House Science Committee testimony April 11/Daniel Golden

I would like to thank the committee for inviting me. I am testifying in my personal capacity as the author of "Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities," rather than as a senior editor at ProPublica. Although my book examines both foreign and domestic espionage at U.S. universities, my testimony today will focus on foreign theft of federally-funded academic research.

The number of foreign students and faculty has mushroomed for the past 40 years. In 2016, the number of international students at U.S. universities topped 1 million for the first time, almost seven times the total in 1975 and more than double the 2000 figure, though the numbers are starting to level off now. The number of foreign-born scientists and engineers working at U.S. colleges and universities rose 44 percent in the decade between 2003 and 2013, from 360,000 to 517,000. In key technical fields such as engineering and computer science, American universities award more than half of doctorates to international students.

Educational globalization has many benefits: diverse perspectives in the classroom; cross-cultural understanding; skilled labor for research; collaboration of the world's best minds in the advancement of learning.

But there's an alarming side-effect. Globalization has transformed American universities into a front line for espionage. Some small but significant percentage of international students and faculty come to help their countries gain recruits for clandestine operations, insights into U.S. government plans, and access to sensitive military and civilian research. Academic solicitation, or "the use of students, professors, scientists or researchers as collectors," tripled from 8 percent of all foreign efforts to obtain sensitive or classified information in fiscal 2010 to

24 percent in 2014, according to the Defense Security Service, a Defense Department agency that protects American technology.

For foreign intelligence services, a university offers a valuable and lightly guarded target. They can exploit the revolving door between academia and government: today's professor of international relations is tomorrow's assistant secretary of state. They can recruit naïve students and guide them into the federal agency of their choice.

Universities undertake a growing amount of government-funded research, much of it sensitive. The U.S. government spent $27.4 billion on academic R&D in 2014, triple the tab in 1990. That includes $2.4 billion from the Pentagon and intelligence agencies – not counting the CIA, which doesn't publicly report expenditures. Academic research offers a valuable, vulnerable, and low-risk target for foreign espionage. Despite pursuing groundbreaking technologies for the Pentagon and the intelligence community, university laboratories are less protected than their corporate counterparts, reflecting a culture oriented toward collaboration and protection. Typically, university researchers aren't required to sign nondisclosure agreements, which run counter to the ethic of openness.

Open campuses make it simple to gather intelligence. Spies with no academic

affiliation can slip unnoticed into seminars, student centers, libraries, and cafeterias – pretty much anywhere except laboratories conducting classified research - and befriend the computer scientist or Pentagon adviser sitting beside them.

Academia's old-fashioned, gentlemanly culture also abets espionage. All it takes for professors in different countries to agree to collaborate on research is a phone call, an email, or perhaps a handshake at a conference. There's not necessarily a contract that explicitly spells out what data or equipment each side has access to. Many science students and faculty are unfamiliar with intellectual property safeguards. In one study, 21 percent of UCLA engineering graduate students couldn't define a patent; 32 percent couldn't define a copyright; 51 percent couldn't define a trademark; and 68 percent – more than two-thirds – couldn't define a trade secret. Never contemplating the possibility of espionage, American professors sometimes comply with requests from acquaintances or strangers overseas for research advice, manuscript reviews, or unpublished data.

University administrations largely ignore the growing threat, in part for financial and reputational reasons. They're ramping up enrollment of full-paying international students, and opening campuses abroad, which are often subsidized by the host countries.

Like their institutions, individual professors may put global prestige ahead of intellectual property. John Reece Roth, an emeritus professor of electrical engineering at the University of Tennessee, was convicted in 2008 and sentenced to four years in prison for using graduate students from China and Iran on U.S. Air Force research that was off-limits to foreigners, and taking a laptop with restricted files to China.

Roth wasn't a Chinese spy. He was simply proud of his renown there. He found it hard to believe that a country where two universities had named him an honorary professor, where his lectures drew large audiences, and where both volumes of his book *Industrial Plasma Engineering* were available in translation, could have any duplicitous intent.

A pivotal moment in educational globalization – and in the rise of academic spying -- was China's opening to the West, and its decision in 1978 to begin sending students to the U.S, which was motivated largely by a desire to catch up in science and technology. Soon afterwards, the FBI began noticing signs of an increase in campus spying, such as a spike in the use of copying paper.

China now accounts for almost one-third of international students in the US, and

about 15% of foreign-born researchers and scientists. Again, the vast majority pose no threat and, like other newcomers, infuse American universities with energy and fresh perspectives. Still, a study conducted for my book found that at least 30 people born or raised in China and charged since 2000 in U.S. courts with economic espionage, theft of trade secrets and similar offenses attended American colleges or graduate schools, including Harvard, Stanford, Columbia, and Cornell.

