Foreign Bribery and Illegal Exports

What the Scientific Community Should Know

— BY MARK BRZEZINSKI and ALEX BRACKETT

INTRODUCTION

As research, exchanges and other opportunities take American scientists to the four corners of the globe, travelers must be aware of two sets of regulations that are witnessing unprecedented upticks in enforcement: U.S. export controls and U.S. anti-bribery laws (formally known as the Foreign Corrupt Practices Act or FCPA). Understanding the basics of these laws—and key pitfalls to avoid—is vital not just for industry, but for any individual or organization actively engaged in activities with non-U.S.[1] colleagues, customers or fellow researchers. This is particularly true as globalization offers a growing number of opportunities for partnering with foreign concerns and engaging with non-U.S. persons in settings such as universities.

U.S. EXPORT CONTROLS AND THE "DEEMED EXPORT" ISSUE

The Cautionary Tale of Professor Roth

On July 1, 2009, former University of Tennessee professor John Roth was sentenced to 48 months in prison for violating the Arms Export Control Act through his export of technical data related to a U.S. Air Force research and development contract. Roth's conviction and sentencing, which were upheld by the Sixth Circuit Court of Appeals on January 5, 2011, set off alarm bells in the halls of academia and beyond, and offer lessons that all scientists who rely on foreign research assistants must heed.

Roth's crime was the export of technical data related to the development of specialized plasma technology for use on advanced forms of unmanned aerial vehicles (UAVs). Roth ran afoul of U.S. export control laws by traveling to China with project plans in hard copy, on his laptop and on a memory stick, sharing project data with a Chinese colleague, and having two non-U.S. students work with him on the project. All of these activities occurred without government knowledge or approval, and in spite of warnings from the university and its Export Control Officer to not share sensitive data with foreign nationals.

Roth's case clearly demonstrates the risks associated with export control violations, and the willingness of U.S. law enforcement to pursue severe penalties against individual violators. It also illustrates the risks of "deemed exports," which in Roth's case occurred when he shared controlled technical data with non-U.S. persons (his foreign students) who worked for him inside the United States.

[1] For purposes of U.S. export control laws and regulations, a "U.S. Person" is a citizen or permanent resident alien of the United States.

Understanding Deemed Exports

The export of U.S. goods and technology is governed primarily by two regimes. Defense articles and services categorized by the United States Munitions List (USML), as well as related technical data, fall under the control of the International Traffic in Arms Regulations (ITAR), enacted under the Arms Export Control Act and administered by the U.S. Department of State. All other U.S. goods and technology[2] fall under the Export Administration Regulations (EAR), which are administered by the U.S. Department of Commerce.

If an item-related technical data or defense service is ITAR-controlled, a license is typically required before it may be exported. By contrast, whether a license is required for EAR-controlled exports will vary substantially based on the items and countries involved. In general, most items and technology that are EAR-controlled do not require a license for export to most countries.

"Deemed exports" are the release or transfer of technology or technical data, whether ITAR or EAR-controlled, to a non-U.S. person inside the United States.[3] Physical export out of the United States is not required, and a release can occur simply by sharing information, such as providing access to drives containing the information. Such transfers of data or technology are "deemed" to be exports to the home country of the recipient, and are subject to the same licensing requirements as if the information were being physically exported from the United States to that country.[4]

Although most non-military goods and technology do not require a license for export to most countries, determining whether an item is subject to particular export controls can be a complicated, fact-intensive and highly technical process. Case-by-case analysis is often required because EAR licensing requirements can vary substantially from country to country. Accordingly, organizations and individuals must understand and take care in handling the technology with which they work, particularly when they collaborate with non-U.S. persons or entities, inside or outside the United States, even in academic and other research settings.

"If an item, related technical data or defense service is ITAR-controlled, a license is typically required before it may be exported."

This is all the more critical given a recent increase in export enforcement, marked by cases such as Roth's, as well as greater cooperation and coordination among immigration officials, export control agents, and prosecutors.

THE NEW FCPA ENFORCEMENT CONTEXT

An Aggressive Enforcement Agenda

For some, the word bribery connotes an image of corrupt businessmen with briefcases full of cash. But over the last decade, U.S. law enforcement has made clear that the forms of corruption it deems improper under the FCPA[5] can appear in many shapes and sizes. As a result, scores of companies, industries and individuals have come to learn that practices they had previously considered fairly innocuous may bring them within the sights of FCPA enforcement efforts that have become increasingly aggressive, high profile and costly for those caught in the enforcement crosshairs.

