State Privacy and Security Coalition, Inc

April 28 2009

The Honorable Marcus L. Conklin
Chairman
Assembly Commerce and Labor Committee

The Honorable Kelvin D. Atkinson
Vice-Chairman
Assembly Commerce and Labor Committee

Re: Opposition to SB 227

Dear Chairman Conklin and Vice-Chairman Atkinson:

The undersigned companies and trade associations write to express our strong opposition to SB 227, which is scheduled to be heard before your Committee on April 29. While well-intentioned, SB 227 would impose an unnecessarily rigid encryption mandate for the transmission of personal information and the storage of personal information on fixed or portable devices that may be moved "beyond the logical or physical controls of the data collector," regardless of whether it is any way foreseeable that personal information will be contained on these devices.

During the past three weeks, we tried very hard to work with the Attorney General's office to formulate technology-neutral compromise language that would further improve data security in Nevada without imposing enormous costs in a difficult economy and picking technology winners and losers. We understood that SB 227 would not be brought up for a quick hearing in the Assembly in light of these ongoing discussions. We understand, however, that the sponsor and Attorney General's office have rejected our proposed suggestions for compromise, so that we have no choice but to oppose this bill.

This bill would impose hundreds of millions of dollars of expenses on Nevada businesses and state and local governments of all sizes, effectively requiring them to encrypt every single laptop or mobile device that might possibly receive or transmit personal information and to purchase expensive and sometimes cumbersome encryption solutions for their Internet connections. This bill would also pick technology winners and losers, declaring that encryption is the only acceptable way of protecting personal information in Nevada, and putting companies and governments in violation of the law if they fail to use it for all personal information traveling outside of their premises.

Nevada law already prohibits businesses from transferring personal information "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. Under Nevada law, the term "encryption"

is defined to mean "any disruptive or protective measure" that renders data "unintelligible or unusable" or that generally prevents or impedes access to or use of data. § 205.4742.

We strongly support a technology-neutral approach, which avoids picking technology "winners and losers" while encouraging innovation in data security protections, as long as such protections successfully render data inaccessible, unintelligible or unusable. Nevada law already requires that the personal information of Nevada residents is protected in transmission without imposing a prescriptive technology mandate or violating the Dormant Commerce Clause of the U.S. Constitution.

SB 227, by contrast, imposes a rigid encryption requirement that would disallow other effective methods of protecting transmissions of personal information from Nevada and storage of personal information on portable computers, back-up tapes, blackberries, etc.

SB 227 prohibits any entity that collects personal information from (1) transmitting personal information "outside of the secure system of the data collector" or (2) moving any "data storage device" beyond the logical or physical boundaries of the data collector, unless secured by encryption. SB 227 defines encryption narrowly to include "[a]n encryption technology that has been adopted by an established standards setting body...which renders data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data" and "[a]ppropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body."

Although encryption is a strong data security protocol in many circumstances, it is not a panacea; there are drawbacks to its utilization. The widespread usage of encryption throughout an enterprise can significantly slow traffic within a company and across public networks, which reduces efficiency and strains bandwidth. Encryption keys can also be lost or compromised. When this happens, the data can be extremely difficult, if not impossible, to recover. Additionally, the administrative, technical, and manpower burdens associated with the deployment of encryption at an enterprise level make it prohibitively expensive and difficult for many businesses.

Encrypting files that contain personal information, and that are transmitted across public networks, imposes major burdens even outside the state, since it may require any recipients of the encrypted communication to obtain compatible software in order to read encrypted files. The costs of the encryption mandate imposed by SB 227, therefore, would not only be borne by Nevada businesses, but also by any entity that receives personal information about Nevada residents, including entities that have little or no connection to Nevada.

While encryption can sometimes be a good data security solution for many companies, it can create significant problems and unintended consequences for others, and, in particular, small businesses. For this reason, Nevada should continue to use its more flexible approach that allows businesses to choose from a variety of data protection methods that protect the security and confidentiality of personal information, even if it decides to further raise security.

Furthermore, SB 227 would needlessly codify requirements contained in payment card network agreements that every merchant that accepts payment cards (debit or credit cards) must agree to in order to use credit and debit card networks. Merchants who fail to do so can be fined by payment networks. This provision would create a broad range of plaintiffs who could sue under these requirements, leading to more litigation against Nevada companies.

SB 227 would also impermissibly and unconstitutionally regulate interstate commerce in violation of well-settled Dormant Commerce Clause principles. The Commerce Clause of the U.S. Constitution provides that "Congress shall have power...[t]o regulate Commerce...among the several States." U.S. CONST. art. I, § 8, cl. 3. The negative implication of the Commerce Clause prohibits states from regulating commerce that impermissibly burdens interstate commerce. *See Lewis v. BT Inv. Managers, Inc.*, 447 U.S. 27, 35 (1980) ("Although the Clause thus speaks in terms of powers bestowed upon Congress, the Court long has recognized that it also limits the power of the States to erect barriers against interstate trade.").

Not only would SB 227 burden Nevada companies with very costly mandates, it would also impermissibly burden interstate commerce in violation of the U.S. Constitution. In imposing a prescriptive technology mandate that applies to all transmissions of personal information by any entity "doing business" in Nevada, SB 227 on its face regulates commerce that may occur substantially outside of Nevada's borders. The encryption requirement is by no means limited to Nevada; entities located in other states may need to purchase compatible encryption software to handle transmissions from Nevada companies and may find their out of state operations subject to the bill if they have any operations in Nevada. Moreover, because it is often highly impractical to employ different sets of data protocols in different states, the effect of the law will fall heavily outside of Nevada.

Nevada's current encryption law only became effective on October 1, 2008. There is no valid public policy rationale for requiring businesses to now use a single technological approach to protect personal information – as this will slow, rather than encourage innovation in data security.

Nevada's current encryption law affords heightened statutory protection to the personal information of Nevada residents. At the very least, the Nevada legislature should study this issue further and defer the imposition of any new technology mandate to determine whether there is any evidence to suggest that a technology mandate approach is warranted.

For all of these reasons, we oppose SB 227, and ask that you oppose this measure when it comes before your Committee for consideration on April 29.

Sincerely,

AOL
Amazon.com
Cisco
eBay, Inc.
Google
Internet Alliance
NetChoice
Reed Elsevier
State Privacy and Security Coalition
TechAmerica
TechNet
Verizon
Yahoo!