“Death of the Internet” Brings Dilemmas for Multinational Boards

By Tony Chapelle
The Financial Times – Agenda

Despite a globally accessible Internet is under threat from a growing number of nations — including China, Russia, Iran, Iraq and Vietnam — limiting online access for their citizens to localized computer data servers. In effect, these are national Internets.

Board members and executives at U.S. multinational companies that provide Internet-related services or that conduct business via the Web — or even that just communicate online — need to devise risk management game plans to address these “splinternets.” At some point, companies either may have to face working within a closed technology system or quitting a country altogether. In addition, complying with foreign laws to store all personal Internet data inside the country where the information was produced could cause enormous changes for corporations.

“This issue is below the radar for the vast majority of boards of directors,” writes Joe Grundfest, a business professor at Stanford University Law School and audit chairperson at private equity firm Kohlberg Kravis Roberts, in an e-mail. “Over time, … corporations may learn that access to a range of foreign markets is constrained unless the corporation operates a local Internet site from within that geography. At that point, the issue may well rise to a board level concern, but by then, it may well be too late. U.S. corporations will have a stark choice — comply with the foreign requirements or lose the market to competitors willing to comply.”

Some government-sponsored limitations were spurred by the June 2013 revelations by Edward Snowden that America collects metadata from most electronic communications inside and outside of the country.

David Goldberg, a board member at Graham Holdings, the former Washington Post Company, recently told an audience at the annual Directors College at Stanford that national webs won’t stop the National Security Agency from spying. But Goldberg says the balkanized webs could give foreign businesses competitive advantages over U.S. corporations.

That prospect doesn’t strike one director as unique. “The fact that some countries restrict the use of the Internet is just another risk of doing business when you’re a global corporation,” says Jan Babiak, chairman of Walgreen’s audit committee. She sits on two foreign corporate boards — Experian in the U.K. and the Bank of Montreal. Babiak points out U.S. companies often enjoy advantages over companies in other countries.

On the other hand, Babiak says, “The more countries a company is in, the more complex [its] footprint will need to be to understand regulations, data privacy restrictions [and] corruption laws. Companies that aren’t [global] don’t have those costs in multiple countries, so they’re more likely to have a domestic advantage.”

One industry that’s been hurt is the cloud computing business. “Market conditions for U.S. cloud providers have deteriorated as a result of new doubts about the security and privacy of cloud data,” write researchers Ira Rubinstein and Joris van Hoboken of New York University Law School in their study, Privacy and Security in the Cloud.

For instance, after the Snowden leak, the German government canceled its contract with Verizon’s German cloud storage company because data would be accessible in the U.S. To comply with foreign regulations, cloud service providers (CSPs) will have to alter where they store information under data localization laws. Geographic redundancy, which is considered a way to preserve information security, also increases the risk of running afoul of jurisdictions such as in the European Union, where transferring citizens’ data across borders violates privacy requirements.

Even though these developments are happening overseas, they will still have a major effect on American business. Over the next three years, international restrictions could cost the global cloud computing industry as much as $180 billion in lost revenues, or a 25% opportunity loss, according to Forrester Research, a management consulting and research firm. Among U.S.-based CSPs already being affected are Salesforce, Amazon, Microsoft, Oracle, Google, IBM’s SoftLayer, Verizon’s Terremark, Rackspace and NetSuite. Meanwhile, Germany’s SAP, which is best known for producing customizable enterprise software, is now a top-10 global player in cloud service and also has to adjust on the fly to localized Internets.

National Internets also could severely limit and damage the flourishing online shopping industry, according to international business consultant Judith Barnett. That portion of the U.S. economy is estimated at $1.5 trillion this year. Barnett, a former Commerce Department deputy assistant secretary for the Middle East and Africa, writes in an e-mail that nation-states ought to separate the issues of telecom spying by intelligence organizations from those of limiting the capacity of global companies to offer their products and of consumers to purchase them.

In China and Vietnam, for example, regulations require that corporations prevent internet users from violating regulations not to communicate criticism of the government. That requires a layer of supervision that some companies may not want to conduct. For example, Google pulled its servers out of China in 2010 after citizens in the United States criticized the company for enabling censorship of users.

So far this summer, Russia’s parliament has passed two more Internet- related laws. One, to take effect in 2016, will require websites to keep any personal data from Russian citizens on servers within the country or suffer a government-imposed block. Such a move will almost certainly mean that Russians will lose access to outside Internet information. That would affect traffic for U.S. companies such as Facebook. Another law, handed down on July 31, mandates that anyone using a public Wi-Fi hotspot

must provide identification papers. Other portions of that law will require websites to identify their users to authorities and for bloggers to register with the Kremlin if they have more than 3,000 followers.

Still, information industry experts say foreign governments may be willing to make concessions in order to trade with Western companies.

“Russia may ratify a law controlling what bloggers are able to say, and China may monitor Internet traffic to see what’s happening, but we still trade very actively with them even after sanctions,” says Steve Durbin, managing director of the Information Security Forum (ISF), a London-based global membership organization that produces information tech research and best practices for corporations and other organizations.

“I’m not seeing a disadvantage for U.S. companies,” Durbin says. “Any business of a significant size wants to trade in the U.S., so a compromise will be reached.”

Meanwhile, Durbin, who visits and advises corporate executives around the world, says he’s seeing American businesses adapt to the rules. In the European Union, which requires that cloud services be hosted within member states and that citizens’ personal data not be moved outside, Google and Microsoft, for example, have agreed to store data on local server farms. “The industry therefore has been transparent and asked the clients what they want,” he adds.

Durbin recommends that boards get assurance that their companies comply with localized Internet laws wherever the enterprise operates. That kind of multi-jurisdictional overview increases the role of legal counsel. Some companies can no longer afford a purely American legal perspective even if the general counsel remains based in the States. In addition, the ISF advises leaders to create partnerships with other companies to share information on Internet developments.

Barnett now heads the Barnett Group to advise companies that aspire to enter the Middle East and Africa. She suggests that corporate directors and executives who are concerned about serious limitations on Internet marketing and sales should lobby to push back. “Boards need to construct reasonable yet strong positions and … advocate to appropriate government officials worldwide to not take such draconian steps.”

Babiak, who formerly oversaw EY’s technology security and risk services practice for 47 countries, bluntly recommends that boards first count the costs and benefits of remaining in countries with oppressive Internet laws. “Any country that’s put restrictions on your ability to do business, such as the data servers that people use, may not be a country that you ought to go to,” she says. “There are other low-hanging fruit elsewhere.”