The FCPA prohibits corrupt payment or offer of payment by any U.S. person (wherever located), or on behalf of any U.S. person, of any thing of value to foreign officials for the purpose of obtaining or keeping any business or business advantage (the anti-bribery provisions). It also penalizes any publicly-held company that maintains inaccurate books and records or inadequate internal accounting controls (the books-and-records provisions). Recent FCPA enforcement efforts have been marked by expansive interpretations of jurisdictional reach, including theories of liability that remain largely untested in U.S. courts. They are also noteworthy for substantial settlements regularly reaching into the tens and hundreds of millions of dollars, with eight of the ten largest settlements of all time occurring in 2010.

And enforcement efforts have by no means been limited to U.S. companies and persons.

[2] "Technical data" and "technology" are essentially the same concepts, just using different terminology for the different export control regimes.

[3] *See* 15 C.F.R. § 734.2(b)(2)(ii); 22 C.F.R. § 120.17(a)(4).

[4] The EAR and ITAR consider citizenship differently. The EAR looks to the foreign national's most recent country of citizenship or permanent residence, while the ITAR looks to the foreign national's most restrictive country of citizenship.

[5] Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, *et seq.*

In fact, it is quite to the contrary. As of January 2011, eight of the top ten FCPA settlements of all time involved foreign companies.

The Focus on Pharmaceutical and Medical Device Companies

Within the last 18 months, FCPA enforcement has included a growing shift into industry-targeted enforcement efforts, most notably of the pharmaceutical and medical device industries. These industries have seen rapid growth in international research and development efforts, as well as expanded overseas manufacturing, marketing and sales. They are grappling with an anti-bribery challenge few considered to be a significant issue just a few years ago.

Assistant Attorney General and Department of Justice ("DOJ") Criminal Division Chief Lanny A. Breuer announced the so-called "Pharma Initiative" during his November 12, 2009, keynote address at the Tenth Annual Pharmaceutical Regulatory and Compliance Congress in Washington, D.C. Breuer's speech outlined an aggressive FCPA enforcement agenda focused on companies and individuals. Since then, Breuer and a number of other DOJ and Securities and Exchange Commission (SEC) officials[6] have cemented the message that FCPA enforcement will only increase in the years to come, as part of a more proactive approach to white collar enforcement. This includes deploying tools not typically used in white collar cases, such as wiretaps and the use of undercover agents.

The Pharma Initiative presents an intriguing case study in FCPA enforcement. As described by Breuer in his November 2009 remarks, it is estimated that U.S. pharmaceutical companies generate one third of their sales, worth $100 billion, outside the United States "where health systems are regulated, operated and financed by government entities to a significantly greater degree than in the United States." Per Breuer, this means that many healthcare providers in foreign countries could be considered "foreign officials" and "it is entirely possible, under certain circumstances and in certain countries, that nearly every aspect of the approval, manufacture, import, export, pricing, sale and marketing of a drug product in a foreign country will involve a 'foreign official' within the meaning of the FCPA."

In November 2009, the DOJ and SEC had at least six active FCPA investigations of major medical device companies. Since then, at least five pharmaceutical and medical device companies, both large and small, have confirmed receiving subpoenas and/or letters from the DOJ and SEC putting them on notice that they are under investigation for their international activities. Several practices appear to be under scrutiny, including:

- Bribery, kickbacks or other improper inducements provided in order to drive drug and device sales;
- Drug trials conducted in foreign locations, and the possibility that improper inducements are being offered to influence their outcomes, either directly or through third parties;[7] and
- Increasing investment in facilities located in regions with poor reputations for corruption.

Because FCPA liability can be triggered by provision of any thing of value in exchange for an improper action by the recipient, and there is no de minimis exception, even the offer of low-level benefits can raise difficult questions. This has forced the pharmaceutical and medical device industries to take a close look at their international activities in anticipation of possible scrutiny.

Targeting Individuals

While Breuer's November 2009 speech caused alarm across the targeted industries, its assertion that a significant focus of the enforcement effort would be the investigation and prosecution of senior executives has had a wider and equally significant impact. According to Breuer, "[e]ffective deterrence requires no less . . . . [F]or our enforcement efforts to have real deterrent effect, culpable individuals must be prosecuted and go to jail." Subsequent speeches by Breuer and other law enforcement officials have pressed the same theme.

In a February 25, 2010 speech before the American Bar Association's 24th Annual National Institute on White Collar Crime in Miami, Breuer warned that "the prospect of significant prison sentences for individuals should make it clear to every corporate executive, every board member, and every sales agent that we will seek to hold you personally accountable for FCPA violations." He described "the aggressive prosecution of individuals" as a cornerstone of the DOJ's "very robust FCPA program," which he held out as a model that "typifies how we are approaching crime in corporate America."

These comments were preceded by a July 2009 civil FCPA settlement between the SEC and Nature's Sunshine Products, Inc. where liability was imposed on two company executives based on a "control person" theory. The individuals were held accountable for failing to adequately oversee personnel charged with maintaining accurate books and records and adequate internal controls, even though the executives were not alleged to have engaged in or been aware of the improper payments.

