Domestic Cybersecurity
LAW 582, POLS 498 | 3 Credits | Spring 2021
Mode of Instruction: Fully Remote
Course Website: https://canvas.unl.edu/courses/103156
Professor Mailyn J. Fidler

Contact Information

E-mail (preferred): mfidler2@unl.edu
Telephone : (812) 219-6749
Faculty Assistant: Vicki Lill (vicki.lill@unl.edu)

Course Schedule

Tuesday/Thursday 4.30-5.50, on Zoom.

Attendance is required, with camera on (see below).

Office Hours

Tuesday/Thursday, 8:00-9:00 pm, on Zoom.

To request an appointment outside of normal office hours, please email me. I am happy to accommodate alternate times if I can.

Course Description

Cybersecurity is one of the most important and challenging emerging legal issues of the 21st century. And yet, no coherent legal framework exists to address these issues. This class will delve into the patchwork of federal and state laws that govern the security of data, addressing the nuts-and-bolts guidance that lawyers will need to help clients comply with regulatory requirements, the legal requirements engineers will need to be aware of, and the competing values that inform how politicians make decisions about regulating cybersecurity. This class will take an interdisciplinary approach and will be suitable for law students as well as students in other fields that are affected by cybersecurity issues, such as computer and political science.

Texts

The assigned text for this course is a selection from *Cybersecurity: An Interdisciplinary Problem* by Bambauer, Hurwitz, Thaw, and Tschider. This text is referred to as the "Cybersecurity Book" on the syllabus. Once available from the publisher, I will provide you with the pdf once you have purchased the text. You have two options for purchase: (1) you may pay me electronically through PayPal (mailynfidler@gmail.com) or (2) you may take a physical check in to my assistant. If you are choosing (2), please let me know, so I can make the appropriate logistical arrangements with her. The cost is $72.86.

The course will also be using excerpts from *Chesney on Cybersecurity Law, Policy, and Institutions*, which is a freely available resource and will be posted on Canvas.

All other readings will be posted on Canvas.

Assignments

Due dates are indicated below and in the syllabus, and "by midnight" means the end of the day indicated, so 11:59 pm of the stated date. The final grade is determined as follows:

- 10% interdisciplinary assignment: students will take a short, open-book quiz on either the technical or legal foundations covered. Students will take the quiz for the field that is not their home discipline. Political science students may choose to take either. **Due Feb. 17** by midnight.
- 20%: regulatory comments assignment. Federal regulators open certain actions open to public comment. Students will draft a comment on a specific regulatory action from the perspective of either a 1) industry trade organization or 2) civil society organization. More details will be posted on Canvas. **Due Mar. 7** by midnight.
- 20%: research memo applying legal & technical analysis to a topic in greater detail. More details will be posted on Canvas. **Due April 8** by midnight.
- 50%: a final, remote, open-book exam. I will conduct a review session before the exam, either on the last day of class or during the exam study period. Exams will be available for students to self-schedule beginning April 26 at 9:00 Central Time. Graduating students and LLM students must complete their exams by Monday, May 3, 2021 at 5 pm Central Time. All other students must complete their exams by Wednesday, May 5, 2021 at noon Central Time.
- Grades may be adjusted up or down one level based on attendance/participation (see below).

Grading

- JD students will be graded according to the College's 9-point scale. The class is not graded on a formal curve, but I will grade relative to other JD candidate performances.
- LLM students will also be graded on the 9-point scale, but compared to each other.
- Undergraduate students will be graded on an A-F scale, relative to other undergraduate members of the class.

Attendance and Participation

This course requires regular synchronous attendance and participation with your camera on at scheduled times. I reserve the right to adjust a final grade up or down one level based on good or poor attendance and course participation. Persistent lack of attendance may result, after notice to the student, in involuntary withdrawal from the course or a failing grade in the course.

If you are unable to attend a scheduled class session remotely, please email me to provide a brief explanation, although you need not provide private or sensitive details. Legitimate reasons for such excused absences include, e.g., illness, family needs, and unavoidable conflicts with medical appointments.

To receive credit for attendance, **your camera must be on for the class**. Brief turn-offs are acceptable—for example, if you need to move locations during class in a shared space. As with attendance, if you have a legitimate reason to have your camera off regularly—for instance, caring for children—please email me, although you need not provide sensitive details.

