Bill Takes Aim at Corporate Involvement in Internet Censorship

12/29/2011 By Allen Smith

A bill introduced Dec. 8, 2011, and referred to the House Committee on Foreign Affairs would require public companies that provide e-mail service to employees and operate in countries that substantially restrict Internet use to include specific information in their annual reports about Internet restrictions, Todd Taylor, an attorney with Moore & Van Allen in Charlotte, N.C., told *SHRM Online* on Dec. 21, 2011.

The bill, **H.R. 3605**, would require the State Department to report each year on the freedom of electronic information in each foreign country and designate Internet-restricting countries responsible for a systematic pattern of substantial restrictions on Internet freedom.

The bill, called the Global Online Freedom Act, states in its findings that "a number of United States businesses have enabled repressive regimes to compromise the security of Internet users engaged in peaceful discussion of political, social and religious issues and severely limit their access to information and communication channels by selling these governments or their agents technology or training."

And, it adds, "a number of United States businesses have provided repressive governments with information about Internet users who were the company's clients or were using the companies' products, that has led to the arrest and imprisonment of the Internet users."

To help discourage companies' complicity in Internet censorship, Internet communications services companies, including companies that provide e-mail or Internet service to employees, would have to include in their annual reports:

Information relating to human rights due diligence, such as company policies relating to human rights and whether the policies are publicly available and communicated to employees, business partners and other parties linked with its operations.

Policies relating to its collection of personally identifiable information, the contents of wire or electronic communications in electronic storage, the contents of wire communications in a remote computing service and how the company assesses and responds to requests by the governments of Internet restricting countries for disclosure of such information or communications.

If a company provides an Internet search engine or Internet content hosting service, all steps taken to provide users with clear, prominent and timely notice when access to specific content has been removed or blocked at the request of an Internet restricting country.

"Well before the Arab Spring, the power of the Internet to expand space for free expression was

well known. That power was all the more evident during the popular uprisings across the Middle East and North Africa," testified Daniel Calingaert, vice president for policy at Freedom House in Washington, D.C., at a Dec. 8, 2011, House hearing on global Internet freedom.

Digital Censorship

"Authoritarian regimes are well aware of the Internet's power and began years ago to introduce extensive controls over digital media," he said before the House Subcommittee on Africa, Global Health and Human Rights. "Some of them, including China, Iran, Saudi Arabia and Vietnam, have built pervasive, multilayered systems for online censorship and surveillance," he added.

These systems consist of blocks on access to social media applications, technical filtering of Internet content, censorship, clandestine use of paid pro-government commentators, intercepts of e-mails, arrests and prosecutions of cyber-dissidents, intimidation of bloggers and online journalists, and digital attacks on opposition and independent news websites.

"Governments increasingly hold hosting companies and service providers liable for the online activities of Internet users," Calingaert remarked. "Intermediary liability is a central component of China's robust censorship apparatus and is spreading in other countries.

In Vietnam and Venezuela some webmasters and bloggers have disabled the comment feature on their sites to avoid potential liability.
Online surveillance is on the rise too, he said. In Iran, China and Thailand, citizens have been detained or investigated because of tweets they made, e-mails sent to friends or content they downloaded at Internet cafes.

There also have been cyberattacks against human rights and democracy activists, he noted.

The United States should take bolder steps, he advocated, remarking that Congress should "require greater transparency by U.S. companies" and introduce export controls on U.S. technology to repressive regimes to censor online content. "Such actions are critical to reverse the global decline in Internet freedom and to enable hundreds of millions of Internet users around the world to gain greater freedom to express their views openly online," Calingaert stated.

In China, several keyword combinations are blocked online, testified Clothilde Le Coz, the Washington, D.C., director of Reporters Without Borders. "Jasmine," the adjective often applied to the revolution that toppled Tunisia's President Ben Ali, is censored. And it now is impossible to search on the Chinese Internet for a combination of the word "occupy" and the name of a Chinese city.

Social Responsibility

"In the wake of the Arab Spring as well as a number of domestic incidents that activists have seized on to criticize government corruption and abuse, the Chinese government has increased its pressure on Internet companies to improve their internal censorship and surveillance systems, citing the danger of 'online rumors' and holding companies responsible for stopping their

spread," testified Rebecca MacKinnon, Bernard L. Schwartz senior fellow at the New America Foundation in Washington, D.C., and co-founder of Global Voices Online.

"Just as companies have a social responsibility not to pollute our air and water or exploit 12-year-olds, companies have a responsibility not to collaborate with the suppression of peaceful speech," she added.

"Companies should be required to report regularly and publicly on how content is deleted or blocked and how user activities are monitored," MacKinnon stated.

She noted that Google has a website called the Transparency Report that tracks the numbers of requests it receives from governments to take down content or hand over user information, broken down by country. "All companies should be required by law to publicly and clearly report on how they gather and retain user information, and how they share that information both with government and other companies," she concluded.

Allen Smith, J.D., is manager, workplace law content, for SHRM.