Digitizing Export Controls

A Trade Compliance Technology Stack?

By William Alan Reinsch & Emily Benson

Introduction

The United States’ export control structure began as an instrument of the Cold War in 1949. When the Export Control Act became law that year, its three main purposes were to protect the domestic economy, advance U.S. foreign policy interests, and control sensitive exports to enhance national security. The initial concept was simple: the United States and its NATO allies wanted to prevent the Soviet Union from acquiring critical dual-use technology that would benefit their military. To do so, they set up an export licensing system that required allied permission to export sensitive items. There was broad agreement on the goal and, in the early years, a surprising degree of operational consensus among the participating countries. Enforcement was straightforward. The items subject to control were, for the most part, physical—if not manufactured products, then intellectual property embodied in blueprints or schematics—and, if necessary, could be stopped and inspected at the port of departure.

Over the past 25 years, following the collapse of the Soviet Union and the end of the Cold War, the United States has transitioned to a system based on end user analysis rather than the broader approach used with the Soviet Union, though the latter has not disappeared entirely. To supplement an approach based primarily on determining the bona fides of end users, the Bureau of Industry and Security (BIS) issues export licenses that include conditions that might, for example, only allow specified users engaging in specified activity to use the exported item. According to current and former government officials interviewed for this project, when BIS began licensing machine tools, for example, some licenses stipulated that the tools could only work under certain circumstances. In other cases, not only were machines restricted for what they could make, but also the end user was required to print out specifics on what the machine was doing while it was operating, representing a paper trail receipt and analog information flow. Those reports would be sent to BIS, where they would await review and possible enforcement action. Critical technology is increasingly exported via digital media, creating complex enforcement problems. Today, the United States faces new challenges with respect to both licensing policy and enforcement. It must now contend with multiple adversaries, including China, and is being challenged in both the security and economic realms.
The current U.S. government approach to export regulation is largely analog. The government engages in constant outreach, both domestically and abroad, to update industry on the status of regulations and to advise companies on developing proper compliance programs. BIS sometimes makes pre-license checks to make sure the end user is legitimate, and post-export, the agency performs end-use checks and onsite reviews to make sure use of the exported technology is consistent with the license’s conditions. This export control compliance typically involves using tips from industry and public and classified information that suggest a lack of regulatory compliance. However, the government also relies on paper audits to look at records and then conduct investigations. Overall, outside of China, the U.S. government has a relatively robust ability to monitor equipment, which may or may not involve in-person investigations. One of the Department of Commerce’s most effective enforcement tools is to send an IT team into a facility overseas to ensure that an export is being used in accordance with the conditions of its export license. The department wields additional enforcement leverage with foreign companies, including denying licenses and adding foreign firms to the Entity List. While many of the Department of Commerce’s tools are non-digital, it possesses a robust set of pressure tools, as the recent Huawei case demonstrates.

The importance of exports to U.S. economic health, particularly in the information and communications technology (ICT) sector, has also complicated licensing policy. If controls are too loose, U.S. adversaries gain technology they can use against the United States; if they are too tight, the United States threatens to starve its high-tech companies of the revenue they need to develop next-generation products.

In 2018, Congress replaced the long-expired Export Administration Act (EAA) with the Export Control Reform Act of 2018 (ECRA). In contrast to the EAA, which assigned authority for export controls to the Department of Commerce, ECRA assigned it to the president, though there is no sign that will mean significant change in the process by which export licenses are considered. One new development, however, was that ECRA gives the president the responsibility of establishing new controls on “emerging” and “foundational” technologies, though ECRA did not define either of those categories. This requirement to designate technologies as emerging or foundational has led to significant uncertainty throughout the private sector. For example, it is relatively easy to understand how artificial intelligence, writ large, could be construed as both emerging and foundational. Recent testimony by the acting under secretary at BIS stated that the Department of Commerce has thus far identified 37 emerging technologies. However, it is also arguable that algorithms that run micro-targeting for advertisements are neither foundational nor emerging and probably should not be regulated by export controls. Similarly, if semiconductors are designated as a foundational technology—and they clearly are “foundational” in the traditional sense—the result could mean wide-ranging license requirements for standard chips used in everyday items.

Enforcement has also changed. More adversaries, more sanctions, and more trade mean a greater enforcement burden, but the biggest challenge has been the digitization of trade, meaning that critical technology exports are increasingly intangible rather than physical products subject to border inspection. Responding to this challenge, enforcement authorities have enhanced their own tactics but have also put a greater compliance burden on exporting companies to exercise greater due diligence in knowing their customers and monitoring the use of their exports. That enforcement challenge has been met through increased resources, outreach to exporters, and overseas presence performing both pre-license checks and post-license inspections.

A new approach to export controls, although it has antecedents, has been to utilize new software and hardware technology to better track the use of exported items and to restrict access to authorized users. This approach could potentially guarantee that access to certain exported advanced technology would be restricted to authorized end users, and it could give enforcement authorities the capability of knowing
if items were being used consistent with the terms of the license authorizing their export. This paper examines this new technological approach and its potential to enhance compliance and enforcement.

