

LSTD517

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

Course Summary

Course : LSTD517 **Title :** Law, Ethics and Cybersecurity

Length of Course : 8

Prerequisites : N/A **Credit Hours :** 3

Description

Course Description: This course focuses on the ways that law, ethics and cybersecurity overlap and intersect. Besides laws related to cybersecurity, the course examines laws related to intellectual property, civil litigation, criminal prosecutions, and privacy. This examination will provide the means to identify and analyze the policies reflected in those laws. Those policies could guide the creation of policies on a business-level, using qualitative risk assessment and planning. An exploration of ethics and cybersecurity, as well as of workplace ethics, will involve the use of an ethical framework.

Course Scope:

This course explores some of the legal and ethical issues involved in a broad survey of cybersecurity topics. Besides examining basic legal and ethics issues involving cybersecurity, this course will allow students to assess civil law remedies available to individuals who have incurred losses due to cybersecurity violations, including for those whose access to justice may be impaired as a result. Likewise, related criminal law matters will be surveyed and appraised. Such evaluations will prepare students to create legal or policy revision proposals that make sense in the modern cybersecurity context.

Objectives

After completing this course the Student will be able to:

Apply general principles of law and ethics to cybersecurity matters;

Integrate laws and ethical rules within cybersecurity contexts;

Differentiate among the social and political factors influencing the research of cybersecurity-related law and ethics;

Critique a cybersecurity-related legal or ethical position, especially within the context of how the situation may affect the general public;

Propose novel amendments to existing laws and policies to better address future cybersecurity-related

issues; and

Reflect on what he or she has learned.

Outline

Week 1: Introduction to Relevant Basic Legal and Cybersecurity Topics

Learning Outcomes

Apply general principles of law and ethics to cybersecurity matters.

Discover legal and ethical concerns linked with cybersecurity.

Integrate laws and ethical rules within cybersecurity contexts.

Interpret how general principles of law and ethics apply to one or more contemporary cybersecurity issues.

Reflect on what you have learned.

Reflect on what you have learned, especially within the context of why legal professionals should pay attention to cybersecurity matters.

Required Readings

See readings in Lessons in the Reading and Resources tab.

Assignments

(1) Post your introduction in the Forum; and

(2) Respond to the question posted in the Forum.

(Initial Post due Thursday and 2 replies due Sunday of this week)

Week 2: How to Investigate Cybersecurity Legal and Ethics Issues

Learning Outcomes

Apply general principles of law and ethics to cybersecurity matters.

Differentiate among the social and political factors influencing the research of cybersecurity-related law and ethics.

Evaluate the legal and ethical concerns associated with cybersecurity-related research.

Required Readings

See readings in Lessons in the Reading and Resources tab.

Assignments

Respond to the question posted in the Week 2 Forum.

(Initial Post due Thursday and 2 replies due Sunday of this week)

Complete the Submit Week 2 Resource Deconstruction Assignment. See details under the Assignment tab

for Week 2 in the classroom.

Week 3: Cybersecurity and Civil (Tort) Law

Learning Outcomes

A. Integrate laws and ethical rules within cybersecurity contexts.

Predict how tort law may evolve in the foreseeable future based on present day legal and ethical concerns associated with cybersecurity.

B. Integrate laws and ethical rules within cybersecurity contexts.

Correlate what you learn about research to legal and/or ethical challenges that your thesis concept could face.

Required Readings

See readings in Lessons in the Reading and Resources tab.

Assignments

Respond to the question posted in the Week 3 Forum.

(Initial Post due Thursday and 2 replies due Sunday of this week)

Complete the Submit Week 3 Privacy Analysis Assignment. See details under the Assignment tab for Week 3 in the classroom.

Week 4: Cybersecurity and Criminal Law

Learning Outcomes

Propose novel amendments to existing laws and policies to better address future cybersecurity-related issues.

Reconstruct an existing cybersecurity-related law or policy to better protect the general public from cybercrime.

Required Readings

See readings in Lessons in the Reading and Resources tab.

Assignments

Respond to the question posted in the Week 4 Forum.

(Initial Post due Thursday and 2 replies due Sunday of this week)

Week 5: Securing the Internet of Things (IoT)

Learning Outcomes

Integrate laws and ethical rules within cybersecurity contexts.

