MAY 2020

Foreign Students and Technology Transfer

Distinguishing the Baby from the Bath Water

Eric L. Hirschhorn

Introduction

For many years, the United States has opened its doors to students from other countries who desire to enroll in U.S. colleges and universities. This has provided the United States with many benefits. These students often have been the best and the brightest of their societies. Many have remained in the United States for some or all of their professional careers and contributed significantly to U.S. society. Even those who have returned home commonly have done so with positive feelings toward the United States. Their presence here has helped their societies and ours better understand one another. Finally, from a somewhat mercenary point of view, they typically have paid full tuition, thus helping balance university budgets and, in effect, subsidizing U.S. students attending those schools.

Developments in recent years, however, have led many observers to question whether the traditional view of foreign students remains accurate. The United States has not previously faced a situation where another country is deliberately and systematically attempting, by fair or foul means, to gain access to its technology. Today we are seeing a new pattern in the immigration of foreign students—particularly Chinese students in the sciences—to study at our academic institutions. The changes include the number of students who come here, the connections that some have with their home governments (particularly the military and intelligence services of those governments), the courses of study they elect, and the proportion who return home after graduation.

Flatly closing the door to foreign students would be a foolish and self-defeating step, but the United States must consider two important questions. First, does the traditional U.S. openness inappropriately ignore or understate the risks attendant upon giving potential adversaries access to important technology? Second, if so, what should the United States do to recalibrate the balance?

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

This article focuses on foreign students and technology transfer, which is only one aspect of a broader issue: how to control the outflow of critical technology from the United States without losing benefits such as international scientific cooperation and an open academic and research environment.

United States Controls on Technology Exports

WHY DOES THE UNITED STATES CONTROL TECHNOLOGY EXPORTS?

Why does the United States care what technology leaves the country? Although the United States controls some exports even if they lack military utility—say, because the United States disagrees with the human rights policies of the recipient country's government—the bulk of U.S. controls are imposed on technology that potentially is useful for military or intelligence purposes. The Defense Department seeks to ensure that if U.S. servicemen and servicewomen have to go into battle, they have the best arms and other equipment that the United States can provide. Export controls and other restrictions on technology transfer are the opposite side of the coin. Their purpose is to ensure that U.S. adversaries on a battlefield do not have comparable capability.

HOW DOES THE UNITED STATES CONTROL TECHNOLOGY EXPORTS?

There are four principal means by which the United States controls outflows of technology:

- Export controls regulate what goods and technology can leave the country, including via "deemed" export, an important concept that is explained below. They also regulate reexports from other countries of "U.S.-origin" goods and technology.
- Visa policies regulate who can enter the United States, for what purpose, and for how long.
- Economic sanctions regulate U.S. persons' business with specified foreign countries, entities, and individuals—usually without regard for whether such transactions might involve goods or technology with military implications.
- The Committee on Foreign Investment in the United States (CFIUS) regulates who from outside the United States is permitted to invest in businesses in the United States.

Also, if work is being done under a federal contract, that agreement may contain its own restrictions on foreign-person involvement, above and beyond what export controls may require.

Of these methods, export controls are the most focused in terms of regulating what *technology* can be transferred.

A. Export Controls

There are three principal sets of U.S. export controls.

- Exports of "dual use" and lower-level military goods and technology are controlled under the Commerce Department's Export Administration Regulations (EAR). "Dual use" items are those with both military and civilian uses.
- Exports of finished military goods (called "end items"), significant military parts and components, and significant military technology are controlled by the State Department's International Traffic in Arms Regulations (ITAR).
- Nuclear-related exports are controlled by the Nuclear Regulatory Commission, where goods are involved, and by the Department of Energy, where technology is involved.

Each set of controls includes the "deemed" export rule, which applies to foreign visitors, including students. Simply stated, transferring technology to a foreign national in the United States—whether orally, in writing, or by permitting visual observation—constitutes a "deemed" export to that individual's home country unless he or she is a green card holder or a "protected individual" (i.e., granted asylum or an applicant for asylum). There are some exceptions, which are discussed below, but unless an exception applies, a transfer of technology to a national of Country X is considered to constitute an export of the technology to Country X.