**Technology Overview**

The key elements of such an approach are not entirely new. They include tools to restrict access to an exported product only to verified end-users and review data to monitor compliance with end-user and end-use based restrictions. Access-restricting technologies such as faceprints, voice identification, or thumbprint identification are widely available for a variety of purposes. Monitoring technology in the past has usually focused on tracking the location of an exported product. New approaches currently in development would combine and expand these functions into a single capability that would provide an access limitation function, track the activities of the exported product to ensure it was functioning in accordance with the conditions of its export license, and include a “kill switch” that would permit the exported item to be turned off remotely. Such an approach combines a “hardware roots of trust” capability consisting of a high-grade specialized chip, with an integrated software suite and identification verification components. Together, they represent moderate but significant progress in the security of devices. The chip would be inserted into a product during the manufacturing phase and would not function as an add-on feature post-production, and the software part of the tool receives continuous updates via the cloud. This continuous software patching reduces the burden on end-users to update their devices manually, meaning the device is always as secure as it can be. The third component of this new technology is identification verification systems, including faceprints, voice recognition, thumbprints, or an equivalent measure, through which verified end users can gain access to the device.

Combining these features into an integrated stack—the sum of technological solutions—would represent a step forward in terms of digitizing export licensing and compliance. By capitalizing on new software, hardware, and identification verification systems, this approach can discern who uses what—and in which ways—effectively restricting access only to authorized users. Hardware that permits tracking is commonplace in today’s digital economy and is used in a wide range of goods from consumer devices, such as mobile phones, to commercial products, such as machine tools and mainframe computers. Identification technology is also not new. While using identification verification systems to log in is sometimes controversial, it is already common practice, including at financial institutions. HSBC, for example, asks customers to login into their account by saying into their devices, “my voice is my password.” Finally, kill switch functions are ubiquitous. Smart devices, such as mobile phones and laptops, contain kill switches that can render the devices inoperable if stolen. Kill switches also have common applications software products, military goods, and machine tools.

---

*By capitalizing on new software, hardware, and identification verification systems, this approach can discern who uses what—and in which ways—effectively restricting access only to authorized users.*

This technology stack generates a constant stream of data, which provides real-time updates about the status of items being used. However, this data generation also poses serious questions about the use of algorithmic review and artificial intelligence for compliance purposes (discussed below). With these tracking capabilities, this new technological approach potentially provides an opportunity to streamline export controls and digitize supply chain governance by giving enforcement authorities the ability to
know whether the items exported are being used consistent with the terms of their export license. Before this technology goes to market, however, there are several considerations that both government and the private sector will likely consider before deciding whether or not to encourage widespread adoption of this new technology approach.

**Comparable Products and Capabilities**

The capabilities of this technology are available individually from several companies. Highly secure, integrated chips, for example, are common, and they have long provided tracking data about the location of products. Radio frequency identification (RFID) technology, commercialized in the 1970s, is a data capture system that can identify people or objects without physical contact or line-of-sight. RFID technologies have been *used* in trusted traveler programs since 1995, including the Real-ID program. Recent governmental actions are employing RFID technology to help identify potential threats from unmanned aerial vehicles (UAVs) and to improve management standards for hazardous waste. Standard big-box stores, such as Walmart, require suppliers to enable RFID for their products, underscoring how ubiquitous tracking technology has become.

Similarly, remote software updates have become standard. One of the benefits of purchasing a new Tesla, for example, is that, rather than having to take a vehicle in for regular tune-ups, bugs in vehicles can be patched via remote software updates—all without leaving the driveway. Perhaps most ubiquitous is biometric data, which people around the world provide, often voluntarily, several times each day for mundane activities such as unlocking an iPhone. Social media company TikTok, which has over 1 billion users, recently *announced* in a standard privacy update that it was collecting users’ faceprint and voiceprint data. Each of these components has become standard in today’s digital world, although the combination of the components into one tech stack offers a potential breakthrough in both security and the digitization of compliance. At present, the most similar integrated stack to this one is most likely a Huawei *product*. An outstanding question regarding this technological solution, and one that product manufacturers could likely play a role in determining, is whether personal login data would be exported back to the United States. For machine tools, for example, manufacturers could ask that the solution be designed in a way that allows the personal verification data to stay on the machine. The U.S. government may have an interest in obtaining that data, but it is technically possible to build the technology stack in a way that would be consistent with foreign countries’ domestic privacy standards.

The challenge for the Department of Commerce is that in order to require or encourage the use of this technological solution, the department must be confident in the ability of the tech stack to deliver. While the government would not be precluded from recommending a particular technology, it is more likely that it would establish standards which could, in theory, be met by multiple products, akin to encryption standards. Additionally, if manufacturers integrated this device into their products, the technology could serve as a liability shield for companies exporting sensitive products. Elements of this approach already exist. For example, geolocation and tracking devices allow companies to see if their products are being operated in Iran and shut down those products if they are not being used consistent with the terms of the export license. Similar to tracking technology, the use of identification verification systems is also widespread. While the use of tracking and identification tools has had some success building in additional product security, the integration of these features into one single technology stack could bring about greater transparency and traceability of sensitive exports.
The Universe of Applicable Goods

HOW BIG IS THE UNIVERSE?