Create legal and ethical bases for integration into a cybersecurity framework.

Required Readings

See readings in Lessons in the Reading and Resources tab.

Assignments

Respond to the question posted in the Week 5 Forum.

(Initial Post due Thursday and 2 replies due Sunday of this week)

Week 6: Cryptocurrencies

Learning Outcomes

Apply general principles of law and ethics to cybersecurity matters.

Discuss whether cryptocurrencies should be accepted.

Integrate laws and ethical rules within cybersecurity contexts.

Design procedures for how cryptocurrencies could be accepted.

Required Readings

See readings in Lessons in the Reading and Resources tab.

Assignments

Respond to the question posted in the Week 6 Forum.

(Initial Post due Thursday and 2 replies due Sunday of this week)

Week 7: Net Neutrality

Learning Outcomes

Critique a cybersecurity-related legal or ethical position, especially within the context of how the situation may affect the general public.

Evaluate the efficiencies (or lack thereof) of the current regulatory and policy net neutrality system that affects Americans' internet usage.

Propose novel amendments to existing laws and policies to better address future cybersecurity-related issues.

Create a draft law that offers new ideas to better address the legal and/or ethical issues that adversely affect the general public.

Required Readings

See readings in Lessons in the Reading and Resources tab.

Assignments

Respond to the question posted in the Week 7 Forum.

(Initial Post due Thursday and 2 replies due Sunday of this week)

Submit Legislative Proposal Assignment. See details under the Assignment tab for Week 7 in the classroom

Week 8: Cyber-related Legislation and Policies

Learning Outcomes

Critique a cybersecurity-related legal or ethical position, especially within the context of how the situation may affect the general public.

Evaluate current cyber-related laws' ability to fit the present cybersecurity environment.

Required Readings

See readings in Lessons in the Reading and Resources tab.

Assignments

Evaluation

Contact between students and instructor can occur by in-class Messages or telephone. However, the best way to reach your instructor is via Messages. Do not use the mycampus email for any correspondence with me about the class. I will copy your personal emails into the course when I answer your questions to make sure you receive my Messages. I expect you to check your classroom messages frequently, and I also expect you to respond back to my messages using the in-class Message tool. If you have questions about this, please ask.

The number of these contacts may vary according to the specific course and individual student need. **FOR ALL MESSAGES, PLEASE PUT YOUR MESSAGE'S SUBJECT IN THE SUBJECT HEADING.** If you have not received a response from me within 48 hours, please follow up, as the message may not have been received.

If you want to contact me telephonically, you may do so by scheduling a time for such. Simply send me an in-class Message, tell me that you would like to talk with me, and offer me two or three dates/times so that we can make it work for both of us as conveniently as possible.

FORUM DISCUSSIONS:

This course includes nine (9) Forum discussions.

- The first one is the mandatory Introduction Forum. It is very important that you participate in the Introduction Forum. Participation in this forum serves as your official entry into the course, which is why we special attention has been drawn to this assignment.
- All of the other eight (8) Forum discussions relate to one of each week's substantive topics.

Students are expected to complete these Forum discussions by Sunday at midnight EST of the week in which they are due. You can find them (along with their respective instructions) in this classroom's "Forum" section, at left.

The Graduate Forum Rubric will be used for grading your participation in each of the Forums. You can find this rubric in the classroom's Forums and Resources sections, at left.

To qualify for the maximum possible points, students need to make an initial post (at least 500 words in length and on topic) and respond to at least two of your classmates' postings in each of these forums (each response must be at least 250 words in length and on topic). Students are encouraged to make longer and more frequent posts to each Forum discussion. Please submit your initial post to the Forum by Thursday at midnight so your classmates can respond to your posting by Sunday. Post your responses to your classmates by the end of the week, Sunday at midnight.

ASSIGNMENTS:

All written submissions are required to be **DOUBLE SPACED, in Microsoft Word, with one-inch margins and Times New Roman, 12 point font.**

This course includes three (3) written assignments:

1. **RESOURCE DECONSTRUCTION:** This assignment requires that you select one of the mandatory reading resources assigned for either Week 1 or Week 2 and deconstruct it into its primary elements, namely:

- The Research Question;
- The Thesis;
- The Claims or argument;
- The Evidence or supporting facts; and,
- The Conclusion(s).

