FU and established international collaboration between FU and Kansai University in Japan. Additionally, Tao facilitated the purchase of equipment for his laboratory at FU. Finally, Tao registered a project with NSFC. This activity was required of Tao by his FU contract and suggests that the unsigned version of the contract viewed by the FBI is substantially similar to a contract signed by Tao and FU.

25. On September 25, 2018, Tao certified he had no employment outside of KU, via an electronic online reporting system, potentially violating Title 18, United States Code, Section 1343. As such, Tao maintained employment with the KU, which provided him continued access to USG research funds from which Tao’s salary was paid, potentially violating Title 18, United States Code, Section 666.

There is Probable Cause to Believe Evidence of the Subject Offenses Will be Found in
the TARGET LOCATIONS, DEVICES, and ACCOUNTS

26. The TARGET LOCATIONS include Tao's primary workplace and his residences. Tao's primary workplace is [Redacted] Tao and his family are in transition between a residence Tao rents, located at [Redacted] in [Redacted]; and a residence Tao owns, located at [Redacted] [Redacted] In August, 2019, surveillance agents observed Tao's spouse, [Redacted] unloading her vehicle at the Cedar Ridge address. Surveillance agents later observed there were fewer boxes than previously observed in the garage of Eisenhower Place residence. Open source research revealed the Eisenhower Place residence was listed as available to rent starting September 2. As of August 16, surveillance agents indicated the Eisenhower Place address appears to be vacant. I nevertheless request permission to search the Eisenhower Place address because (a) it may not actually be vacant, and (b) even if it is vacant, we have no way to know what Tao may have left behind in the process of moving. There is probable cause to believe that evidence of the subject offenses will be found at Tao's workplace and residence. Tao took specific steps to enable remote access to his KU email by enabling an email forwarding feature on his KU email account, and by configuring his Gmail account to send emails as his KU email account. Google logon information for the Gmail account revealed Tao logged in from KU assigned IP addresses, as well as IP addresses belonging to Sprint Inc., and Cogent Inc. As a result, there is probable cause that evidence of the subject offenses will be found at the TARGET LOCATIONS.

27. The TARGET DEVICES include computers, phones, and data storage devices that include but are not limited to thumb drives, hard drives, network attached storage devices, servers, and removable media such as flash media, CD-Rs, DVD-Rs, and Bluray discs. Google security notifications suggests Tao has logged into his Gmail account from more than one computer and more than one phone. Additionally, Tao offers his WeChat⁸ identification (ID) as a means of communication to potential recruits. For example, on or about November 30, 2018, Tao emailed Huang Yuli and offered to communicate via WeChat utilizing his ID “franklin-tao”. Huang responded on or about the same day expressing interest in Tao’s research team at FU and agreed to add Tao’s WeChat ID for a call at Tao’s convenience. Historical messages may be found on devices utilizing WeChat. Documents such as contracts, applications, or purchase orders may be stored electronically on data storage devices. As a result, there is probable cause that evidence of the subject offenses will be found on TARGET DEVICES.

28. The TARGET ACCOUNT includes cloud storage space utilized by Tao, along with additional information described in greater detail in Attachment B, Section II. Tao received a subscription notification on his Gmail account from Google on July 10, 2019, for a 100 Gigabyte Google One⁹ account. Tao utilizes his Gmail account to conduct FU business.

⁸ WeChat is a messaging and social media application used on mobile devices and computers that enable users to communicate via text, photo, voice, video, and location sharing. Voice and video calls can also be made via the application.

⁹ Google One is a subscription plan that increases the storage capacity of a standard Google account, which offers 15GB of free storage shared across Google Drive, Gmail, and Google Photos.

Documents such as contracts, applications, or purchase orders may be stored electronically on cloud storage. As a result, there is probable cause that evidence of the subject offenses will be found on the TARGET ACCOUNT.

TECHNICAL BACKGROUND

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant requested herein would authorize the seizure of electronic

storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes

described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the

chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

33. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media

often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying

storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

35. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

36. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email accounts listed in Attachment A.

37. Subscribers obtain an account by registering with Google. Google asks subscribers to provide basic personal information during the registration process. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may

constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

38. A Google subscriber can store data in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

39. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

40. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to

the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

41. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

42. In my training and experience, Google is able to provide information that will assist law enforcement in identifying other accounts associated with the TARGET ACCOUNT, namely, information identifying and relating to other accounts used by the same subscriber. This information includes any forwarding or fetching accounts¹⁰ relating to the TARGET

¹⁰ A forwarding or fetching account related to the TARGET ACCOUNT would be a separate e-mail account that can be setup by the user to receive copies of all of the e-mail sent to the TARGET ACCOUNT.

