Joel Michael Schwarz, "International Use of U.S. Corporate Intranets: Legal Risks and How to Avoid Them," *ACCA Docket* 20, no. 2 (2002): 28–45.

INTERNATIONAL USE OF U.S. CORPORATE INTRANETS:

Legal Risks and How to Avoid Them

■ By Joel Michael Schwarz

Suppose you are counsel for a large corporation located in Silicon City, USA, that has offices all over the world.[1] Last year, your information technology ("IT") department decided to link some of your international offices into your Silicon City-based corporate intranet. Recently, an employee in your intranet-linked India office asked you whether he could transmit encryption software to a Hong Kong company. If the employee were to send the encryption software from the United States, you knew that you would need a prior review by the U.S. Department of Commerce's Bureau of Export Administration ("BXA"),[2] as well as a license for the export. But because the corporate office is in India and the recipient company is in Hong Kong, you elected not to seek such review. The entire transaction ostensibly occurred outside of the United States, right? Well, maybe not.

The advent of the public internet and corporate intranets has revolutionized the way that companies conduct business. Today, at the click of a computer mouse, you can share documents and communicate electronically with all of your company's offices, regardless of their location. Linking all of your corporate offices, nationally and internationally, into a single intranet might seem like an efficient use of resources, but there are serious real-world considerations to bear in mind. Although corporate intranets may be borderless, countries still observe borders to enforce their laws. Ignore these borders, and your company may risk civil or criminal liability.

What you might not have realized in the case of the software transmission to Hong Kong is that your Indian office actually accesses the internet through your company's proxy servers located in Silicon City. A proxy server, which will be explained in detail later, acts as an intermediary between a corporate intranet and the public internet. All internet-bound requests and all inbound responses for computers anywhere within the company, at any office linked into the intranet, filter through the proxy server. Therefore, the encryption software export technically occurred through Silicon City and may be subject to U.S. law and BXA review.

Joel Michael Schwarz is counsel on ecommerce for Metropolitan Life Insurance Company ("MetLife") in New York City. He formerly served as the New York Attorney General's special counsel for internet matters in the Securities Bureau, investigating and prosecuting internet fraud and crime. He lectures around the world and testifies before various U.S. and international governmental entities on various ecommerce topics. He has completed certification in advanced information technologies from New York University.

Now, suppose that an employee in your Hong Kong office, also linked into the corporate intranet, logged into a radical underground Taiwan-based website that advocates free speech and an end to communism and posted inflammatory messages on its message board. He vehemently disagreed with China's human rights policy and its policy toward reunification with Taiwan. Unfortunately for you, China, which now rules Hong Kong, has prohibited the posting of any information that it deems subversive, harmful to China's reputation, or harmful to its reunification efforts with Taiwan. Ordinarily, filters that the Taiwanese website owner uses to screen for Chinese internet protocol ("IP") addresses and domain names registered to Chinese businesses or internet service providers ("ISPs") would have prevented your outspoken employee from accessing the website. But because the Hong Kong office employee entered the internet through the Silicon City-based proxy server of your corporate intranet, he appeared to be in the United States. Thus, the screening mechanisms did not filter out his message.

Is your company subject to lawsuit or legal process in China because of the sentiments that your employee posted on the Taiwanese website?

Before agreeing to incorporate international offices into your domestic corporate intranet, you should consider the potential legal pitfalls. You may unintentionally subject your foreign offices to U.S. encryption regulations, for example, and expose your parent company to foreign law. The use of laptops by employees traveling outside of the country also may present a legal risk. Although only time will tell whether the risks highlighted in this article will result in legal action, it is imperative that you maintain a close working relationship with your IT managers and executives and continue to monitor the legal landscape.

TECHNOLOGY BASICS

One way to open up communication with your IT managers is to gain a better working knowledge of the relevant technology. Many continuing education programs offer courses on such subjects as web architecture, routing, and networking. These programs are often designed to provide a foundational introduction to information technology and present an excellent opportunity for you to gain a finer appreciation for the computer terminology and subject matter that you encounter on a daily basis. Although you may know how to bandy about such terms as availability, redundancy, and firewall, few in-house counsel truly understand this technology and how it affects their companies. Once you have gained a command of the technological underpinnings, you can more comfortably and confidently deal with your IT managers and give your company a tremendous competitive edge. Some intranet/internet basics follow:

Proxy Servers

Every computer, whether on the corporate intranet or the public internet, has an internet protocol address. You have probably seen hundreds of IP addresses in electronic documents and emails without being aware of them. An IP address consists of four sets of numbers separated by periods. Thus, an IP address might be 107.34.67.123.

Every computer in your corporate intranet has an internal IP address that is generally known only within your company. In order to mask these internal computers from the public internet, your company probably uses a proxy server, which mediates between your internal computer workstations and the internet, providing security, administrative control

(such as filtering), and caching services.[3] Caching is the storage and serving up, from within the company, of frequently requested webpages, in order to avoid the delay of having to download them over the internet.

