Syllabus – LAW 516 and GOVT 464: Foundations of Cybersecurity and AI Practice

Antonin Scalia Law School & Schar School of Policy and Government– Fall 2025

Ali Jessani & Kathryn Mauler

Brief Course Description:

Cybersecurity preparedness is a pressing local, national, and global concern, affecting the competitiveness of small and large organizations, as well as the security of governments. At the same time, artificial intelligence (AI), particularly generative AI, is becoming increasingly relevant in every industry, and creating unique challenges for institutions leveraging this rapidly growing technology.

This course serves as the first part of the Cybersecurity + AI Clinic program and is **required for students who wish to participate in the spring 2026 clinical component**. The Clinic program uses a service-learning approach to introduce students to the cyber threat and privacy harm landscape, cybersecurity and AI risk management, and information governance consulting. While many cybersecurity and AI discussions focus on global or federal reform efforts, this course emphasizes the practical challenges that information governance professionals engage with every day to account for these evolving threats and risks.

The primary goal of the course is to give students practical tools and knowledge to be better cybersecurity professionals, as well as the necessary background for client engagements that students will perform in the spring semester. **Successful completion of this course is required to join the spring 2026 clinic**, where students will work in supervised teams to deliver pro bono cybersecurity and AI risk assessments and recommendations to under-resourced organizations.

Learning Outcomes:

Upon successful completion of this course, students will be able to:

- Identify significant concepts related to privacy, cybersecurity, and AI risk management of interest to managers, policymakers, and organizational leaders;
- Review and design critical organizational resources, such as privacy policies, incident response and recovery plans, and cybersecurity and AI best practices;
- Demonstrate increased awareness and sensitivity to the legal and ethical implications of cybersecurity, privacy, and AI decisions;
- Communicate with clients about the cyber threat landscape, organizational vulnerabilities, and risk mitigation strategies;
- Apply critical thinking, logical reasoning, and problem-solving skills through applied service-learning; and
- Collaborate confidently on interdisciplinary teams to support cybersecurity, privacy, and AI projects.

Class Format:

Between 10 and 20 students, both undergraduate and law students; three credits, in-person only. Active participation in class discussions is required, and students are expected to be fully prepared for each class session. This is an in-person course, so all students are expected to be in class for each class session.

Class Details:

Tuesdays, 4-6 PM ET
Fuse at Mason Square (see Canvas Syllabus for room)

Grading:

Student performance will be evaluated according to the following breakdown:

- In-Class Participation: 10%
- Midterm Project: 25%
- Final Exam: 65%

Scalia Law School and Howard University students will be graded separately.

For the final exam, no access to the Internet or resources other than a student's notes and the readings will be permitted. The exam will ask students to analyze the legal and policy issues discussed in the course and proffer legal and policy proposals.

Class Participation:

Class attendance and participation will also factor into grading, consistent with Antonin Scalia Law School policy. Students who will miss more than two class sessions must receive advance permission from the instructors and may be required to complete additional work to receive credit for the course.

Office Hours:

Appointments can be made to meet in person, over Zoom, or by telephone. Professors will provide staff information for making appointments in class.

Faculty Contact Information:

Professor Ali Jessani ajessani@gmu.edu	Professor Kathryn Mauler kciano@gmu.edu

Course Materials:

The course does not use a textbook; the syllabus includes readings from a variety of sources. Most course materials are available through the links provided below or through a quick Internet search.

Please be sure to pull and read all materials well ahead of the relevant class session.

Any slides, study guides, or other material prepared by the professors are their intellectual property and shared for class and student use only; students should not input such material into AI systems, which, depending on their configuration and terms of use, may be able to assert claims of ownership over such material.

