

Syllabus – Law 416: Cybersecurity Law Seminar (JM/LLM only)

George Mason University Law School – Spring 2024

Profs. John T. Hendricks & John F. Stephens

Brief Course Description:

This seminar course will provide students exposure to the key legal and policy issues related to cybersecurity, including the legal authorities and obligations of both the government and the private sector with respect to protecting computer systems and networks, as well as select national security aspects of the cyber domain. The course will include a survey of federal laws, executive orders, regulations, and cases related to surveillance, cyber intrusions by private and nation-state actors, data breaches, and privacy and civil liberties matters, among other things. The course will also explore the legislative and technology landscape in this dynamic area and will provide students with opportunities to discuss cutting-edge issues at the intersection of law, technology, and policy.

Learning Outcomes:

By the end of the course students should have acquired/be able to:

1. Understand the different types of cybersecurity threats posed to computer systems and networks.
2. Identify national security and private sector implications from threats in the cyber domain.
3. Apply the legal authorities and obligations of government and the private sector to protect computer systems and networks.
4. Critically analyze the national security policy decisions, directives, and actions for developing and implementing cybersecurity policy in relation to federal laws, executive orders, regulations, and ongoing cases.

Class Format:

- Seminar of 10-20 J.M. AND LL.M. students; two credits; one two-hour class per week.
- **Active participation in class discussions is required and students are expected to be fully prepared for each class session.**
- This course will meet via Zoom.

Grading:

- Grades will be based on an 20-25 page final paper on cybersecurity law (75% of grade) and class participation (25% of grade, based on weekly attendance and material contributions to class discussions) consistent with the law school grading policy.
- The professors will take class attendance, consistent with the law school policy.

Final Paper Due Date:

Monday, May 6, 2024 – 11:00 p.m. ET

- Papers are due via email to **both professors** by no later than the date and time above.
- **Late papers will receive a full grade deduction for every day the paper is late based on law school policy**, so please turn papers in on time.

Class Schedule:

- Tuesdays, 8:00 p.m. ET – 10:00 p.m. ET

Office Hours:

- By appointment only; students should contact the professor(s) in advance via email and offer three days and times when they would be available for a telephone call or videoconference. Whenever possible, professor(s) will send Zoom calendar invitation to confirm. Please bear in mind that the professors teach remotely from the Pacific Time Zone, so morning (i.e., in the Eastern Time Zone) appointments are limited.
- In-person office hours, on campus, may be available occasionally; the professors will inform students in advance of opportunities to meet in person.

Faculty Contact Information:

John T. Hendricks
jhendr3@gmu.edu

John F. Stephens
jstephe@gmu.edu

Instructor Expectations and Course Rules/Structure:

- This course will be taught via Zoom for J.M. and LL.M. students.
 - Students attending via Zoom are expected to attend and participate via video the same as they would in person.
 - Please be mindful of the mute button
- Students are expected to complete the assigned readings before each week's class and to come prepared to discuss them.
 - Socratic dialogues will be employed to facilitate learning outcomes. **If unforeseen circumstances prevent a student from preparing for class, the student nonetheless is encouraged to attend and should inform the professors 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.
 - Ideas and theories are welcome and encouraged to be challenged, but such critiques should never take the form of personal attacks on another speaker within the classroom setting.
 - The instructors seek a safe academic environment wherein ethical and philosophical issues can be intellectually explored.
- If students participating online need to step away from their computer for a brief time during class due to personal, family, or professional obligations, the instructors ask that they do so discreetly and then return as soon as feasible.
 - The instructors understand that online classes can pose added difficulties for all involved and want to be accommodating to the extent practicable.
 - If students step away, they should **mute their microphone and disable their video** to maintain privacy and reduce background noise for the other students.
- Students must use their Mason Live email account to receive important University 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.

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.

Course Materials:

All course materials are cases or articles available on Westlaw or Lexis-Nexis, posted on TWEN, or linked below. Materials posted on TWEN are indicated below.

In consideration of the developing nature of this area of law, it is likely that the syllabus and readings will be updated over the course of the semester; therefore, **please regularly check your email and TWEN for updates to the syllabus and readings.**

///
///
///
///

Course Assignments:

Week 1: Introduction to Computer Networks and Cyber Threats

1. Leiner, Cerf, et. al., [A Brief History of the Internet](#), 39 ACM SIGCOMM Computer Communication Review 22 (v. 5) – pp. 22-31 (TWEN or use link)
2. Congressional Research Service, [Cybersecurity: A Primer](#) (Dec. 8, 2022) - pp. 1-2 (TWEN or use link)
3. Robert M. Chesney, [Chesney On Cybersecurity Law, Policy, And Institutions](#) Introduction to Key Terms & Concepts – pp. 11-16 (hereinafter “Chesney on Cybersecurity”) (TWEN or use link)
4. Microsoft Corp., [Microsoft Digital Defense Report October, 2023](#) (Executive Summary) - pp. 1-11 (TWEN or use link)
5. Office of the Director of National Intelligence, [Annual Threat Assessment \(the US Intelligence Community\)](#) (Feb. 6, 2023)-pp. 4-5, 8, 12-13, 15, 17, 23-24 (TWEN or use link).

