**CIS 481 – Intro to Information Security**

**CLASS EXERCISE # 3 – Option B**

Grading ID: A7386

**Problem 1**

In the United States, there is no single, uniform law that governs disclosure of data breaches. Instead, most states have passed piecemeal legislation with various covered elements and disclosure requirements. Companies can be (and are) held to entirely different compliance standards depending on which state an affected individual lives in. Kentucky is one of the last states to pass such legislation. See: <https://www.bakerlaw.com/files/uploads/Documents/News/Articles/INTELLECTUAL%20PROPERTY/2015/Haggerty-Patrick-Article-May-2015-Bench-Bar.pdf>

1. Who are considered covered entities (information holders) under the KY legislation? Who are explicitly excluded? Why do you think that KY chose to exclude these entities? (5 pts.)

In KY, covered entities are information holders, which are defined as any person or entity that conducts business in KY. People who are subject to HIPAA and GLBA are explicitly excluded from coverage. I think that the law is written this way because it is meant to be comprehensive, where it can be applied to a multiplicity of Kentucky business types that are all regulated uniquely. In contrast, HIPAA and GLBA standards are very strict, uniform, explicit, and apply only to the health care and financial sectors respectively.

1. What is the KY definition of PII? (8 pts.)

The KY definition of PII is “an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the name or data element is not redacted: (1) Social Security number; (2) Driver’s license number; or (3) Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual’s financial account.” The law only applies to unencrypted and unredacted computerized data—it does not apply to paper records.

1. Would acquisition of encrypted data be considered a breach that would trigger notification requirements in KY? (2 pts.)

No, because notification is only triggered on unencrypted or unredacted data.

BakerHostetler maintains a comprehensive comparison of the various state data breach laws at: <http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf>

1. Compare the summary of Kentucky’s data breach law to California’s. Which is more comprehensive? Explain. (4 pts.)

In general, California’s data breach law is more comprehensive than Kentucky’s. It extends the definition of personally identifiable information beyond the standard that Kentucky uses. California does not require a risk of harm analysis prior to the notification’s trigger, allowing the public to find out about potentially dangerous breaches sooner. California requires the notifications to occur within a specific timeframe, whereas Kentucky does not. Lastly, California has provisions that allow an individual to permit a private cause of action to seek damages.

Companies are frustrated by the inconsistencies inherent in the piecemeal laws in 47 (and counting) states and have asked for one national law. Review the BakerHostetler blog post on this subject at: <http://www.dataprivacymonitor.com/data-breach-notification-laws/dear-lawmakers-your-new-breach-notice-laws-should-address-these-issues/>

1. If you were lobbying for national data breach legislation on behalf of a company, what would be your top three issues for the legislation to address? (6 pts.)

As a lobbyist, there would be several issues that I would want the legislation to address:

Notification timing – those affected should be able to quickly take action before excess damage is caused.

Discovery – Potential breaches should be reported for investigation and notification as soon as suspicion of a breach arises, once again, to potentially limit damages.

Risk of Harm – Companies should not wait and determine the risk of harm, affected individuals should be immediately notified.