**EMCS2600: The Future of Cybersecurity: Technology and Policy**

Assignment: Module 7 Review Questions

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

###### Question 1: In at most 200 words provide your assessment of the likely impact of the exterritorial application of domestic laws on the management of personally identifying information.

The likely impact of the exterritorial application of domestic laws on the management of personally identifying information is ongoing **conflict** between foriegn localities and American conglomerates. Since international law is historically based on white supremacy not norms, as demonstrated by the Treaty of Westphalia, it is no wonder that the modern American corporate structure continues to selectively support laws as a means of expanding its own power and wealth. White supremacy is not about hate, it’s about consolidating wealth and power in the hands of whites and therefore it will bend religious, ethical and legal standards to meet that end. Whether it’s a company operating in a foriegn country with American companies trying to force our norms on the management of PII, or the PII of foriegn nationals being mined by the NSA, the true conflict has very little to do with the user and more to do with the struggle for leverage. When competing laws are in play because companies from different countries want to participate in each other’s markets the development of international norms seems ideal but improbable. When it does happen it will most likely be done to appease the rich and powerful, not uphold human rights.

###### Question 2: In at most 200 words explore the pros and cons of the legalization of active cyber defense.

I see very little cons to this very limited bill. It amounts to a common sense approach to cyber defense that is already being implemented by companies nationwide. The bill “gives permission” for defensive maneuvers like watching an enemy, stopping them, revealing their identity and destroying stolen information. The only “cons” would be when defensive actions were taken in error or if a company falsely and maliciously claimed someone was attacking them to destroy, attack or monitor something or someone they shouldn’t. This is not a problem with the law however, since every action subject to regulation ( even in other areas of law enforcement ) could be taken mistakenly or on false pretext. This is the reason police in some states are required to wear body cameras, for example. The devil is in the details. The law should require that defensive actions be monitored and verified by a neutral third party, ideally someone authorized by an organization like MITRE. I am sure there will be competing claims against defensive actions, but once again this type of hypothetical is an issue with the law, and should be determined on a case by case basis.