Domestic Cybersecurity
LAW 582 | 2 Credits | Spring 2023
Course Website: https://canvas.unl.edu/courses/147549
Professor Mailyn J. Fidler

Please turn Canvas notifications on. I will communicate with you primarily through the Announcements function of Canvas.

Contact Information

E-mail (preferred): mfidler@unl.edu
Telephone : (812) 219-6749
Faculty Assistant: Sabrina Ehmke Sergeant (sehmke2@unl.edu)

Course Schedule

Thursday 1.30-2.45
Friday 1.30-2.30

NOTE: This course meets for a shorter amount of time on Fridays.

We will **NOT** have class on the following days:

- Friday, February 3 (although there is an asynchronous video to watch)
- Friday, March 10
- April 28 onward

Office Hours

Thursday, 3-4.30 pm, no appointment needed.

To request an appointment outside of normal office hours, please email me. I am happy to accommodate alternate times if I can. Such appointments may happen over Zoom.

Course Description

Cybersecurity is one of the most important and challenging emerging legal issues of the 21st century. And yet, no coherent U.S. legal framework exists to address these issues. This class will delve into the patchwork of U.S. 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 address not only what little black letter law exists with respect to cybersecurity, but also policy and technical considerations. Note that this class is U.S.-focused.

What kind of course is this?

This course will effectively run as a seminar. It does not have a final exam. It does have a heavy and varied reading load and multiple assignments. I approach the course this way to try to give you practice in the flexibility and self-led learning that is required to work in this field. Standards for course participation and reading comprehension are higher than in other classes because that is one of the skills this course requires you to develop.

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. Please see the instructions I posted on Canvas regarding the option to purchase the relevant pages in pdf form for a reduced price. That said, because cybersecurity is a rapidly changing field, this text is used largely only for foundational readings. We will be drawing from a wide and untraditional pool of readings. These 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:

- 5% area expert: students are responsible for being active discussants in every class. That said, students will each take one class day to be the assigned "expert" for the day. I will have them present some of the major ideas from the articles, and suggest areas for discussion, as well as being our go-to for confusion/clarifications about readings. I suggest you spend about twice as much time on the readings for the day you are the "expert."

- 5% intersectional cybersecurity paragraph: following our investigation of hacker culture, counterculture, race, and gender as it relates to cybersecurity, students will write one paragraph about the cybersecurity risks, developments, or attacks in an area of life/work/hobbies that matters to them. **Due Feb. 9 at midnight.**

- 10% interdisciplinary quiz: students will take a short, open-book quiz on the technical foundations covered. **Due Feb 19 by midnight.**

- 26.67%: 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 March 10** by midnight.

- 26.67%: legal compliance assignment. Using one of the federal regulatory schemes we study, advise a company on its compliance based on a fact pattern. More details will be posted on Canvas. **April 11** by midnight.

- 26.67%: research memo applying legal & technical analysis to a topic in greater detail. More details will be posted on Canvas**. Due May 15 at midnight for graduating students and by May 19** by midnight for the remainder.

- Grades may be adjusted up or down one level based on attendance/participation (see below).

Late Policy

A late assignment will be marked down one point on the 9-point scale. So an assignment that would have gotten a 9 would get an 8, and so on. However, I understand that important circumstances arise that might warrant exceptions, such as mental/physical health issues or family deaths, etc. Please contact me to discuss if you feel you are in such a circumstance.

Grading

- The class will be graded according to the College's 9-point scale. The class is not graded on a formal curve, but I will loosely grade relative to the performance of others in the class.

Attendance and Participation

This course requires regular synchronous attendance and participation. 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.
That said, life happens. Each student may miss one class without consequence per semester. (Because this is a 2-credit class, this number is lower than I allow for my other 3-credit classes, for those of you that have had me elsewhere.) To ensure I don't call on you when absent, please email me ahead of time to note you are using your free day.

If further life circumstances arise, please contact me to discuss your attendance needs. You need not disclose sensitive details, but we should touch base to ensure your continued progress.

Illness & Recording Policy
Illnesses (most importantly COVID) are excused. Please just let me know so I can take you off the cold call list. Please stay home! I will happily make up any missed content with you. If you are ill, you are welcome to Zoom into class, although I may not be able to facilitate your speaking participation. I do not record classes, nor do I allow recording classes.

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

I take plagiarism extremely seriously. 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. It also includes the use of assisted composition such as ChatGPT. My policy 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 Academic Advisor Jill Stohs 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 Cold-Calling

I will usually start each class with some cold-calling to get the ball rolling. However, unlike my other classes, simply responding to these cold calls will not be enough to earn a satisfactory participation grade. You must participate outside of these cold-calls. I still use cold-calls as a tool of equitable class participation, not as a punitive measure to check your work. Cold-calling helps us get a good mixture of voices. You are always welcome to say you don't know as long as you're willing to work with me on teasing out a response.

