Hughes Hubbard & Reed

Congress Debates P2P Security

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

In a previous post, we discussed "The Secure Federal File Sharing Act" (H.R. 4098), a bill introduced in the House that was aimed to improve security in federal computing by barring federal employees and contractors from downloading, installing, or using peer-to-peer (P2P) software absent prior official approval. The House ultimately passed this bill on March 24, 2010. On June 14, 2010, Senators Claire McCaskill (D-MO) and Robert F. Bennett (R-UT) introduced a companion bill under the same name in the Senate (S. 3484). This bill has been referred to the Senate Homeland Security and Governmental Affairs Committee. The House bill was prompted by a series ofembarrassing leaks of government-held data on everything from nuclear facilities to Army officers' Social Security numbers to confidential congressional ethics investigations. Those ethics panel leaks were labeled by the Recording IndustryAssociation of America as "a powerful catalyst to enact real reforms toprotect consumers." A recent report revealing the troubling degree of insecurity in federal government file transfers will probably only add urgency to the debate on the Senate bill. The study, titled "Why Encrypt? Federal File Transfer Report," was released on May 11, 2010 by MeriTalk, a government IT network, in conjunction with Axway, a company specializing in business-to-business integration software. The report surveyed 200 federal IT and information security professionals. It found that an alarming number of these personnel use unsafe file-transfer methods, including physical media (66%), FTP (60%), and personal email accounts like Gmail or Yahoo (52%). Although 80% claimed their agency had adequate transfer-security policies, only 58% said employees were aware of those policies, and just 42% said such policies were consistently followed. It will be worth staying tuned to see whether these damning statistics will convince the entire Senate to bolster federal file-transfer security — and raise awareness about the issue — by passing the Secure Federal File Sharing Act. One might also wonder whether these legislative developments would influence private-sector policymakers — in corporations and other institutions — to follow the federal government's lead in banning P2P software use. In any event, P2P security initiatives in the private sector may get a direct boost from the federal government through "The P2P Cyber Protection and Informed User Act", introduced by Senators John Thune (R-SD) and Amy Klobuchar (D-MN). If the Secure Federal File Sharing Act seeks to protect the government and the public alike from the dangers of data leaks within federal networks, the Thune-Klobuchar legislation seeks to protect all individual users of P2P software from inadvertently exposing their own private files to the public. Thune said his bill will take aim at "the privacy and security threats associated with" P2P file-sharing. Klobuchar explained to the Minneapolis Star Tribune that "without proper precautions, P2P software can allow anyone on the network to gain access to all the files on your computer, not just the ones you intend to share." She said that because such software often "allow[s] access to private financial or family records, it's an invitation to identity thieves and sexual predators." The Klobuchar-Thune

bill, whose companion legislation has already been passed in the House as the "Informed P2P User Act" (H.R. 1319), includes two major components. First, it would require all P2P software to provide a user with "clear and conspicuous" notice of the program's function, and obtain the user's consent, before the software is downloaded or installed. Second, the bill would make it illegal to prevent a user from blocking, disabling, or removing P2P software. The bill would bestow enforcement authority upon the FTC, which in February 2010 notified about 100 private and publicorganizations that they had suffered P2P-based data breaches. It would be worth speculating on whether this wider regulation of P2P software could ultimately have a chilling effect on the general public's use of programs like uTorrent, Shareaza, Ares, Limewire, and BitComet. If so, one might imagine that content owners may get behind the bill in an effort to stem the losses from P2P-based infringement. The bill has received support from the RIAA, the Direct Marketing Association, Stop Child Predators, and 41 state attorneys general. Stay tuned.

Related Areas of Focus

Media, Technology & Commercial Transactions