Another important aspect of U.S. export controls arises from membership in four international export control groups, each with about 40 member nations. These are the Wassenaar Arrangement, which controls goods and technology with military utility; the Australia Group, which controls items useful for chemical or biological warfare; the Nuclear Suppliers Group; and the Missile Technology Control Regime. Controls agreed upon in these groups are enforced by each member nation. Many U.S. export controls are based on these groups' lists. Other U.S. controls, however, are unilateral in character. If a unilaterally controlled item is readily available elsewhere, restricting exports of that item only from the United States may not prevent a disfavored end user from acquiring it.

The Commerce Department's export control rules—the Export Administration Regulations (EAR)—are the ones most commonly applicable to foreign-student activities.[1]

- The Commerce Department, working with the Departments of Defense, State, and Energy as well as about 40 countries (the "multilateral" part of the equation), decides which technologies and commodities have strategic implications.
- In addition to controls agreed upon in the four multilateral groups, the United States frequently imposes unilateral controls on certain items.
- The goods and technologies to be controlled then are listed, with specific technical parameters, in several hundred entries on the Commerce Control List (CCL). Each individual entry includes information about when licenses are required to export the covered items to specified countries.
- If a license is required, a "license exception" may be available, but an exporter may not use such an exception if it has reason to doubt the *bona fides* of any other parties to the transaction.
- If a license is required for a particular proposed export and no license exception fits the transaction, the would-be exporter must apply to the Commerce Department for an export license.
- The Departments of Commerce, State, Defense, and—if the item is nuclear in character—Energy decide whether the license should be granted. Consideration of a license application frequently includes checking whether the Intelligence Community has adverse information about the proposed end user or the stated end use.

These listing and licensing processes are roughly similar for the State Department's system for higher-level munitions items, and the NRC and DOE systems for nuclear-related items.[2]

---

1 Export Administration Regulations, 15 C.F.R. 730-774 (2020), https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title15/15tab_02.tpl.
2 International Traffic in Arms Regulations, 22 C.F.R. 120-130 (2020), https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title22/22cfr120_main_02.tpl; Export and Import of Nuclear Equipment and Material, 10 C.F.R. 110 (2020), https://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=10:2.0.1.1.20; and Assistance to Foreign Atomic Energy Activities, 10 C.F.R. pt. 810 (2020), https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title10/10cfr810_main_02.tpl.

Certain types of information are excluded from the EAR altogether. Some are based on the *intrinsic* nature of the information. For example, information that is not "technology," such as general descriptions of an item, pricing information, and delivery information, is not "subject to the EAR."

Other types of information are excluded based upon the context in which they are to be transferred. Several of these exclusions are particularly significant insofar as foreign students are concerned:

- Information conveyed in catalog courses—that is, standard courses that are listed in an institution's printed or online catalog—and in associated teaching laboratories is not "subject to the EAR," even if it is listed on the CCL. The course or associated lab where the information is released must be at an academic institution, but that institution need not be located in the United States
- "Fundamental research," which is "research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community," also is excluded from the EAR's controls if it is not subject to proprietary or contractual restrictions. The exclusion of fundamental research comes from President Ronald Reagan's National Security Decision Directive 189, published in 1985. NSDD-189 says that if the government wants to protect such information, it should apply a national security classification to it (e.g., "Confidential," "Secret," or "Top Secret").
- "Published" information, including information that is *intended* to be published, generally is excluded from export controls. Examples mentioned in the Commerce Department regulations include information that is (1) available by subscription (e.g., a scientific journal); (2) available at libraries or similar public collections (e.g., a book or doctoral dissertation); (3) distributed at a conference that is generally accessible to the public; (4) posted on a website or other location offering unlimited public access (e.g., a blog); and (5) submission to a journal, research group, or conference with the intent that it will be made available publicly if accepted.
- Patent information is another exception, unless it has been subjected to an invention secrecy order.

These excepted classes of information are considered not "subject to the Export Administration Regulations." The State Department's International Traffic in Arms Regulations and the Energy Department's nuclear technology export rules also contain exceptions for publicly available data and the results of fundamental research.