This course will involve me calling on students at random during class. As I will explain during the first class, this method allows for high engagement and equity in class participation. Even if you do not know the answer, I expect you to respond and work with me in a back-and-forth to the benefit of the class.

The College of Law's attendance policy applies to this class:

> Students are required to attend classes regularly and to prepare all assigned work thoroughly. Inadequate class attendance or preparation may result in the student being dropped from the course or may adversely affect the final grade the student receives in the course. A first year student who is dropped from a course will receive a failing grade for the course.

Plagiarism and Conduct

This course is subject to the College of Law's Honor Code, available at: https://law.unl.edu/honor-code/ and the University of Nebraska Code of Student Conduct, available at: https://studentconduct.unl.edu/student-code-conduct.

Please note that plagiarism involves using anyone else's work as your own without attribution. This applies to other current or former students work, any information available on the Internet, and materials written by your instructor. The course will use TurnItIn analysis through Canvas.

Disability Accommodations

Students with disabilities are encouraged to contact Assistant Dean Marc Pearce for a confidential discussion of their individual needs for academic accommodations. It is the policy of the University of Nebraska-Lincoln to provide flexible and individualized accommodation to students with documented disabilities that may affect their ability to fully participate in course activities or to meet course requirements. To receive accommodation services, students must be registered with the Services for Students with

Disabilities (SSD) office, 132 Canfield Administration, 472-3787 voice or TTY.

My Approach to Readings

My bargain is this: I try to assign no more than 4 pieces to read of roughly 40 pages total length each class. In addition, I include a little bit of guidance about how to approach the readings and list them in the recommended order of reading. In return, I ask that you read them.

Acknowledgements

I am grateful to Gus Hurwitz, Alan Rozenshtein, Asaf Lubin, David O'Brien, Nomi Conway, and Kendra Albert, whose materials and suggestions contributed to the development of this syllabus.

Course Schedule

UNIT I – Introduction and Cybersecurity Values
This section asks: what is cybersecurity? What are we securing? This section's readings present views of cybersecurity as a risk-management tool, as a cultural tool, and as a safeguard of privacy. What else might technical cybersecurity measures secure?

Class 1 – January 26 -- Canceled due to snow

Class 1 – January 28 – Introduction
- *Cybersecurity Book*, Chapter 1 (all but Section D)
- *Cybersecurity Book*, Chapter 3, p. 59-62, 73-80
- Bruce Schneier on SolarWinds Hack in the *Guardian* (Canvas)

Class 2 – February 2 – Security Culture
- Excerpt from *From Counter Culture to Cyberculture: Stewart Brand, the Whole Earth Network and the Rise of Digital Utopianism* by Fred Turner (Canvas)
- Excerpt from *Black Software: the Internet & Racial Justice, from the AfroNet to Black Lives Matter* by Charlton McIlwain (Canvas)
- DIY Feminist Guide to Cybersecurity (Canvas)
- Explore hacker culture via Hack_Curio (Canvas)

Class 3 – February 4 – Privacy and Security
- Derek Bambauer, *Privacy versus Security*, 103 J. OF CRIM. L. AND CRIMINOLOGY 667 (2013) (Canvas)
- David Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHICAGO L. REV. 221 (2016) – Section II and Section III B-D (Canvas)
- Daniel Solove, Nothing To Hide, Select Marked Excerpts (Canvas)

UNIT II – Technical and Legal Foundations
This section presents basic technical and legal background for navigating cybersecurity questions. We will primarily focus on the structure of the Internet, how encryption works, what the primary cybersecurity threats are, and the basic legal tools used in addressing cybersecurity problems (common law, statute, administrative regulations, and constitutional law).