Almost all the interviewees for this project—both private sector and government experts—concluded this tech stack would be applicable to a relatively small universe of items. There are some exports for which this technology clearly would not work, such as parts or components. Furthermore, this technology stack could not be embedded in microprocessors, making it not useful for exports of finished semiconductors, although it would be a useful addition to equipment that manufactures microprocessors. However, there are some categories of items where this technology would provide a clear benefit in terms of security. The most prominent is machine tools, which are integral to the production of dual-use goods. A larger example would be a 5G base station, where this tech stack could track not only the product’s location but also who the end users are and how they are operating the station. “Memory coherence” machines and other comparable large systems require major computational power to solve difficult mathematical and scientific questions. For example, the human genome cannot be unlocked without a high-performance computer. Supercomputers are also used to identify and measure highly sensitive subjects, such as nuclear missile trajectories. Even if the universe of applicable goods is relatively small, the types of goods covered would be highly consequential, and facilitating the export of a greater number of these goods, however small, would benefit U.S. industry without sacrificing national security interests.

In public comments to BIS in 2020, Microsoft and OpenAI argued that this new technology “should be reserved for the most sensitive technologies,” but it is possible to envision a much broader universe of applicable items. An existing use case with this technology stack is its use in Xbox gaming consoles, where the technology can monitor user behavior and shut down consoles in case of misuse. This raises questions about the broader universe of Internet of Things (IoT) goods, which could include items such as smart night vision goggles used by foreign police forces. It may seem onerous to collect identification verification data for forces consisting of thousands of individuals, but as financial institutions and social media companies have already demonstrated, users are increasingly providing biometric login credentials by the billion on a daily basis. Another category where this tech stack may be applicable is autonomous items, such as dual-use drones or autonomous undersea vehicles searching for critical minerals in the seabed. While it may not be the explicit intent of Microsoft to encourage the use of its solution in these types of goods, it is easy to foresee a scenario in which private companies may want to use this tech stack as both an additional legal shield and a mechanism for gathering additional data.

When measuring how many items might use this technology, another area of concern relates to what degree a tracking device would disincentivize companies and end users from using the technology. Several experts interviewed for this paper suggested that manufacturers would likely be reluctant to include a tracking chip and surveillance software in their products if they believed the U.S. government could potentially gain access to the data. Furthermore, it is possible that end users would only accept the technology if they had no choice. In other words, a manufacturer might only be willing to include the tech stack in its product if doing so were a condition of obtaining a license and if there were no foreign availability of an equivalent product without the device. In general, government interviewees stressed that the government would have a keen interest in accessing the data, while private sector interviewees underscored significant industry concerns about being compelled to share data with the government and how that would significantly reduce product desirability, particularly in cases where foreign equivalent products exist.
EFFECTS OF COST ON MARKETABILITY

Price is another concern that could potentially affect market size. If the cost of the solution increases the cost of the end product beyond the point sustained by market demand, this could dampen the technology’s desirability. The problem of cost is particularly acute when it comes to smaller companies, which may not be able to afford this technology; a requirement to include it would indicate a government policy that favors larger firms. For larger companies, however, if including this tech stack in an end product increases the possibility of obtaining authorization to export in volume, then it could be well worth pursuing.

Another cost concern relates to combing the data that the tech stack generates. Product manufacturers may be compelled to hire additional staff to monitor and analyze the data, increasing the overall financial burden of using the suite of tools. However, processing the data could be relatively inexpensive through the use of specialized algorithms. In general, private sector experts interviewed for this product argued that if the benefits of exporting the product outweighed the cost of compliance, they would include the technology stack in their products.

DATA STREAMS: GOVERNING AND COLLECTING INFORMATION

Interviewees for this project generally welcomed the approach and thought it would be useful in compliance but acknowledged certain limitations. Interviewees repeatedly questioned who would monitor, collect, and analyze the flow of data from the exported devices. If the universe for applicable items is ultimately relatively small, monitoring would be fairly easy because the affected companies are not very numerous and typically only onboard a handful of new end users each year. In other words, such situations produce a relatively small amount of data that the Department of Commerce can easily process and analyze. However, in certain cases, it may be necessary for the Department of Commerce to conduct an in-person review post-export. For example, engineers evaluating wing spars in-person would be able to discern whether or not they were for use in civilian or military aircraft, and making that determination would be more difficult if it were based solely on a data stream. However, sending personnel to foreign destinations does not necessarily enhance compliance and would not be more cost effective than remote data monitoring. The view expressed by most of the current and former government officials interviewed was that the licensing agencies had neither the bandwidth nor the technical capability to analyze this kind of data, particularly if there were a large number of exported items providing it in volume. As one former government official asked, “If I’m a guy with a gun and a badge, how do I know what all these 1s and 0s mean?” If the government chose to receive the data directly, it is likely that the Department of Commerce would need technical support from other agencies, such as the National Institute of Standards and Technology (NIST).

Although there are multiple possibilities, interviewees for this paper—both in the public and private sectors—believed the most appropriate approach was for the product manufacturer to receive, analyze, and interpret the data and to report any anomalies to the government. Then, the government should have the burden of deciding what action to take, if any. Several companies interviewed expressed concern about the idea of handing over immense swaths of data, both personal and commercial, to the government. If private firms were required to share data with either a developer of a technology stack like this one or the government, the potential for data leaks, including proprietary data, would increase. Furthermore, some interviewees argued that even if the government were not responsible for monitoring the constant flow of data generated by this approach, some agencies would nevertheless be eager to access the data stream. As one former official put it, “The NSA [National Security Agency] is drinking from the firehose.”