To summarize, vast quantities of technology, some of it valuable from a military or intelligence standpoint, are readily available to foreign students—and indeed, to anyone who is interested in acquiring it. As an example, many years ago I was hired as an expert witness by the defense team for an East German physicist who had been charged with espionage. The case was pending in Boston, and the physicist was freed on bail while the pretrial proceedings took place. A condition of bail was that the defendant call in daily to a designated probation officer. When he failed to call one day, the lead FBI agent called defense counsel in a lather, saying that he was about to close Logan Airport and the railway stations, set up roadblocks, and the like. The lawyer asked for a few minutes to try locating her client. Shortly thereafter, the defendant called the probation officer to check in and apologize for having lost track of the time. At a court hearing the following week, the FBI agent asked defense counsel how she had located him so quickly. "It was easy," she replied. "I called the MIT Library and had him paged."

B. Visa Policies

The visa system is another potential tool for limiting the export of U.S. technology. The system can be used to control who can come to the United States to take specific jobs or academic courses of study. But current grounds for rejecting visa applications due to concerns about potential intellectual property theft are limited.[3] Consular officers "can consider 'whether there are reasonable grounds to believe that a visa applicant seeks to enter the United States to engage solely, principally, or incidentally in activity to *violate or evade* U.S. law prohibiting the export . . . of goods or technology.'"[4] Under current practice, according to the staff of the Senate Permanent Subcommittee on Investigations, this means that "consular officials must base a denial on a *specific* anticipated violation of an *already existing* export law" and may not deny a visa if the applicant seeks to gain information lawfully, even if it is in a sensitive area such as robotics or artificial intelligence.[5] The November 2019 subcommittee report noted that the State Department denies fewer than 5 percent of Chinese visa applications.[6]

Also, the decision to issue a visa only determines that the individual will be allowed to enter the country. It does not, in and of itself, constrain those who *provide* information to visa holders nor does it constrain what information a visa holder may acquire while in the United States. It only determines *who* may enter the United States and for *how long* a period. The application process identifies who intends to study in the United States and what course of study is contemplated, so it can be used to exclude students from particular countries who are planning to pursue particular subjects, but it is somewhat of a blunt instrument because it likely will bar the entry of many students whose courses of study pose no threat of loss of significant technology. Past efforts to increase the role of the visa process in controlling technology exports have been met by objections that the volume of visa applications is too high, that consular officers lack technical knowledge, and that the listings of proposed courses of study are insufficiently specific to permit an informed evaluation by the U.S. government.

C. Economic Sanctions

Economic sanctions restrict trade and financial transactions between persons subject to U.S. jurisdiction, on the one hand, and specified countries, entities, and individuals, on the other. Administered by the Treasury Department's Office of Foreign Assets Control (OFAC), sanctions typically are imposed without regard to the subject matter of the trade or financial dealings (i.e., for foreign policy rather than national security reasons and not focused on technology).[7] As such, they, like visa restrictions, are a relatively blunt instrument for protection against technology leakage.

D. Foreign Investment in the United States

As its name implies, CFIUS reviews foreign investments in the United States. One factor that CFIUS considers is whether the business proposed to be acquired possesses controlled technology, but that is far from the only factor and rarely the dispositive one. (This is partly because foreign ownership of a U.S. company does not include the right to see controlled technology; that is permitted only if authorized by the export

---

3 Permanent Subcommittee on Investigations, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans* (Washington, DC: U.S. Senate, November 2019), p. 78, https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China%27s%20Talent%20Recruitment%20Plans.pdf.

4 Ibid. (Quoting June 6, 2018 congressional testimony of Edward Ramotowski, deputy assistant secretary for consular affairs, U.S. Department of State) (emphasis added).

5 Ibid., 79 (emphasis added).

6 Ibid., 80.

7 Office of Foreign Assets Control, Department of the Treasury, 31 C.F.R. 501-598 (2019), https://www.law.cornell.edu/cfr/text/31/chapter-V.

control laws.) Moreover, the CFIUS process focuses on takeovers of existing commercial ventures. That renders it less relevant in the academic context than the commercial, though university faculty sometimes become involved in start-ups in which foreign interests may wish to invest.