Class 4 – RECORDED – Technical Foundations
- *Cybersecurity Book*, Chapter 5, p. 133-188 (all)

Class 5 – February 9 – Technical Foundations, Con't
Guest Speaker: Prof. Stephen Cooper, Director of the Jeffrey S. Raikes School of Computer Science and Management at UNL
- Public Key Encryption Explainer (Canvas)
- Lessig Code is Law (Canvas)
- Bruce Schneier, Technologists v. Policy Makers (Canvas)

Class 6 – February 11 – Cybersecurity Threats

- *Cybersecurity Book*, Chapter 4, 81-91, 106-132
- Managing Technical Debt (Canvas)

Class 7 – February 16 – Legal Foundations
- *Cybersecurity Book*, Chapter 6, 189-206, 210-225
- The Internet "Blackout" of 2012 (SOPA/PIPA) (Canvas)

INTERDISCIPLINARY QUIZ DUE Feb 17 by midnight

UNIT III – Federal Legislation and Regulation
Federal legislation and regulation of cybersecurity is a messy patchwork. This section focuses on which federal agencies can regulate cybersecurity and how they do so, and asks whether they do it well. It also looks at how Congress has and has not successfully regulated cybersecurity by statute. Here, our legal tools are primarily statutory and administrative and the entities regulated are private actors.

Class 8 – February 18 – Privacy Statutes & Cybersecurity
- FAS Data Protection Law Summary, p. 8-36 (Canvas)
    - NOTE: read only GLBA, HIPAA, Communications Act, and Federal Securities sections
- Nuala O'Connor, Reforming the U.S. Approach to Data Protection and Privacy, CFR Net Politics (2018) (Canvas)
- Charlotte Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 Annals of Health L. 1 (2017), p. 10-16.

Class 9 – February 23 – Regulatory Approaches to Cybersecurity (FTC)
- *Chesney on Cybersecurity*, pg. 28-34
- FTC Uber Complaint (Canvas)
- Solove & Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2011), p. 619-627 (Canvas)
- Gus Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 Iowa L. Rev. 955 (2016), p. 984-988 (Canvas)

Class 10 – February 25 – Regulatory Approaches to Cybersecurity (NIST & FCC)
- *Chesney on Cybersecurity*, pg. 80-89 ("Critical Infrastructure") (Canvas)
- NIST Common Vulnerability Scoring System (Part I) (Canvas)
- Mike Sherling, *FCC Likely Regulators*, 569 Fed. Comms. L. J. 567 (2014) Parts I-III (Canvas)
- Jim Dempsey, IOT Security Act & NIST, Lawfare (Canvas)

Class 11 – March 2 – Hacking Statutes
- Paul Ohm, CFAA Chapter (Canvas)
- Orin Kerr, *Cybercrime's Scope,* 78 N.Y.U. L. Rev. 1596 (2002), through Part II (Canvas)
- Aaron Schwartz CFAA Indictment (Canvas)
- *Van Buren* Explainer (Lawfare) (Canvas)

REGULATORY COMMENTS ASSIGNMENT DUE MARCH 7 at midnight

UNIT IV – Government as "Hackers"
This unit looks at law enforcement and national security actors at the federal level and their abilities to circumvent cybersecurity measures in the name of national security, and the legal constraints that govern those abilities. Here, our primary legal tools are statutory (criminal procedure) and constitutional.

Class 12 – March 4 – Access Statutes
- FAS ECPA Reader, p. 1-50 (Canvas)

Class 13 – March 9 – Encryption Debates, Past
- Lessons from the Crypto Wars, p. 1-11 (Canvas)
- Don't Panic: Making Progress on the "Going Dark" Debate, p. 1-15 (Canvas)
- Steven Morrison, *Breaking iPhones Under CALEA and the All Writs Act*, Cardozo L. Rev. (Canvas), Introduction and Section II
- Cindy Cohn and Andrew Crocker, U.S. Export Controls and "Published" Encryption Source Code Explained, EFF (2019).

Class 14 – March 11 – Encryption Debates, Present
Guest Speaker: Riana Pfefferkorn, Research Scholar, Stanford Internet Observatory
Readings TBD

Class 15 – March 16 – National Security Apparatus & Cybersecurity
- Summary of Snowden Revelations, Lawfare (Canvas)
- Robert Litt, An Overview of Intelligence Collection, July 18, 2013 (Canvas)
- Landau, NSA Subverts NIST Algorithm, Lawfare (Canvas)
- Benjamin Jensen and J.D. Work, Cyber Civil-Military Relations: Balancing Interests on the Digital Frontier, War on the Rocks, Sept. 4, 2018 (Canvas)

Brief Return to Unit III – Federal Legislation and Regulation
Class 16 – March 18 – Drafting Cybersecurity Legislation
Guest Speaker: Collin Anderson, Privacy and Cybersecurity Fellow, Senator Richard Blumenthal
Readings TBD

UNIT V – State Law Approaches to Cybersecurity
States are important actors in the cybersecurity field. Any common law approaches to cybersecurity happen in state courts, and states have taken the lead in terms of passing cybersecurity statutes. Our primary legal tools here are common law and constitutional law, as well as state statutory law. On the last day of this unit, we will look at state law enforcement, which deals with criminal procedure.

