EXHIBIT 37

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH AN EMAIL ADDRESS STORED AT GOOGLE LLC	Case No. 19-mj-8160-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 search warrant for information associated with certain accounts that are stored at premises controlled by Google LLC, an email provider headquartered at 1 Redacted California, 94043, in the Northern District of California ("Google," also "the Provider"). The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II 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 Counterintelligence 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 sufficient 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 exits . . . 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 Life Science Research Lab (LSRL) Building B, Redacted, Lawrence, Kansas. CEBC's research focuses on sustainable technology to conserve natural resources and energy. The CEBC performs proprietary research as well as U.S. 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 three 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 and is 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 program[1] sponsored by the Chinese government. According to Student #1, Tao took that position in May of 2018. 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 a 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 contact, Tao is to be a full-

[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.

[2] Student #1 later told agents that she obtained the unsigned contract by accessing Tao's email account, with Tao's permission and at Tao's direction, but that she provided it to KU and to the FBI because she was angry with Tao over not crediting her on a published research article.

time employee of FU, and is to be provided a job incentive of 550,000 yuan (approximately $80,116 USD)[3] per year to include the Ministry of Educations Distinguished Professor award of 200,000 yuan (approximately $29,133 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 $1,456,664 USD), and research funds worth 20 million yuan (approximately $2,913,328 USD). In return, the contract 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

[3] Conversion of Chinese Yuan and US Dollar based on US Federal Reserve Bank exchange rate for June 28, 2019.

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

---

[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.

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.

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 STM[6] groups in Japan about an opening for a faculty

---

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.

[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.

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.

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. 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 him continued access 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 ACCOUNT

18. There is probable cause to believe that evidence of the subject offenses will be found in the TARGET ACCOUNT because Tao lists the TARGET ACCOUNT as his email address on his resume and because it appears he uses the TARGET ACCOUNT to communicate about his work on behalf of Fuzhou University. For example, in an email to his KU department chair on or about February 25, 2019, Tao provided his Curriculum Vitae (CV). In the personal information header of the CV, Tao lists both his KU email address and the TARGET ACCOUNT. Notably, Tao did not list FU in either his "Current Position" or "Professional Training" sections.

19. Tao also appears to use the TARGET ACCOUNT to conduct FU business. For instance, in an email to Tao on February 7, 2019, an individual expressed interest in a research position in Tao's lab. Tao responded to this e-mail, from his KU email address stating, "I replied to you through my gmail." There were no other emails found between Tao and this applicant. As a result, it is probable that Tao used the TARGET ACCOUNT to continue the correspondence.

TECHNICAL BACKGROUND

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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 accounts[7] relating to the TARGET 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 address[8] 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

[7] 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.

[8] 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.

determining who controls the TARGET ACCOUNT and will also help to identify other e-mail accounts and individuals relevant to the investigation.

27. 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 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.

28. 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 inculpate 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

29. Based on the foregoing, I request that the Court issue the proposed search warrant. 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 the requested warrant at any time in the day or night.

30. 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.

31. 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 July 11, 2019.

James P. O'Hara

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

ATTACHMENT A

Property to Be Searched

This warrant 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. 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.

II. Information to be seized by the government

All information described above in Section I 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 back from account inception 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.