Until recently, CFIUS rules applied only to investments that would give a foreign party control of an existing U.S. business. Under new rules, enacted in 2018 and effective in early 2020, a foreign investment in a U.S. business—even if passive and amounting to less than "control" of the business—is subject to CFIUS review if that business "produces, designs, tests, manufactures, fabricates, or develops" any technology that is on the export control lists mentioned above or that otherwise has been identified by the federal government as a "critical" technology.[8]

Foreign Students and Technology Transfer

A number of factors, some inconsistent with one another, bear upon the issue of foreign students and technology transfer:

- As noted above, the United States has succeeded over many generations in prospering—as an economy and as a culture—by attracting smart people from other lands to study here and remain to pursue their careers in science, the arts, and other fields. Many of our country's Nobel laureates in the sciences (physics, medicine, and chemistry) have been foreign born. The heads of a number of our leading companies also were born elsewhere.

- A concomitant of that factor is the traditional openness of U.S. academic institutions and open exchanges of research results. This is reflected, for example, in the exceptions outlined above for information disclosed in catalog courses, information that has been or will be published, and information that results from fundamental research.

- The U.S. government—quite reasonably and sensibly—desires to prevent the spread of technologies with potential military and intelligence applications to actors (state and non-state) who might wish to harm the United States or its allies, engage in terrorist activities, or proliferate weapons of mass destruction.

- Controls on technology transfer, even to foreign nationals, can raise substantial First Amendment issues. Several Reagan-era opinions of the U.S. Department of Justice conclude that the First Amendment may prohibit prior restraint of technology transfers, even for data reflecting "applied" research, unless the transfers directly assist a foreign enterprise or involve the sale of the data.[9] If those opinions accurately state the law, the government ordinarily cannot prohibit the publication of technology in journals, online papers, and similar sources. A leading court decision holds that even technology transfers with potential military implications can be controlled only if the technology is "significantly and directly related to specific articles on the [United States] Munitions List."[10] Another line of cases states that encryption source code is "speech" for First Amendment purposes and is protected accordingly.[11] The current Supreme Court, although conservative

8 50 U.S.C. § 4565 (2018).

9 Constitutionality of the Proposed Revision of the International Traffic in Arms Regulations, 5 Op. O.L.C. 202, 212-13 (1981); accord Constitutionality of Proposed Revisions of the Export Administration Regulations, 5 Op. O.L.C. 230, 233 (1981). "O.L.C." is the Office of Legal Counsel, which is the de facto general counsel's office of the Department of Justice.

10 United States v. Edler Indus., 579 F.2d 516 (9th Cir. 1978).

11 Bernstein v. Department of State, 922 F. Supp. 1426, 945 F. Supp. 1279 (N.D. Cal. 1996), 974 F. Supp. 1288 (N.D. Cal. 1997), *aff'd*, 176 F.3d 1132, *opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

on many issues, has been fairly expansive in defining what "speech" is protected. As a result, the outcome of any technology transfer cases heard there, even cases with a "national security" overlay, would be difficult to predict.

- As discussed above, the fact that so many important technologies are available from a host of countries means that unilateral (i.e., U.S.-only) controls on technology transfer are less likely than multilateral controls to be effective in keeping critical technology out of the hands of bad actors.
- Finally, there are financial considerations for cash-strapped academic institutions.
    - Foreign students often pay full tuition.[12]
    - Foreign students frequently are employed in laboratories and other research facilities for modest wages.
    - Research grants, particularly those from the federal government (e.g., Department of Defense, National Science Foundation, Department of Energy) or private sponsors with proprietary information, frequently prohibit participation by foreign nationals unless an export license has been obtained.
    - Academic institutions receive donations and contracts from foreign governments and institutions. Sometimes these payments are substantial. They generally are permitted but must be reported to the U.S. government if they exceed $250,000 from one "foreign source" within a calendar year—a requirement apparently more honored in the breach than in the observance.[13] Recent activity on that front includes the "Thousand Talents" program, which recruits U.S. academics and other experts to assist China's development efforts, and some significant donations from foreign governments other than China.

This article asks whether the traditional U.S. model of attracting smart people from elsewhere to come here remains valid. The rise of an aggressive China may affect the traditional calculus of encouraging foreign students to study in the United States with the expectation that most will remain here for their professional careers. Hardly a week goes by without another reported instance of illegal Chinese exfiltration of U.S. technology. The means are many. They include employees of technology and defense companies, cyber and computer exfiltration schemes, government employees, outright spies, and—of particular interest here—faculty, staff, and students at academic institutions.[14] Prosecutions in the past several years have included defendants affiliated with Harvard University, the University of Tennessee, Boston University, and Boston's Beth Israel Deaconess Medical Center.