ACCOUNT, all other Google accounts linked to the TARGET ACCOUNT because they were accessed from the same computer (referred to as “cookie overlap”), all other Google accounts that list the same SMS phone number as the TARGET ACCOUNT, all other Google accounts that list the same recovery e-mail address¹¹ as do the TARGET ACCOUNT, and all other Google accounts that share the same creation IP address as the TARGET ACCOUNT.

Information associated with these associated accounts will assist law enforcement in determining who controls the TARGET ACCOUNT and will also help to identify other e-mail accounts and individuals relevant to the investigation.

43. Google’s Law Enforcement Request System (“LERS”) web portal indicates, if a Google user enables “Web and App Activity” on their account, user searches and activity from Google services are saved to the users Google Account. This includes “clicks” and “queries.” A “query” is the phrase or term requested in Google Search, and a “click” is the URL that was clicked following a Google Search. From Google Fiber’s Privacy Notice, Google uses technical information collected from the use of Google Fiber Internet for network management, security, or maintenance purposes and may associate that information with the Google Account a user registers with their Google Fiber Internet. Information such as URLs of websites visited or content of communications may be associated with a user’s Google Account. In my training

¹¹ The recovery e-mail address is an additional e-mail address supplied by the user that is used by Google to confirm your username after you create an e-mail account, help you if you are having trouble signing into your Google account or have forgotten your password, or alert you to any unusual activity involving user’s Google e-mail address.

and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify co-conspirators and possible future targets of the subject's scheme.

44. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored

electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

45. Based on the foregoing, I request that the Court issue the proposed search warrant. As the search warrant also pertains to Google, because the warrant will be served on Google, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of that part of the requested warrant at any time in the day or night.

46. I further request that the Court order that all papers in support of this application, including the affidavit, search warrant, and search warrant return, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation. However, I seek authority to release the documents as discovery in related criminal cases without the need for these pleadings to be unsealed.

47. For the same reasons, I further request, pursuant to 18 U.S.C. § 2705(b), that the Court prohibit Google from disclosing the existence of this warrant and its service on the account to the subscriber or any other person. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the email account would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy or tamper with evidence, change patterns of behavior, intimidate potential witnesses, notify confederates, or flee from prosecution.

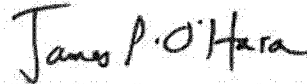
Respectfully submitted,



Stephen Lampe
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on August ¹⁹~~22~~, 2019.

SL



Honorable James P. O'Hara
Chief U.S. Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched is as listed:



Redacted

Redacted

This warrant also applies to information associated with franklin.tao.2017@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at

Redacted

ATTACHMENT B

Particular Things to be Seized

I. Property to be seized at the PREMESIS

1. All records relating to violations of 18 U.S.C. § 666 and 18 U.S.C. § 1343 by Feng Tao occurring after June 1, 2014, including but not limited to the following:
 - a. Records and information relating to Tao's application, recruitment, contracting, payment by, and awarding of the Changjiang Scholarship, Chinese Talent programs, and Chinese Universities.
 - b. Records and information relating to the University of Kansas and Fuzhou University; and
 - c. Records and information relating to the e-mail accounts franklin.tao.2017@gmail.com, franklin.feng.tao@ku.edu and aliases for those accounts.
2. Computers or storage media used as a means to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h. evidence of the times the COMPUTER was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
 - m. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

II. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, all non-content email header information, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connection, log files, and means and source of payment (including any credit or bank account number);
- c. Any accounts linked to the target account by cookies, SMS number, recovery email, creation IP, or forwarding or fetching email addresses.
- d. All searches and activity associated with the account to include “clicks” and “queries,” URLs of sites visited and any content of communication.
- e. The types of services utilized;
- f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.
- g. All files contained within the Google Drive associated with the account.

III. Information to be seized by the government

All information described above in Section II that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 666 (“Theft or Bribery Concerning Programs Receiving Federal Funds”) and 18 U.S.C. § 1343 (“Fraud by Wire, Radio, or Television”) involving Feng Tao and others known and unknown, and dating from July 11, 2019, to the issue date of this search warrant, for each account or identifier listed on Attachment A, evidence of how the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner.