BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Reproduced with permission from Privacy & Security Law Report, Vol. 7, No. 1, 1/7/2008, pp. 40-42. Copyright © 2008 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Encryption

State Data Security Standards

A legal standard for information security has started to emerge from state information privacy laws and Federal Trade Commission enforcement actions. A Nevada law that will take effect later this year and requires encryption in transit for all personal information takes a leap, the authors argue, by directly mandating encryption for personal data. While the Nevada law does not specify what type of encryption is required, proposed regulations in New Jersey would specify encryption for both stored and in transit communication. Compliance with detailed security standards could become unmanageable if multiple states specify distinct security requirements purporting to govern interstate computer systems, according to the authors.

New State Attempts at Data Security Laws Offer Uncertain Promise

BY ALAN CHARLES RAUL, EDWARD MCNICHOLAS AND COLLEEN THERESA RUTLEDGE

Over the last several years, states have created a patchwork of information privacy laws, which, in combination with Federal Trade Commission enforcement actions, has begun to frame a legal standard for information security. Nevada, however, recently took a leap that others have avoided by directly mandating encryption for personal information. Whether this step will or should be followed, however, is an open question.

Nevada's Encryption Law

Effective Oct. 1, 2008, the new Nevada law, Nev. Rev. Stat. 597.970, mandates encryption in transit for all personal information. Specifically, the measure provides that ''a business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.'' Nev. Rev. Stat. 597.970.

ISSN 1538-3423

Significantly, Nevada's measure provides no specification whatsoever of the type of encryption required. It defines encryption merely as "the use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant, to: (1) Prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound; (2) Cause or make any data, information, image, program, signal or sound unintelligible or unusable; or (3) Prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network." Nev. Rev. Stat. 205.4742. Although such flexibility will certainly not tie the requirements to any particular set of technologies, the breadth of the definition of encryption allows for encryption that does not satisfy current baseline industry standards (usually 128-bit secure socket layer (SSL) encryption)—which could actually bless security precautions across Nevada that are lower than current best industry practices.

Although this provision applies only to businesses "in" Nevada, it will likely have significant effect beyond Nevada's state line.

The scope of the Nevada measure is largely controlled by its definition of personal information. The term "personal information" is defined as a person's first name or first initial and last name in combination with a Social Security, drivers license, or identification card number, or in combination with an account, credit or debit card number and its access code/password. Nev. Rev. Stat. 603A.040. This definition does not include health information, and it provides an exception for truncated Social Security numbers which block out the last four digits of the Social Security number, publicly available information *and encrypted data*. *Id*.

Although this provision applies only to businesses "in" Nevada, it will likely have significant effect beyond Nevada's state line. The statute does not define what may be considered a "business in this state," and, the Nevada Supreme Court has interpreted "doing business" in Nevada through a two part inquiry into the nature of the company's business in the state; and the quantity of business conducted by the company in the state, which is "often a laborious, fact-intensive inquiry resolved on a case-by-case basis." *Executive Mgmt. Ltd. v. Ticor Title Ins. Co.*, 38 P.3d 872 (Nev. 2002). Accordingly, businesses with significant contacts with Nevada may feel compelled to comply with the encryption law, regardless of the location of their headquarters or operational facilities, in much the same way that California's data breach law quickly affected businesses across the country.

Interaction with Data Breach Notification Laws

In the hopes that notification of a breach allows people to take precautions, California became the first state to enact a data breach notification statute in 2002. Cal. Civil Code § 1798.29 (2002). Since then, 39 states (including Nevada), the District of Columbia and Puerto Rico have followed suit.[1] All of these statutes, however, consider a breach to have occurred only when unencrypted personal information is lost. Thus, although they do not require encryption per se, they have been implicitly promoting encryption for the last five years.

Significantly, the new Nevada law applies only to data in transit. Nev. Rev. Stat. 597.970. As of now, no law specifically mandates encryption for *at rest* personally identifiable information. Accordingly, lost backup tapes and laptop cases may not be affected by the provision.

Nevada's decision to require encryption, however, may undercut compliance with its breach notification decision for data in transit. The problem is that the "personal information" covered by the Nevada encryption law is the same information that is subject to Nevada's security breach notification law. Thus, by complying with the breach notification law for data in transit, Nev. Rev. Stat. 603A.220, a company will be *ipso facto* confessing to a breach of the Nevada encryption law, Nev. Rev. Stat. 597.970. A clearer disincentive to comply with the data breach law in such circumstances would be difficult to imagine. Indeed, the new law may well guarantee a lawsuit for every reportable Nevada data breach involving data in transit with a cause of action for negligence per se listed first.

Other Existing Information Security Regimes

This new Nevada measure adds to Nevada's more general data security law (Nev. Rev. Stat. 603A.210), which, along with its breach notification law (Nev. Rev. Stat. 603A.220), are emblematic of most state data protection regimes instituted in the last decade. In the first wave of state mandated security measures over personally identifiable information, a handful of states enacted measures similar to Nev. Rev. Stat. 603A.210, which requires that "[a] data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure." This law also mandates contractual security provisions for agreements that involve the transfer or sharing of personal data of Nevada residents. Nev. Rev. Stat. 603A.210(2). Other states with similar data security measures include Arkansas, California, Maryland, North Carolina, Rhode Island, Texas and Utah.[2] Similar laws took effect in New York and Oregon in January 2008.[3]

[1] Nevada's data breach disclosure law states in relevant part that "[a]ny data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay . . . ." Nev. Rev. Stat. 603A.220.