Course Specific Policies:

- Students are expected to complete the assigned readings and to come prepared to discuss them.
- Instructors will employ Socratic dialogues (i.e. cold calling) to facilitate learning.
- If unforeseen circumstances prevent a student from preparing for class, the student should attend nonetheless and inform the instructors in advance if they are not prepared to be called upon.
- All students are expected to treat each other and the instructors with courtesy and respect.
- The instructors seek a welcoming academic environment wherein critically important ethical and philosophical issues can be intellectually explored. Ideas and theories are welcome and encouraged to be challenged, but such critiques should never take the form of personal attacks on another speaker.
- Students must use their GMU email account to receive important University and Law School information, including communications related to this class. The instructors will not respond to messages sent from or send messages to a non-Mason email address.
- Generative AI tools may be used in this course for the following purposes, and with the following guidelines:
    - Permitted Uses: Students may use AI tools to brainstorm ideas, create outlines, study, explore concepts, draft written work, edit drafts, and generate practice questions or study aids.
    - Prohibited Uses: Students may not use AI tools during the midterm exam or the final exam.

- Expectations: Students must use AI tools responsibly, verify the accuracy of any facts or citations, and disclose when AI tools are used to create course work products. Any use of AI that contributes to submitted work must be properly cited. Upon request, students should be prepared to provide the transcript of AI prompts and responses.

- Academic Standards: Misuse of AI tools, including use during restricted assessments, will be treated as a violation of academic integrity standards.

Class Recordings Prohibited:

- Pursuant to Academic Regulation 4-2.2, no portion of a class session or an examination may be preserved by means of a recording device such as an audio recording device, camera, or computer.

- Any exceptions to this policy must be expressly authorized in writing by the instructor(s).

- The instructors do not intend to record the weekly course meetings.

Note on Assignments:

- Given the fast-developing nature of this topic, the instructors will likely be updating the assignments listed below throughout the semester. Please stay alert to such amendments.

Course Assignments:

Class 1 (August 19, 2025): Introduction to Cybersecurity and AI

1. *AI Data Security,* Cybersecurity and Infrastructure Security Agency (May 2025)
2. Ali Jessani, *Chatbots, AI, and the future of privacy,* International Association of Privacy Professionals (Mar. 31, 2023)
3. Andre Slonopas, *What Is Cybersecurity: The Realities of the Digital Age*, American Public University (Nov. 22, 2023)
4. Bernard Marr, *The Difference Between Generative AI And Traditional AI: An Easy Explanation For Anyone*, Forbes (Aug. 23, 2023)
5. Federal Privacy Council, *Fair Information Practice Principles* (Jan. 24, 2022)(Video)
6. Lawrence Lessig, *The Path of Cyberlaw*, University of Chicago Law School (1995)
7. Matthew Ferraro et al., *Ten Legal and Business Risks of Chatbots and Generative AI*, Tech Policy Press (Feb. 28, 2023)
8. *What Is Cybersecurity?* Cybersecurity and Infrastructure Security Agency (Feb. 1, 2021)
9. Colleen McClain, et al., *Views of Data Privacy Risks, Personal Data, and Digital Privacy Laws*, Pew Research Center (Oct. 18, 2023) – skim

Class 2 (August 26, 2025): Privacy, Compliance, and Ethical Considerations

1. Ben Tarnoff, *What Is Privacy For*, The New Yorker (Oct. 5, 2024)
2. Teach Privacy, *Why Privacy Matters: Interview with Neil Richards* (Dec. 1, 2021)
3. Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, Columbia Law Review (2014)
4. Geoffrey Fowler, *I Tried to Read All My App Privacy Policies. It Was 1 Million Words*, The Washington Post (May 31, 2022)
5. Julie E. Cohen, *What Privacy Is For*, Harvard Law Review (2013)
6. Omar Tene & Jacqueline Klosek, *U.S. Privacy Outlook for 2025: Horror Vacui*, IAPP (Jan. 7, 2025)
7. Samuel Warren & Louis Brandeis, *The Right to Privacy*, Harvard Law Review (1890)
8. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, The New York Times (Sep. 6, 2021)

Class 3 (September 2, 2025): Common Cybersecurity Threats and Attack Vectors

1. David Sanger & Nicole Perlroth, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, New York Times (May 14, 2021)
2. Leiner, Cerf, et al., *A Brief History of the Internet*, 39 ACM SIGCOMM Computer Communication Review (v. 5), pp. 22–31 (2009)
3. FTC v. Wyndham Worldwide Corp, 799 F.3d 236 (3rd Cir. 2015)
4. *Most Common Cyber Attack Vectors in 2025* (Apr. 28, 2025)
5. Sanger, Krause, & Perlroth, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, New York Times (May 8, 2021)
6. The White House, *National Cybersecurity Strategy* (Mar. 2, 2023) – Executive Summary and Pillar 1

