INTELLECTUAL PROPERTY ALERT

ROBINSON BRADSHAW & HINSON

FEBRUARY 2009

Expansion of U.S. Data Security Law

By Robert M. Bryan and John M. Conley

It seems as if a new data security disaster is in the headlines every day. In late January, for example, a federal class action suit was filed against Heartland Payment Systems over a credit card data security breach that may be the largest in history. The news from the public sector is no better, as the U.S. Department of Veterans Affairs has just announced that it is paying $20 million to settle a class action resulting from a 2006 data breach that exposed the personal information of millions of current and former military personnel.

Stories like these have triggered a rapid expansion of legal privacy protection in the United States. Historically, this country has lagged far behind Europe in the recognition of privacy as a problem needing legal action. There are still tens of millions of Europeans who remember living under totalitarian regimes that kicked in doors in the middle of the night and demanded to see "papers." Consequently, more than a decade ago, the European Union took a strong position in favor of protecting personal data against any intrusion, public or private, and imposed strict controls on the collection and transmission of such data.

Lacking a comparable historical experience, the United States has been reluctant to view the protection of data privacy as a fundamental right and has been more focused on the cost of data protection and the impact of those costs on business. Until very recently, regulation of privacy came from a patchwork of federal and state sources. With the exception of a few specific sectors such as banking and healthcare, this regulation was weak. The rapid increase in identity theft has changed public thinking and made it clear that an increased level of data protection is necessary in the United States to protect the continued growth of electronic commerce.

The changing role of the Federal Trade Commission (the "FTC") vividly illustrates the rapid evolution of American privacy law. Until the last few years, the FTC's focus was on privacy policies. Companies were not generally required to have a policy but, if they did, they had to live up to whatever promises they made. The FTC has long treated (and still treats) a failure to live up to the terms of an announced privacy policy as an unfair trade practice that violates Section 5 of the FTC Act. Now, however, the FTC has begun to apply Section 5 as if it were a general national data security law. In a series of recent cases, the FTC has taken the position that it is an unfair trade practice for any business to fail to maintain an information security program that is reasonably designed to

protect customers' personally identifiable information, or PII. The consent decrees in these cases indicate that an adequate program must have at least four elements: (i) an employee r esponsible for the program; (ii) the identification of significant internal and external security risks; (iii) the design and implementation of reasonable safeguards to control those risks; and (iv) the periodic evaluation and adjustment of the program.

The states, led by California, have become even more aggressive. One of the first California initiatives concerned notification of victims in the event of a breach of data security. The 2003 law requires "any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, [to] disclose any breach of the security system...to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Personal information includes a name plus a social security number, a driver's license number, or a financial account number together with the required access code, as well as any health information. The notice, which can be written or electronic, must be given in "the most expedient time possible and without unreasonable delay." A company that fails to give notice may be exposed to civil lawsuits, including class actions. Forty- five states, including North Carolina, have now enacted notice laws that are based on the California model and there is increasing talk of a federal notice requirement.

California has also been the leader in requiring that companies maintain a minimum level of data security. Businesses that hold personal information about California residents are required to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." The California law does not specify what constitutes "reasonable security procedures." Other states have begun to follow California's lead in imposing general security requirements, and some of those laws include more specific data security requirements.

Perhaps the most drastic recent change in the law originated in Nevada and has been followed in Massachusetts. A new Nevada law requires that a company encrypt PII before transferring the data "outside of the secure system of the business." A similar Massachusetts regulation, which takes effect on January 1, 2010, may be even stricter. Whereas the Nevada law regulates the transmission of PII, the Massachusetts version also requires the encryption of all portable PII, including data stored on laptops or removable memory devices. In both cases, the scope of the state law is unclear, particularly as it relates to businesses that are physically located outside the state but electronically collect information from state residents. There is also some doubt that the states have the authority to impose their encryption requirements on transactions involving interstate commerce. So the ultimate impact of these laws on business remains to be seen.

On a practical level, the future of data security law is clear: every company that collects or maintains PII should develop and implement a reasonable data security program. There are multiple sources for sensible suggestions for a program, including the Federal Trade Commission manual establishing "best practices" for protecting personal information (which is available on the FTC website) and the California Business Privacy Handbook (which is available on the California privacy website). In our April seminar, we will pull together suggestions from these and other sources to present a pragmatic plan for compliance with the data security obligations.