Class 17 – March 23 – Common Law Approaches
- *Chesney on Cybersecurity*, p. 36-46
- *William McGeveran, Duty of Data Security, 103 Minn. L. Rev. 1136 (2019), Intro & Parts II & III (Canvas)*
- Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (Canvas)

- Real Estate Cybersecurity Complaint (Canvas)

Class 18 – March 25 – Software Liability
- Jane Chong, Bad Code, Lawfare (2013)
- Bryan Choi, *Crashworthy Code*, 94 Wash. L. Rev. 39 (2019), through Part II (Canvas)
- Cyber Solarium Software Liability Bill Proposal 2020 (Canvas)

Class 19 – March 30 – Data Breach Notification Statutes
- Daniel Solove and Danielle Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Tex. L. Rev. 737 (2018), Introduction & Part I (Canvas)
- Nebraska Data Breach Statute --- Nebraska Revised Statutes 87-801 through 87-808 (Canvas)
- Kosseff Critique of California Data Breach Law (Canvas)
- Equifax Complaint, SF City Attorney's Office (Canvas)

Class 20 – April 1 – Cyber Insurance
Guest Speaker: Professor Asaf Lubin, Indiana University Maurer School of Law
- Ben-Shahar & Logue, How Insurance Substitutes for Regulation, CATO Institute (Canvas)
- Cyber Insurance and Systemic Market Risk, East-West Institute (Canvas)
- Renee Dudley, How Insurance Companies are Fueling a Rise in Ransomware Attacks, Propublica (Canvas)
- Cyber Warfare and the Act of War Exclusion, Blaney McMurtry LLP (Canvas)

Class 21 – April 6 – State Law Enforcement and Cybersecurity
- Mailyn Fidler, *Local Police Surveillance and the Administrative Fourth Amendment*, 36 Santa Clara High Tech. L. J. 481 (2020) (Intro and Part I only) (2020) (Canvas)
- *Carpenter* (majority opinion) (Canvas)
- *Carpenter* explainer (Canvas)
- Judge Owsley 2012 Order (Canvas)
- *Williams v. SF Complaint* (Canvas)

UNIT VI – Other Topics in Cybersecurity

Research Memo Assignments Due April 8 at Midnight

Class 22 – April 8 – Software Export Controls & Human Rights
- Mailyn Fidler, *Proposed U.S. Export Controls: Implications for Zero-Day Vulnerabilities and Exploits*, Lawfare, June 10, 2015.
- Mailyn Fidler, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, I/S: A Journal of Law and Policy for the Information Society (2015), pg. 463 to 474.
- Joint Civil Society Wassenaar Comments, Sections II, IV(A) and IV(C)

Class 23 – April 13 – Return to Security Culture: Section 230 and Content Moderation

- Jeff Kosseff, *What's in a Name? Quite a Bit, If You're Talking About Section 230*, Lawfare (Canvas)
- Zoe Bedell and John Major, What's Next for Section 230? A Roundup of Proposals, Lawfare (Canvas)
- Albert et al., FOSTA in the Legal Context, Introduction (Canvas)
- C.A. Goldberg, WTF is the CDA230? (Canvas)
- Olivier Sylvain, Discriminatory Designs on User Data, Knight First Amendment Institute (2018), from "Discriminatory Designs on User Content and Data: The Example of Online Housing Marketplaces" to the end

Class 24 – April 15 – Cybersecurity Careers // Exam Practice
Guest Speaker: Wesley Tiu, Latham & Watkins

Class 25 – April 20 – Cybersecurity Careers // Biden Administration Cyber Priorities
Guest Speaker: Jen Silk, Paypal Cybersecurity

Class 26 – April 22 – Review Session

FINAL EXAM