[2] Ark. Code Ann. § 4-110-104, Cal. Civ. Code § 1798.81.5, Md. Code Ann., Comm. Law § 14-3503, N.C. Gen. Stat. §§ 75-60 to 75-67, R.I. Gen. Law § 11-49.2-2, Tex. Bus. & Com. Code § 48.102 and Utah Code Ann. § 13-44-201.

[3] S.6909C/A.10076D, 2006 Leg. Sess. (N.Y. 2006) *available at* http://op.bna.com/pl.nsf/id/dapn-6u2hps SB 583, 74th Leg., Reg. Sess. (Or. 2007) *available at* http://www.leg.state.or.us/07reg/measures/sb0500.dir/sb0583.intro.html.

In addition to Nevada, states with general data security measures include Arkansas, California, Maryland, North Carolina, Rhode Island, Texas and Utah. Similar laws took effect in January in New York and Oregon.

This wave of statutory mandates for information security will undoubtedly reinforce a standard for information security based on "reasonable and appropriate security safeguards"—a standard also adopted by the FTC in actions alleging unfair acts or practices for failure to maintain reasonable and appropriate security results. See *In re DSW, Inc.*, No. 052-3096, 2005 WL 3366974 (F.T.C. Dec. 1, 2005) (final approval by *In re DSW Inc.*, No. 052-3096, 2006 WL 752215 (F.T.C. March 7, 2006)); *In re BJ's Wholesale Club Inc.*, File No. 042-3160, 2005 FTC LEXIS 90 (F.T.C. May 7, 2005). Similarly, the Privacy Act (which is applicable to the federal government's protection of personal information in its files) has also long required "appropriate safeguards" against unauthorized disclosure of sensitive data. 5 U.S.C. § 552a(e)(10).

The FTC has recommended, but not mandated, encryption, particularly for data in transit.

Consistent with its precedents, the FTC has recommended, but not mandated, encryption, particularly for data in transit. Currently, the FTC recommends that businesses

> encrypt sensitive information that you send over public networks (like the internet), and consider encrypting sensitive information that is stored on your computer network or on disks or portable storage devices used by your employees. Consider also encrypting email transmissions within your business if they contain personally identifying information. . . . When you receive or transmit credit card information or other sensitive financial data, use secure sockets layer (SSL) or another secure connection that protects the information in transit.

FEDERAL TRADE COMMISSION, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2007). California's Office of Privacy Protection also recommends that businesses control access to Social Security numbers by "protect[ing] records containing SSNs, including backups, during storage by encrypting the numbers in electronic records or storing records in other media in locked cabinets." CALIFORNIA DEP'T OF CONSUMER AFFAIRS, OFFICE OF PRIVACY PROTECTION, RECOMMENDED PRACTICES ON PROTECTING THE CONFIDENTIALITY OF SOCIAL SECURITY NUMBERS, 11 (2007).

New Jersey Regulations on the Horizon

Not to be outdone, New Jersey is also proposing to adopt a set of regulations that would create much more specific requirements for industry, including requirements for user authentication access, access controls to files that contain personal information, testing, firewalls configuration standards, anti-spyware protections, current patches, wireless security, and of course, encryption. 39 N.J.R. 1397. These regulations seek to implement New Jersey's Identity Theft Prevention Act (ITPA), which was signed into law on Sept. 22, 2005.[4] Unlike the Nevada provision, New Jersey's rules would specify encryption for both stored and in transit communication at no less than the Federal Information Processing Standard (FIPS), which is currently 128-bit to 256-bit. New Jersey Admin Code § 13:45F-3.2(a)(3). Similarly, it would provide detailed guidance for encryption and other security of all wireless systems.

Although some may be inclined to criticize Nevada's failure to clearly provide specific technical requirements, the New Jersey proposal would certainly go to the other extreme of codifying particular technical standards. The comment period ended on June 15, 2007. The New Jersey Division of Consumer Affairs has not finalized or released any further information on the proposal. It will certainly be worth attention to see what form of the regulation, if any, is ultimately adopted.

A Compliance Challenge

Compliance with detailed security standards will no doubt be more complex than the simple text of the statute would indicate, and could indeed become entirely unmanageable if multiple states specify distinct security requirements purporting to govern interstate computer systems. States should certainly heed to the effects on interstate commerce and the potentially perverse incentives created by such provisions. Without a doubt, there is certainly a danger that specifying security requirements when technology changes faster than the legislature's understanding will result in unworkable, irrelevant, and potentially unconstitutional statutory regimes.

The new Nevada law (which requires "encryption," but does not elaborate on what constitutes encryption), and the proposed New Jersey regulations that prescribe "encryption" precisely, may be hints that legislatures and administrators are less than fully satisfied with the prospect of relying on more general common law or adjudicatory standards to ensure the effectiveness of industry security standards. But it is clear that this debate is just beginning.

Alan Charles Raul and Edward McNicholas are partners in the information law and privacy practice of the Washington, D.C. office of Sidley Austin LLP. Colleen Theresa Rutledge is an associate in that practice. The views expressed herein are those of the authors personally and do not necessarily reflect the views of any governmental or private entity, client, or association.

[4] N.J. STAT. ANN. § 56:11-28 et seq. (2005).