Goals of this course

By the end of this course:

- Students should achieve minimal technical competence. After this course, they should have the base knowledge and navigational ability be to roles that require them to learn new technical details in legal settings, as well as the confidence that they can learn these details.
- Students should be able to assess the purpose of a document within the cybersecurity world; namely, students should develop the skill of determining whether a document offers a theoretical perspective, a historical perspective, a doctrinal perspective, etc. Students should be able to digest that material as needed for its purpose.
- Students should be able to read and write a wide variety of style of documents, as required in the motley world of cybersecurity law.

- Students should be able to easily switch between legal analysis and policy recommendation mode.

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 – Thursday, February 2 -- Introduction
- *Cybersecurity Book*, Chapter 1 (all but Section D)
- *Cybersecurity Book*, Chapter 3, p. 59-62, 73-80 |p. 69 – 72, 83 – 90
- Bruce Schneier on SolarWinds Hack in the *Guardian* (Canvas)
- Brooklyn Hospital Hack NYT Article (Canvas)
- Derek Bambauer, *Privacy versus Security*, 103 J. OF CRIM. L. AND CRIMINOLOGY 667 (2013) (Canvas)

Class 2 – Friday, February 3 – Technical Foundations [ASYNCHRONOUS]
- *Cybersecurity Book*, Chapter 5, p. 133-165 | p. 151-184
- Bruce Schneier, Technologists v. Policy Makers (Canvas)

Instead of meeting in person, you will watch a series of short videos by Code.org & Khan Academy (https://www.khanacademy.org/computing/code-org/computers-and-the-internet).

I'm assigning these instead of me recording a lecture on the topic for a few reasons -- they have graphics, they're broken down into six-minute increments, and you can tailor your viewing experience to your level of expertise. Also, they're just generally better production value than what I can offer! For most folks, I'd recommend watching the "How the Internet Works" videos 2-6 ("Wires, Cables, and Wifi" through "Encryption"). These videos are about 30-40 minutes in total. There is an additional set of videos about how computers work if you'd like to go over that material.

Class 3 – Thursday, February 9 – Security Culture
- Lessig Code is Law (Canvas)
- Read either:
  - *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, OFFICE OF THE HOMELAND SEC. INSPECTOR GEN. (2022)
  - OR *Truth Cops: Leaked Documents Outline DHS's Plans to Police Disinformation,* THE INTERCEPT (2022).
- Read either:
  - *From Counter Culture to Cyberculture: Stewart Brand, the Whole Earth Network and the Rise of Digital Utopianism* by Fred Turner (Canvas)

    - OR Excerpt from *Black Software: the Internet & Racial Justice, from the AfroNet to Black Lives Matter* by Charlton McIlwain (Canvas)
- Read either:
    - DIY Feminist Guide to Cybersecurity (Canvas)
    - OR explore hacker culture via Hack_Curio (Canvas)

INTERSECTIONAL CYBERSECURITY PARAGRAPH DUE Feb. 9 at midnight

UNIT II – Technical 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 3 – Thursday, February 10 – Encryption (TENTATIVE)
Guest Speaker: Prof. Keith Schwarz, Lecturer in Computer Science at Stanford University

- *Cybersecurity Book*, Chapter 5, p. 166-182 | p. 184-201
- Public Key Encryption Explainer (Canvas)

Class 5 – Thursday, February 16 – Cybersecurity Threats

- *Cybersecurity Book*, Chapter 4, 81-91, 106-132 | p. 91- top of 107; 121-146
- Managing Technical Debt (Canvas)
- LastPass Breach NYT Article (Canvas)
- Bolt-On vs. Baked-In Cybersecurity (Canvas)

INTERDISCIPLINARY QUIZ DUE TBD

UNIT III – Federal 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. Note that much of federal cybersecurity regulation happens by way of federal privacy legislation.

Class 6 – February 17 – Federal Cybersecurity Regulation, Introduction

- Haber and Reichman, *Functional Separation of Powers in Cyber* (Canvas)
- *Cybersecurity Book*, 196-202 [Rules vs. Standards] | p. 216-222
- CISA Summary (Canvas)
- Sectoral Regulation Critique Packet (Canvas)

Class 7 – February 23 – Cybersecurity Legislation

- David Thaw, *Efficacy of Regulating Cybersecurity* (Canvas) [HIPAA & GLBA]
- *Cybersecurity Book*, 370-379 [HIPAA details] | p. 414-424
- *Cybersecurity Book*, 379-385 (FISMA) | p. 424-429
- Add reading on SEC disclosure rules/Sarbanes-Oxley
- ADDPA Packet (Canvas)

Class 8 – February 24 – Regulatory Approaches to Cybersecurity (FTC)

- 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)
- FTC Uber Complaint (Canvas)

Class 9 – March 2 – Regulatory Approaches to Cybersecurity (NIST & FCC)

- Lawfare, *NIST Commentary*
    - *Compare to* Jim Dempsey, IOT Security Act & NIST, Lawfare (Canvas)
    - *Skim* NIST Common Vulnerability Scoring System (Part I) (Canvas)
- Sherling, *FCC Likely Regulators*, (2014) Parts I-III (Canvas)
- New bill on Critical Infrastructure Incident Reporting summary (Canvas)

Class 10 – March 3 – Anti-Hacking Statutes

NOTE: Mr. Schwartz's case involves suicide.

