COLLABORATIVE INNOVATION TECHNOLOGIES

Balancing Creative Workplaces with Global Compliance

Collaboration technologies used to improve innovation hold significant promise, but they also can expose manufacturers to risks involving the transfer of sensitive information to prohibited destinations.

By Christopher Swift

ON DECEMBER 15, 2014, TWO SCHOOLCHILDREN IN TWO separate countries participated in an experiment that could transform the future of work. Seated at computers in Mexico and the United States, the pair connected over a live videoconference supported by Skype's new "Live Translate" application. Each discussed their schools, their homework, and their dreams – one in English, the other in Spanish. And as Skype's online application provided simultaneous translation, the students' classmates burst into smiles, and then, ultimately, cheers.

Christopher M. Swift is an attorney with Foley & Lardner LLP, focusing his litigation practice on national security and international affairs. Dr. Swift was formerly an Enforcement Officer in the U.S. Treasury Department's Office of Foreign Assets Control. Foley & Lardner is a member of the Manufacturing Leadership Council.

Applications like Skype's Live Translate are just one element in a growing universe of Collaborative Innovation Technologies (CITs). Where conventional communications tools merely facilitate connections, CITs foster deeper and richer forms of collaboration. Some, like Skype's application, help users transcend national borders and language barriers. Others envision Augmented Reality (AR) and Virtual Reality (VR) systems that allow colleagues on opposite sides of the globe to share the same immersive workspace. Coming at a time when international competition drives more customized, customer-centric solutions, these emerging technologies could represent the future of manufacturing innovation.

The practical implications are profound. Used creatively, CIT would allow designers, engineers, and managers from different countries and facilities to work collaboratively on a daily basis. By fostering creative, innovative working environments, they can break silos, remove bottlenecks, and streamline solutions—ultimately creating a more resilient and lucrative enterprise. CIT could also help small and medium-sized manufacturers expand their global reach. From attracting international talent to building their customer base, the ability to connect and collaborate with customers anywhere in the world will make it easier to satisfy customers and sustain revenues. This is particularly true for custom applications and high-tech manufacturing, where the services companies provide to customers may be just as important as the products they ultimately make.

Yet for all their promise, these collaborative technologies could also bring unexpected peril. This is because the same systems that foster communication and collaboration between legitimate corporations can also be used for more nefarious purposes. Like any company that conducts business across national boundaries, manufacturers using CIT need to adapt their existing practices to new sources of commercial and compliance risk.

Cross-Border Exposure

U.S. export controls are a case in point. Traditionally, manufacturers focused on the products they made and the places to which they shipped. By determining the proper classification for goods under the Export

Administration Regulations (EAR) or the International Traffic in Arms Regulations (ITAR), it was relatively easy to identify prohibited destinations. The same was largely true for the various economic sanctions programs administered by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC). So long as manufacturers identified parties in sanctioned countries, they could stop prohibited shipments and payments before they occurred.

CIT breaks this product-centric paradigm. Rather than emphasizing specific articles or goods, it enables sharing and collaboration on an international—and often multinational—basis. And in doing so, it fosters the sort of exchanges that could facilitate the transfer of data, technology, and technical information to controlled destinations. Under the ITAR, this could include sharing blueprints for innocuous metal components used in aerospace or defense platforms. In the case of the EAR, it might involve collaborating with foreign persons to operate sophisticated manufacturing equipment. Stated simply, U.S. export control laws can restrict the release of information in much the same way that they prohibit the actual shipment of sensitive goods.

Similar restrictions apply to services. Under the ITAR, U.S. companies cannot help their foreign customers design, build, modify, operate, or even repair weapons systems without prior authorization from the U.S. State Department. The same is true for many components and subsystems that are specially designed for military purposes. In both cases, the goal is to prevent U.S. companies from sharing their technical skills, knowledge, and experience with their foreign counterparts—at least until they secure the proper government authorization.

Similarly, most OFAC sanctions programs prohibit the provision of services to blacklisted countries, entities, or individuals—even in cases when export control laws do not apply. This approach examines transactions rather than the underlying articles or technology. The result is a complex, multi-layered system of regulations governing customers, products, and services in equal measure. Combined with restraints on releasing or transferring information controlled under the ITAR and EAR, these measures cover the full spectrum of innovation and collaboration that CIT enables.