---

12 "Foreign students, usually paying full tuition, represent a significant revenue source everywhere, from the Ivy League to community colleges." Anemona Hartocollis, "Colleges Running Low on Money Worry Students Will Vanish, Too," *New York Times*, April 16, 2020, at A1 (Wash. ed.).
13 20 U.S.C. § 1011f (2018). This reporting requirement was enacted in 1998. Higher Education Amendments of 1998, Pub. L. No. 105-244, § 101(a), 112 Stat. 1581, 1593-95; and see, e.g., "U.S. Department of Education Launches Investigation into Foreign Gifts Reporting at Ivy League Universities," U.S. Department of Education, press release, February 12, 2020, https://www.ed.gov/news/press-releases/test-0.
14 Not all Chinese spying is conducted in academic institutions, defense companies, or the federal government. See, e.g., Dina Temple-Ralston, "The Chinese Spy in the Iowa Corn Field," Washington Post, March 6, 2020 (book review of Mara Hvistendahl, *The Scientist and the Spy: A True Story of China, the FBI, and Industrial Espionage)*, https://www.washingtonpost.com/outlook/the-chinese-spy-in-the-iowa-corn-field/2020/03/05/b3c2f110-4d03-11ea-9b5c-eac5b16dafaa_story.html.

In the fall of 2015, President Barack Obama and President Xi Jinping agreed that China would cease its cyber-espionage against U.S. intellectual property.[15] This past December, Assistant Attorney General for National Security John Demers spoke at the annual RSA Conference. He reported that ironically, the result of that agreement has been the Chinese intelligence services "becoming involved in developing and expanding the *insider threat"* [emphasis added].[16] This includes China's Thousand Talents program, which recruits U.S. technology experts to work in and with China as well as insiders in U.S. companies and institutions who implant malware on computers to exfiltrate data to China.[17] Demers pointed to academia as a particular target of these efforts.

Speaking at the same conference, William Evanina, head of the National Counterintelligence and Security Center, called the insider threat "the most vicious and pernicious threat that we face as a nation and [a] private sector."[18]

Kevin Nealer, a senior adviser at CSIS, wrote recently that "Chinese intelligence programs have undermined trust in educational exchanges, particularly in STEM fields, and [have] required stepped up counterintelligence responses. These are the direct result of China's discriminatory intellectual property policies and its asymmetric, offensive approach to commercial espionage."[19]

Even Ambassador Craig Allen, a longtime proponent of the U.S.-China relationship, concedes that "U.S. concerns over China's policies and practices in the high-tech sphere are very real."[20] Allen cautions, though, that the price of protecting our technologies from one another may be the dulling of "both . . . countries' cutting edge and the [undermining of] technological advancement overall."[21]

The data on Chinese who study abroad are sobering. As recently as 2000, about 40,000 Chinese students were studying abroad, and only a handful returned to China afterward.[22] By 2018, however, China's Ministry of Education reported that there were 662,100 Chinese studying abroad, 480,900 of whom (73 percent) returned to China afterward.[23] A recent news story reported that about 1.6 million Chinese students now are studying abroad and that about 400,000 of these individuals are at academic institutions in the United States.[24]

How Does the U.S. Academic Community Fit into This Framework?

Regrettably, a few academics seem to think that the rules outlined above are not for them. A University of Tennessee professor was convicted not long ago for employing Chinese nationals to work with technolo-

---

15 "Fact Sheet: President Xi Jinping's State Visit to the United States," The White House, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states. "The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." Ibid.

16 Andrew Eversden, "How China Poses an insider threat," Fifth Domain, February 26, 2020, https://www.fifthdomain.com/show-reporters/rsa/2020/02/26/how-china-poses-an-insider-threat/ .

17 For details on six scientists' discharges for failure to disclose substantial payments from Thousand Talents program, see Jeffrey Mervis, "Moffitt Cancer Center details links of fired scientists to Chinese talent programs," *Science Magazine*, January 19, 2020, https://www.sciencemag.org/news/2020/01/moffitt-cancer-center-details-links-fired-scientists-chinese-talent-programs.

