Hughes Hubbard & Reed

States Jump Into the Security Breach Breach

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

As discussed in our recent webinar "Whose Data Is It Anyway: Privacy in the De-Centralized Digital World", currently there is no comprehensive federal statutory scheme to govern the protection of privacy. While lawmakers and agencies at the federal level continue to grapple with developing useful legislation to address privacy and security breach concerns, lawmakers in three states recently introduced legislation in attempts to strengthen their respective state's security breach notification systems. These separate initiatives come on the heels of the issuance of a "Green Paper" on privacy by the U.S. Department of Commerce Internet Policy Task Force, entitled "Commercial Data Privacy and Innovation in the Internet Economy: A DynamicPolicy Framework". One of the Green Paper's key proposals is ensuring "nationally consistent security breach notification rules" through a federal commercial data security breach notification law that sets national standards, addresses how to reconcile inconsistent State laws, and authorized enforcement by state authorities. In early December, 2010, California State Senator Joe Simitian (D-Palo Alto) introduced a bill that, if enacted, would establish requirements for any notice sent to consumers in the event of a security breach. The legislation is intended to update Simitian's landmark 2003 privacy protection which required any business or state agency that loses unencrypted personal information to send a security breach notification letter to consumers whose privacy was compromised and inspired more than 40 states to adopt similar legislation. The proposed bill requires any breach notice to disclose to consumers details of the security breach, including the types of information that were subject of the breach and the date the breach occurred. While the bill is intended to compel business or agencies to be more forthcoming with consumers regarding details of any security breach, former Governor Arnold Schwarzenegger vetoed similar proposals in 2009 and 2010, citing lack of proof that the bills would benefit consumers and would be overly burdensome on businesses. Lawmakers in Virginia introduced legislation in January of this year to expand notificationrequirements following a breach of security with respect to medical information. While under current Virginia law, the requirement to provide notice only applies to organizations, corporations or agencies "supported wholly or principally by public funds", the amended bill would extend the state's requirement to notify individuals of a breach of their medical information to all individuals and public and private entities. The bill also allows the state's Attorney General to impose a civil penalty of up to $150,000 per breach of the security of the system or a series of similar breaches of a similar nature that are discovered in an investigation. The same day that the Virginia bill was introduced, lawmakers in Oregon proposed House Bill 2851 an amendment to the Oregon Consumer

Identity Theft Protection Act. Oregon is currently one of a majority of states whose breach notification laws do not apply to hard-copy records. The newly-introduced legislation would close that gap by requiring notice of an unauthorized disclosure of data contained in such hard copies. While not necessarily inconsistent, the recent proposals in California, Virginia and Oregon make it clear that state regulatory and enforcement schemes in the privacy area have not all achieved a uniform point of evolution. For many years, California had a security breach notification requirement on its books. Virginia's regulation on medical information breaches didn't cover private entities. And Oregon did not provide protection for privacy breaches resulting from disclosure of information on hard copy documents. While the federal government speaks of uniform standards, it is still too early to tell whether those standards will take the form of a detailed, robust notification system, be based on the lowest common denominator among the current state schemes or fall somewhere in between those extremes. We will continue to follow the ongoing developments, at both the state and federal levels, as this debate will no doubt evolve in the coming months and years.

Related Areas of Focus

Media, Technology & Commercial Transactions