Syllabus – Law 416: Cybersecurity Law Seminar
George Mason University Law School – Spring 2015
Profs. Jamil N. Jaffer & Robert L. Strayer

Brief Course Description:

This seminar course will provide students exposure to the key legal and policy issues related to cybersecurity, including the legal authorities and obligations of both the government and the private sector with respect to protecting computer systems and networks, as well as the national security aspects of the cyber domain including authorities related to offensive activities in cyberspace. The course will include a survey of federal laws, executive orders, regulations, and cases related to surveillance, cyber intrusions by private and nation-state actors, data breaches, and privacy and civil liberties matters, among other things. The course will also explore the legislative and technology landscape in this dynamic area and will provide students with opportunities to discuss cutting-edge issues at the intersection of law, technology, and policy.

Class Format:

Seminar of 10-20 students; two credits; one two-hour class per week. Active participation in class discussions is required and students are expected to be fully prepared for each class session.

Grading:

Substantive grades will be based on class participation (15%) and student’s successful completion of a 20-30 page paper on cybersecurity law (85%).

Paper Due Date: TBD

** Please note that late papers will receive a 1/3 grade deduction for every day the paper is late beyond the due date established in class (i.e., an A- paper that is three days late would receive a B-), so please turn papers in on time. **

Class Details:

Mondays: 8:00 pm – 9:50 pm.

Office Hours:

By appointment.
Faculty Contact Information:

Jaffer Contact Info: jjaffer@gmu.edu
202-247-8390 (cell)

Strayer Contact Info: rob.strayer@gmail.com
(202) 277-0783 (cell)

Course Materials:
The bulk of the course materials are cases or articles available on Westlaw or Lexis-Nexis or materials posted on TWEN. Materials posted on TWEN are indicated below.

** Given the developing nature of this area of law, it is likely that the syllabus and readings will be updated over the course of the semester; therefore, please regularly check your email and TWEN for updates to the syllabus and readings. **

Course Assignments:

Week One – Introduction to Computer Networks and Cyber Threats

2. Leiner, Cerf, et. al., A Brief History of the Internet – pp. 1-9 (TWEN)
6. Mandiant Report, APT1, Exposing One of China’s Cyber Espionage Units – pp. 2-26 & 63-65 (TWEN)

Week 2 – Vulnerabilities, Federal Cybersecurity, and the Economics of Cyber Threats


Week 3 – Anonymity, Privacy, and Data Mining

1. The White House, Big Data: Seizing Opportunities, Preserving Values (May 1, 2014) – pp. 1-69 (TWEN)

Week 4: Protecting the Internet: Encryption and Interception


Economist, Cryptography for Dummies (Nov. 29, 2014) – pp. 1-4 (TWEN)

In Re: Grand Jury Subpoena (US v. Doe), 670 F.3d 1335 (11th Cir. 2012), http://www.leagle.com/decision/In%20FCO%2020120223106

Additional Readings TBD

Week 5: Intercepting Metadata and the Section 702 Program

Readings TBD

Week 6: Cyber Security and the Fourth Amendment

Readings TBD

Week 7: Information Sharing: Legislation and Public-Private Partnerships

Readings TBD

Week 8: Data Breach and Federal Trade Commission Regulation through Unfair Trade Practices

Readings TBD
Syllabus: Cybersecurity Law

Week 9: Securing Critical Infrastructure; Case Study of Defense Contractors

NOTE: PROPOSED PAPER TOPICS DUE THIS WEEK

Readings TBD

Week 10: Regulation of Financial Services and Energy Sectors by Federal Agencies

Readings TBD

Week 11: Procurement Vulnerabilities

NOTE: FINAL PAPER TOPICS DUE THIS WEEK

Readings TBD

Week 12: Law of Armed Conflict in Cyberspace

Readings TBD

Week 13: Role of International Institutions

Readings TBD

Week 14: The Role of Hackers and Offensive Actions

Readings TBD