These concerns are particularly pronounced in companies adopting so-called "next generation" manufacturing processes emphasizing higher precision, greater automation, and data-driven production. This is because many of the most innovative manufacturing systems draw on machines, components, and software subject to the EAR. And because the EAR draws no distinction between an Iranian consul-

Collaborative innovation technologies can break corporate silos, remove bottlenecks, and streamline solutions to create a more lucrative enterprise.

tant on a CIT-enabled videoconference and an Iranian consultant on the production line, the same degree of vigilance is required.

Personal Connections

It is easy to view these cross-border risks in terms of countries and markets. From nuclear negotiations with Iran to easing the embargo on Cuba, there is growing public awareness of the role that sanctions export trolls play in U.S. foreign policy. But in many instances, the risks that are most likely to affect U.S. manufacturers stem from individuals rather than nations and regimes. Consequently many of the most successful compliance strategies boil down to two principles: know your customers, and know your people.

These principles will be particularly important in CIT-enabled workspaces. As a general rule, the ITAR and EAR draw few distinctions between an Iranian national working in Toronto and one living in Tehran. In both instances, it is their nationality that matters, not their employer or their location. Similar rules apply under U.S. economic sanctions. So long as a person or company appears on OFAC's list of Specially Designated Nationals (SDNs), their physical location makes no difference. The same is true for individuals who are ordinarily resident in comprehensibly sanctioned countries like Cuba, Iran, and Sudan. Unless these persons take up permanent residence in another country, the sanctions apply wherever they go.

These rules can have a direct impact on cross-border collaboration, particularly in cases where manufacturers form multinational teams to solve design and production problems. Although CIT makes it easier to attract and interact with top-tier talent, it also requires a reasonable level of due diligence into the individuals comprising the team. In many instances, foreign nationals may not realize that they are subject to economic sanctions, much less recognize that certain products and technologies are controlled for export to their home country. Ignorance offers few defenses, however. Because sanctions and export control laws impose strict liability for even inadvertent and unintentional violations, U.S. manufacturers have strong incentives to screen their foreign partners.

Significantly, the same concepts also apply to foreign nationals located inside the United States. Whether working in the same facility or linked via videoconference, foreign students and individuals on work visas still retain their nationality for the purposes of U.S. export control laws. This means that any transfer of ITAR- or EAR-controlled articles, technology, or technical information to such individu-

The new collaborative technologies make it easier to interact with top talent wherever it is, but they also require due diligence into those talented individuals.

als would implicate the same prohibitions described above. With manufacturers seeking highly skilled employees from countries like China, India, and Russia, knowing one's people is now more important than ever.

The recent trend toward "on-shoring" manufacturing does not necessary eliminate these risks. From guest workers and graduate students to foreign customers and visitors, many manufacturers continue to interact with non-U.S. nationals. And while it is true that different companies face different levels of exposure, bringing plants and production home does not mean disengaging with the wider world. If anything, manufacturers engaged in on-shoring are likely to remain engaged with many of the same customers, markets, and partners that they possessed when "outsourcing" their production.

Knowledge and Oversight

Manufacturers confront these challenges regardless of whether they use CIT-enabled solutions. Indeed, none of these rules are new. Nor is there anything intrinsically risky about using CIT per se. So rather than changing the game, these emerging technologies underscore the importance of managing the human dimension in one's business. Manufacturers that embrace CIT without adequately considering these risks may invite government enforcement actions, civil and criminal penalties, and reputational harm. Conversely, those with adequate screening processes and strong compliance programs will be well-positioned to reap the rewards.

In this limited sense, managing sanctions and export controls are similar to the challenges posed under the Foreign Corrupt Practices Act (FCPA) and other anti-corruption laws. Like the FCPA, these regulations make manufacturers liable for the actions of their employees and certain third-party agents. They also implicate transactions in many of the same high-risk countries, including China, Russia, and the Middle East. This

The recent trend toward "on-shoring" manufacturing does not necessarily eliminate the risks associated with foreign nationals.

means that companies with effective anti-bribery and anti-corruption programs are somewhat more likely to have some of the practices and procedures necessary to comply with sanctions and export controls. Although these laws are much more complex than the FCPA, core compliance conceptions like employee training, partner vetting, and maintaining third-party risks still apply.

