Course: Cybersecurity Law
LAW 795
Section 512

Instructor: Jerry M. Bodman

Class Times and Office Hours: The class will meet Thursday evenings from 6:15 to 9:00. I will generally be available immediately before and after class. If you desire another time, please let me know and we can make arrangements.

Contact Information: Please direct all electronic correspondence to my UB email account. If you wish me to phone you, please pass your number in the email.

Course Description: This course will explore cybersecurity technology and law beginning with an brief introduction to the basics of the Internet, core concepts and terms of cybersecurity, and an overview of the current cybersecurity threat landscape. Following a review of foundational legal principles, the coverage will shift to anti-hacking laws, an overview of government institutions with cybersecurity authorities, state laws, industry specific requirements, privacy-related topics, issues related to network monitoring, public-private cybersecurity partnership, and finally discussion about creation of an incident response guide.

Learning Outcomes: By the end of the course, the successful student will be able to:

- Identify and explain basic cybersecurity concepts and terminology;
- Identify and explain federal agencies with cybersecurity roles;
- Explain the NIST Cybersecurity Framework and its five core functions;
- Identify foundational law and explain how it is applied to cybersecurity problems;
- Explain basics of privacy as it relates to cybersecurity;
- Explain the basics of data breach;
- List and explain public-private partnerships in cybersecurity; and
- Demonstrate the ability to advise a client on a cybersecurity issue through completion of a client memo.

Materials: Jeff Kosseff, *Cybersecurity Law*, (1st Ed. 2017); supplemental reading

Grading: Grades for this course will be based on class participation (20%) and the exam (80%). Class participation scores will be based on the following:

- Attendance;
- Preparation for class as demonstrated through participation; and
- A client memo (2-3 pages, details will be provided in class) will count for 5% of the total grade).

Expectations: The goal of any law school course is for you to develop solid skills that will improve your ability to be great lawyers. This course is no different. At the end of the course, you should be able to demonstrate how lawyers solve problems in this area of law. I have high expectations for student performance in class and on assignments. You should be prepared to contribute in every class. If you find that you are not well prepared for class and have a valid reason for it, please let me know before class starts.

Attendance: Class attendance is a primary obligation of each student whose right to continued enrollment in the course and to take the examination is conditioned upon a record of attendance satisfactory to the professor. A student who exceeds the maximum allowed absences (generally 20% of class sessions) as illustrated below may be compelled to withdraw from the course, or may be barred from sitting for the final exam. Students who are forced to withdraw for exceeding the allowed absences may receive a grade of FA (failure due to excessive absence). This policy is consistent with American Bar Association Standards for Law Schools.

See http://law.ubalt.edu/academics/policiesandprocedures for more details.

Computers: Students may use laptop computers for class related purposes.

Class Cancellation: If the instructor must cancel a class, notices will be sent to students via email and posted on the classroom door. If there is inclement weather, students should visit the University of Baltimore web site or call the University's Snow Closing Line at (410) 837-4201. If the University is open, students should presume that classes are running on the normal schedule.

Academic Integrity: Students are obligated to refrain from acts that they know or, under the circumstances, have reason to know will impair the academic integrity of the University and/or School of Law. Violations of academic integrity include, but are not limited to: cheating, plagiarism, misuse of materials, inappropriate communication about exams, use of unauthorized materials and technology, misrepresentation of any academic matter, including attendance, and impeding the Honor Code process.

The School of Law Honor Code and information about the process is available at http://law.ubalt.edu/academics/policiesandprocedures/honor_code/.

Title IX Sexual Misconduct and Nondiscrimination Policy: The University of Baltimore’s Sexual Misconduct and Nondiscrimination policy is compliant with Federal laws prohibiting discrimination. Title IX requires that faculty, student employees and staff members report to the university any known, learned or rumored incidents of sex discrimination, including sexual harassment, sexual misconduct, stalking on the basis of sex, dating/intimate partner violence or sexual exploitation and/or related experiences or incidents.

Policies and procedures related to Title IX and UB’s nondiscrimination policies can be found at: http://www.ubalt.edu/titleix.

Disability Policy: If you are a student with a documented disability who requires an academic accommodation, please contact Leslie Metzger, Director of Student Services, at 410-837-5623 or lmetzger@ubalt.edu.

Homework for the First Day of Class: In addition to completing the reading for the first day of class, please be prepared to answer the following questions:

- Who are you? Provide a snapshot of your experiences and education background.
- What is your focus (e.g. business, health, national security)?
- Why are you taking the course?
- What is (at least) one thing you hope to learn by taking this course?

Schedule and Reading Assignments

Week 1: Introduction & Foundational Concepts

NOTE: The reading for the first week looks intense but it really is to get you exposed to the range of subject specific content so we can discuss it later.

Why take this course?

- National Research Council. 2014. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington, DC: The National Academies Press. https://www.nap.edu/download/18749
    - Read Chapter 1, pages 7-17
- Ethical obligations regarding use of technology
    - ABA Formal Opinion 477R – Securing Communication of Protected Client Information
        - https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf
    - ABA Formal Opinion 483 – Lawyers' Obligations After an Electronic Data Breach or Cyberattack
        - https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf
- Yahoo Counsel Leaves After Hack Investigation Finds Lack of Action
    - https://www.bloomberg.com/news/articles/2017-03-01/yahoo-counsel-bell-leaves-after-hack-probe-finds-lack-of-action

Background: History of the Internet

- How the Internet Was Invented | The History of the Internet, Parts 1, 2, and 3
    - https://www.youtube.com/watch?v=1UStbvRnwmQ
    - https://www.youtube.com/watch?v=1CsPHKJWiw0
    - https://www.youtube.com/watch?v=eYkXD_cGUYU
- https://www.internetsociety.org/internet/history-internet/brief-history-internet/

Cybersecurity - Concepts and Terminology

What is cybersecurity?

- Jeff Kosseff, Defining Cybersecurity Law, 103 Iowa L. Rev. 985 (2018) https://ilr.law.uiowa.edu/assets/Uploads/ILR-103-3-Kosseff.pdf. Read sections I, II, and III.

Threat Landscape – Discussion of terms and concepts

- Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks
  - https://www.paulweiss.com/media/3158666/30sept15cybersecurityalert-final.pdf. Read pages 1-10

- 2018 Verizon Data Breach Investigations Report (quick review is fine but be ready to ask questions)
  - https://enterprise.verizon.com/content/dam/resources/reports/2018/DBIR_2018_Report.pdf

- 2016 California Data Breach Report (quick review is fine but be ready to ask questions)
  - https://oag.ca.gov/breachreport2016

Case study: Target Breach

- https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412 - pages 2-25

Optional reading

Worldwide Threat Assessment of the US Intelligence Community

- https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf (Just skim looking for “cyber” related content)

Tracking GhostNet: Investigating a Cyber Espionage Network, Information Warfare Monitor

- http://www.nartv.org/mirror/ghostnet.pdf

Mandiant, APT1: Exposing One of China’s Cyber Espionage Units

- https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

VPNFilter – Router Exploitation

- https://blog.talosintelligence.com/2018/05/VPNFilter.html

Exploits & Vulnerabilities

- Ablon, Lillian and Andy Bogart, Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. Santa Monica, CA: RAND Corporation, 2017.
  - https://www.rand.org/pubs/research_reports/RR1751.html. Read chapters 2-4.

- Fidler, Mailyn, Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis (Summer 2015). I/S: A Journal of Law and Policy for the Information Society. Vol. 11.2 (2015). Available at SSRN: https://ssrn.com/abstract=2706199
    - Read Sections I and II