INTELLECTUAL PROPERTY ALERT

ROBINSON BRADSHAW & HINSON

NOVEMBER 2009

Mixed News on Privacy Law Front

By Robert M. Bryan and John M. Conley

The past week brought privacy protection news from both the Federal Trade Commission and the state of Massachusetts, the author of the nation's most comprehensive data protection scheme. Under mounting pressure from Congress, on October 30, the FTC delayed the implementation of its Red Flags Rule for privacy protection, this time until June 1, 2010. The Rule applies to financial institutions and a broad range of "creditors" that includes most businesses that provide financing or extend credit. It requires affected businesses to develop and implement written programs to help identify, detect, and respond to patterns, practices, or specific activities ("red flags") that might be evidence of identity theft. In pressuring the FTC, members of Congress were responding to concern about the burden of compliance on recession-strapped small and medium-sized businesses. (For a fuller discussion of the Rule, see http://www.rbh.com/pdf/article_jconley_privacystandards.pdf.

On November 4, the Massachusetts Office of Consumer Affairs issued regulations -- now scheduled to take effect on March 1, 2010 -- to implement the state's expansive new Standards for the Protection of Personal Information (for the full text see http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf). The standards include the following key points: a sweeping requirement that "every person that owns or licenses personal information about" a Massachusetts resident must implement a written information security program that contains administrative, technical, and physical safeguards; a requirement that third-party service providers provide contractual guarantees of information security (this provision does not take effect until March 1, 2012); and, perhaps most controversially, the required encryption of all personal information that will travel across public networks or be transmitted wirelessly. The security program requirement is flexible, taking into account the business' size and resources, the nature and scope of its data collection, and its particular security needs. As the final regulation is written, the encryption requirement applies as long as encryption is "technically feasible." This language is not entirely consistent with FAQs currently posted on the website of the Massachusetts Office of Consumer Affairs and Business Regulation, which apply a reasonableness standard to the encryption requirement. http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf. At present, there is no basis for resolving this apparent inconsistency. Because the regulations are not highly detailed, a number of other questions also remain unresolved, including their application to interstate commerce. http://www.rbh.com/pdf/article_jconley_MAIdentityTheft.pdf