Week 2 Discussion

**One continued problem with cryptography is the restrictions associated with cryptographic export. Find at least on article (not from Wikipedia) that discusses this topic, and summarize what you found. Did it surprise you? Was it what you expected? Include citations for your resources.**

[**E**](https://cyberactive.bellevue.edu/webapps/discussionboard/do/message?action=list_messages&course_id=_489488_1&nav=discussion_board_entry&conf_id=_590647_1&forum_id=_1999542_1&message_id=_36985190_1#)

The US government has had a long and storied past of attacking and limiting cryptographic exports. This foundation first starts with defining cryptographic systems as a munition through the International Traffic in Arms Regulations.1 Software is codified thoughts that tell a computer what to do. In my opinion, this becomes a first amendment issue but that is just my opinion. Then the arbitrary definition of what is strong encryption versus what is weak encryption in a Commerce Control List regulation that in no expedient way can be updated to roll forward with the pace of technology.2 High end computers of today are tomorrow's disposable electronics. It's a quagmire of bad short term decision after bad short term decision. The kicker is that these restrictions only affect small size businesses that can scale to have international based wings or to law abiding private citizens who don't have the wherewithal to navigate these regulations.

If this wasn't enough it turns out that the USA government is playing both sides of the table. Edward Snowden leaked details about a code named project Bullrun in the NSA that alleges the systematic attack on current and future cryptographic standards.3 So on every front we can see that the USA government wants to put the genie back in the bottle. This continued attack on being able to pry into secrets may explain the current drumbeat around the next generation of mobile broadband called 5G. Maybe there is some merit to ensuring a critical infrastructure is locally sourced but for that equation to balance out the local source has to be more trustworthy than the foreign sources for hardware and software. These same institutions tried to force the Clipper Chip on everyone so they could have a built in backdoor.4

We seem to be doomed to repeat the same mistakes.

1 . International Traffic in Arms Regulations: U.S. Munitions List Categories I, II, and III. (2018, May 24). Retrieved from <https://www.federalregister.gov/documents/2018/05/24/2018-10366/international-traffic-in-arms-regulations-us-munitions-list-categories-i-ii-and-iii#sectno-citation-> 124.14.

2. Commerce Control List Supplement No. 1 to Part 774 Category 5 -Info. Security-page 1 Export Administration Regulations Bureau of Industry and Security. (2019). Retrieved from <https://www.bis.doc.gov/index.php/documents/regulations-docs/2337-ccl5-pt2-4/file>

3. Larson, J. (2019, March 9). Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security. Retrieved from <https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption>.

4. Levy, S. (1994, June 12). Battle of the Clipper Chip. Retrieved from <https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html>.