The story of one Chinese graduate student at Duke University illustrates how vulnerable academic research is to foreign raiders, and how little universities do to protect it. I came across this saga when, through a public records request, I obtained the agenda of an October 2012 meeting of the National Security Higher Education Advisory Board, which was established in 2005 as a forum for university presidents and US intelligence officials to discuss matters of mutual importance. One agenda item stated that Duke University professor David Smith "will discuss how, without his knowledge, a Chinese national targeted his lab and published and exploited Dr. Smith's research to create a mirror institute in China. The episode cost Duke significantly in licensing, patents, and royalties and kept Smith from being the first to publish ground-breaking research."

I soon learned that Smith was a renowned researcher who had helped launch the fast-growing field of meta-materials, or artificial materials with properties not

found in nature; that his lab had invented the first “invisibility cloak,” though it only concealed objects from microwaves, not the human eye; and that his lab had Pentagon funding to develop ways of cloaking weapons. And I identified the Chinese national as Ruopeng Liu, a former graduate student in Smith’s lab. Through interviews with Smith and other lab members, I discovered that Liu had left a trail of suspicious behavior. He arranged for Chinese scientists to visit the Duke lab and photograph its equipment, and passed them data and ideas developed by unwitting colleagues at Duke. He deceived Smith into committing to work part-time in China by enlisting him under false pretenses to participate in a program called Project 111, which the Chinese government established in 2006 to spur “scientific” renewal of Chinese universities by recruiting famous scientists as “overseas academic masters.” And he secretly started a Chinese website based on the work at Duke.

To be sure, it seems likely that Liu was poaching the research for his own benefit, rather than for Chinese intelligence. Also, he didn’t explicitly broke the rules, mostly because there was no formal collaboration agreement and Duke’s guidelines didn’t anticipate this sort of situation. Still, his actions smacked of economic espionage.

After numerous warnings from other members of the lab, and questions from the

Pentagon, Smith finally began to suspect Liu, and took away his key to the lab, but Duke still awarded Liu a doctorate. Coincidentally or not, a week after Liu's dissertation defense, Duke trustees approved negotiations with Chinese officials to build a campus in the city of Kunshan, which would supply the land and facilities for free. Once he had received his degree, Liu returned to China, where he used Duke's research to start a competing institute and business with Chinese government support, and became a billionaire.

In an interview for my book, Liu defended himself by noting that the invisibility research was basic, not export-controlled or classified. "I worked in fundamental research and published papers and they can be seen by anyone in the world," he said.

Yet there are advantages even to stealing open research: namely, saving time and avoiding mistakes. With a mole in a U.S. university laboratory, researchers overseas can publish and patent an idea first, ahead of the true pioneers, and enjoy the consequent acclaim, funding, and surge in interest from top students and faculty. In fact, a foreign government may be eager to scoop up a fundamental breakthrough before its applications become so important that it's labeled secret—and foreign students lose access to it. One former FBI official whom I interviewed had a term for such promising science: "pre-classified."

Liu “was definitely filled with intent,” and his actions “could have tremendous economic impact in the future,” Prof. Smith told me. “I think if people understood how something like this happens, and how those with potentially ill intent can take advantage of the natural chaos that occurs in US academic environments, they might become more aware and avoid things like this in the future.”

Project 111, for which Liu was a recruiter, is one of a vast array of Chinese “brain gain” programs that, intentionally or not, encourage theft of intellectual property from U.S. universities. Unlike Project 111, most of these initiatives target scientists of Chinese descent. Unhappy with the high percentage of Chinese students at Western universities who chose to stay abroad after earning their degrees, China’s national, provincial, and municipal government have embarked on aggressive efforts to lure back the most successful expatriates.

Of the slew of initiatives, the best known are the Hundred Talents Program and the Thousand Talents Program. Hundred Talents seeks up-and-coming scholars under age forty. Thousand Talents, established in 2008 by the Communist Party’s powerful Organization Department, woos prominent professors of Chinese ethnicity under age fifty-five. “The Chinese government has been the most assertive government in the world in introducing policies targeted at triggering a reverse brain drain,” one study concluded in 2012.

These programs offer such generous salaries, laboratory facilities, research funds, housing, medical care, jobs for spouses, top schools for children and other incentives that a borderline candidate may be tempted to improve his chances by bringing back somebody else's data or ideas. One former FBI agent summed up the implicit message to Chinese researchers in the US this way: "Don't come home empty-handed."