1. **PRIVACY LAW ANALYSIS:** For this assignment, students are required to submit a paper that is no more than 4 pages long. Students will:

- find a law review article in the library concerning ethics, privacy law, and cybersecurity;
- use the IRAC method (Issue, Rule, Analysis and Conclusion) to analyze your selected law review article, especially with regard to how the public may be adversely affected by your topic.

1. **LEGISLATIVE PROPOSAL CREATION:** From within the range of general cybersecurity topics discussed in this course, choose one narrow legal and/or ethical topic that adversely affects the general public in some way(s). Create a draft statute or regulation or policy that offers new ideas to better address the legal and/or ethical issues that currently hamper your selected topic by adversely affecting the general public. Within 10 - 12 pages, address all of the following:

- Identification of the current statute or regulation or policy that underlies your selected topic;
- Analysis of the legal and/or ethical challenges to your selected topic;
- Presentation of your new proposed statute or regulation or policy that better addresses the legal and/or ethical challenges to your selected topic, along with an analysis that justifies your proposal (share both pros and cons for your proposal); and
- Summary of all of the above for your conclusion.

Grading:

Name	Grade %
Forums	39.00 %
Forum 1	4.33 %
Forum 2	4.33 %
Forum 3	4.33 %
Forum 5	4.33 %
Forum 6	4.33 %
Introduction	4.33 %
Forum 4	4.33 %
Forum 7	4.33 %
Forum 8	4.33 %
Legislative Proposal Week 7	30.00 %

Week 7 Legislative Proposal Creation	30.00 %
Introduction	1.00 %
Introduction	1.00 %
Article Deconstruction	10.00 %
Week 2: Article Deconstruction	10.00 %
Analysis	20.00 %
Week 3 Privacy Law Analysis	20.00 %

Materials

Book Title: Various resources from the APUS Library & the Open Web are used. Links provided inside the classroom in the Lessons section.

Author:

Publication Info:

ISBN: N/A

Your readings are listed below. However, all readings are available to you in the lessons tab of this classroom under Readings and Resources. Please access all required readings there.

Week 1: Why Professionals Should Care About Cybersecurity

Ryan K. Baggett, Chad S. Foster, & Brian K. Simpkins, *Chapter One: Introduction: Technology Securing the Homeland* in *Homeland Security Technologies for the 21st Century*, 1 – 13 (2017), psi.praeger.com.

Ryan K. Baggett, Chad S. Foster, & Brian K. Simpkins, *Chapter Two: Ethical and Privacy Implications of Technology* in *Homeland Security Technologies for the 21st Century*, 1 – 19 (2017), psi.praeger.com.

Keren Elazari, *Hackers: The Internet's Immune System*, YouTube, (March 2014), https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system.

Committee on Developing a Cybersecurity Primer: Leveraging Two Decades of National Academies Work, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, & National Research Council, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, 1 – 134 (2014), <https://ebookcentral-proquest-com.ezproxy1.apus.edu/lib/apus/reader.action?docID=3379336>.

Cynthia D. Waddell, *Understanding the Digital Economy: Data, Tools and Research*, *The Growing Digital Divide in Access for People With Disabilities: Overcoming Barriers to Participation in the Digital Economy*, 1 – 29 (ICDRI, 1999), http://www.icdri.org/CynthiaW/the_digital_divide.htm.

Jan L. Jacobowitz & Justin Ortiz, *Happy Birthday Siri! Dialing in Legal Ethics for Artificial Intelligence, Smart Phones, and Real Time Lawyers* (January 8, 2018). *Texas A&M University Journal of Property Law*; *University of Miami Legal Studies Research Paper No. 18-2* (2018). *Available at* <https://ssrn.com/abstract=3097985>

Gregory Bufithis, *Hon. John M. Facciola at the Georgetown Cybersecurity Law Institute*, YouTube, <https://youtu.be/3STFwbuKOso> (July 3, 2013).

MrKilswitch88, *Electronic Voting Fraud (sic)*, YouTube, <https://youtu.be/Ts5PftZ1kkg>, (October 14, 2012).

Week 2: How to Investigate Cybersecurity Legal and Ethics Issues

Aaron J. Burstein, *Conducting Cybersecurity Research Legally and Ethically*, (University of California, Berkeley School of Law, 2008),
https://www.usenix.org/legacy/event/leet08/tech/full_papers/burstein/burstein_html/.