Often times, especially at larger corporations, separate pieces of equipment perform many of these functions in a layered configuration. One piece of hardware/software might serve as a proxy server, hiding all of the computers inside the corporate intranet, while others work in combination as a gateway to the internet (a gateway server), a firewall protecting the company's internal technology (a firewall server), and a cache engine, caching commonly accessed documents. For simplicity of reference, however, this article refers to the functions performed by the proxy server, gateway server, cache engine, and firewall, collectively, as the same physical machine, the proxy server.

Whenever your internal users send information over the internet, the proxy server literally strips off the IP addresses of their computers, replacing them with its own IP address. In essence, your proxy server acts as a security guard, jealously guarding your internal systems from prying eyes. It thereby makes it more difficult for a hacker to target an individual computer within your company. Every communication emanating from the intranet appears to be coming from the same location, namely that of the proxy server.

For example, if your corporate intranet links offices in the United States and Hong Kong, all of your U.S. and Hong Kong employees' computers would present the proxy server's IP address to the outside world. Similarly, all responses to computers within your corporate intranet would indicate the IP address of the proxy server, which forwards the information to the appropriate internal users.

Websites on the public internet also have IP addresses. After all, web servers, which are computers themselves, host websites. When you type in a domain name to access a website, that domain name is "resolved" to an IP address, and the IP address is used to retrieve the requested webpage. At its most basic level, domain name resolution involves consulting a server that has a list of IP addresses and their associated domain names and converting the domain name to the associated IP address. So, for example, if you typed in ACCA's

domain name, www.acca.com, the server would convert the domain name to its IP address, 207.196.111.50.

Filtering

In order to limit the type of information flowing in and out of a corporation, most corporate systems run filtering software that automatically screens inquiries. It is not uncommon for corporate systems to use filtering to restrict the websites that individuals within the company may access. Filtering occurs through the use of IP addresses or domain names.

When two systems interact with each other on the internet, they log each other's IP addresses. IP addresses themselves actually correspond to three regions around the world, managed by regional internet registries ("RIRs").[4] The American Registry for Internet Numbers ("ARIN")[5] acts as an internet registry for North America, South America, the Caribbean, and sub–Saharan Africa. The Asia Pacific Network Information Centre ("APNIC")[6] is responsible for the Asian Pacific region,[7] and Réseaux IP Européens Network Coordination Centre ("RIPE NCC")[8] covers Europe, the Middle East, the North of Africa, and parts of Asia.[9] Basically, each of these registries manages large blocks of IP addresses, which it assigns out to companies within its region.

This geographic distribution permits your company's systems to filter out inquiries based on IP addresses. Your company's proxy server can check an entity's IP address against a list of prohibited IP addresses and, if appropriate, deny access. Say, for example, you would like to filter to exclude Asian companies. Your system could secure the list of IP addresses registered with APNIC and exclude all incoming inquiries from those IP addresses.

Domain name filtering takes IP address filtering one step farther. Such filtering involves resolving an IP address to a domain name and consulting a preprogrammed list of prohibited domain names to see whether the domain name in question resides on that list. For example, if you were filtering out all requests from Chinese domain names, you could resolve an IP address to its associated domain name, and if the domain name ended in China's top-level domain, .cn, such

as hongkongcompany.cn, you could deny access to that system.

Routing

The final piece of this technological puzzle pertains to the transmission of information from one location to another. Whether a computer transmits information into or out of your corporate intranet, that information will likely travel to its destination through devices known as routers. These devices literally route or send the information to the destination computer, identified by its IP address.

Currently, there are 4,294,967,296 potential IP addresses.[10] Because of the vast number of IP addresses, it would be inefficient to route to every IP address individually. To expedite transmission, routers send information to large blocks of IP addresses, known as networks. A network can include hundreds, thousands, and even tens of thousands of IP addresses. In fact, your company likely owns a network of IP addresses, as do many other major corporations. Thus, when routing information to an IP address, the router first determines which company owns the network within which the IP address falls. It then forwards the information to the location that the company provided for routing of information to its network. In turn, once the network receives it, the company routes the information to the specific computer of destination.

Now that you have the basics of the technology, let's turn to some of the legal issues identified in the introduction.

FOREIGN ACTIVITY THAT VIOLATES U.S. LAW

Arguably, any time you use a proxy server to send information from within your corporate intranet onto the public internet, you should assess that information in light of federal, state, and local laws applicable in the forum in which the proxy server resides because the transaction technically occurs through that server. To better understand the legal significance of the use of your proxy server in a transaction and because of the unsettled state of the law in this area, we will analyze the significance that the Organization for Economic

Co-operation and Development has placed on the use of a server in ecommerce transactions. We will also explore the few federal court decisions that have latched on to the use of a computer server/system within a state as the basis for the assertion of jurisdiction by that state.

OECD "Permanent Establishment"

Recent changes to the commentary on Article 5 of the Organization for Economic Co-operation and Development's ("OECD") Model Tax Convention are helpful to our analysis of proxy server use as the basis for asessing legal obligations.[11] Although the OECD Convention deals with ebusinesses that conduct their business primarily through web servers, the criteria that it evaluates apply in our context, too.

