Cybercrime Treaty Opens Pandora's Box

By Peter Piazza

After four years and 27 drafts, the European Committee on Crime Problems has approved the Convention on Cyber-Crime, an international treaty requiring signatory countries to adopt cybercrime laws and cooperate with other countries in investigations. The treaty is expected to be adopted by the Council of Europe's Committee of Ministers this month. The United States has observer status with the option to choose to ratify the treaty.

The treaty has been lauded by those interested in protecting intellectual property rights, because of the emphasis on fighting copyright infringement. Otherwise there is little consensus about the treaty except that it is a Pandora's box that raises as many questions as it answers.
Opposition to the convention has come from several quarters, including business groups and privacy advocates. One common complaint is that law enforcement was too heavily represented at the expense of business and consumer interests.

"Essentially, the convention is a wish list for prosecutors," says Mark Rasch, vice president of cyberlaw at Predictive Systems, a security consulting company. "It gives them much greater subpoena authority and greater procedural authority." He agrees that there is a need to harmonize procedural rights and definitions of cybercrime. "Otherwise, we run the risks that certain nations will become cybercrime havens," he says. But instead of providing clear answers to cybercrime concerns, Rasch says the treaty raises some ominous questions.

"The real problem from a civil libertarian's standpoint is that the treaty does nothing to restrict the authority of law enforcement to enter upon, either actually or virtually, the territory and sovereignty of another country." He cites the recent "cyberwar" between U.S. and Chinese Web-page defacers. "If we and China were both signatories to this treaty, we might have to either prosecute [the American culprits] here or extradite them to China."

David Sobel, chief counsel of the Electronic Privacy Information Center (EPIC), says that the treaty has not reached a balance between law enforcement requirements and privacy concerns. "The law enforcement powers are spelled out with a great deal of specificity," he says, "while privacy provisions are vague. Privacy language has the feel of an afterthought, and that's not surprising because it was."
Sue Ashdown, executive director of the American ISP (Internet service provider) Association, finds several aspects of the treaty disturbing. First, the treaty defines a "service provider" broadly as "any public or private entity that provides to users of its service the ability to communicate by means of a computer system."

Second, complying with data retention requests from law enforcement agencies around the world would be a burden. The treaty would require service providers "to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days," with the option to renew. "Dealing with [requests to preserve data] on an increasing basis, that's something that a small ISP will have difficulty doing," Ashdown says.

Law enforcement requests are overly broad, she adds. "It would be one thing if they were very narrow: 'This is what we need, so go save that.' But the requests are more like, 'Save everything between A and Z, because we might be able to find something in the middle. She says ISPs would be hard-pressed to comply with these provisions.

Data retention also raises privacy issues, according to Barbara Dooley, president of the Commercial Internet Exchange (CIX), an ISP trade association. Data examined by law enforcement could include information about people not under investigation.

The treaty should be ready to go to member nations for signature by November.