In addition to industry reluctance to share data with the government, customers themselves may also resist requirements to share data with the U.S. government, or their respective governments might refuse
to permit them to do so. Therefore, it may assuage customer concerns if the U.S. government only received notice of noncompliance, which would occur if the data stream were sent to the manufacturer of the exported product. While a significant portion of the data combing could be automated, companies and end users would still need to be comfortable with this level of intrusion into their business. Furthermore, using algorithms to comb data invites further questions about who would build the algorithm, measure its accuracy, and monitor its overall performance. This would require engineers to game out all possible scenarios for items exported with the tech stack, including what they could possibly produce. Algorithms would also need to include alert systems that would flag anomalous data. Recent studies have concluded that algorithms can operate ineffectively, largely based on how they were designed and by whom. In the case of export controls, architects of algorithms would need highly specialized training in export control compliance as well as product specification and capabilities. In other words, programmers would need to build algorithms capable of detecting product misuse on a scale from minute deviations to large-scale changes in production output.

A related question concerns who would decide when to invoke the kill switch or “unplug” option. The consensus view was that the decision should be the responsibility of the government. Many government interviewees believed the Department of Commerce would likely consult with other agencies, including the Department of Defense, to define the conditions that would necessitate invocation of the kill switch. For example, if a foreign university using a weather measuring tool suddenly began testing related to nuclear reactions, this end-use shift could result in the tool being shut down, but the U.S. government would first have to define which specific behaviors would result in such strong enforcement measures. Another consideration is the product shutdown itself. For example, if a flight simulator is shut down remotely, the probability that someone is physically hurt is next to nothing. However, if this kill-switch were invoked in an aircraft scenario, the results could be much different. That scenario also illustrates why the decision about what, if any, action to take in the event of evidence of non-compliance is not binary—the choice is not simply whether to turn something off. The government could decide to continue monitoring to determine if the suspicious event was an isolated case; it could make inquiries of the end user; or it could send an enforcement team to inspect the item. Monitoring the data stream and invoking the kill switch also presents questions about where liability would attach.

From the government’s perspective, the manufacturer’s responsibilities are defined by the terms of the license as well as applicable law. For example, the government could include a license condition stipulating that the product manufacturer submit regular reports or specific reports noting any anomalous data. Historically, the government has allowed end users to submit quarterly reports detailing what their items have been manufacturing. In highly sensitive cases, the government has tended to deny licenses for items like machine tools whose capabilities were too sensitive and for which quarterly monitoring and reporting was deemed insufficient. This new technological approach could widen the scope for the government to grant additional licenses that may otherwise have been denied. Either way, the burden would be on the exporter to report anomalous data to the government.

Otherwise, liability would normally be defined in the contract between the end user and the exporting manufacturer. In other words, the contract of sale would determine what happens when an end user is unhappy or when a mistake is made. If a kill switch were employed, for example, the contract would likely define what legal recourse, if any, the end user had, and it would likely stipulate that the end user may only utilize the product in a manner consistent with the terms of the export license. Furthermore, the end user would know that the product contains the technology stack, including the kill switch. In other words, if the end user is unhappy about an outcome, it would amount to a contractual dispute. If
the manufacturers had employed the kill switch at the direction of the government, the government’s sovereign immunity would protect it from suit. Limitations on legal recourse could serve as a deterrent to end users buying products that contain this tech stack.

While similar capabilities—such as tracking tools or identification verification systems—exist throughout the technology ecosystem, the combination of these capabilities into one stack offers the potential to enhance export control and compliance, although it is not a panacea. Private sector interviewees for this project indicated they already used tracking systems to determine the whereabouts of sensitive items. For example, companies can see if a mainframe computer suddenly appears in Iran, in which case the company immediately notifies the U.S. government. In such cases, the add-ons of this new approach—namely the ability to see who is using a product and the ability to shut it down—would represent a significant security enhancement both for private firms and the U.S. government. Nevertheless, serious questions remain about privacy concerns the approach raises and the willingness of firms to use a tracking tool sanctioned by the U.S. government. Other questions remain about the government’s interest in combing data generated by the tech stack and whether the government would request open channels to that data. Another potential limitation of this new technology is that the government may choose to require or encourage its use with a very small number of end products. However, if the universe of applicable items is sizable, the export control implications of this technology could be substantial. As a result, other important questions to assess are which companies would employ this technology, and what the overall market size for it might be.

---

While similar capabilities—such as tracking tools or identification verification systems—exist throughout the technology ecosystem, the combination of these capabilities into one stack offers the potential to enhance export control and compliance, although it is not a panacea.

Role of the Government and Options

If the government is interested in promoting use of the product, it would first need to decide what approach would be most effective. It could: (1) require the use of this type of technology stack as a condition of license approval for items in specified ECCN categories; (2) require that specific exports include access limitation and monitoring capabilities but the government would not specify a particular tool that would have to be adopted; or (3) recommend the use of such a product (either specifically or via technical parameters) but make case-by-case licensing decisions.