That same month, Frederick Bourke, co-founder of the high-fashion handbag company Dooney & Bourke, was convicted of an FCPA violation and subsequently sentenced to more than a year in federal prison.[8] Bourke was accused only of having known or consciously avoided knowing about a bribery scheme related to the sale of a state-owned oil company in Azerbaijan, demonstrating the risk of third parties creating liability. Bourke, an

[6] The DOJ and SEC share FCPA enforcement jurisdiction.

[7] According to a June 22, 2010, report by the Office of Inspector General of the Department of Health and Human Services, it is "estimated that between 40 percent and 65 percent of clinical trials investigating FDA-regulated products are conducted outside the United States," with 78 percent of all subjects who participated in clinical trials enrolled at foreign sites and 54 percent of all trial sites located outside the United States. HHS, Office of Inspector General, *Challenges to FDA's Ability to Monitor and Inspect Foreign Clinical Trials* (June 22, 2010), at http://oig.hhs.gov/oei/reports/oei-01-08-00510.pdf (last visited Mar. 13, 2011).

[8] FCPA trials are rare. Of the few that have gone to trial since 1991, none has resulted in acquittal.

investor who did not pay any bribes and actually lost money, was convicted because he put his "head in the sand" regarding a deal that was too good to be true in a country with a reputation for corruption.

The DOJ and SEC have since secured convictions, pleas or other settlements in a number of individual prosecutions,[9] including the March 2011 guilty plea of Jeffrey Tesler, a UK citizen involved in the payment of $180 million in bribes over ten years to Nigerian government officials in order to secure $6 billion in contracts to build liquefied natural gas facilities. As part of his plea, Tesler agreed to forfeit nearly $149 million. Cases such as this indicate that law enforcement has no intention of backing off Breuer's mandate to hold culpable individuals accountable.

EMPHASIS ON COMPLIANCE PROGRAMS

Organizations faced with the complex issues and aggressive enforcement environments outlined above have valid reason for concern. However, there are simple, direct steps they can take to insulate themselves from deemed export and FCPA-related risks, such as deploying a risk-based compliance program.

Compliance programs are an increasingly familiar concept, strongly endorsed and encouraged by U.S. law enforcement and the U.S. Sentencing Guidelines. While not mandated by law, the presence or absence of risk-based compliance programs is often one of the first avenues of inquiry in any government investigation. As Breuer stated in his February 2010 speech, organizations can expect to face criminal charges "when the criminal conduct is egregious, pervasive and systemic, or when the corporation fails to implement compliance reforms, changes to its corporate culture, and undertake other measures designed to prevent a recurrence of the criminal conduct."

At their core, compliance programs should derive from a comprehensive risk analysis that categorizes the level of risk and what parts of the organization are most likely to be impacted. This should be supported through tiered training that provides base-level awareness to a wide audience, and more in-depth instruction to a targeted audience of personnel in key positions relevant to risks and program responsibilities. The program should be actively overseen by a high-level official, with regular program audits and reviews conducted to ensure it remains appropriately tailored to the organization's activities and risk profile. The organization should continually reassess and revise the program based on audit and review results, and based on the resolution of specific compliance issues.

Although these efforts do require commitment of resources, such investment is minimal in comparison to the potential downside of an export control or FCPA enforcement action occurring in the absence of a compliance program.

Mark Brzezinski is a partner at McGuireWoods law firm. His practice focuses on regulatory and legal compliance pertaining to sanctions, Export Administration Regulations and the Foreign Corrupt Practices Act. Alex Brackett is an attorney in McGuireWoods LLP.

[9] Both the DOJ and SEC have been focused on FCPA enforcement actions against individuals overall, with a significant recent rise in such cases. Reports indicate that between 2005 and the third quarter of 2010, approximately 104 individuals have faced such enforcement actions. This breaks out by year as follows: 2005 (8 individuals charged), 2006 (9), 2007 (17), 2008 (16), 2009 (42), 2010 (12, as of September 2010).

[10] Pursuant to the U.S. Sentencing Guidelines and the DOJ's Filip Memo governing charging decisions for corporate defendants, a key consideration regarding whether a company has an effective ethics and compliance program is whether the program was in place before law enforcement scrutiny began. See USSG § 8B2.1; USAM, Title 9, Chapter 9-28.000. Recent amendments to the Sentencing Guidelines, effective as of November 1, 2010, include key changes impacting how ethics and compliance programs and the lines of reporting within them should be organized, and provide guidance as to how the compliance program should respond to issues "including assessing the compliance and ethics program and making modifications necessary to ensure that the program is effective."