CYBERSECURITY LAW AND POLICY
David Sella-Villa
Spring 2025

SYLLABUS (v1)

Welcome to Cybersecurity Law and Policy (LAWS 806). I look forward to working with you this semester. I will do my best to make your experience in this course worthwhile, and in turn I will expect from each of you full engagement and dedication to learning together as an intellectual community.

Please read this syllabus carefully. It explains how the course will be taught and graded. I will update the syllabus from time to time.

Contact Information

David Sella-Villa
Phone: 304-377-2072
Email: sellavid@mailbox.sc.edu
Office Location: Room 333
Hours: Mondays 2:00pm – 4:00pm, Wednesdays 2:00pm – 4:00pm, or by appointment

Class Meetings

Our class meets from 2:40pm – 4:05pm in Room 288 on Tuesday and Thursdays. The first-class meeting will be on Tuesday, January 14, 2025. There may be some class sessions when we do not meet in person. I will let you know in advance when those sessions will be. The course will also feature some guest lectures.

Learning Outcomes

Prior technical understanding is not required to succeed in this course. Students in this course will study the applicability of both criminal sanctions and civil remedies against cybersecurity attacks by non-governmental individuals or entities and the availability of other measures that impose costs upon foreign state actors who engage in cybersecurity attacks. The course also will cover legal responsibilities and potential liabilities that encourage potential victims of attacks to better secure their systems against attack. Government regulations, disclosure requirements after an attack, potential civil liability of system operators, and cybersecurity insurance are addressed in detail. The course will look at ways in which governmental entities are able to protect against or mitigate harm from a cyber- attack. Other topics that may be covered include the drafting of a legally adequate response plan and consideration of issues related to lawful hacking, as well as government use of hacking for intelligence gathering and espionage. Prior technical understanding is not required to succeed in this course. At the start of the course, students will be introduced to the anatomy of a typical cybersecurity attack and to the terminology most frequently used in cybersecurity discussions.

The American Bar Association standards for accrediting law schools require not less than one hour of classroom or direct faculty instruction and two hours of out-of-class student work per week for each credit awarded for a class. According to the standards, fifty minutes suffices for one hour of classroom time, while an hour for out-of-class time is sixty minutes. This is a three-credit class. That means that we will spend approximately 39 in-class hours together, and you

should expect to spend at least 85 hours preparing for class, working on the short paper, and taking the final exam.

Class Structure & Grades

Each class will be a combination of lecture, class discussion, and review of hypotheticals and real-world examples. Discussion is necessary to enhance everyone's learning. The determination of your grade will be made as follows:

Class Participation – 30%
Short Paper – 20%
Final Exam – 50%

About once per week a portion of class time will be dedicated to drafting a written response to questions presented in class. Between three (3) and five (5) of these in-class writing assignments will serve as "pop quizzes" and count towards your Class Participation grade. During class time you will be asked to submit that class session's writing assignment via Blackboard. These in-class writing assignments will account for one half of your Class Participation grade. As long as you make a good faith effort to answer the question(s) presented, you will receive full participation credit on that in-class writing assignment. The first "pop quiz" will not occur until after January 23, 2025.

Speaking up during class time counts as one form of active participation. Submitting written questions before or after class also counts as active participation. Bringing topical news stories to my attention, either via email or in person, to discuss in class also counts as active participation. Responding well if cold called counts as active participation. Please participate in the manner that you feel most comfortable. Your goal should be to show me that you are engaged with the material.

Both the Short Paper and Final Exam will need to be submitted via TWEN. Specific submission instructions will be provided for both the Short Paper and Final Exam. Both the Short Paper and Final Exam will be graded anonymously. **Please note – your AEGS number for your Short Paper will be different from AEGS number you will use for the Final Exam.**

The Short Paper instructions will be distributed in February and will be due March 3, 2025, at 5:00 pm. If you are late turning in the Short Paper, your grade will be reduced by one full letter grade per each 24-hour period of tardiness. This chart provides an example of how tardy submissions will affect grades.