One such case involved a research assistant at Medical College of Wisconsin, Huajun Zhao. In March 2013, he was arrested and charged with stealing three vials of a cancer-fighting compound from his professor, Marshall Anderson, who had patented it. Zhao, who claimed that he invented the compound and wanted to bring it to China for further study, had applied for funding from Chinese agencies that support overseas recruitment. One application was an "exact translation" of an old grant proposal by Anderson. Zhao later pleaded guilty to a reduced charge of illegally downloading research data.

While espionage services are active on university campuses, students and professors may be even more vulnerable to recruitment or research theft when they're off campus, participating in academic conferences. Intelligence officers flock to conferences for the same reason that lawyers chase ambulances and Army recruiters concentrate on low-income neighborhoods: they make the best hunting grounds. As Willie Sutton famously said when asked why he robbed

banks, “Because that’s where the money is.” While a university campus may have only one or two professors of interest to an intelligence service, the right conference—on drone technology, perhaps, or ISIS— may have dozens.

The FBI warned American academics in 2011 to beware of conferences, citing this scenario: “A researcher receives an unsolicited invitation to submit a paper for an international conference. She submits a paper and it is accepted. At the conference, the hosts ask for a copy of her presentation. The hosts hook a thumb drive to her laptop, and unbeknownst to her, download every file and data source from her computer.”

Foreign countries target academic research with cyber as well as human espionage. Last month, the U.S. Justice Department indicted nine Iranians affiliated with a Tehran-based company called the Mabna Institute for hacking into144 American universities since 2013 to steal sensitive data and intellectual property on behalf of the Islamic Revolutionary Guard Corps, which gathers intelligence for the Iranian government. Using a technique known as “spear-phishing,” they allegedly compromised the accounts of 8,000 professors worldwide, and almost 3,800 in the U.S., by sending them emails that appeared to come from colleagues at other schools.

How should the US government, and universities, respond to the surge in academic espionage? That’s a hard question, and as an investigative

reporter, I'm far more proficient at exposing problems than at prescribing solutions. But, because of the significant benefits of the globalization of higher education, which I enumerated earlier, I don't believe in capping or curtailing the influx of international students and professors.

Instead, I think universities should be smarter and more sophisticated about the intelligence ramifications of research collaborations, student and faculty exchanges, academic conferences, and international admissions. For example, I'd like to see more training and courses in intellectual property rights; contractual agreements for cross-border collaborations that spell out each side's access to data and equipment; and orientation sessions for conferences and study-abroad programs that include tips on recognizing come-ons from intelligence agencies. And if students or alumni are exposed as foreign spies, universities should deny or revoke their degrees, rather than looking the other way.

Long overlooked, foreign espionage on campus is finally drawing attention. China's "use of nontraditional collectors, especially in the academic setting, whether it's professors, scientists, students, we see in almost every field office that the FBI has around the country," FBI Director Christopher Wray testified to Congress earlier this month. "It's not just in major cities, it's in small ones as well,

it's across basically very discipline. And I think the level of naivete on the part of the academic sector about this creates its own issues. They're exploiting the very open research and development environment that we have."

Academia ignores espionage at its peril. As long as American universities conduct vital research, place alumni and faculty in the upper echelons of government and business, and—perhaps most important—remain a bastion of access and international culture in a fearful, locked-down world, they will attract attention from intelligence services. Ultimately, unless they become more vigilant, spy scandals could undermine their values, tarnish their reputations, and spur greater scrutiny of their governance, admissions, and hiring.

As Americans, we're all concerned, and rightly so, about foreign intelligence services interfering in our elections. Like democratic elections, a robust, open, and intellectually curious system of higher education is a hallmark of our society. We should take pains to protect it as well.

Summary of major points:

* The globalization of American higher education has many benefits, but one worrisome side-effect is targeting of universities by foreign and domestic intelligence agencies.
* Universities have paid little attention to this threat, and are ill-prepared to deal with it. Collaborations with foreign researchers rarely have written agreements regarding access to data and equipment, and courses on intellectual property are rarely offered except in law schools.
* China is especially active in seeking research secrets at US universities. In one case at Duke University, a Chinese graduate student used a variety of strategies to poach Pentagon-funded research on ways of concealing weapons. After returning to China, he started a competing institute and company with Chinese government funding.
* China's "brain gain" programs, which woos China-born scientists in the US to return home, create potential incentives for research theft.
* American research is at risk not only on campus but also at academic conferences, where foreign intelligence services may try to cultivate professors or download data from their laptops.
* Foreign countries target American university research with cyber as well as human espionage.