Does SOPA + PIPA = CISPA?

by Lynne Bradley, director of ALA Office of Government Relations

They're back! It may be in a different wolf's costume, but the issues surrounding privacy, surveillance, and copyright issues are again before Congress in *CISPA*. At this writing, *Cybersecurity Information Sharing and Protection Act* of 2011 *(CISPA,* H.R. 3523) is one of several bills scheduled in the U.S. House of Representatives during "Cybersecurity Week" in late April.

Like the bills "postponed" earlier this year—*Stop Online Piracy Act (SOPA,* H.R. 3261) and *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* of 2011 *(PIPA,* S. 968), *CISPA* raises major threats to our basic rights under the old bromides of cybersecurity and the surveillance needs of law enforcement.

If passed, H.R. 3523 would permit corporations like Google, Facebook, and AT&T to share vast amounts of electronic communications and personal information with the government and, likely, even with other companies in the name of cybersecurity. ALA remains concerned that essentially all private communications could be obtained by the government and used for many purposes, even enforcement of copyrights.

The bill defines "cybersecurity purpose" as . . . theft or misappropriation of private or government information, *intellectual property,* or personally identifiable information (emphasis added).

CISPA would trump all current privacy laws including the 48-state library record confidentiality laws as well as the federal *Electronic Communications Privacy Act,* the *Wiretap Act,* the *Foreign Intelligence Surveillance Act,* and the *Privacy Act*. A whole new system for our nation's privacy laws and policies would be established and extraordinary intrusions into established privacy rights and civil liberties would be legalized.

Cybersecurity is a very serious, legitimate concern for our nation, our libraries, and higher education institutions. ALA recognizes that legislation is needed to clarify and create an appropriate regime for the government and the private sector to battle cyber-threats. But H.R. 3523 would permit, even require, these companies, ISPs, and other entities to monitor all online communications and share personal information with the government without effective oversight just by claiming the sharing is for "cybersecurity purposes." The government would be able to retain and use the shared information for other purposes, as well.

While most libraries are not typically defined as ISPs (although some could be), ISP services often are some part of the connections in most network or communication systems. The library consequences could relate to cloud computing, higher education networks, privatized libraries and networks, and network/vendor contracts whether intended or not, leading us to assume that libraries, academia, and library users would be seriously affected.

At this writing, ALA has communicated to House members its opposition to H.R. 3523 unless major amendments can be made. The political process is in flux, but we know that major grassroots efforts halted *SOPA* and *PIPA* and have already brought more exposure to the problems with *CISPA*. ALA asks academic librarians to monitor the status of *CISPA* and the other cybersecurity bills (www.districtdispatch.org/) as Congress proceeds in the coming weeks and months. The Senate starts its work sometime in May. Contact your state's U.S. senators and representatives using ALA's Legislative Action Center at http://capwiz.com/ala/home/ to ask Congress to make significant changes to *CISPA* to protect personal privacy, limit needless data collection and retention, and avoid use of this legislative vehicle to address international copyright problems.

Corey Williams is assistant director, ALA Office of Government Relations, e-mail: cwilliams@alawash.org