Law and Technology Disconnect: Tennessee Just Killed Encryption Safe Harbor

Apr 11, 2016

Categories:

Blockchain and Digital Assets
Blogs
Publications

So what's the big deal? First, encryption of personal data is a data security best practice, particularly for data in transit and is the current state of the art. While encrypted data may conceivably be hackable (depending on the strength of the encryption), it nevertheless provides the best available protection. Encryption is routinely used by businesses and professional firms for protection of the confidentiality and privacy of clients and customers. Encrypted data is not, as the sponsor of the Tennessee amendments, Sen. Bill Ketron argued "now being stolen almost as easily as unencrypted [data]." Far from it.

Data breach notification is expensive. It potentially sends waves of panic to those whose data has been allegedly compromised. It can create huge reputational losses to the business. Yet despite this, a literal reading of the Tennessee notice statute as now amended, requires notice even if the data is encrypted and simply can't be accessed by the bad guys.

So let's take a fairly standard situation: a business provides laptops to its employees. The data on the laptop is encrypted and the laptop is password protected. Contained on the laptop is personally identifiable information of the business' customers. Employee Sam has his laptop stolen. Happens all the time. In the past, the loss would not be of concern since notice would not be required because encryption protects the data. Now, reading literally the Tennessee law, the business must give notice of the theft and loss conceivably to all its customers who are residents of Tennessee even though whoever stole the laptop could access none of the information on it. Not a pretty situation.

Certainly, as some have pointed out, the Tennessee law still provides that a notice of a breach requires that the unauthorized access of data "materially compromise the security, confidentiality or integrity of personal information" and that notice is required

where personal information is "reasonably believed to have been acquired". Some say if the data is encrypted, then there is no such material compromise and no reasonable belief that personal information has been acquired.

But at the very least, the burden of showing these criteria are met is now higher since the loss of encrypted data is no longer per se exempt from notice requirements. (Query, how else could you make the required showings other than by demonstrating that the data is encrypted?).

And an argument could be made–valid or not–that the amendment makes any consideration of encryption or non-encryption of the material irrelevant. Under this argument, the "material compromise" and "reasonably believed to have been acquired" language can only be met by showing something else entirely. Stated simply under this theory: encryption of data no longer eliminates the obligation to give notice of a breach in Tennessee. Indeed, the literal language of the statute and the legislative history and comments of Sen. Ketron might support such a claim even if practicalities do not. And again, what more could a business show to meet the material and reasonableness criteria than demonstrating strong encryption?

And remember that the Tennessee law defines the "information holder" for data breach notification purposes, as "any person who conducts business in the state", irrespective of where that holder may be based or headquartered, if that firm collects personal data of Tennessee residents.

But wait, there is more. Tennessee formally only required that notice be given without reasonable delay consistent with the needs of law enforcement, and measures necessary to determine the scope of the breach and restore the integrity of the system. This gave businesses some time to investigate, determine what had been lost and make sure the systems were secure and not subject to any additional breach.

As of July 1, however, the world changes in Tennessee. Now, notice must be given by at most 45 days, period. No longer is there an extension of time to investigate and restore; the only way the 45-day period can be extended is if law enforcement makes a request

that notice be delayed. Only 5 other states have a maximum time to give notice as short as 45-days and only one, Florida, has a shorter time. Giving notice before you figure out the scope and fix the problem can't be good: "We have had a breach. But we don't know how extensive it is. And we don't know yet how to fix it". Again, not a pretty situation.

The Tennessee change may also affect several other issues and requirements. Incident responses plans may be substantial impacted and rendered in whole or in part obsolete. Likewise, vendor contracts often contain notice provisions that may create conflicting requirements with the new law. Cyber insurance policies also could contain various inconsistent requirements and may not even cover breaches that involve encrypted data.

And there are litigation risks: anyone injured by failure to give notice can bring a private cause of action in Tennessee. While query what damages there may be for a violation when the data is encrypted, such standing concepts have not precluded litigation in other well and not so well known data breach situations.

So what's business to do?

At the very least, if you maintain any personal information on Tennesseans, review your incident response plan in light of the new 45-day requirement and the encryption implications. Also review what service providers may have personal information relating to Tennessee residents and what your contracts with them say. Plus, your insurance policies should be re-reviewed. And your data protection policies, your level of encryption and how you might meet the "no material compromise" and "no reasonable belief that information has been acquired" safe harbors should be thought through. Conduct your privacy professionals and legal counsel for help.

Given the new 45-day window, now more than ever this review and planning should be done before a breach not after.

———

FBT Gibbons

Please contact Stephen E. Embry at (502) 568-0253 or sembry@fbtlaw.comfor an questions concerning this article.

FBT Gibbons