In considering when the use of equipment within a state/country constitutes the permanent establishment of a presence there, such that the company using the equipment would be subject to local tax obligations, the OECD looks to the company's use of the equipment and queries whether it exceeds the threshold of conducting "preparatory or auxiliary" activities.[12] The OECD also assesses whether the computer equipment at a given location is "fixed,"[13] and "whether the business of an enterprise may be said to be wholly or partly carried on at a location where the enterprise has [the] equipment such as a server at its disposal."[14] Additionally, although "a permanent establishment may exist even though no personnel of that enterprise is required at that location for the operation of the equipment," a permanent establishment is more likely to be found when a technology center and support staff exist at the same locale as the servers.[15]

The Convention distinguishes between companies whose use of servers and other equipment in a given forum is preparatory and fortuitous and companies whose use of such equipment is purposeful and substantial. Your company's use of an intranet proxy server would appear to be more than just preparatory or auxiliary. Although your proxy server might not be used solely for the consummation of transactions, such as the OECD envisions, your company does indeed employ its proxy server as an integral and vital part of its business. This server generally aids and facilitates

all aspects of your company's business, which probably includes consummating corporate transactions. It also serves as the intermediary/gateway/security guard for all information passing in and out of your company's intranet.

As we have discussed, proxy servers do much more than passively route information; they are integral to your company's access to the internet. Indeed, if the proxy server is inoperable, your company will probably not be able to access the internet. Additionally, because the proxy server often exists in your technology center, which includes support staff, your company has an even greater substantive nexus with that location. Based upon these contacts, your company arguably engages in a level of commercial activity within the state in which the proxy server and the technology center reside, such that all activity that occurs through that server could be deemed subject to its laws. A few recent federal court decisions have likewise justified the assertion of state jurisdiction over a company on the basis of its use of a server within the state, further emphasizing the legal significance of proxy servers.

Jurisdiction

In *Intercon, Inc. v. Bell Atlantic Internet Solutions, Inc.*,[16] the Tenth Circuit held that the fact that the defendant had "purposefully availed" itself of plaintiff's Oklahoma mail server for about four months was an adequate basis for asserting jurisdiction over the defendant in Oklahoma. Similarly, in *CompuServe v. Patterson*,[17] the Sixth Circuit ruled that the Texas defendant had purposefully availed himself of CompuServe's systems in Ohio, thus giving that state jurisdiction over the case.

Although the Sixth Circuit found that Patterson had a number of contacts with Ohio, it noted that "the most salient facts of the relationship" were that

Patterson chose to transmit his software from Texas to CompuServe's systems in Ohio, that myriad others gained access to Patterson's software via that system, and that Patterson advertised and sold his product through that system. Though all this happened with a distinct paucity of tangible, physical evidence, there can be no doubt that Patterson purposefully transacted business in Ohio.[18]

It is therefore arguable that federal and state governments might have an interest in applying their laws to activities that occur through and emanate from a company's proxy server.[19] Thus, even in a transaction between two non-U.S. entities, if at least one of those entities links to your intranet, you may need to consider it in light of the laws of the forum in which your company's proxy server is located because the transaction technically occurred through that proxy server.

Risk Scenarios

Returning to the encryption hypothetical in the introduction, if your Indian office links into your intranet and attempts to send encryption software to a Hong Kong entity, you may have to consider that transmission in light of the BXA regulations. This transaction, which uses your U.S. systems and U.S. proxy server, could implicate U.S. laws that would not otherwise be applicable to the transaction. Certainly, U.S. encryption regulations would have very little weight if corporations could skirt them by merely having a foreign office within the same corporate intranet send the information on behalf of a U.S.-based company.

Lest you think that concerns about the use of encryption technologies are not germane to your company, consider two other instances of encryption use that are probably already occurring at your company.

Suppose, for example, that one of your employees, while visiting India on a business trip, decides to dial remotely into the corporate intranet to check her email. Upon reading her email, she notices a request from a Chinese client for a file on which she has been working. This file contains highly proprietary, market-moving information that must be kept confidential. Your corporate policy requires encryption of such files before transmission. Ordinarily, the employee would ask your advice before sending the encrypted file out of the United States, but because she is in India, it does not occur to her to seek counsel. Nonetheless, when she sends the file from within your system, she accesses the internet through your U.S.-based proxy server, thus potentially subjecting the transaction to U.S. law. When she hits the "send" button, she exports encryption technology, potentially in violation of BXA regulations.[20]

Another common risk scenario involves the use of virtual private networks ("VPNs") in remote communications between an employee and your corporate intranet. At its most basic level, a VPN encrypts information on both ends of a communication over the public internet. When an employee remotely logs in to your corporate intranet using VPN software installed on her laptop and running on the intranet, she establishes an encrypted communication session. The employee's laptop encrypts the information before sending it over the public internet, and your corporate intranet decrypts it on the other end. This process then reverses when information is transmitted from within the intranet back to the laptop.

Every time information goes over the VPN connection, in either direction, it is encrypted. Thus, if an employee logs in from outside the United States, the VPN session imports and exports encryption technology, potentially in violation of BXA regulations.