Ronald Deibert & Masashi Crete-Nishihata, *Blurred Boundaries: Probing the Ethics of Cyberspace Research*, *Review of Policy Research*, 531 – 537 (2011),
<http://web.a.ebscohost.com.ezproxy1.apus.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=62e1ec00-88b5-4d5c-96a8-665594d0c516%40sessionmgr4008>.

Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 *Wake Forest L. Rev.* 393 (2014).

Harold Abelson, Peter A. Diamond, Andrew Grosso, & Douglas W. Pfeiffer (support), *Report to the President: MIT and the Prosecution of Aaron Swartz*, 1 – 182 (2013), <http://swartz-report.mit.edu/docs/report-to-the-president.pdf>.

Australian National University, *Cybersecurity: Mapping the Ethical Terrain* YouTube
<https://youtu.be/do1G7MwKH1s> (2014).

Week 3: Cybersecurity and Civil Law

Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 *Yale L. J. F.* 614 (2018). https://www.yalelawjournal.org/pdf/Solow-Niederman_qthw8784.pdf

Josip Car, Woan Shin Tan, Zhilian Huang, Peter Sloot, & Bryony Dean Franklin, *eHealth in the Future of Medications Management: Personalisation, Monitoring and Adherence*, 15 *BMC Medicine* 73 (2017).

Tobias Holstein, Gordana Dodig-Crnkovic, & Patrizio Pelliccione, *Ethical and Social Aspects of Self-Driving Cars, Computers and Society* (2018). <https://arxiv.org/pdf/1802.04103.pdf>

Dan Zureich & William Graebe, *Cybersecurity: The Continuing Evolution of Insurance and Ethics*, 82 (2) *Defense Counsel Journal* 192 (2015)

Janice C. Sipior, Burke T. Ward & Linda Volonino, *Privacy Concerns Associated With Smartphone Use*, 13 *Journal of Internet Commerce* 177 (2014).

Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 *Nat'l Sec L & Pol'y* 119 (2010).

CXOTalk, *AI & Privacy Engineering With Michelle Denedy (Cisco) and David Bray (FCC)*, YouTube, https://www.youtube.com/watch?v=ThaLKe_W4ml (April 30, 2017).

Week 4: Cybersecurity and Criminal Law

Joshua B. Hill & Nancy E. Marion, *Chapter Two: History Of Cybercrime*, in *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century* (2016). <https://psi-praeeger-com.ezproxy2.apus.edu/Topics/Display/2058279?cid=138&sid=2057721>

Tim K. MacKey & Bryan A. Liang, *Pharmaceutical Digital Marketing and Governance: Illicit Actors and Challenges to Global Patient Safety and Public Health*, 9 *Globalization and Health* 45 (2013),
<https://doi.org/10.1186/1744-8603-9-45>

Ira Rubinstein, *Privacy Localism* (February 15, 2018). NYU School of Law, Public Law Research Paper.
<https://ssrn.com/abstract=3124697>

Graeme Horsman, *A Call for the Prohibition of Encryption: Panacea or Problem?*, *EEEE Security and Privacy Magazine* (2018). <http://hdl.handle.net/10149/621677>

Shaen Corbet & Constantin Gurdgiev. *Regulatory Cybercrime: A Hacking-Based Mechanism to Regulate*

and Supervise Corporate Cyber Governance? (January 23, 2017). <https://ssrn.com/abstract=2904749> or <http://dx.doi.org/10.2139/ssrn.2904749>

Devanch Parikh, Harshvardhan Shani & Piyush Patel, *Organized CyberCrime and the State of User Privacy* (2017). <http://www.ijirst.org/articles/SALLTNCSP035.pdf>

Center for Strategic and International Studies, *The Economic Impact of Cybercrime*, YouTube, <https://www.youtube.com/watch?v=VtvYsaXiLQs> (February 21, 2018)

Week 5: Securing the Internet of Things (IoT)

Tan Ming Hui & Walid Lemrini, *The Fourth Industrial Revolution: An Orwellian Nightmare?*, RSIS Commentaries, No. 029. Singapore: Nanyang Technological University (2018). <http://hdl.handle.net/10220/44450> (4 pages)

Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16:1 Duke Law & Technology Review 161 (2018).