18 Eversden, "How China Poses an insider threat."

19 Kevin G. Nealer, "Trading Iron Curtains for Chinese Walls: Is It Different This Time?," in *China's Uneven High-tech Drive: Implications for the United States*, ed. Scott Kennedy (Washington, DC: CSIS, February 2020), https://www.csis.org/analysis/chinas-uneven-high-tech-drive-implications-united-states.

20 Craig Allen, "For Cooperative Innovation, China Must Lead the Way," in ibid.

21 Ibid., 52.

22 U.S. Senate Permanent Subcommittee on Investigations, *Threats to the U.S. Research Enterprise*, 35

23 Ibid.

24 Alexandra Stevenson and Tiffany May, "Stranded Students Present Dilemma for China," *New York Times*, April 6, 2020, A17 (Wash. ed.).

gy controlled on the U.S. Munitions List.[25] He did so despite explicit warnings that this would violate the Arms Export Control Act.[26] This past January, the chair of Harvard University's Chemistry Department was indicted for lying to authorities about contracts and funds received from the Thousand Talents program.[27]

Even among the vast majority of professors who recognize that the rules do apply to academia, there is a level of discomfort with that fact. For example, many prominent research universities pushed back when the FBI alerted them last year to concerns about the Thousand Talents program and provided them with the names of participants. Chancellor Patrick Gallagher of the University of Pittsburgh, a leading U.S. research university, noted that "[c]ollaborations between scientists across national boundaries have been subject to unprecedented scrutiny. Established practices have been prohibited on technicalities. And researchers, particularly immigrants and visitors from China, have been the target of aggressive investigations and public sanctions."[28] Gallagher said that although the University of Pittsburgh "will continue to uphold all laws governing research, innovation and international partnerships while fostering a vibrant and globally engaged university," it also will advocate for "sensible and clear government actions that address real threats without causing irreparable harm to our nation's research universities, which are still admired around the world."[29] Similar expressions came from such other leading research institutions as Yale, Johns Hopkins, the University of California at Berkeley, Carnegie-Mellon, and MIT.[30]

Chancellor Gallagher is right, at least up to a point: This is a difficult and complicated issue, and the United States should take care not to throw the baby out with the bath water. How can we ever know in advance who will stay and who will return to their native country? After all, it would not be unusual for someone who plans to return home after school to decide, after a year or two here, that they would rather make their life in the United States, or conversely, for someone who had anticipated staying here after graduation to decide that home indeed is where their heart is. People see a side of life here that they did not expect that they like or do not like. People fall in or out of love. A family at home experiences a crisis that requires the student's (or young professional's) presence. People receive attractive job offers, whether from academia or the commercial sector, in this country, in their home country, or in third countries. The list of variables goes on and on.

What to Do?

Recently, Secretary of Defense Mark Esper spoke at CSIS's Global Security Forum. He was asked whether the United States should restrict the admission of students who come from potential adversaries such as China and plan to study technical subjects. One might have expected him to say "yes" but—somewhat surprisingly—he responded only that we need to know who the students are and what they are studying. Importantly, he did not take up the opportunity to suggest that we should restrict students' entry or courses of study any more than is done today.

If the secretary of defense is not clear on what the United States ought to do, I hesitate to offer a solution of my own. It seems clear, though, that the current landscape differs significantly from the historic par-

25 United States v. Roth, 628 F.3d 827 (6th Cir. 2011).
26 Ibid.
27 "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases," U.S. Department of Justice, press release, Jan. 28, 2020, https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.
28 Patrick Gallagher, "In Support of Global Engagement," University of Pittsburgh, updated March 5, 2020, https://www.chancellor.pitt.edu/spotlight/support-global-engagement.
29 Ibid.
30 U.S. Senate Permanent Subcommittee on Investigations, *Threats to the U.S. Research Enterprise*, 98 n. 590.

adigm and that the academic community needs to work closely with the federal government to ensure that an appropriate balance—one that reflects the considerations noted above—is struck. At a minimum, this review should include whether the exception for "catalog courses" ought to be narrowed or otherwise refined, whether the visa process can be made more robust, and whether the Intelligence Community can provide additional information about the backgrounds of applicants for student visas.

Eric L. Hirschhorn *is a senior adviser (non-resident) with the Scholl Chair in International Business at the Center for Strategic and International Studies in Washington, D.C. He previously served as the undersecretary of commerce for industry and security at the U.S. Department of Commerce.*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.