



Nevada's New Privacy Statute: How Businesses Should Respond

Bryce K. Earl - Santoro, Driggs, Walch, Kearney, Holley & Thompson.

Rod Murchison - Code Green Networks

Nigel Johnson - Zix Corporation

On October 1, 2008, Nevada Revised Statute (NRS) 597.970 goes into effect. The statute was passed in 2005, but the legislature delayed implementation for three years to give companies time to take appropriate measures for compliance. Most companies, however, have not used the three years to become compliant, perhaps based upon some very good legal and technical reasons.

Legal Issues

On the legal side, companies may be uncertain regarding the meaning of specific terms in the statute and the consequences for violating the statute. Basically, NRS 597.970 requires the encryption of personally identifiable information over electronic transmissions. The statute reads:

“A business in the 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 in the business unless the business uses encryption to ensure the security of electronic transmission.”

The statute further defines “personal information” and “encryption,” but leaves other terms undefined, such as “facsimile,” “secure system,” “ensure the security” and even “electronic transmission.”

With respect to the primary exception of “facsimile,” given the prevalent convergence of traditional paper fax machines with electronic systems, at what point does a “facsimile” become a violation of the statute? For example, is it a violation if a “facsimile” is sent: (a) from a computer rather than feeding paper through a separate fax machine or (b) from a traditional fax machine, but received by a system that automatically converts the document to a TIFF or PDF file attached as an e-mail? The undefined word “facsimile” represents a gray area in which a business might violate the statute without meaning to do so.

The other undefined terms represent similar gray areas. Is an employee, vendor, or a potential customer considered a “customer?” If not, is it then okay to transmit names and Social Security numbers or accounts numbers of employees? If a company does not have a “secure system,” does any electronic transmission of personal information, even within the company, constitute a violation of the statute? The answer for many of these questions is “possibly, based upon the language in the statute.”

Even the defined terms raise some issues. “Encryption” is defined broadly and includes “any protective or disruptive measure . . . to prevent, impede, delay or disrupt access to any data” (See NRS 205.4742). Is a password-protected document (not generally considered within standard encryption protocols) sufficient for this definition? Further, as a practical matter, anyone who uses encryption on one end requires the recipient to use decryption at the other end, an issue not covered in the statute. In court, attorneys and judges will likely be able to come up with fairly reasonable definitions to clarify the ambiguities, but there’s an even larger issue: there is no specific language in the statute that defines the penalty for violating the statute.

This statute is the last subsection in the general Section 597 of the Nevada Revised Statutes covering Miscellaneous Trade Regulations and Prohibited Acts. Earlier subsections specifically identify the penalties, which include criminal (misdemeanor/felony), regulatory (fines, suspension/revocation of

license), and civil penalties (damages, attorneys fees, judicial relief). Even the other subsections added in 2005 pertaining to certain alcoholic business and an updated lemon law identify penalties. However, the penalties are noticeably absent in 597.970. Such absence may have consequences that range from no enforcement to potential unlimited liability.

The upshot of this situation is that to minimize significant legal risk, all Nevada companies should promptly review (and, if necessary, revise) their existing policies pertaining to access and transmission of personal information, evaluate the security of their IT systems that play a role in storage & transmission of sensitive data, deploy systems that can identify, block and encrypt transmissions of sensitive information in real-time, and then educate customers on the updated implementation.

Technical Issues

To safeguard personal or sensitive data whose transmission could activate Nevada statute 597.970, companies should deploy security systems that will adequately identify personal information in any electronic transmission and, if necessary, block or encrypt the transmission. In evaluating and deploying such security systems, consideration should be given to systems that can perform the following actions:

- **Registration and discovery** – Companies should be able to devise and implement a set of rules that identify whether or not data is sensitive or personal. This is done with network-based appliances and/or software that allows companies to define policies identifying the data (using techniques such as database fingerprinting, file fingerprinting, exact file matching, pattern matching, regular expressions, and lexicons/dictionaries), and then safely import that data in a way that provides high-speed data inspection and confirmation of a “match” when sensitive data transmissions are detected.
- **Data inspection** – The system should be able to inspect data in storage, on servers, as it travels over the network, and as it is used on desktop systems. This requires the system to be able to identify data even when it is enclosed within a compressed archive, part of a PDF file, part of a document such as a spreadsheet, presentation, word processor document, or transmitted via e-mail, webmail, and even a “Web 2.0” application.
- **Data blocking** – The system should be able to block the transmission of sensitive data whenever necessary. This is especially important for web-based e-mail systems and “Web 2.0” applications, which are often encrypted and a rapidly growing conduit for data loss.
- **Data encryption** – The system should be able to encrypt sensitive data before it is transmitted to outside recipients via approved corporate email solutions. The method used to encrypt the email message should be easy for the recipient to comprehend, and the process for securely decrypting the message should be straightforward.
- **User notification** – Users should be notified when they are attempting to send sensitive or personal data and the violation is deemed to be minor. Most sensitive data transmissions are inadvertent, so notification helps users understand why their transmission was blocked and modify their behavior going forward to comply with corporate policy. For more severe

violations, the solution should be able to block the transmission and alert administrators immediately.

- **Logging and reporting** – IT administrators should be able to generate detailed logs and reports on encryption and transmission blocking-related activities in order to prove compliance with the statute.

These requirements can be met today with Data Loss Prevention (DLP) and email encryption solutions available from several different security vendors. Companies considering DLP and email encryption solutions should look for systems that not only offer a comprehensive feature set, but which can be deployed relatively easily and quickly at a reasonable cost.

Bryce K. Earl – Bryce K. Earl is a shareholder with Santoro, Driggs, Walch, Kearney, Holley & Thompson. Mr. Earl advises on a wide range of data privacy regulations and compliance strategies associated with intellectual property. For information on Mr. Earl visit, www.santorodriggs.com/active/b_earl.html.

Code Green Networks – Code Green Networks delivers data loss prevention solutions that protect private employee and customer information and safeguard intellectual property across all electronic communications channels. The company's easy-to-deploy, easy-to-manage content inspection appliances rapidly detect and prevent potential data leaks, helping organizations automate compliance and mitigate risks from internal breaches that can result in loss of revenue, financial penalties and irreparable damage to a corporation's image, brand and customer loyalty. For more information about Code Green Networks, visit www.codegreennetworks.com

Zix Corporation - ZixCorp protects millions of email addresses including those of some of the nation's most influential institutions. ZixCorp's unmatched Email Encryption Service allows customers to communicate seamlessly and securely with no additional work. Each ZixCorp customer is enrolled in the ZixDirectory, ZixCorp's global repository with more than twelve million members. With ZixDirectory, customers eliminate the need to build their own directory of encryption keys to communicate securely with their partners and customers. For more information about ZixCorp visit www.zixcorp.com.