DOMESTIC SYSTEMS SUBJECTED TO A FOREIGN JURISDICTION

Companies often take great pains to use subsidiaries or affiliates in foreign countries to insulate themselves from local obligations and liabilities. By implementing a single intranet that links domestic and international offices, does your company defeat these efforts?

Arguably, if you link all of your corporate offices via a single, common intranet, activities that take place over that intranet could be subject to the laws of every country in which a connected office exists. U.S. companies have already faced legal actions in foreign countries for conduct consummated over the internet, despite their apparent lack of contact with those countries. How much stronger would the argument for foreign jurisdiction be if a company linked offices in those countries into its domestic corporate system? Into the very system used to commit the act that gave rise to the foreign action?

Yahoo and Dow Jones Cases

The recent prosecution of Yahoo.com and Yahoo France in a French court for information posted on its U.S.-based servers clearly illustrates the potential exposure.

In *Union of French Jewish Students and League against Racism and Anti-Semitism v. Yahoo! Inc. and Yahoo France,*[21] the plaintiffs alleged that Yahoo.com had violated a French law prohibiting engagement in activities that glorify the Holocaust by permitting French citizens to bid on Nazi memorabilia. Yahoo actually allowed the Nazi items to be posted only on the Yahoo.com website, which is located in and targeted to the United States, not on Yahoo.fr, which is written in French, located in France, and targeted to French citizens. Nonetheless, despite Yahoo.com's argument that requiring its removal of the Nazi memorabilia auctions from the Yahoo.com website would require it to violate the First Amendment, the French court found for the plaintiffs and ordered Yahoo to remove the items or face substantial per diem monetary penalties. Yahoo subsequently filed an action in the U.S. District Court for the Northern District of California, seeking to overturn the French court's order, alleging, in part, that it compelled Yahoo to engage in an unconstitutional prior restraint on freedom of expression.[22]

On November 8, 2001, the federal court ruled that "Yahoo Inc.'s First Amendment rights trump [the] French court['s] order seeking to force the Internet portal to prevent users there from viewing Nazi memorabilia or pay a $13,000-a-day fine."[23] Attention now shifts back to France's response.

The Yahoo case is not merely an isolated instance spurred by unique public policy concerns. Earlier this year, in a widely publicized case, Australia's Victorian Supreme Court ruled that a plaintiff could sue the U.S. publishing giant Dow Jones & Company for defamation in an Australian court because the plaintiff and others had downloaded the allegedly libelous article in Victoria.[24]

Dow Jones is currently appealing this jurisdictional ruling, arguing that "the article was written in America, by an American for American consumption, and published when it was placed on Dow Jones' servers" in New York.[25] As difficult a battle as Dow Jones now faces, how much tougher would it be if the company had an office in Australia linked into its domestic system? Such a foreign office could be the basis for jurisdiction in Australia because it would provide a direct physical

nexus with the system through which the allegedly defamatory act would have occurred.

Chinese Regulations

Let's return to the freedom-loving employee in the Hong Kong office who posted the inflammatory message about China on a Taiwan-based website. Because China does not grant its citizens a First Amendment right, your Hong Kong-based employee's internet posting criticizing China for its policy on Taiwan would be illegal under Chinese law and might subject the employee to liability. And because your Hong Kong office accesses the internet through your Silicon City-based proxy server, the Chinese police might consider your U.S. system a key link in the crime or, at the very least, a potential source of evidence. Although U.S. law might otherwise shield the employee's conduct, it might not protect your company from liability for activity facilitated through your U.S. systems that has a spillover effect in China.

Privacy Concerns

The use of a common international intranet also creates wrinkles with regard to various countries' privacy laws.

The European Commission's Directive 95/46/EC on Data Protection, which took effect October 1998, prohibits the transfer of personal data to non-European Union ("EU") nations that fail to meet the EU's standards for "privacy protection." In July 2000, the EU and the U.S. Dept. of Commerce approved safe harbor provisions that permit a U.S. company to continue to exchange personal information with companies within the EU as long as the organization annually self-certifies

> that it agrees to adhere to the safe harbor's requirements, which include elements such as notice, choice, access, and enforcement. It must also state in its published privacy policy statement that it adheres to the safe harbor. The Department of Commerce will maintain a list of all organizations that file self certification letters and make both the list and the self certification letters publicly available.[26]

Thus, before accessing and/or transmitting personal information over your corporate intranet from an EU-based office to an office in the United States, you should probably undertake these mandatory

certification steps. The EU Directive prohibits the transfer of personal data to countries outside of the EU that fail to enact adequate privacy protections without regard to whether the transfer occurs over the internet or an intranet or via another method.[27]

SCREENING MECHANISMS

As explained earlier, the use of a common international corporate intranet can interfere with other companies' preprogrammed screening logic to filter out transactions based on geography. It, therefore, increases the likelihood that your system might engage in problematic, if not illegal, transactions.

If a company's proxy server were to log an IP address registered with RIPE, it would presume that the server of the entity displaying the IP address was in Europe, the Middle East, the North of Africa, or parts of Asia. Conversely, an entity displaying an IP address registered with ARIN presumably would not belong to a company in Asia, because ARIN does not manage IP addresses for Asia.

