PROSKAUER ROSE LLP

A Moment of Privacy

A newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose

JULY 2009

Edited by

Kristen J. Mathews

Welcome to "A Moment of Privacy," a newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose LLP.

"A Moment of Privacy" addresses one legal development each month in the area of privacy and data security law. We answer the questions our clients are asking, in a way that we hope gives practical information to our readers. If you send us your question, you may find your answer in an upcoming newsletter.

And now for this month's question:

Q: In the context of wireless network security, I hear a lot about WEP vs WPA, but I do not know what they mean, nor do I know what legal considerations need to be taken into account when choosing between them. Can you give me the rundown on this so that I can speak intelligently with my company's information technology specialists?

A: WEP and WPA are two alternative ways to secure a wireless network from unauthorized interception, and WPA is more secure than WEP. In fact, researchers have reported consistently for several years that it is relatively easy to break into a WEP-secured wireless network. For that reason, as discussed further below, industry standards as well as regulators require that WPA (instead of WEP) be used to secure wireless networks that are used to transmit sensitive information such as credit card numbers.

Nonetheless, many companies are still using WEP.

Earlier this month, the PCI Council (the custodian of the payment card industry's data security standards) released its "Information Supplement: PCI DSS Wireless Guideline" which reiterates the PCI Data Security Standards' requirement that wireless networks associated with payment card environments must implement WPA on legacy wireless implementations by June 30, 2010. (New wireless applications have been required to implement WPA since March 31, 2009.) Complying with the PCI Data Security Standards is contractually required of entities that store, process or transmit payment card data.

Driving this point home is a recent settlement between TJX and 41 state attorneys general arising from the massive credit card data breach suffered by TJX in late 2006. Pursuant to the settlement, TJX is required to implement WPA (or equivalent) security on its wireless systems. TJX's use of WEP security on its in-store wireless networks was allegedly in part to blame for the security breach that compromised tens of millions of payment cards.

Have a question? E-mail Kristen J. Mathews at kmathews@proskauer.com.

Privacy and Data Security Practice

Our Privacy and Data Security Practice is an outgrowth of our Internet, intellectual property, technology media & communications, labor and employment, health law, First Amendment, international law and litigation practices. Indicative of our experience and reputation in this relatively new field of law is the fact that the venerable Practising Law Institute (PLI) asked our Firm to create its first-ever treatise on the subject of privacy and data security law, called "Proskauer on Privacy," which was published in late 2006.

Privacy and Data Security Practice Group Partners:

Grégoire Goussu
33.1.53.05.60.11 – ggoussu@proskauer.com

Kristen J. Mathews
212.969.3265 – kmathews@proskauer.com

Jeffrey D. Neuburger
212.969.3075 – jneuburger@proskauer.com

Anthony J. Oncidi
310.284.5690 – aoncidi@proskauer.com