

## Some Infosec Legal Reflections as We Ring in 2009

By Randy V. Sabett – ISSA member, Northern Virginia, USA chapter



Year end usually means a little time for reflection, even for us lawyers. As 2008 closes out, let's ignore for a moment the financial mess out there and look back at a few select infosec legal and liability developments that made headlines...and consider what the new year may hold.

### PCI

In my practice, PCI DSS continued in 2008 to be one of the top information security drivers for many organizations. The combination of updated PCI requirements and the stepped up enforcement of the DSS by the card associations presented an environment that led to the realization that "Hey! PCI is real!" Hannaford and other breaches have shed light on the porosity of what would appear to be otherwise secure networks, including those that are PCI-compliant. Vulnerabilities continue to emerge, including one in the WPA encryption standard, which is mentioned as a WEP replacement in the recently released v1.2 of the PCI DSS. The DSS recognizes the need for pragmatic risk-based security when it states that "a company should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission." Watch for more on this and other PCI issues in 2009.

### New or updated state laws

As you well know, at the state level, numerous data breach notification and "reasonable security measures" laws have been enacted. We are seeing a new trend, though: an increased focus on more granular laws. For example, Minnesota has incorporated a few concepts from PCI into its laws. Even more focused: laws in Nevada and Massachu-

setts now affirmatively require encryption. Note, however, that Massachusetts recently announced the compliance date for its encryption regulations would be delayed from Jan. 1, 2009 to May 1, 2009, citing the need to provide flexibility to businesses. Encryption-specific laws are definitely a trend to watch for in 2009.

### CNCI

The Comprehensive National Cybersecurity Initiative (CNCI or "Cyber Initiative") continues to be a somewhat elusive matter since much of it remains classified. According to various reports, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 established the CNCI on Jan. 8, 2008. You may recognize certain pieces of the CNCI – so far the Trusted Internet Connections (TIC) effort and Project 12 have been made public. TIC endeavors to reduce the number of government Internet connections, while Project 12 focuses on public/private partnership issues. We'll see more on the roll out of the CNCI, along with implementation of the recommendations of the Commission on Cyber Security for the 44th Presidency, as 2009 progresses.

### Funding

Despite the downturn in the markets as we exit from 2008, venture capital firms remain interested in companies that have some connection with information security (particularly those that produce so-called "dual use" products that have uses in both commercial and military applications). In addition, merger and acquisition activity is very robust in the information security space. Though the market continues to contract, information security still will be needed in every sector of the economy. So watch for more deals in 2009.

### HIPAA enforcement

The HHS Office of Inspector General (OIG) issued a critical report recently that focused on the ineffective enforcement of the HIPAA Security Rule. Stating that the Centers for Medicare and Medical Services (CMS) "had taken limited actions to ensure that covered entities adequately implement the HIPAA Security Rule" and "had not provided effective oversight or encouraged enforcement of the HIPAA Security Rule by covered entities," the OIG placed pressure on CMS to step up its enforcement. If you are a covered entity, watch out for more on security rule enforcement in 2009, and if you are a business associate, you can be certain there will be flow down to you.

### Trend summary

So what will we see in the area of legal infosec issues in 2009? I think there likely will be greater regulation and enforcement, more proactive requirements (both from the government and from industry), more deals, and, hopefully, a safer environment for all...and, now, to all a good night. Have a great holiday season! See you in the new year.

### About the Author

Randy V. Sabett, J.D., CISSP, is a Partner in the Internet, Communications, and Data Protection (ICDP) practice group at Sonnenschein Nath & Rosenthal LLP, an adjunct professor at George Washington University, and a member of the Commission on Cyber Security for the 44th Presidency. He may be reached at [rsabett@sonnenschein.com](mailto:rsabett@sonnenschein.com).