Export Controls And The Internet Of Things

This article is part of Ice Miller’s Smart Connections | Internet of Things Guide. This guide can serve as a shared resource for your peer group discussions to give everyone the background they need on the business and legal issues behind connected devices. Click here to learn more.

Computers, smart phones and the internet have changed many things about the way we live and work. They have put travel agents, record stores, mail carriers and photo developers out of work. They have given us something to do in elevators other than stare at the floor numbers as they change. They have also given us new ways to communicate with others and given others new ways to gather information about us.

Some of this is new, but not all of the issues that this new technology raises are completely new. As communication technology has evolved from smoke signals and flags to telegraphs, telephones, radios, faxes, desktops, laptops, cell phones, smart phones and now appliances, some things have remained constant:

1. Someone will figure out a way to use the new technology for advertising.

2. Someone will use the new technology for military communications.

3. Someone will use the new technology to try to transmit — or gather — information before others do, and use that information to their advantage.

4. Someone will try to intercept or get access to other people’s private information.

Whenever confidential information is gathered or communicated — whether it is information about when a refrigerator filter needs to be changed, where the Fifth Fleet is going next, or how many miles a teenager drove on her way to the “library” — anyone who uses, manufactures or sells products that gather and communicate information needs to be aware of the fact that there are rules about how that technology and information can be used.

Previous articles in this publication have discussed data privacy and security issues, and some jurisdictions (such as the European Union) have laws that are stricter than those that apply in the United States. If medical information, social security numbers or credit card information is involved, the rules can be even more complicated. HIPAA regulations, for example, can affect how you collect, use, store and transmit health information, even if you are not a health care provider. Many
people don't think about export control issues in the domestic context, because fitness trackers and smart phones are so common that they don't seem terribly important from a national security standpoint. They should.

While many U.S. export controls focus on physical goods, like aircraft carriers, guided missiles and biological weapons, some export control rules also control encryption and communication technology and information. For example, if it is illegal to export parts for a nuclear submarine (it is), it is also illegal to export blueprints, diagrams or specifications about those parts. Under the export laws administered by the U.S. Department of Commerce and the U.S. Department of State, an "export" can include disclosing controlled information to a non-U.S. person even while that foreign person is in the United States. In other words, you can't export a missile without permission, you can't export parts for that missile, you can't export the specifications for that missile, and you can't show a foreigner how to make a missile while they are visiting the United States.

This means that if the new TV in your office’s conference room has a camera for video conferencing, you need to make sure that you don't have a whiteboard in the background that shows controlled information on it during an international video conference. It also means that if someone emails you a controlled diagram and you have that email on your tablet with you when you travel, you should be careful about who sees it. In addition, any device that encrypts the information it is communicating may help you keep it private, but the encryption technology itself — whether it is used for banking, military or just personal privacy purposes — may be subject to export control regulations. If you have never read the license agreement when you upgraded your computer or smartphone software, you might be surprised to learn that by accepting it, you have agreed to use it only in accordance with applicable export controls.

In most cases, buying a consumer product at a big-box store for use by Americans in the U.S. is not very risky (from an export control standpoint). If the product gathers or communicates confidential information, however, or if you are going to take it or send it overseas, you may be involved in a regulated activity that requires a license, even if that information is being used for benign purposes. As a consumer, a good plan to start is by reading the license agreement before you click "I accept."

As a manufacturer or supplier of smart goods or information-gathering services, you need to learn what the rules are to avoid regulatory problems (and/or bad press) if information your products gather is used in a way that the customer wasn't aware or didn't intend. As one example, to ensure that sensitive data does not fall into the wrong hands, the Department of Commerce’s Bureau of Industry and Security administers the Export Administration Regulations, which closely regulates the international transfer of not only commercial and dual-use goods, but also the technologies that protect the information associated with these goods. The EAR includes a Commerce Control List that identifies the various types of EAR-controlled items, including encryption technology. Businesses that are based in the U.S. and plan to export encryption products must evaluate whether the EAR requires them to first file an encryption registration, commodity classification request, or a self-classification report with the Department of Commerce. The consequences for businesses that fail to comply with EAR requirements can be steep, and the Department of Commerce can assess criminal or civil monetary penalties against violators.

**Conclusion**

The internet of things phenomenon is revolutionizing the way consumers and
businesses use, exchange and think about data. Both consumers and businesses must be cautious of the regulatory complexities that may restrict or prohibit seemingly innocuous transfers of information or exports of products. Businesses seeking to capitalize on the internet of things to send information or smart technologies abroad must be especially mindful of their obligations under applicable U.S. export controls laws and regulations.

This publication is intended for general information purposes only and does not and is not intended to constitute legal advice. The reader should consult with legal counsel to determine how laws or decisions discussed herein apply to the reader's specific circumstances.