PAUL HASTINGS

STAY CURRENT

January 2020

Follow @Paul_Hastings

Harvard Professor Arrested for Allegedly Hiding Ties to China: What Universities Can Do to Protect National Security While Promoting an Open Academic Environment

By Behnam Dayanim, Scott M. Flicker, Charles A. Patrizia, Robert P. Silvers, Talya Hutchison & Holly S. Flynn

On January 28, 2020, Charles Lieber, chair of the Chemistry and Chemical Biology Department at Harvard University, was arrested and charged with making false statements to U.S. Government agencies regarding his ties to Wuhan University of Technology ("WUT"). On the same day, two Chinese nationals who worked as researchers in Massachusetts were separately indicted for their involvement in transferring sensitive research to China.

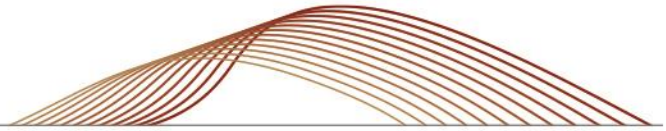
The issues presented by joint Chinese-U.S. academic research activities are not new, as illustrated by the separate case of the University of Tennessee electrical engineering professor who served four years in prison for sharing technical data with Chinese national graduate students. But the frequency and intensity of the U.S. government focus is unprecedented and likely only to increase. Both professors and students will be under scrutiny.

The new enforcement environment raises difficult questions for universities and other research institutions. They must adhere to the law, while also protecting the open and inclusive environments that define their communities. Below, we provide brief descriptions of the most recent arrests and outline steps universities and research institutions can take to support their learning ecosystems while complying with U.S. law and national security regulations.

Recent Enforcement against Individuals

According to the FBI affidavit in support of the criminal complaint in the Harvard case, a WUT professor allegedly recruited Lieber for China's Thousand Talents Plan, which seeks to develop scientific and technical expertise in China. WUT's agreement under the Thousand Talents Plan allegedly promised Lieber up to $50,000 per month as compensation for research and mentorship of scholars, an additional $158,000 per year, and $1.74 million in research funding for a joint Harvard-WUT laboratory.

Participating in such a program with a Chinese university is not itself unlawful. Rather, the U.S. government indicted Lieber because, as part of securing simultaneous research grants from the



Department of Defense ("DOD") and the National Institutes of Health ("NIH"), he allegedly made false statements to those agencies to conceal the extent of his involvement in the Thousand Talents Program.

During the time that Lieber was receiving funding from WUT, he also received over $18 million in research grants from the DOD and the NIH. Both of these agencies require grant recipients to disclose foreign research collaboration and any foreign sources of funding. Lieber allegedly failed to disclose his collaboration with WUT scientists and the money he received from WUT. Furthermore, when both agencies inquired as to his affiliation with WUT, Lieber purportedly denied being a part of the Thousand Talents Plan and suggested that WUT exaggerated his role there. Because NIH inquired through Harvard University, Lieber also allegedly caused the university to make false statements. Harvard has announced that is initiating its own internal investigation.

Simultaneously with the Lieber arrest, U.S. authorities also arrested two researchers for allegedly smuggling sensitive research to China. The first researcher, Yangqing Ye, a Chinese national and People's Liberation Army ("PLA") officer, allegedly misrepresented her military position on her application for a J-1 non-immigrant visa, then passed sensitive documents obtained through her research at Boston University back to her PLA commanding officers. The second, Zaosong Zheng, a Chinese national who obtained a J-1 visa in order to conduct cancer research at Beth Israel Deaconess Medical Center (a teaching hospital of Harvard Medical School), was caught with vials containing biological specimens and other research materials stolen from his laboratory on a flight to Beijing.

Compliance Considerations for Research Universities

1. Confirm that research leads understand the requirement to disclose to the institution and to grant authorities any foreign support or funding or cooperation arrangements.

In 2018, federal agencies granted $127.2 billion in funding for research and development, accounting for 21.9 percent of all research and development funding in the United States. Multiple agencies that provide such grants, including the NIH, require that recipient institutions disclose (1) all other sources of funding for federally-funded projects ("Other Support" disclosures) and (2) whether any federally-funded research will be performed outside the United States ("Foreign Component" disclosures). While the institution generally makes these disclosures on behalf of its faculty, the accuracy of these disclosures depends on research leads appropriately identifying sources of funding and foreign collaboration that must be disclosed. It is therefore essential that research leads fully comprehend the kind of grants and collaborations that would trigger a disclosure and understand their responsibility to disclose.

Disclosure of foreign funding or foreign collaboration does not automatically cause an institution to forfeit federal funding. However, failure to disclose can be costly. A Michigan research institution, Van Andel Research Institute, agreed to pay $5.5 million in a settlement with the Department of Justice in December 2019 for failing to disclose that its researchers had received Chinese government grants.

2. Assure the institution complies with requirements regarding foreign sources of funding.

Because research institutions submit disclosures on behalf of their researchers, the officers of such institutions must be able to identify potential subjects of Other Support or Foreign Component disclosures. Officers should work closely with researchers to keep track of all sources of funding for research projects and all foreign partner organizations so that the required disclosures can be made.

The complaint against Lieber alleges that he caused Harvard University to make false statements. Research institutions can be held liable, under 31 U.S.C. § 3729(b)(1), for making false statements if they know about funding or collaborations that should be disclosed or demonstrate deliberate ignorance or reckless disregard for the truth of the same.

If a research institution determines that a previously-made statement was in fact false, it should confer with counsel and consider submitting a voluntary self-disclosure to the Department of Justice. The Department of Justice imposes lesser penalties (or even no penalties at all) on entities that disclose misconduct or errors in reporting in a proactive, timely, and voluntary manner.