First, the government could mandate the use of this technology stack as a license requirement for items such as those covered under ECCN 2B001 (e.g., five-axis machine tools used in milling or grinding, which are used to manufacture critical military technologies such as submarines, engine parts, and nuclear weapons) or ECCN 3B001 items (e.g., lithography equipment used in semiconductor manufacturing). However, such a requirement could incentivize other countries to manufacture a comparable good without a U.S. government-mandated tracking device. This has happened before when unduly tight U.S. export control regulations led to the expansion of the night vision goggles industry in foreign countries. This again underscores the importance of foreign availability in determining whether to integrate this or a similar technology. However, making the inclusion of this tool a condition of an export license is problematic
because the government would not normally endorse specific products of private companies and because creating an artificial economy for a specific product it is not the core function of BIS.

For the second option, the government could make a general statement that would not require a tech stack with these capabilities but signal higher chances of application approval for those that do. It could identify a list of sectors where its recommendation would apply, such as machine tools or high-performance computers. This government approach could support increased compliance without mandating the inclusion of these technology tools. Additionally, if manufacturers voluntarily integrated this device into their products, the technology could serve as a liability shield—a safe harbor—for companies exporting sensitive products.

The most likely outcome is the third option, where the government recommends the inclusion of this suite of capabilities while leaving room to grant licenses on a case-by-case basis. In other words, for selected exports, the government would encourage the use of the technology without requiring it but would take its presence or absence into account when deciding whether to approve a license. While this recommendation would not necessarily create a market for the product per se, it would represent a small but significant step forward in helping companies digitize and enhance their export compliance tools.

Beyond licensing and enforcement considerations, the U.S. government also needs to consider its allies before heading too far down the path of digitization. Among close allies on export controls, such as Germany and the Netherlands, legal authority over national security export controls is linked to multilateral regimes. This means they are not able to control beyond the items on regime lists (although they now have authority to control non-listed items for human rights or public security). The United States, on the other hand, has more flexibility in its approach to export authority, leaving ample room for policy asymmetry among allies. However, if the United States were to decide to require or encourage the use of this new technological approach, it would also be in its interest to seek policy convergence with the governments of foreign producers in order to prevent the foreign availability of comparable products without the embedded tools.

**Concerns**

**HACKABILITY**

Several concerns surround the deployment of this new technology. One significant issue concerns hackability, or to what degree the product itself could remain tamper-proof. Technology firms are no stranger to vulnerabilities, which they confront constantly, as the 2017 Meltdown and Spectre attacks illustrate. By the time these attacks were discovered in January 2018, their perpetrators were able to access all Intel x86 microprocessors and all IBM Power processors. These experiences demonstrate that technologies can never really operate with complete security. Cloud-based technology solutions come with cybersecurity risks of their own and represent a distinct attack surface, but pushing compliance into the cloud increases basic cyber hygiene by centralizing the ability for all end points to be more secure. One way of mitigating risk is to decompartmentalize the stack into sub-components of the technology, which this new approach can accommodate by offering distinct solutions that consist of an integrated hardware element, a separate cloud-based software solution, and user verification credentialing. Each of these individual channels makes the tech stack more impervious to attacks. Even so, industry and government must make a concerted effort to ensure that potential vulnerabilities are discovered prior to wholesale deployment of the technology.
Overall, concerns about hackability relate to the near inevitability that it is only a matter of time before a competitor or adversary develops a similar technology stack. While it may not matter if a foreign adversary develops a similar set of tools, many experts interviewed for this project—government and private sector alike—expressed alarm at the idea that imports from China would someday have an equivalent technology embedded. It could potentially lead to the data of American end users being harvested, particularly if, in the future, the United States is dependent on certain specialized high-tech imports from China. Another concern is that it is difficult to build something that cannot be defeated. Overall, the impermeability of the technology will likely weaken over time, meaning the deployment of this tech stack would be a game of delay, not denial. However, this does not mean that the new solution is not worthwhile. If, in the interim, benefits accrue for both the government and U.S. private sector, this new approach is worth pursuing. If, on the other hand, this technology is a digitized Maginot Line, then resources would be better spent elsewhere. In other words, if the product is compromised and disabled, the inclusion of the suite of tools would not have provided any benefit. However, if the product is compromised and data is transferred to another party, or if a security breach enables a nonauthorized user to operate the equipment, then the approach will have created a problem that would not have existed in its absence.

DATA PRIVACY AND IDENTIFICATION VERIFICATION

One of the most common concerns among interviewees related to privacy. Foreign end users and governments may be reluctant to use a product with an embedded tracking system that the U.S. government has endorsed and to which it may have access. However, several companies interviewed have already employed tracking devices to assist their compliance programs. One company has worked with the Department of Commerce and the FBI regarding black market operators in the United States and abroad. However, when selling products to Europeans, the European firms typically insist that this type of technology be disabled due to concerns about a potential backdoor to the National Security Agency. Nevertheless, in the case of sanctioned countries, such as Russia, companies’ incentives to use this product are naturally higher, meaning it could increase the likelihood of employing the new approach as an extra level of security for compliance. The pervasiveness of basic tracking technology further underscores the added security benefits of the tech stack, which provides more valuable data than simple geolocation coordinates.