> ### ALTHOUGH U.S. LAW MIGHT OTHERWISE SHIELD THE EMPLOYEE'S CONDUCT, IT MIGHT NOT PROTECT YOUR COMPANY FROM LIABILITY FOR ACTIVITY FACILITATED THROUGH YOUR U.S. SYSTEMS THAT HAS A SPILLOVER EFFECT IN CHINA.

As noted earlier, whenever you link offices outside of the country into your corporate intranet, enabling them to access the internet through a U.S. proxy server, all of those offices project your U.S.-based system's IP address and associated domain name. This projection makes it difficult for other systems to determine the physical location of the computer accessing the internet from behind your proxy server. A computer in your Hong Kong office and a computer in your Chicago office, for example, would both present the same IP address (the proxy server's) to the outside world, thus frustrating the ability of others to perform the screening necessary for them to comply with local law.

Suppose your company's London affiliate goes on the internet to purchase some goods from Mexico and wants price information. Using your company's Silicon City-based proxy server as its access point, the London affiliate would appear to originate in the United States. The Mexican company's web servers, therefore, would calculate the prices for the goods assuming that the North American Free Trade Agreement applied to the transaction and provide more favorable quotes. In reality, however, the benefits of this treaty do not extend to Europe.

Your Silicon City-based proxy server would have misled the Mexican company, and as a result, it may have violated the law. A misleading IP address might also discourage companies from engaging in transactions with your foreign office because they mistakenly believe it is subject to U.S. law, which prohibits the transaction in question.

CURRENTLY, PROBABLY THE MOST EFFECTIVE METHOD FOR RESOLVING ALL THREE OF THE ISSUES OUTLINED ABOVE WOULD BE TO CONNECT YOUR FOREIGN OFFICE TO YOUR CORPORATE INTRANET, BUT PROHIBIT IT FROM ACCESSING THE INTERNET THROUGH YOUR INTRANET.

The same issues can arise with regard to domain name filtering. As you will recall, domain name resolution involves the conversion of an IP address to its associated domain name. If your Hong Kong office were to access the internet through your proxy servers in Silicon City, the resolution of the IP address would yield a domain name registered to your Silicon City-based company. This domain name, therefore, would slip by filters set to screen out Chinese domain names, which end in .cn.[28] As a result, your Hong Kong office would gain access to a system that it would not otherwise be able to access.

SOLUTIONS

To recap, when you link a foreign office into your domestic corporate intranet, you may (1) engage your domestic corporate system in foreign transac-

tions, thereby potentially subjecting the transactions to U.S. law that would not otherwise apply, (2) subject your corporation to lawsuits and legal process by and in foreign countries, and (3) defeat filtering technologies designed to screen out, on a geographical scale, interaction with your system. Problems may also arise when employees use corporate laptops outside of the country. The following question remains: how can you avoid or, at the very least, minimize your company's exposure to these risks?

Technological Answers

Take the following technological steps to avoid or minimize your company's exposure to the risks outlined above:

Use a Local ISP for Internet Access

Currently, probably the most effective method for resolving all three of the issues outlined above would be to connect your foreign office to your corporate intranet, but prohibit it from accessing the internet through your intranet. In order to accomplish this, you would work with your IT team to configure the foreign-office computers so that they cannot access the internet through your U.S.-based proxy server. As a further precaution, you could direct your IT team to configure your U.S.-based proxy server to block computers from the foreign office from accessing the internet.

So does that mean that your foreign office would not have internet access? No, just that it would not have access through your corporate intranet. Instead, your foreign office would have to negotiate with a local ISP to secure internet access. Your IT people could configure the foreign office's computers to connect to the local ISP for all internet access. Your foreign office would then be able to communicate internally over your intranet with all of your corporate offices, regardless of location. At the same time, whenever those computers logged into the internet, they would display the IP address and domain name appropriate for their region because internet access for those computers would go through the local ISP. This arrangement would in turn enable filtering by other systems. In essence, your company would gain the efficiencies and security of using a common intranet, while ensuring that your foreign offices were clearly delineated and segregated to the outside world.

ONLINE:

- Bureau of Export Administration, U.S. Dept. of Commerce, "Commercial Encryption Export Controls," at www.bxa.doc.gov/Encryption/Default.htm.

- Adam Creed, "Dow Jones Appeals Internet Defamation Decision," Sept. 21, 2001, at www.newsbytes.com/news/01/170349.html.

- Encryption:

  - Department of Justice's frequently asked questions pertaining to encryption and encryption policy, available at www.cybercrime.gov/cryptfaq.htm.

  - "Navigating the U.S Government's Export Restrictions on Encryption Technology," available on ACCA Online℠ at www.acca.com/protected/legres/MCC/Rubinoff2.PDF.

  - "NetAction's Guide to Using Encryption Software," includes a discussion of encryption, the expected effect that September 11ᵗʰ might have on encryption policy, and links to various legal resources and guides pertaining to encryption policy and the use of encryption, available at www.netaction.org/encrypt/legality.html.