Managing risk does not require turning a company upside down or creating endless speculation and expense.

Manufacturing executives can also draw general lessons from their efforts to protect trade secrets and prevent industrial espionage. Indeed, many of the measures businesses already use to screen employees and secure their facilities can be adapted to support sanctions and export control compliance. The same is true for data, networks, and servers—including the information systems that may support new CIT applications. In the knowledge economy, cyber security, facility security, and data protection go hand in hand with sanctions and export control compliance.

This observation is particularly true for aerospace, defense, and high-tech manufacturers that support classified U.S. government programs. It also applies to companies with U.S. government contracts, which often contain provisions mandating compliance with U.S. export control and sanctions law. In these cases, inadvertently releasing controlled data to foreign persons can have serious commercial consequences, with debarment and the cancellation of lucrative contracts swiftly eclipsing the associated legal costs. With the U.S. Department of Defense and other federal contracting agencies probing deeply into their suppliers' international activities, routine audits can launch civil and criminal enforcement actions involving multiple agencies with overlapping jurisdictions.

Government enforcement agencies may also assert jurisdiction through other means. Because the EAR and ITAR apply to all U.S.-origin products, the Departments of Commerce and Homeland Security have the authority to inspect shipments before they leave the United States. OFAC, in turn, requires U.S. financial institutions to continuously screen wire transfers and other transactions for sanctioned countries, entities, and persons. Under these circumstances, a manufacturer's freight forwarder, customs broker, or bank can be the first to discover a violation—and are often the first to report it.

Compliance Strategies

Managing these risks does not require turning a company upside down. Nor should they be an endless source of speculation and expense. Instead, manufacturers that collaborate across borders, hire foreign nationals, or serve international customers should adopt a risk-based approach tailored to their unique business profile. As a general rule, the exposure is greater for those making controlled products, using controlled technologies, and selling into high-risk foreign markets. Government contracts can also compound this exposure, even in cases where other risk factors are not present. And much like the FCPA, reliance on third-party agents, dealers, and distributors in foreign markets can present serious concerns.

With these observations in mind, manufacturers that embrace CIT and other forms of cross-border collaboration should carefully consider how these technologies change their global profile. And for those companies that already export, operate, or manufacture abroad, the goal should be to leverage these tools in a manner that catalyzes innovation and growth without incurring additional risk. To those ends, manufacturing leaders should embrace three related compliance strategies:

- **First**, manufacturers should conduct global risk assessments examining where the company operates, what products and services it provides, and how it interacts with foreign parties. Developing and understanding this profile is essential to distinguishing between the compliance challenges that actually exist and those that reside in the realm of speculation. It also provides a basis for tailoring solutions that are relevant to the enterprise and its evolving needs.
- **Second**, manufacturing executives should evaluate existing compliance programs to ensure that they are fit for purpose. In many instances, U.S. companies underestimate the degree to which their foreign agents and affiliates are dealing with blacklisted parties. In others, cautious leaders with a limited understanding of the applicable laws may over-emphasize risk at the expense of legitimate (and potentially lucrative) business pursuits. Neither outcome is consistent with effective compliance.
- **Finally**, manufacturers must treat international compliance as a dynamic endeavor rather than a cost center. As policymakers respond to changing world events, business leaders must also adapt to changing regulatory requirements. There is, to put it simply, no "one and done." Like every aspect of business leadership, managing global risk requires a commitment to auditing performance, evaluating outcomes, and investing in continuous self-improvement.

In the final analysis, the greatest risks are those that manufacturers ignore. Companies that do not know their customers, agents, and employees invite unpleasant—and ultimately expensive—surprises. Conversely, those that proactively engage partners and manage relationships are often in a better position to manage their risk—even when their potential exposure is much greater. In this sense, effective global compliance depends on culture and leadership as much as it does on policies and procedures. As one of our wiser clients recently observed, "Bill To" and "Ship To" are addresses, not customers. **M**

Many of the measures already used to screen employees and secure facilities can be adapted to support sanctions and export control compliance.