Do I Need A Lawyer? If You Have to Ask, You Probably Do

Brian M. Gaff, Stephen G. Huggard, and Gregory W. Carey
Edwards Wildman Palmer LLP

The fifth in a series of articles providing basic information on legal issues facing people and businesses that operate in computing-related markets focuses on common legal pitfalls that businesses encounter and when and why businesses should be prepared to get legal advice.

Companies in computing-related markets must be vigilant about not violating—intentionally or unintentionally—a plethora of federal laws that affect most businesses and business transactions. Given the growing number of government laws and regulations focused on commercial activities, companies might not be aware that they've crossed a line until it's too late. In this month's installment, we focus on several areas of federal law that can get businesses into trouble.

Be sure to check the IEEE Computer Society's website for the podcast that accompanies this article (www.computer.org/portal/web/computingnow/computing-and-the-law).

WHAT TO DO WHEN THE GOVERNMENT COMES KNOCKING

Unfortunately, it's more likely than not that at some point a company will receive a letter of inquiry or a subpoena from a government agency—or a business will find itself in the position of having a federal agent make a "house call." In most cases, your company won't be the government's focus. Rather, the "target" will be a customer, employee, or other third party. Usually, this initial contact from the government will catch companies off guard, in which case they need to consider the following.

Always consult a lawyer before "cooperating"

If a federal agency has requested that specific documents or information be turned over, that's a clear signal that some type of substantive investigation into a violation of federal law is under way, in which case the company being asked to provide information or documents should absolutely engage an attorney. In addition to helping a company navigate through how to best respond to the government, an attorney can also attempt to determine how the company fits into the government's investigation and what risks are involved in providing information to the government.

Federal agents love to show up unannounced. The FBI, IRS, and FDA are but three agencies that can appear at your door without warning.

Company employees must be trained ahead of time to understand that they're under no obligation to answer a law enforcement agent's questions before having a chance to consult a lawyer. In some cases, the basic instinct is to try to cooperate fully without getting lawyers involved—especially if the person being questioned is confident that neither he or she nor the company has anything to hide or is not the "target." But this is likely exactly what the agents want. In fact, surprise visits often are done solely because agents think they'll get more information out of someone who hasn't had time to carefully evaluate whether a lawyer should be called.

Remember, agents are almost certainly aware of facts they aren't sharing with you. Just as important, remember that while many of these visits are unannounced, in many cases, they could have been

0018-9162/12/$31.00 © 2012 IEEE Published by the IEEE Computer Society

predicted. If you or your customers have received warning letters or other correspondence from the government that indicates its displeasure with your operations, you should expect a heightened interest in your activities and should retain counsel upon the first contact from the government, if not before. You should note that an investigation can easily spread from the initial area of inquiry as the agents "follow the evidence."

If you do talk to the government, tell the truth

Martha Stewart went to prison for lying to government investigators about her trades—not for insider trading. Similarly, Barry Bonds was convicted for providing a "misleading and evasive" answer to federal investigators—not for participating in a steroid distribution ring. These convictions were based on broad federal laws that make it a crime to knowingly make any false statement—no matter how small or seemingly inconsequential—to any federal agent or agency.

Prosecutors love these laws because often times proving "false statement" charges is easier than proving the more complicated charges that were the basis for the investigation in the first place. So, a person who does talk to the government must tell the whole truth.

LAWS THAT CAN GET BUSINESSES INTO TROUBLE

The following are just a few examples of the various federal laws and regulations that can be landmines for most companies in computing-related markets.

US export and trade-related laws

Most companies are cognizant of US embargoes and know that export laws regulate things like the shipment of tangible products, such as computers and related technology, out of the country. Many companies, however, are unaware of the actual breadth and complexity of the US export laws.

For example, the export laws don't just focus on the shipment of goods out of the country. Merely providing a foreign national access to certain computer-related technology inside the US is an export transaction that may require a license from the Department of Commerce, depending on the foreign national's country of origin. Many companies aren't aware that US export laws put an affirmative obligation on exporters to take certain steps, such as checking government "export denial lists" and doing due diligence on customers in some cases, before undertaking an export transaction.

Broad federal laws make it a crime to knowingly make any false statement—no matter how seemingly inconsequential—to any federal agent or agency.

Computer and technology companies need to be especially vigilant regarding compliance with export laws. Many countries subject to US embargoes, especially Iran, have complex networks of middlemen and front companies that focus on obtaining US-origin goods and technologies, such as computers and related intellectual property, from unsuspecting US companies.

When the US government is alerted to such transactions, agents will almost certainly trace the goods back to the US company from which the goods or technology originated. That company will then be put in a position of proving that it had clean hands. At that point, the assistance of an attorney is crucial. Of course, it would have been better to have consulted counsel before engaging in the transaction. The mere engagement of counsel can be powerful evidence that the company had no bad intent.

US antibribery laws

The US Foreign Corrupt Practices Act is a broadly worded law that makes it a criminal offense for, among other things, any US person or company to pay money or provide anything of value—directly or indirectly—to foreign government officials with the intent to obtain or retain business.

As a result of this broad language, the FCPA covers much more than the typical bribery scenario such as the direct payment of cash. For example, in many countries where corruption is simply a way of life, bribes may be recharacterized as "commissions" or "fees" and end up being improperly recorded on the paying company's books as such. Such payments could easily be violations of the FCPA.

Additionally, many computer companies do business in countries such as China, where it's common for the government to partly own or control "private" companies. In such cases, US companies must be aware that employees of these private companies might qualify as "foreign government officials," which could make seemingly innocent gifts to those people (no matter what the value) violations of the FCPA.

Not only do companies need to investigate any instances of possible bribery, but every company that does business abroad needs to have a robust FCPA compliance program—often designed by a lawyer with FCPA expertise—focused on avoiding violations in the first place.

Laws relating to computers and data storage

All businesses, especially computer and technology companies, need to understand the various federal laws that can be violated when their computers or systems are used improperly. For example, the US

Computer Fraud and Abuse Act makes actions like intentionally accessing a computer without authorization and hacking into a competitor's computer systems federal offenses for which an employer can be held liable for its employees' conduct.

Along these same lines, a company can be held liable for violations of federal copyright laws if an employee infringes on copyrights by downloading and sharing copyrighted material, such as movies or songs, using a company computer.

Also, many companies aren't aware that in instances in which they learn that child pornography is on a company computer or an ISP learns that a website containing child pornography exists on its server, they are required to notify a law enforcement agency and take steps to prevent any further transmission of the images—or face civil or criminal penalties themselves. "Transmission" in this context is a broad concept—even downloading the images to a thumb drive and giving them to counsel could be a problem. Therefore, it's crucial for companies to have internal controls and compliance policies that address these issues.

Unfortunately, doing business these days comes with a wide variety of legal pitfalls. Because of the scope and complexity of federal laws that expose a company to severe civil and criminal penalties, companies need to be proactive and have effective compliance programs in place to educate employees and avoid violations in the first place.

In the end, time and money spent trying to avoid violations will pay enormous dividends, putting a company in a much better position for the day when the government does come knocking.

Brian M. Gaff *is a senior member of IEEE and a partner at the Edwards Wildman Palmer LLP law firm. Contact him at bgaff@edwardswildman.com.*

Stephen G. Huggard *is a partner at Edwards Wildman Palmer. Contact him at shuggard@edwardswildman.com.*

Gregory W. Carey *is an associate at Edwards Wildman Palmer. Contact him at gcarey@edwardswildman.com.*