In the case of this new technology, privacy is split into two categories: user (personal) data and company (industrial) data. The use of login credentials is an area of concern when it comes to personal data and privacy. For example, the European Union’s General Data Protection Regulation (GDPR) prevents the outflow of personal data to non-EU countries, meaning it is possible that the European Commission would need to be involved at some level for this technology to function, if it permitted the outflow of personal data, and in the absence of a Privacy Shield equivalent. While the tech stack could be developed in a way that prevented personal data from leaving the device, it is likely that the U.S. government would require that the full stream of data be available for review in cases of anomalies. Furthermore, depending on the precise design of the credentialing software, this component itself may, in the future, fall under licensing requirements at the domestic level. As one expert interviewed put it, “The sophisticated are going to ask about it, and the unsophisticated are going to freak out.” However, the use of this technology stack would strengthen export compliance and make the export control regime more effective.

To date, foreign countries’ domestic privacy frameworks, adequacy agreements, and digital chapters of free trade agreements build in protections for personal data but explicitly seek to reduce trade barriers to the trade of commercial data. For example, the European Union’s GDPR only covers personal data. Similarly, the data protection chapter of the Digital Economy Partnership Agreement (DEPA), which New Zealand, Singapore, and Chile signed, also applies only to personal, non-commercial data. This potentially portends
good news for the adoption of the approach, especially if it can be ensured that personal login credentials do not leave the device. In this case, data generated by a product could be exported back to the United States in a manner consistent with foreign countries’ privacy standards as outlined in third-party digital trade agreements. However, should the United States government require that identification verification data be made available upon request, it is possible a foreign government would need to approve the transnational transfer of that data. As a recent CSIS report notes, “Chinese law requires that various forms of data, including ‘personal information and important data,’ be stored in China and undergo a government security review before transfer out of the country, if deemed necessary.” In addition to significant privacy concerns, this new approach potentially invites legal involvement from a foreign government, creating another disincentive for companies to use it.

As an increasing number of countries pursue digital protectionism, stronger barriers to digital trade potentially imperil the efficacy of this technology stack. While a foreign government would not necessarily be involved in the product acquisition process, a government with strong data localization requirements would not want to allow the transborder release of specific reporting data. Data sovereignty issues are deep and complicated by the ability to restrict personal data flows so that the suite of tools is transmitting only commercial data that is absolutely necessary. Even omitting China, countries such as Germany may have fundamental problems with a proprietary chip feeding data to a cloud and U.S.-based locations. Some end users may be uncomfortable with the possibility that their data would be shared with the United States or the Five Eyes countries, but European and Chinese firms likely would express significant hesitation at using the technology and, in some cases, might be required by their government to reject it. However, since this new approach can be broken down into distinct components of technology, it would likely withstand foreign data regulations that might otherwise interfere with the product’s operability. Furthermore, the technology stack can be designed in a way that effectively localizes data on the exported product, meaning login credentials would not need to leave a product if they are being constantly monitored by an internal algorithm.

In addition to whether the extrapolation of commercial data is consistent with a foreign country’s digital privacy standard, companies interviewed for this paper also expressed concerns regarding leakage of proprietary industrial data. If the data includes elements of “secret sauce,” foreign companies may be concerned that a U.S. entity or the U.S. government could access valuable intellectual property. On the other hand, experts interviewed for this project noted that entities such as China’s Semiconductor Manufacturing International Company have concluded that enhancing production capacity is worth the cost of using an invasive surveillance tool, further underscoring that lack of foreign availability reduces barriers and increases incentives for foreign firms to purchase products that contain the technology stack, despite persistent privacy concerns.

HUMAN DECISIONMAKING

As it currently functions, the export control regime has significant human glue and trust components. Certifications are issued electronically, and enforcement officials sometimes follow up in person. When entities violate the terms of their license conditions, there are legal and economic repercussions. The deployment of digital export control mechanisms could reduce human understanding of export controls. While in some ways lacking agility and certain monitoring capabilities, the current export control regime is not without teeth, and it benefits from human intervention at all levels. Many experts interviewed for this project expressed general but profound concerns about relying on technology to achieve compliance. Humans may be able to discern more easily than machines certain features that indicate civilian versus military use. In other words, while technology can be very beneficial, it can also weaken human systems.
and cultures of compliance. Nevertheless, there is ongoing and widespread concern about the efficacy of the current export control regime and the degree to which paper trails can be trusted, particularly since foreign firms can fabricate data and since the data is usually monitored infrequently. Therefore, this new technology fills a crucial gap in both monitoring and compliance and represents a step toward digitizing certain elements of export controls.

The current export control regime is not without teeth, and it benefits from human intervention at all levels. Many experts interviewed for this project expressed general but profound concerns about relying on technology to achieve compliance.

INTERNATIONAL IMPLICATIONS
This new approach also could prompt international reactions. Another consistent concern that interviewees espoused relates to how the suite of tools could potentially incentivize foreign firms or governments to manufacture competing products without it in order to capture market share by making a product that would be more attractive in the marketplace. That would also incentivize them to develop their own domestic capabilities, which would contravene long-term U.S. interests.