3. Understand the regulatory framework for deemed exports when providing research results or summaries to foreign institutions and when working with researchers who are not U.S. nationals.

In addition to the reporting requirements described above, the U.S. government imposes certain limitations on sharing sensitive information and equipment with foreign nationals who are in the United States. Research institutions can comply with these limitations while attracting top talent from around the world and promoting an open learning environment.

Researchers collaborating on a cross-border project engage in exports when they share technical data with each other. Furthermore, when information is communicated to foreign nationals within the United States, the communication can constitute a "deemed export" if the information is subject to restrictions under U.S. export control laws. This can include sharing export-controlled information with graduate students and academics in the United States on a student or other visa. While "fundamental" academic research falls outside the scope of most export restrictions, the line between what is and is not permitted can be blurry. When results of research are to be published and shared broadly within the research community, that information likely is not controlled for export. However, the exclusion does not apply if the research is subject to proprietary or national security restrictions; for example, if the Department of Defense has restricted the results of a project it funded from public dissemination, a license would still be required if foreign nationals were to be involved in the project.

Certain categories of information are more sensitive and are subject to licensing requirements under the International Traffic in Arms Regulations ("ITAR"), regulating military technologies, or the Export Administration Regulations ("EAR"), regulating "dual-use" items that could have both military and civilian applications. Examples of such items include drone technology, radar and LIDAR, certain toxins or chemical agents, and microchips meeting certain specifications. Whether a license is required for a deemed export depends on (1) the item and (2) the nationality of the recipient. So that foreign nationals can continue to contribute to research projects, research institutions should have a program in place to identify license requirements and apply for licenses as needed.

4. Implement a strong insider threat program for the prevention of intellectual property theft and economic espionage.

The U.S. government has increasingly focused on theft of trade secrets and intellectual property from universities and research institutions. These organizations can and must simultaneously permit appropriately open sharing of information while also having tools in place to detect anomalous or inappropriate acquisition of data. The two recent Massachusetts indictments show the need for a strong insider threat program. In the Ye case, the defendant is accused of sending electronic files from the Boston University network to PLA officers in China. In the Zheng case, the defendant allegedly intended

to use stolen materials to publish Beth Israel Deaconess Medical Center research under his own name in China.

The National Insider Threat Task Force of the Office of the Director of National Intelligence has published an Insider Threat Program Maturity Framework that outlines the elements of a strong insider threat program. Key elements include ongoing training to create a culture of awareness and prevention, user activity monitory capabilities for IT resources that can access sensitive data (especially government data), and analytics to detect anomalous activity. Both physical and network security measures should be tailored to the sensitivity of a research project. Institutions should work with their counsel to ensure their insider threat programs align with best regulatory security practices and comply with applicable privacy and other laws.

5. Establish proactive relationships with Relevant U.S. Law Enforcement and Supervisory Agencies.

The Lieber case and accompanying indictments of Ye and Zheng show that the FBI is paying close attention to the international relationships of U.S. research teams, especially relationships with Chinese counterparts. It would benefit research institutions that maintain international ties to liaise proactively with the FBI and other relevant law enforcement or supervisory agencies before any criminal investigation or charges to identify potential areas of risk and to establish points of contact in advance of potential issues.

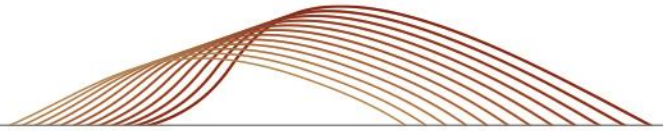
6. Consider providing training and posting appropriate polices to assure continued awareness.

The steps described above require ongoing awareness and participation on the part of every individual in a research institution. Many universities, including Columbia, MIT, and the University of California (just to name a few), have implemented export control policies that empower researchers to undertake projects involving foreign nationals and foreign collaborators while maintaining compliance with U.S. laws and regulations. An effective export compliance program, insider threat program and government contractor ethics program all include periodic trainings to ensure all members of a community know how to comply with the various applicable regulatory frameworks. New team members should be made aware of these requirements, and update trainings should take place on a regular basis. The more each individual within a research institution knows about his or her compliance responsibilities, the more confident the institution as a whole can be in working with foreign nationals and foreign institutions.

Next Steps

In this current environment of increased scrutiny of research institutions and cross-border collaboration, universities would be well advised to undertake these steps to mitigate risk of U.S. law violations while ensuring the promotion of an open academic environment and research collaboration:

- Identify your institution's foreign collaborators and sources of funding;
- Establish or enhance an export controls compliance program, including deemed exports considerations;
- Implement a strong insider threat program;
- Establish law enforcement relationships; and



- Conduct regular trainings to promote awareness and understanding of these compliance issues.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Washington, D.C.

Behnam Dayanim
1.203.551.1737
bdayanim@paulhastings.com

Timothy L. Dickinson
1.202.551.1858
timothydickinson@paulhastings.com

Scott M. Flicker
1.202.551.1726
scottflicker@paulhastings.com

Corinne A. Lammers
1.202.551.1846
corinnelammers@paulhastings.com

Charles A. Patrizia
1.202.551.1710
charlespatrizia@paulhastings.com

Robert P. Silvers
1.202.551.1216
robertsilvers@paulhastings.com

Talya Hutchison
1.202.551.1930
talyahutchison@paulhastings.com

Holly S. Flynn
1.202.551.1908
hollyflynn@paulhastings.com

New York

Peter B. Axelrod
1.212.318.6067
peteraxelrod@paulhastings.com