Week 2: Nation-State Hacking, Political Manipulation, and Federal Law

1. [Chesney on Cybersecurity](#) – *Holiday Bear and SolarWinds* – pp. 3-9 (TWEN or use link)
2. Kevin Mandia, [FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community](#) (Dec. 8, 2020) – pp. 1-3 (TWEN or use link)
3. Brian Barrett, [SolarWinds Hack is Historic Mess](#), Wired (Dec. 19, 2020) – pp. 1-3 (TWEN or use link)
4. [Chesney on Cybersecurity](#) – *Holiday Bear and SolarWinds* – pp. 43-66 (TWEN or use link) (note: there is no need to read the internally referenced articles unless they are of interest to you).
5. Congressional Research Service, [The Designation of Election Systems as Critical Infrastructure](#) (Sept. 2019) – pp. 1-2 (TWEN or use link)
6. White House, [Executive Order 14028: Executive Order on Improving the Nation's Cybersecurity](#) (May 12, 2021) – pp. 1-18 (TWEN or use link)
7. Microsoft Corp., [Microsoft Digital Defense Report 2022 –Report](#): pp. 30-48; 52-53 (TWEN or use link)

Week 3: Hacking, Ransomware, and the Computer Fraud & Abuse Act

1. David Sanger, Clifford Krause, & Nicole Perlroth, [Cyberattack Forces a Shutdown of a Top U.S. Pipeline](#), New York Times (May 8, 2021) – pp. 1-4 (TWEN or use link)
2. David Sanger & Nicole Perlroth, [Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity](#), New York Times (May 14, 2021) – pp. 1-3 (TWEN or use link)
3. Julian Barnes, [U.S. Military Has Acted Against Ransomware Groups, General Acknowledges](#), New York Times (Dec. 5, 2021) – pp. 1-2 (TWEN or use link)
4. [Chesney on Cybersecurity](#) – *Computer Fraud & Abuse Act* – pp. 17-21 (TWEN or use link)
5. *U.S. v. Morris*, 928 F.2d 504, 504-11 (2d Cir. 1991) (Westlaw/LEXIS)
6. *Van Buren v. United States*, 141 S. Ct. 1648, 1651-69 (2021) (Westlaw/LEXIS)

///
///
///
///

Week 4: Economics of Cyber Threats

1. Nicole Perlroth & David Sanger, [Nations Buying As Hackers Sell Flaws In Computer Code](#) (July 13, 2013) – pp. 1-5 (TWEN or use link)
2. The White House, [Heartbleed: Understanding Why We Disclose Cyber Vulnerabilities](#) (Apr. 28, 2014) – pp. 1-2 (TWEN or use link)
3. Ross Anderson, [Why Information Security Is Hard – An Economic Perspective](#) (2001) – pp. 1-7 (TWEN or use link)
4. [Chesney on Cybersecurity](#) – *Private Lawsuits* – pp. 84-94 (TWEN or use link)
5. Gen. Keith Alexander, et al, [Clear Thinking About Protecting the Nation in the Cyber Domain](#), *Cyber Defense Review* (2017) – pp. 1-10 (TWEN or use link)
6. Gen. Keith Alexander & Jamil N. Jaffer, [China Is Waging Economic War on America. The Pandemic Is an Opportunity to Turn the Fight Around](#), *Barron's* (Aug. 4, 2020) – pp. 1-3 (TWEN or use link)

Week 5: Private Hacking Enforcement and Cybersecurity Regulation:

1. [Chesney on Cybersecurity](#) – *Civil Liability Under the CFAA* – pp. 30-42 (TWEN or use link)
2. [Chesney on Cybersecurity](#) – *The Role of Regulators* – pp. 67-70 (TWEN or use link)
3. *FTC v. Wyndham Worldwide*, 799 F.3d 236, 240-258 (3rd Cir. 2015) (Westlaw/LEXIS)
4. *LabMD, Inc. v. Federal Trade Commission*, 894 F.3d 1221, 1223-38 (11th Cir. 2018) (Westlaw/LEXIS)
5. [Chesney on Cybersecurity](#) – *Private Lawsuits* – pp. 95-103 (TWEN or use link)