- Mark Grennan, "Firewall and Proxy Server Howto," Feb. 26, 2000, a foundational discussion of the basics of firewalls and proxy servers, available at www.linusdoc.org/HOWTO/Firewall-HOWTO-2.html.

- Jim Hu and Evan Hansen, "Yahoo Auction Case May Reveal Borders of Cyberspace," CNET NEWS, Aug. 11, 2000, an article on the French case against Yahoo! and filtering technologies, available at news.cnet.com/news/0-1005-200-2495751.html.

- IP address regional registries:

  - American Registry for Internet Numbers ("ARIN"), covering North America, South America, the Caribbean, and sub-Saharan Africa, at www.arin.net.

  - Asia Pacific Network Information Centre ("APNIC"), for the Asian Pacific region, at www.apnic.net.

- Réseaux IP Européens Network Coordination Centre ("RIPE NCC"), for Europe, the Middle East, the North of Africa, and parts of Asia, at www.ripe.net.

- Shannon Lafferty, *In U.S. Court, Yahoo Beats French Order over Nazi Memorabilia,* THE RECORDER, Nov. 8, 2001, at www.law.com (use search word, yahoo).

- National Office for the Information Economy, "Access Prevention Techniques for Internet Content Filtering," Dec. 1999, an assessment of different types of filtering systems and how they work, available at www.noie.gov.au/publications/NOIE/consumer/CSIROfinalreport.html.

- U.S. Department of Commerce, "Safe Harbor Overview," available at www.export.gov/safeharbor/sh_overview.html.

ON PAPER:

- Jack L. Goldsmith, *Against Cyberanarchy,* 65 U. CHI. L. REV., no. 4 (Fall 1998), 1199, article on internet jurisdiction issues, including the application of borders in cyberspace, multijurisdictional regulatory problems, and the issue of spillover effects of one country's laws into another country.

- James C. Goodale, *Could the WTC Attack Have Happened without the Internet?* N.Y.L.J., Oct. 5, 2001, Communications and Media Law section, p. 3.

- Michael Kende, "The Digital Handshake: Connecting Internet Backbones," Office of Plans and Policy, Federal Communications Commission, OPP Working Paper No. 32, Sept. 2000, FCC discussion of internet backbones and how systems are connected.

- Joel Michael Schwarz, *Practicing Law Over the Internet: Sometimes Practice Doesn't Make Perfect,* 14 HARV. J.L.& TECH., no. 2 (Spring 2001), at 657, in which § III(B)(2), "Location of Practice," discusses case law pertaining to the use of a server as the basis for placing the locus of activity within a forum.

Because the foreign office's internet access would now occur through a local ISP, not your domestic proxy server, you would probably not have to worry about U.S. law applying to transactions that occurred between your foreign office and another foreign entity. Similarly, the concern about subjecting your U.S. systems to legal suits and process in other countries, solely because of your foreign office's use of the proxy server, would no longer apply. Of course, this solution would not foreclose the jurisdictional argument that might arise upon your linking a foreign office into your corporate intranet. By using a local ISP for internet access, however, you could argue that you have taken substantive steps to localize the activities of the foreign office and to clearly differentiate this office from your U.S. office.

Forward the IP Address of the Foreign Office

In order for you to link a foreign office into your intranet, whether or not you permit that office's computers to access the internet, you will need to contract with a regional backbone provider or other provider of telecommunication services to physically connect that office into your Silicon City-based systems. Simplistically speaking, this connection could be equated to running a long telephone extension cord from the foreign office into your Silicon City-based system; only in this case, the extension cord is virtual. Internet backbones provide the major infrastructure and cabling used to transmit information over the internet, both throughout the United States and between the United States and other countries. One of the more famous backbones is UUNet. Backbones can be thought of as the internet's interstate and international highway system. Most of the networks that make up the internet connect to and rely upon these internet backbones to move traffic around the country and the world. The networks that link into these backbones can be thought of as the state and local highways that connect to the interstate highways. In order to exchange information transmitted on one backbone, but destined for a network connected to another backbone, these backbones interconnect with one another at certain points, known as network access points ("NAPs"). This connection will usually be through a VPN or a dedicated line. Although this connec-

tion will not enable internet access for individual computers in the foreign office, just connectivity between the foreign office and your Silicon City-based system, the regional backbone provider still assigns an IP address to all traffic running from the foreign office to the Silicon City system (over that private connection). Because this backbone provider is regional, the IP address assigned to those communications will likely be regionalized to where the foreign office is located. To resolve the filtering problem discussed earlier, your IT team can therefore configure your U.S.-based proxy server to present both its own IP address and the IP address assigned to the foreign office computer transmitting the information (that IP address actually belonging to the backbone provider). Essentially, you can forward that IP address, specific to the local provider's region of the world, along with the proxy server's IP address, for use in filtering based upon location.

BY USING A LOCAL ISP FOR INTERNET ACCESS, HOWEVER, YOU COULD ARGUE THAT YOU HAVE TAKEN SUBSTANTIVE STEPS TO LOCALIZE THE ACTIVITIES OF THE FOREIGN OFFICE AND TO CLEARLY DIFFERENTIATE THIS OFFICE FROM YOUR U.S. OFFICE.