Class 4 (September 9, 2025): Cybersecurity Risk Management

1. Chantal Bernier, *Six Guidelines for Managing Legal Risk in AI Adoption*, Dentons (July 21, 2025)
2. Marisa Krystian, *What is a Data Governance Framework? Guide with Template*, Rippling (Feb. 10, 2025)
3. NIST*, Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014)
4. *Van Buren v. United States*, 141 S. Ct. 1648 (2021)

Class 5 (September 16, 2025): Data Governance

1. Ali Jessani, *When Is AI PI? How Current and Future Privacy Laws Implicate AI and Machine Learning*, IAPP (July 9, 2020)
2. Department of Transportation, FHWA Data Governance Primer (July 2025)
3. IBM, *What is Data Governance?* (Sept. 20, 2024)
4. NIST, *NIST Privacy Framework* (Apr. 14, 2025)
5. Office of Management and Budget, Federal Data Strategy (July 2020)

6. Webinar: Daniel Solove, *The New Data Governance: Beyond Compliance in Privacy and AI Access* (2024)

Class 6 (September 23, 2025): Incident Response Management

1. Emily Stewart, *Companies Lose Your Data and Then Nothing Happens*, Vox (Apr. 21, 2022)
2. NIST, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile* (Apr. 3, 2024)
3. Steve Adler, *Nuance Communications Settles MOVEit Lawsuit for $8.5 Million*, The HIPAA Journal (Aug. 15, 2025)
4. William McGeveran, *The Duty of Data Security*, Minnesota Law Review (2019)
5. Woodrow Hartzog & Daniel Solove, *Breached! Why Data Security Law Fails and How to Improve It* (Chapter 1) (2022)

Class 7 (September 30, 2025): Incident Response Simulation

1. Anthony M. Freed, *Inside the DarkSide Ransomware Attack on Colonial Pipeline*, CyberReason
2. CISA, *Incident Response Plan Basics*
3. Federal Trade Commission, *Data Breach Response, A Guide For Business* (Aug. 2023)
4. Office of the Australian Information Commissioner*, Responding to Data Breaches - Four Key Steps* (Feb. 2025)
5. Hon. Joe Reeder and Cadet Tommy Hall, *Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack*, The Cyber Defense Review (2021)
6. *SolarWinds Knocks Out Most of SEC's Claims in Novel Cybersecurity Case,* O'Melveny (August 9, 2024)

MIDTERM DUE ON THIS DATE: One page executive summary on real-life incident and remediation steps. Details will be provided in prior classes.

Class 8 (October 7, 2025): Case Study – Healthcare (Guest Speaker - Kirk Nahra)

1. Kirk Nahra*, HIPAA Privacy and Security for Beginners*, Wiley (July 2014)
2. Kirk Nahra, *A Public Service Announcement about the HIPAA Privacy Rule*, Wiley (July 2014)
3. Kirk Nahra, *Moving Towards a New Health Care Privacy Paradigm*, Wiley (2014)
4. Kirk Nahra, *Why health care privacy is a mess — and why it isn't likely to get better soon*, IAPP (Mar 20, 2025)
5. Kirk Nahra, *Regulator Concerns and the Benefits of AI in Health Care*, The SciTech Lawyer (Winter 2025)
6. Ali Jessani, *Health Privacy in 2025 and Beyond*, WilmerHale (Mar 18, 2025)
7. 45 C.F.R. Section 160.103 (Definitions) – read "covered entity," "health plan" (skim the subparts), "health care provider", and "business associate"
8. 45 C.F.R. Section 164.501 (Definitions) – read "treatment," "payment" and "health care

operations" and "marketing"

Class 9 (October 14, 2025): Managing Cyber Attacks Against Governments and Critical Infrastructure