In addition, an ongoing point of concern among Europeans is the U.S. CLOUD Act, which requires cloud providers to comply with U.S. government requests for data. In September 2021, France's cybersecurity chief argued that U.S. cloud providers should be excluded from critical EU industries, including the health and financial sectors. The exclusion of U.S. cloud providers from certain critical EU industries may indicate a future unwillingness by the Europeans to accept technologies such as this stack.

This technology suite also raises important questions about the future of the multilateral export control regime. Not unlike the World Trade Organization, the Wassenaar Arrangement has become fractured, particularly over the question of China. In addition, the regime process is generally regarded as too slow to keep up with rapidly changing technology. Instead, supportive governments could pursue plurilateral “mini” export control regimes, each of which would affect a key item where there is only a small number of producers. Such an approach would also open the door to multilateral support for the suite of tools. Foreign availability would become less of an issue if allies worked together to develop a cohesive policy for digitizing export controls. However, the multilateralization of this type of technology would subject the United States to those same parameters, meaning allied governments may want to access data produced on foreign machines used in the United States. To avoid a further bifurcation of the global technology regime, the international community should consider multilateral solutions that break down barriers, not erect them.

Another potential international implication is that foreign use of the tech stack could potentially imperil U.S. national security interests. For example, if a European government included the stack in autonomous drones that the United States was using for covert operations in the Sahel and there was significant outcry in Europe to halt U.S. actions in the Sahel, the European government could require its manufacture to use the kill switch to terminate functionality of the U.S. drones and down the machines. However unlikely this scenario, it nevertheless underscores that a range of far-reaching consequences are possible and deserve consideration prior to the widespread adoption of this approach.
Conclusion: There Is a Future to Write

With technological advancements such as faster machine learning, smarter supercomputing, and more durable autonomous drones, speed is important. Countries are under increasing pressure to move more quickly to maintain competitive edges over their challengers. When countries are in a competitiveness race, they can respond by running faster or by tripping their competitor. Both approaches can be appropriate but running faster is the most effective in the long run, which the Biden administration has recognized.

There remains, however, a role for an export control policy that fully protects U.S. critical technology while advancing industry interests that bolster U.S. technological leadership. To achieve this balance, the government must determine what constitutes a sensitive good, decide the circumstances under which it can be exported, and then maintain an effective enforcement program to make sure exported items are being used in the place and the way the government intended. While individual elements are currently available on their own, the distinct components of these digital tools assembled into one stack—an integrated chip, cloud-based software updates, personal login credentialling, and a kill switch function—could permit the government to enhance compliance and fine tune its risk assessments for specific exports. This would permit it to maintain a particularized system based on end user analysis and avoid moving to a system of broad-based controls and blanket denials.

While individual elements are currently available on their own, the distinct components of these digital tools assembled into one stack—an integrated chip, cloud-based software updates, personal login credentialling, and a kill switch function—could permit the government to enhance compliance and fine tune its risk assessments for specific exports.

Experts interviewed for this project largely concluded that the suite of tools provides compliance capabilities that are important and useful but also acknowledged the yet to be resolved questions the technology poses. Current capabilities allow companies to track where their items are, but this new approach would provide a valuable data stream with more than location information. By discerning who is using it and how, the tech stack provides manufacturing exporters and the U.S. government alike with detailed information that could enhance compliance and provide additional intelligence regarding foreign adversaries’ activities.

Experts agreed that the approach would likely increase compliance, but they also largely thought it would most likely be appropriate for a small universe of items. While this new approach is technically compatible with an extensive universe of items—for example, IoT goods, such as smart night vision goggles or gaming consoles—its use as a compliance tool means it would probably be employed only in select cases for a targeted set of items such as lithography equipment used in semiconductor manufacturing, high-performance computers, or machine tools that produce goods with non-civilian applications. Determining the universe of applicable goods is a decision for the government to make as it refines its export control regime.

Experts also cited areas of concern, namely hackability, privacy, the use of identity verification systems, and international risks associated with the use of this approach. While it is more or less inevitable that
it will be compromised at some point, that is far from a unique feature of a technology product. The vast majority of today’s technology can be hacked, as the Meltdown and Spectre attacks demonstrate, and yet consumers and the government continue to use such products since the benefits of these technologies outweigh the associated risks.

Several experts interviewed for this project also expressed concern that it would only be a matter of time before a competitor, including China, would develop something similar. Policymakers must therefore consider the implications of this technology not if, but when, a similar technology stack is embedded in foreign goods used on U.S. soil. From a strict compliance point of view, that would not necessarily be a bad thing. Other governments with companies producing sensitive items are as interested in compliance with domestic laws as the United States, and a suite of tools that enhances compliance might be welcomed by other governments.

The other side of that issue, however, is privacy, which all experts interviewed pointed to as a key issue surrounding the use of this suite of tools. The primary concern among experts was that inclusion of such an invasive approach would make it less desirable to end users, particularly in cases where there is foreign availability of comparable products. Another privacy concern experts identified is that exporting companies would need to ensure that the inclusion of this technology stack in their products is consistent with local privacy laws. However, as noted above, for sensitive personal data, including biometric data, the suite of tools can be designed and installed in such a way that personal information does not leave the product.