Any system interacting with a computer from the foreign office would be aware of both IP addresses and would be able to deny the access request of the foreign office if either of the IP addresses met its filtering criteria. Your company would then be able to link all of your international offices into one intranet and communicate internally through that intranet, regardless of the offices' location. Moreover, because both IP addresses would be available to other systems, those other systems could engage in filtering based upon IP address or domain name.

This solution would not, however, resolve the two other issues discussed in this article. Specifically, we would still have the concern about implicating U.S. law in transactions between your foreign office and another foreign

entity because the internet access of that foreign office would still be occurring through your Silicon City-based system. Similarly, the concern about subjecting your U.S. system to foreign law suits and legal process in other countries would also likely apply.

WHENEVER AN EMPLOYEE REMOTELY LOGS IN TO YOUR INTRANET FROM OUTSIDE OF THE UNITED STATES AND USES YOUR INTRANET TO ACCESS THE PUBLIC INTERNET, THAT EMPLOYEE POTENTIALLY IMPLICATES YOUR COMPANY IN ACTIVITIES THAT VIOLATE LOCAL LAW.

Develop Corporate Policy on Laptop Use

Virtually every country has its own laws and regulations pertaining to the use of the internet and electronic communications. Whenever an employee remotely logs in to your intranet from outside of the United States and uses your intranet to access the public internet, that employee potentially implicates your company in activities that violate local law. And of course, by accessing the internet through your U.S.-based proxy server, that employee might also subject her activities during that session to U.S. law. The VPN example discussed earlier illustrates the potential legal pitfalls.

In order to avoid problems associated with employee laptop users remotely accessing your corporate intranet, you should consider establishing a general corporate policy that requires legal review—or review by a trained IT person—before an employee may use a laptop in a foreign country. Although this requirement might seem onerous on its face, there are many factors that you should consider when assessing international laptop use. Simply carrying a laptop into certain countries could be deemed violative of the laws of these countries. Countries, such as China, that censor speech and information, could deem criminal the mere presence of certain information on a laptop. For example, China requires the registration of "all communications software."[29] Would the presence of unregistered VPN communications software on an employee's laptop therefore violate this requirement?

Even if you approve an employee's use of a laptop abroad, you may still wish to implement a policy prohibiting that employee from remotely using the corporate intranet to gain internet access. Arguably, by permitting that employee to access the internet through your intranet, any of his or her activities that violate local law could potentially embroil your company in a foreign legal battle.

Communicate with IT Managers

Your IT managers are probably making decisions on a daily or weekly basis that have legal consequences of which they are unaware. You may have encountered a situation already in which your IT department has transmitted personal information to another entity for the purpose of testing a new system without adequate contractual or security protections.

In order to protect your company in today's electronic environment, you must communicate openly and regularly with your IT executives and managers. Some executives and managers understand the legal significance of their actions and will contact you before undertaking those actions. Others are unaware of the legal effects of their actions or realize that their actions may have legal significance, but are reluctant to contact your legal department, either because they do not feel comfortable doing so or because they believe they will get the run-around and will not receive a timely response. As in-house counsel handling ecommerce matters, you must work diligently to bring all IT executives and managers on board in order to protect your company. Gaining additional familiarity with the technology, perhaps through the continuing education courses discussed earlier, could facilitate this process.

CONCLUSION

Long before they ever used the internet for commercial purposes, many U.S. companies had established affiliates and subsidiaries in foreign countries. When doing so, they usually isolated the activities of these offices to insulate the parent corporation from foreign laws. By linking foreign offices into a common intranet, however, companies may now unknowingly be defeating the very barriers that they had set up to protect themselves.

Given the unsettled state of the law, you would be wise to consider the political and legal character of a country before agreeing to permit a corporate office there to link into your U.S.-based intranet. Arguably, if your company links all of its offices via a single intranet, activities that take place over that common intranet could be subject to the laws of every country in which an office connected to that intranet is located. You should also keep in mind the inability of other systems to filter out a foreign office when it accesses the internet through your corporate intranet. Similarly, before permitting a foreign office or an employee in another country to use a laptop to access the internet through your intranet, you should consider the possibility that the action might require application of U.S. law.

Although the problems and pitfalls discussed in this article are currently only possibilities, you would be ahead of the game if you spoke now with your IT executives and managers and gained a better understanding of the exposure that your company might face. Electronic communication has opened up a Brave New World. Understanding the technology, as well as the people who use it, is key to mitigating risks and protecting your company from unexpected consequences.

In the long term, it is likely that, as regulators and legislators become more technologically savvy, they will revisit many of our technology-related laws and regulations. In the near term, however, it is clear that, since the terrorist attacks of September 11, 2001, debate pertaining to the exportation of encryption has increased. Congress has begun calling for a tightening of U.S. encryption laws.[30] Some of the encryption issues highlighted in this article may therefore arrive on your desk sooner than you think.