Time submitted	Original Grade	Adjusted Grade
3/3, 4:50 pm	B+	N/A
3/3, 5:05 pm	B+	C+
3/4, 11:00 am	B+	C+
3/4, 10:00 pm	B+	D+

The Final Exam will be scheduled during the exam period. You will have 4 hours to complete and submit the exam. The exam will be open book. Late exam submissions will be addressed on a case-by-case basis. I reserve the right to score your exam a zero if it is submitted late.

In addition to your participation grade, I reserve the right to reduce your grade for failing to attend class regularly or by being disruptive to the learning environment in class.

Use of Artificial Intelligence Tools

General Use

Use of artificial intelligence (AI) tools, including ChatGPT, is permitted in this course for students who wish to use them. To adhere to our scholarly values, and the standards of the legal profession, students must cite any AI-generated material that informed their work (this includes in-text citations and/or use of quotations, and in your references or footnotes). Using an AI tool to generate content without proper attribution qualifies as academic dishonesty.

Additionally, please note that the Final Exam questions are being specifically designed with the limitations of AI tools in mind. If a student simply submits AI-generated answers without adding language reflective of his or her own critical thought or creativity, the student will likely receive a low grade for that portion of the Final Exam.

Short Paper

On the Short Paper, you will be required to use an AI tool as part of the paper assignment. Specific instructions on how to use the AI tool and how to incorporate its outputs into the assignment will be provided in the Short Paper instructions.

Blackboard

All students are enrolled on the Blackboard course website. The Blackboard site will contain announcements, the syllabus, reading materials, and the short paper assignment. Please check Blackboard regularly.

I will use the Course Content Section to post materials that we will review in class. To prepare for class you only need to read the assignments listed in the syllabus. You will be expected to access Blackboard during class to review the other materials.

Reading Assignments

The primary textbook for the course is CYBERSECURITY IN CONTEXT: TECHNOLOGY, POLICY, AND LAW, by Chris Jay Hoofnagle & Golden G. Richard III. Either the tangible or electronic version are acceptable for this course.

The reading assignment for each week of class are listed below. ***Please check the page numbers carefully***. Any reading assignments not included in the primary textbook are listed under "Other Reading" and will be provided to you on Blackboard in the Course Content section. I will also use the Course Content Section to post materials that we will review in class. To prepare for class you only need to read the assignments listed in the syllabus. You will be expected to access additional materials during class.

Week #	Class Meeting Dates	Subject	Textbook Sections (Pages)	Other Reading

1a	Tu. 1/14	Defining Cybersecurity	1.1 (3-6) [but not 1.1.1] 1.2 (12-13), 1.2.4 - 1.2.6, (24-27) 2 - 2.1 (59-85)	Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985 (March 2018), pgs. 1006-1010 Ido Kilovaty, *Availability's Law*, 88 TENN. L. REV. 69 (Fall 2020), pgs. 95-103
1b	Th. 1/16	Key Themes	3.1, 3.2 [but not 3.2.1] (111-23), 3.3 (125-138) 5.1 (only) (198), 5.2.4 - 5.2.7 (222-24) 5.3 – 5.4 (226-31) 10 - 10.1 (393-396)	Charlotte A. Tschider, *Locking down "Reasonable" Cybersecurity Duty*, 41 YALE L. & POL'Y REV. 75 (2023), pgs. 85-102
2a	Tu. 1/21	Cybersecurity Frameworks	8.5 – 8.6 (346-358)	Derek E. Bambauer, *Cybersecurity for Idiots*, 106 MINN. L. REV. HEADNOTES 172 (Fall 2021), pgs. 185-190 NAIC Model Laws, Insurance Data Security Model Law (Oct. 2017), pg. 1-11 The 18 CIS Critical Security Controls
2b	Th. 1/23	Anatomy of a Cybersecurity Incident	1.2.1 (14-16) 2.2 - 2.2.1 (86-92)	FTC v. Ring, Complaint, pgs. 1-17 FTC v. Blackbaud, Complaint, pgs. 1-5
3a-b	Tu. 1/28 & Th. 1/30	FTC Cybersecurity Enforcement	6.1 (250-65)	FTC v. Ring, Complaint, pgs. 18-20 FTC v. Ring, Stipulated Order FTC v. Blackbaud, Consent Package, pgs. 6-21 (of the PDF)