Week 6: Electronic Surveillance: Background Legal Principles

1. *Katz v. United States*, 389 US 347 (1967) (Westlaw/LEXIS)
2. *Smith v. Maryland*, 442 U.S. 735 (1979) (Westlaw/LEXIS)
3. *United States v. McLaren*, 957 F. Supp. 215 (M.D. Fla. 1997) (Westlaw/LEXIS)
4. *United States v. Warshak*, 631 F.3d 266, 282-290 (6th Cir. 2010) (Westlaw/LEXIS)
5. Paul Rosenzweig, *The Evolution of Wiretapping*, *Engage* – pp. 83-87 (Sept. 2011) (TWEN)

Week 7: Electronic Surveillance & Technological Advances

1. *In re: Google Street View Electronic Communications Litigation*, 794 F.Supp.2d 1067 (N.D. Cal. 2011) (Westlaw/LEXIS)
2. *United States v. Jones*, 565 U.S. 400 (2012)
3. *Riley v. California*, 134 S. Ct. 2473 (2014)
4. *Carpenter v. United States*, 138 S. Ct. 2206 (2018)

NOTE: PRELIMINARY PAPER TOPICS DUE BY START OF WEEK 8 CLASS

///
///
///
///
///
///

Week 8: Metadata and Foreign Intelligence

1. *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (Westlaw/LEXIS)
2. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702*, Executive Summary – pp. 5-15 (July 2014) (TWEN or use link) ******(Note: If printing out, please only print pp. 10-20 of the PDF; file is very long)******
3. *In re: Directives*, 551 F.3d 1004 (FISA Ct. Rev. 2008)(Westlaw/LEXIS)

Week 9: Cybersecurity and the Fourth Amendment

1. DOJ Office of Legal Counsel, *Legal Issues relating to the Testing, Use and Deployment of an Intrusion Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch* (Jan. 9, 2009) – pp. 1-35 (TWEN)
2. DOJ Office of Legal Counsel, *Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch* (August 2009) – pp. 1-6 (TWEN)
3. *In re: Yahoo Mail Litigation*, 7 F.Supp.3d 1016 (N.D. Cal. 2014) (Westlaw/LEXIS)

Week 10: Privacy and Encryption

1. Congressional Research Service, *Data Protection and Privacy Law: An Introduction* (May 2019) – pp. 1-2 (TWEN)
2. Congressional Research Service, *Data Protection Law: An Overview* (Mar. 2019) – pp. 1-7, 25-40 (TWEN)
3. Congressional Research Service, *EU Data Protection Rules and US Implications* (Aug. 2018) – pp. 1-2 (TWEN)
4. Congressional Research Service, *Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress* (Apr. 3, 2020) – pp. 1-5 (TWEN or use link)
5. *In Re: Grand Jury Subpoena*, 670 F.3d 1335 (11th Cir. 2012) (Westlaw/LEXIS)
6. Department of Justice, *Government's Ex Parte Application for an Order Compelling Apple, Inc. to Assist Agents in Search: Memorandum of Points and Authorities* (Feb. 16, 2016) – pp. 3-20 (TWEN)
7. Jamil N. Jaffer & Daniel J. Rosenthal, *Why Apple's Stand Against the F.B.I. Hurts Its Own Customers*, New York Times (Apr. 8, 2016) – pp. 1-3 (TWEN)

NOTE: FINAL PAPER TOPICS DUE BY START OF WEEK 11 CLASS.

Week 11: Protecting the Private Sector: Information Sharing & Collective Defense

1. [Chesney on Cybersecurity](#) – *Facilitating Information Sharing to Better Protect the Private Sector* – pp. 114-116, 121-132 (TWEN or use link)
2. CNBC, The Controversial “Surveillance” Act Obama Just Signed (Dec. 22, 2015) (TWEN)
3. Executive Order 14028, [Improving the Nation's Cybersecurity](#) (May 12, 2021) – pp. 1-3, 5-7, 8-9, 11-12 (TWEN)
4. Keith B. Alexander, et. al., *Clear Thinking About Protecting the Nation in the Cyber Domain*, Cyber Defense Review (Mar. 2017) – pp. 29-36 (TWEN)
5. Chris Inglis, [National Cyber Policy Will Disrupt Crime and Instill Hope](#), Wall Street Journal (Oct. 28, 2021) (TWEN or use link)

Week 12: US State Laws Comprehensive Survey

1. [*IAPP: US State Comprehensive Privacy Laws Report 2023*](#), Legislative Session.
2. [*Comprehensive Consumer Privacy Bills*](#), US State Privacy Legislation Tracker (2024).

Week 13: Federal and Domestic Privacy Developments and the WORLD at Large.

1. [*IAPP-EY Privacy Governance Report*](#), (2023).
2. [*A View from DC: Updating the Map of Location Privacy Safeguards*](#), Cobun Zweifel-Keegan, CIPP/US, CIPM IAPP.
3. [*A View from Brussels: European Strategy for Data Takes Shape*](#), (2024), Isabelle Roccia, CIPP.

NOTE: FINAL PAPERS DUE BY MAY 6, 2024 AT 11:00 P.M. ET.