NOTES

1. As used in this article, an office can refer to a company's foreign subsidiary, foreign affiliate, or foreign office of the parent company. For ease of reference in this article, the terms are used interchangeably.
2. *See* Bureau of Export Administration, U.S. Dept. of Commerce, "Commercial Encryption Export Controls," at www.bxa.doc.gov/Encryption/Default.htm.
3. *See* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212840,00.html for further explanation of proxy server.
4. Under the current, 32-bit IP addressing scheme, the entire range of IP addresses available for assignment is from 0.0.0.0 through 255.255.255.255. Certain ranges of IP addresses within this span may not be available because they have been reserved for predetermined functions.
5. *See* www.arin.net/arinintro.htm.
6. *See* www.apnic.net.
7. APNIC is responsible for 62 economies in Asia and Oceania, including Hong Kong, China, and India, among others. *See* www.apnic.net/info/about.html.
8. *See* www.ripe.net.
9. *See* www.ripe.net/ripencc/about/.
10. Every IP address consists of four sets of numbers separated by periods. For example, previously, we had discussed the IP address 107.34.67.123. Each of the numbers in the IP address is referred to as a "byte" of information. Thus, the number 107 is the first byte of information, the number 34 is the second byte of information, and so forth. Basically, an IP address consists of four bytes of information. As you may know, although humans use decimal numbers, which are based on the number 10, computers use a more simplistic method of counting, called "binary" and based on the number two. At its most basic level, a byte consists of eight of these binary digits, called "bits." Therefore, because an IP address consists of four bytes and each byte consists of eight bits, an IP address consists of 32 bits or 32 of these binary digits (you may occasionally hear or read about 32-bit IP addressing. Such a statement means that our current IP addressing scheme uses 32 bits.) Thus, if we have 32 bits in an IP address and each bit has two parts because it is based on the number two, we have a potential number of numerical IP address combinations of two to the 32d power or 4,294,967,296 potential addresses.
11. OECD Model Tax Convention, Changes to the Commentary on Article 5, adopted Dec. 22, 2000, Committee on Fiscal Affairs; a compiled list of the recommended additions to the Commentary on Article 5 of the Model Tax Convention are in the "Draft Contents of the 2002 Update to the Model Tax Convention," which is available at www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-documents-22-nodirectorate-no-10-no-22,FF.html; *see also* www.oecd.org.
12. *Id.*
13. *Id.* at proposed para. 42.4.
14. *Id.* at at proposed para. 42.5.
15. *Id.* at at proposed para. 42.6.
16. 205 F.3d 1244 (W.D. Okla. 2000).
17. 89 F.3d 1257 (6th Cir. 1996), *reh. en banc den.*, 1996 U.S. App. Lexis 24796.
18. *Id.* at 1264-65. *But see* Amberson Holdings L.L.C. v. Westside Story Newspaper, 110 F. Supp. 2d 332 (D. N.J. 2000).
19. Indeed, a law enforcement agency investigating suspected illegal internet activity by someone within a company will usually track the IP address of the proxy server because

that IP address will appear to any systems into which the employee logs. Similarly, if an employee were to send an email, the IP address included in the email header would probably reflect the address of the company's email server, also located in the company's technology center.

20. Pursuant to BXA regulations, companies are restricted in the level of encryption that they may use in encrypting information sent to certain coutnries. This hypothetical presumes that the woman exceeded the level of encryption permitted for use in sending information to China.

21. Tribunal de Grande Instance de Paris (Final Order issued Nov. 20, 2000).

22. Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme et al., No. C00-21275, complaint filed (N.D. Cal., Dec. 21, 2000).

23. Shannon Lafferty, *In U.S. Court, Yahoo Beats French Order over Nazi Memorabilia*, THE RECORDER, Nov. 8, 2001, found at www.law.com, with search word: yahoo.

24. Adam Creed, "Dow Jones Appeals Internet Defamation Decision," Sept. 21, 2001, found at www.newsbytes.com/news/01/170349.html.

25. *Id.*

26. *See* U.S. Dept. of Commerce, Safe Harbor, at www.export.gov/safeharbor/sh_overview.html ("How Does an Organization Join?").

27. According to the U.S. Dept. of Commerce, the "scope of the Directive is very broad," leading the author to believe that there would be no difference between exportation of personal data over the internet and exportation of such data over a corporate intranet. *See* www.export.gov/safeharbor/sh_workbook.html.

28. Obviously, the use of one of the generic top level domain names, such as .com or .net, prevents filtering based upon country code. In order to ensure the success of country-code filtering, companies would have to abstain from purchasing generic top level domain names for their foreign offices.

29. Leon A. Kappelman, "The Big Picture: Free Speech vs. Free Markets," INFORMATIN WEEK, Apr. 17, 2000, available at www.informationweek.com/782/82uwlk.htm.

30. It is widely believed that the September 11th terrorists used encryption and steganography, which is the hiding of encrypted information in another piece of publicly available data, such as hiding an encrypted letter in an image, in planning the World Trade Center and Pentagon attacks and in eluding U.S. intelligence resources. *See* James C. Goodale, *Could the WTC Attack Have Happened without the Internet?*, N.Y.L.J., Oct. 5, 2001, Communications and Media Law section, p. 3.