Miles Brundage *et al.*, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (2018). <https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf>

Emily Gorcenski, *The Ethics of the Internet of Things*, YouTube, https://www.youtube.com/watch?v=xLL7Fo_em2E (May 14, 2017)

Week 6: Cryptocurrencies

Joanna Diane Caytas. *Blockchain in the U.S. Regulatory Setting: Evidentiary Use in Vermont, Delaware, and Elsewhere*. The Columbia Science and Technology Law Review. Posted May 30, 2017. <http://stlr.org/2017/05/30/blockchain-in-the-u-s-regulatory-setting-evidentiary-use-in-vermont-delaware-and-elsewhere/>

Elizabeth S. Ross, *Nobody Puts Blockchain in a Corner: The Disruptive Role of Blockchain Technology in the Financial Services Industry and Current Regulatory Issues*, 25 (2) Cath. U. J. L. & Tech 353 (2017). <http://scholarship.law.edu/jlt/vol25/iss2/7>

Mehdi Benchoufi & Philippe Ravaud, *Blockchain Technology for Improving Clinical Research Quality*, 18 Trials 335 (2017).

Matthew Weeks, *Hacks, Exploits, and Ethical Issues in Cryptocurrency*, YouTube, <https://www.youtube.com/watch?v=k-dmZuMZmm8> (December 11, 2017).

Week 7: Net Neutrality

Alex Chung & Chi Xing, *The Ethics of Net Neutrality*, <http://web.cs.ucdavis.edu/~rogaway/classes/188/fall11/p211.pdf> (2017)

Luca Belli & Primavera De Filippi, *The Value of Network Neutrality for the Internet of Tomorrow: Report of the Dynamic Coalition on Network Neutrality* (2013). <https://ssrn.com/abstract=2468534> or <http://dx.doi.org/10.2139/ssrn.2468534>

David R. Morrow, *When Technologies Make Good People Do Bad Things: Another Argument Against the Value-Neutrality of Technologies*, 20 Sci Eng Ethics 329 (2014).

Tristan Harris, *How a Handful of Tech Companies Control Billions of Minds Every Day*, YouTube, https://www.ted.com/talks/tristan_harris_the_manipulative_tricks_tech_companies_use_to_capture_your_attention_language=en#t-245226 (July 26, 2017).

Week 8: Cyber-related Legislation and Policies

White House, United States of America, *National Strategy to Secure Cyberspace*, <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=199137> (2003)

Ryan Hagemann, Jennifer Skees, & Adam D. Thierer. *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future* (February 5, 2018). Forthcoming - Colorado Technology Law Journal <https://ssrn.com/abstract=3118539>

W. Perry Hicks & Alan J. Ponce, *SB 219 – Autonomous Vehicles*, 34:1 Georgia State University Law Review 231 (2018). <https://readingroom.law.gsu.edu/cgi/viewcontent.cgi?article=2911&=&context=gsulr&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fstart%253D10%2526c>

Scott Shackelford & Austin Brady, *Is it Time for a National Cybersecurity Safety Board?* (January 12, 2018). Albany Law Journal of Science and Technology, 2018. <https://ssrn.com/abstract=3100962> (18 pages)

Justin Daniels, *You Hold The Key to Overcoming Cyber-Threats*, YouTube, <https://www.youtube.com/watch?v=HvcJntjqVaM> (November 14, 2017)

Other Resources

In addition to the required course materials listed above, the following resources (including but not limited to public domain web sites) are useful. Please abide by the university's academic honesty policy when using Internet sources as well. Note web site addresses are subject to change.

