Joshua White
CS644
Professor: Dr. Jeanna Matthews
(Week 2 LEET Conference Papers)

Short Paper Review of:
Conducting Cybersecurity Research Legally and Ethically

Citation:

- Aaron J. Burstein. 2008. Conducting cybersecurity research legally and ethically. In *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats* (LEET'08), Fabian Monrose (Ed.). USENIX Association, Berkeley, CA, USA, , Article 8 , 8 pages.

Cursory Author(s) Affiliation(s):

- University of California, Berkeley (School of Law)
  - NSF Funded

Claims:

- Clarify the issues of cyber security research by explaining the generally applicable laws
- Offer guidelines for evaluating ethical issues that may come up in this area of research

Likes:

- I like that it concentrated on US law, I've taken “International Telecommunications” which required extensive knowledge of telecom law around the world, it was refreshing to see a paper that intended to fucus in detail on one countries laws.
- The specifics on the laws surrounding data collection and running malware in testbeds is obviously directly applicable to many different projects we work on and as such is very relevant.
- It was nice to see a specific reference to the law regarding why we require written agreements before sharing data sets.
- I had always wondered why we were not allowed to share some data-sets with the government but were allowed to share them with other companies assuming all of the paperwork existed.
- I've worked with DHS's PREDICT database for a couple of years now and this paper certainly clarifies why so much paperwork is involved for each new dataset.
- I found it interesting that Tort law applied in the event of a negligent researcher. I've had Tort Law as a course and this was never mentioned.

- I didn't know that HIPAA contained exceptions for research.

Dislikes:

- The authors made no mention as to the extent of the laws surrounding cyber security research or if there were any new laws/groups of laws that would be coming into effect that may supersede the existing ones.
    - Personally I would have liked to have read “the policy/law makers see this is a problem so they have plans for a special set of laws just for research in this area.” Perhaps that's simply to wishful of thinking. However with the amount of cyber security research done under government funding by this point you would think they would have done so.

Repeat / Add to Work?

- I found a lot of the references quite useful, what was said in this paper was well researched. I just wish there was a lot more specifics as to what could and couldn't be done. Perhaps some case scenarios. I found this paper to be extremely interesting/applicable to both my graduate work and job. I could definitely see future research work based on this paper, perhaps in identifying new laws/exceptions and devising case scenarios. Again, much like “Exploiting Machine Learning to Subvert Your SPAM Filter” (Paper 7), I'm not sure that enough work exists to make this a thesis topic.