- Paul Ohm, CFAA Chapter (Canvas)
- *Orin Kerr, Focusing the CFAA in Van Buren (Canvas)*
- Edgar, *Why Van Buren is Good News for Cybersecurity*, Lawfare (Canvas)
- Aaron Schwartz CFAA Indictment (Canvas)
- CFAA & NSO Group excerpts (Canvas)

UNIT IV – 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 11 – March 9 – Common Law Approaches

- Kerr*, Common Law History (Canvas)*
- Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (Canvas)
- William McGeveran, *Duty of Data Security, 103 Minn. L. Rev. 1136 (2019), Intro & Parts II & III (Canvas)*
- Real Estate Cybersecurity Complaint (Canvas)

REGULATORY COMMENTS ASSIGNMENT DUE March 10 at midnight

Class 12 – March 23 – 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)
- Sharma, SOSSA Liability Lawfare Article (Canvas) (2022)

Class 13 – March 24 – 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 14 – March 30 – Ransomware

- Countering Ransomware: A Whole-of-Government Effort (Lawfare) (Canvas)
- Lubin, *The Law & Politics of Ransomware* (excerpts) (Canvas)
- Neprash & Rozenshtein, *New Data Quantifies Ransomware Attacks on Healthcare Providers* (Lawfare) (Canvas)
- Abely, *Ransomware, Cyber Sanctions, and the Problem of Timing* (Canvas)

UNIT V – Special Topics in Cybersecurity

Class 20 – March 31 – Offensive Cybersecurity

- Corcoran, Examples of Active Cyber Defense (Canvas)
- Active Cyber Defense Bill (Canvas)
- Cook, *Hacking Back in Black* (Canvas)
- Pell, *Private Sector Defense* (Lawfare) (Canvas)
- Eichensehr, Public-Private Cybersecurity (excerpts) (Canvas)

Class 21 – April 6 – Cyber Insurance

Guest Speaker: Professor Asaf Lubin, Indiana University Maurer School of Law

- **TBD**

Class 19 – April 7 – 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* explainer (Canvas)
- Judge Owsley 2012 Order (Canvas)
- *Williams v. SF Complaint* (Canvas)

COMPLIANCE ASSIGNMENT DUE April 11 at midnight.

Class 22 – April 13 – Cryptocurrency Cybersecurity

Tentative Speaker: Amy Aixi Zhang, Policy Counsel at Paradigm (crypto VC firm)

- Readings TBD

Class 21 – April 14 – Space Cybersecurity

Tentative Speaker: Lauryn Williams, Senior Advisor, Office of the National Cyber Director, The White House

- Falco, *Cybersecurity Principles for Space Systems* (Canvas)
- Trump 2020 Space Cyber Policy (Canvas)
- Tallinn Manual 2.0 Chapter 10 (Space) (Canvas)
- Space ISAC 2022 Plan (Canvas)

"Security" and Cybersecurity

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. On the last day of this unit, we will look at state law enforcement, which deals with criminal procedure.

Class 15 – April 20 – Federal Law Enforcement Electronic Access Statutes

- Pell, Cybersecurity & ECPA Overview, Lawfare (Canvas)
- FAS ECPA Reader, p. 1-50 (Canvas)
- U.S. Commercial Hacking Investigation (NYT) (Canvas)
- Steven Morrison, *Breaking iPhones Under CALEA and the All Writs Act*, Cardozo L. Rev. (Canvas), Introduction and Section II

Class 16 – April 21 – National Security & Cybersecurity

NOTE: The first two readings of today include aspects of the Snowden revelations. If you plan to seek government security clearance in the future, they may care about you reading these documents. If you are in that situation, you may skip the first two readings.

- Summary of Snowden Revelations, Lawfare (Canvas)
- Robert Litt, An Overview of Intelligence Collection, July 18, 2013 (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)
- *Chip Export Controls*, Lawfare (Canvas)
- *Tiktok Ban,* Lawfare (Canvas)

Class 17 – April 27 – Federal Encryption Debates

- Lessons from the Crypto Wars, p. 1-11 (Canvas)
- Don't Panic: Making Progress on the "Going Dark" Debate, p. 1-15 (Canvas)
- Kostyuk & Landau, Dueling over Dual_EC_DRBG excerpts (Canvas)
- Cindy Cohn and Andrew Crocker, U.S. Export Controls and "Published" Encryption Source Code Explained, EFF (2019).
- Pfefferkorn EARNIT Blog Post (Canvas).

RESEARCH MEMO DUE May 19 (pending check of when graduates' grades are due)

Days I've Included In the Past, for Reference:

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

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)