1. Brian Humphreys, *The Designation of Election Systems as Critical Infrastructure*, Congressional Research Service (Sept. 2018) – pp. 1-3
2. Derek Johnson, *Court upholds FCC data breach reporting rules on telecom sector*, Cyberscoop (August 15, 2025)
3. Jason Miller, *Real-World AI in Cyber Threat Detection*, BitLyft (July 30, 2025)
4. New York University, *AI-Assisted Cyberattacks and Scams*

Class 10 (October 21, 2025): Cybersecurity in Specific Sectors and Supply Chain Risks

1. Chernenko, Demidov, & Lukyanov, *Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms*, Council on Foreign Relations (February 2018)
2. Coalition for Secure AI, *The AI Supply Chain Security Imperative: 6 Critical Controls Every Executive Must Implement Now*
3. Adarryl Roberts, *Utilization of Artificial Intelligence (AI) to Illuminate Supply Chain Risk*, Defense Logistics Institute (May 1, 2025)
4. Palo Alto Networks, *Top GenAI Security Challenges: Risks, Issues, & Solutions*
5. White House, *Winning the Race: America's AI Action Plan* (July 2025)
6. White House, *Executive Order on Advancing United States Leadership in Artificial Intelligence Infrastructure* (Jan 14, 2025)

Class 11 (October 28, 2025): Ethics and Emerging Technologies

1. Gabrielle Rejouis, *Why Is It OK for Employers to Constantly Surveil Workers?*, Slate (Sep. 2, 2019)
2. Kirk Nahra and Ali Jessani, *Privacy Concerns at the Intersection of Generative AI and Healthcare*, WilmerHale (Oct. 27, 2023)
3. Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186
4. UK Information Commissioner's Office, *What about fairness, bias, and discrimination?*
5. Video: CBS, *Godfather of artificial intelligence talks impact and potential of AI* (Mar. 1, 2023)
6. Office of Management and Budget, *Federal Data Strategy* (July 2020) – re-read

Class 12 (November 4, 2025): Efforts to Regulate AI in the US and Abroad

1. Ali Jessani et al., *A Comparative Perspective on AI Regulation*, Lawfare (July 19, 2023)
2. Laurie Harris, *Regulating Artificial Intelligence, U.S. and International Approaches and Considerations for Congress*, Congressional Research Service (June 4, 2025)
3. FTC, *FTC Announces Crackdown on Deceptive AI Claims and Schemes* (Sep. 25, 2024)
4. Life Institute, *High-level summary of the AI Act* (Feb. 27, 2024)
5. Richard Sentinella and Cobun Zweifel-Zeggan, *US State AI Legislation: Reviewing the 2025 Session*, IAPP (July 16, 2025)
6. Joe Duball, *How Proposed AI Enforcement Moratorium Cuts into US State-Level*

Powers, IAPP (June 27, 2025)

7. White House, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*
8. White House, *Winning the Race: White House AI Action Plan* (July 2025) – re-read

Class 13 (November 11, 2025): Communication for Information Governance Professionals

1. Corrin Jones, *Warnings and Lessons of the 2013 Target Data Breach*, Red River, (July 1, 2025)
2. Forbes Communications Council, *Data Privacy Laws: Global Implications for PR and Communications* (May 29, 2024)
3. Kelly Miller and Keri Pearlson, *How to Build a Cyber Crisis Communications Plan*, MIT Sloan Management Review (Sep. 16, 2024)
4. *Purdue University Crisis Communications Plan*
5. Press Release, *SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures*, SEC (Oct. 20, 2023)
6. Target, *Message from CEO on Payment Card Issues* (Dec. 20, 2013)
7. White House, *Statement by Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger on SolarWinds and Microsoft Exchange Incidents* (Apr. 19, 2021)

Class 14 (November 18, 2025): Working as an Information Governance Professional

1. Ben Wolford, *What is a GDPR data processing agreement?*
2. Meta, *Privacy Policy* (Jun 16, 2025)
3. Meta, *Terms of Service* (Jan 1, 2025)
4. *Risk Assessment: An Overview*, Thomson Reuters (June 3, 2024)
5. SalesForce, *Data Processing Agreement* (May 2025)
6. UK Information Commissioner’s Office, *Sample data protection impact assessment: online retail* – all seven steps