While privacy enhancements can be integrated in the design phase, two questions emerge regarding privacy and the role of governments. First, it is possible the U.S. government could compel companies to share personal data with the government. This is a policy question for the U.S. government to determine since it could stipulate data-sharing requirements as a condition of an export license. Second, some experts expressed concern about potential leaks of commercial data and trade secrets as a result of hacking, including by the foreign government where the product is exported. It is possible, for example, that a host country such as China could obtain sensitive data either surreptitiously or pursuant to its own laws. Other experts expressed concerns about proprietary data leaks. Here, since it is most likely that the data stream will be going back to the exporting manufacturer, the manufacturer would represent an additional point of vulnerability when it comes to data security. Overall, interviewees regarded operational considerations such as hackability and privacy protections as relevant but not dispositive in determining the desirability of the tech stack.

Insofar as the use of this new approach would disincentivize foreign companies from purchasing products, this economic consideration is relevant but only important in cases where there is foreign substitute available without the same feature. Given the size of the universe of applicable items, it is unlikely that foreign availability would be a major concern for product manufacturers. Moreover, in cases where close allies were producing similar goods, allied governments could agree among themselves to harmonize their export control regimes so that all similar products included this or a similar technology stack.

Experts also expressed concerns about whether foreign governments would resist the inclusion of this suite of tools. European governments, for example, might focus on the privacy implications of the approach rather than the compliance advantages it provides. Allies need to resolve this question, possibly through the Wassenaar Arrangement and the other export control regimes. In cases where there is no current foreign availability, the inclusion of this tech stack in U.S. exports may encourage foreign governments to develop their own comparable items without it in the hope of deriving an advantage over the United States in the marketplace. This is similar to the “designing out” problem that has occurred with some U.S. products in the past—notably commercial communications satellites. In the interim, however,
the technology stack offers enhanced compliance and could help facilitate exports that may otherwise have been impossible under current export control rules.

Overall, this new suite of tools is designed to be one of the most secure stacks in technology. Furthermore, it would be constantly updated to make sure that it is as secure as it can be at all times. In a universe of possibilities, companies and governments alike must constantly engage in risk assessments. The suite of tools represents a highly secure and novel combination of existing tools into one integrated product, and the compliance benefits of the technology outweigh the risks that accompany it. In other words, this technology offers a low-risk enhancement to the existing export control regime. The new technology would enable exports that would otherwise be denied, while also permitting the government to refrain from imposing sweeping sectoral controls.

It is ultimately the task of the United States government to decide how it wants to approach this suite of tools. There are three primary options. First, the government could require its use as a condition of license approval for items in specified ECCN categories. Second, the government could require that specific exports include specific capabilities of the approach—such as access limitation and monitoring capabilities—but not specify that a certain company's suite of products itself be included in order to obtain an export license. Third, the government could recommend use of the tech stack but not explicitly link license approvals to it. Requiring the approach discussed in this paper or a similar technology stack that meets the same technical parameters may be counterproductive if it encourages foreign manufacturers to seek a competitive advantage by developing comparable products that lack such capabilities. Taking the presence of such a tool into account when considering license approvals would likely produce less resistance, both from manufacturers and from foreign governments.

As the Biden administration fine-tunes its export control policy and geopolitical strategy regarding China, it should consider the ability of new technologies to close important gaps in export control compliance and to enable exports that would otherwise be denied. Export control policy can play an important role in bolstering U.S. interests, but export restrictions that are too broad risk denying U.S. industry the revenues it needs to develop next-generation technologies while China continues to subsidize its own technological progress. New technologies such as the one discussed in this paper would help advance the administration’s agenda of supporting American firms engaged in international trade, while avoiding the pitfalls of defining “sensitive” items too broadly. The adoption of this new technology stack offers the private sector and government alike the opportunity to increase the number of sensitive exports, enhance short- and long-term security, and digitize the export control regime. While not without risks, the government-encouraged adoption of this or a similar approach would signal to domestic industry and foreign partners alike that the United States is a digital leader in export control regulation—and that it is advancing policies that simultaneously protect U.S. geopolitical and commercial interests.

William Alan Reinsch holds the Scholl Chair in International Business at the Center for Strategic and International Studies (CSIS) in Washington, D.C. Emily Benson is an associate fellow with the Scholl Chair in International Business at CSIS.

This report was made possible by generous support from Microsoft.
ACKNOWLEDGMENTS
Throughout this project, CSIS scholars received invaluable support and input from a wide range of experts and current and former policymakers, who are listed below. The program thanks them, as well as other participants who chose not to be listed, for their counsel. All contributors participated in an individual capacity and not on behalf of the institutions with which they are affiliated. The views expressed in this paper do not necessarily reflect the views of those consulted.

Rich Ashooh  Karen Bland  Stéphane Chardon  Jeannette Chu  Steve Clagett
Paul Freedenberg  Eric Hirschhorn  Jun Kazeki  Kevin Kurland  Michael Laychak
Bruno Leboullenger  Peter Lichtenbaum  Karen Nies-Vogel  Chris Padilla  Kevin Wolf

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2021 by the Center for Strategic and International Studies. All rights reserved.