Cybersecurity Program Guide: <https://www.apus.edu/apus-library/online-research/research/research-guides/guides-by-program.html>

Cyber Security: Action Against Cybercrime: <http://www.slideshare.net/bijayguyz/cyber-security-prt>

Site Name Web Site URL/Address

Findlaw <http://www.findlaw.com>

Cornell
Legal
Information
Institute <http://www.law.cornell.edu>

Basic
Outlining
(from the
Purdue
Online
Writing Lab
(OWL) <https://owl.english.purdue.edu/owl/resource/544/02/>

Library of
Congress <https://www.congress.gov/> or
<https://www.loc.gov/>

United
Nations <http://www.un.org/en/>

American
Bar
Association
(ABA) <http://www.americanbar.org/aba.html>

Purdue
Online
Writing Lab
(OWL) <http://owl.english.purdue.edu/owl/>

Course Guidelines

Writing Expectations

All written submissions should be submitted in a font and page set-up that is readable and neat. They should use correct grammar and checked for spelling and other errors prior to submission. Specific details are provided in the assignment section as assignment formats vary. Uploaded documents in the assignment section should be in word (.doc, .docx) format. Faculty may require assignments be submitted to Turnitin.com. Turnitin.com will automatically analyze a paper and report instances of potential plagiarism or overuse of quotes for the student to edit before submitting it for a grade. The expectation is that the writing will be in your words after analysis of the sources.

Citation and Reference Style

The central function of legal citation is to allow the reader to efficiently locate the cited source. All courses in the Legal Studies program require that any narrative essay or composition format follow the legal citation guidelines set forth in The Bluebook: A Uniform System of Citation. Do not purchase The Bluebook, as it is available at the APUS library. Use this link to access: <http://ezproxy.apus.edu/login?url=https://www.legalbluebook.com>

Late Assignments

Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. As adults, students, and working professionals, I understand you must manage competing demands on your time. Should you need additional time to complete an assignment, please contact me before the due date so we can discuss the situation and determine an acceptable resolution.

Deductions

Late forum posts, assignments, and exams may be penalized five (5) points per day.

Netiquette

Online universities promote the advancement of knowledge through positive and constructive debate – both inside and outside the classroom. Forums on the Internet, however, can occasionally degenerate into needless insults and “flaming.” Such activity and the loss of good manners are not acceptable in a university setting – basic academic rules of good behavior and proper “Netiquette” must persist. Remember that you are in a place for the rewards and excitement of learning which does not include descent to personal attacks or student attempts to stifle the Forum of others.

Technology Limitations: While you should feel free to explore the full-range of creative composition in your formal papers, keep e-mail layouts simple. The Sakai classroom may not fully support MIME or HTML encoded messages, which means that bold face, italics, underlining, and a variety of color-coding or other

visual effects will not translate in your e-mail messages.

Humor Note: Despite the best of intentions, jokes and especially satire can easily get lost or taken seriously. If you feel the need for humor, you may wish to add “emoticons” to help alert your readers: ;-), :)

Disclaimer Statement

Course content may vary from the outline to meet the needs of this particular group.

Online Library

The Online Library is available to enrolled students and faculty from inside the electronic campus. This is your starting point for access to online books, subscription periodicals, and Web resources that are designed to support your classes and generally not available through search engines on the open Web. In addition, the Online Library provides access to special learning resources, which the University has contracted to assist with your studies. Questions can be directed to librarian@apus.edu.

Charles Town Library and Inter Library Loan: The University maintains a special library with a limited number of supporting volumes, collection of our professors' publication, and services to search and borrow research books and articles from other libraries.

Electronic Books: You can use the online library to uncover and download over 50,000 titles, which have been scanned and made available in electronic format.

Electronic Journals: The University provides access to over 12,000 journals, which are available in electronic form and only through limited subscription services.

Tutor.com: AMU and APU Civilian & Coast Guard students are eligible for 10 free hours of tutoring provided by APUS. [Tutor.com](https://www.tutor.com) connects you with a professional tutor online 24/7 to provide help with assignments, studying, test prep, resume writing, and more. Tutor.com is tutoring the way it was meant to be. You get expert tutoring whenever you need help, and you work one-to-one with your tutor in your online classroom on your specific problem until it is done.

Legal Studies Program Guide: This should be your starting point as you explore the resources available for the Legal Studies Program! <https://www.apus.edu/apus-library/online-research/research/research-guides/school-of-security-global-studies/legal-studies-paralegal-studies>

University Policies

[Student Handbook](#)

- [Drop/Withdrawal policy](#)
- [Extension Requests](#)
- [Academic Probation](#)
- [Appeals](#)
- [Disability Accommodations](#)

The mission of American Public University System is to provide high quality higher education with emphasis on educating the nation's military and public service communities by offering respected, relevant, accessible, affordable, and student-focused online programs that prepare students for service and leadership in a diverse, global society.

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.