ISSC476

Course Summary

Course : ISSC476 **Title :** Surveillance Legislation and Policy
Length of Course : 8 **Faculty :**
Prerequisites : N/A **Credit Hours :** 3

Description

Course Description:

This course examines legislative and policy areas related to surveillance and privacy. The ability for organizations and governments to remotely monitor and track individuals has given rise to legal and ethical concerns which are addressed. This course will examine how laws have had to change to account for the new possibilities of privacy violations.

Course Scope:

Course Description:
This course examines legislative and policy areas related to surveillance and privacy. The ability for organizations and governments to remotely monitor and track individuals has given rise to legal and ethical concerns which are addressed. This course will examine how laws have had to change to account for the new possibilities of privacy violations.

Course Scope:

This course is one in a series of courses that examine surveillance in the information technology, cybersecurity, government, legal, and common-civilian sectors. Furthermore, the measure towards this criterion includes how surveillance has been used previously and how it is being utilized currently, how the information of said surveillance is monitored and used, and how the policies are generated along with how the policies remain legal if the policies are altered. The scope of the course criterion will be done so via the observation of the Department of Defense Certification and Accreditation (DICAPP), Risk Management Framework (RMF), National Institute of Standards and Technology (NIST), and the Cyber Security & Information Systems Information Analysis Center (CSIAC).

Objectives

CO1: Evaluate the previous and current methods of surveillance.

CO2: Profile the previous and current policies associated with surveillance.

CO3: Analyze the legal policies of surveillance utilization amongst organizations and government agencies.

CO4: Analyze how laws of surveillance are processed.

CO5: Analyze how and why the law of surveillance is altered.

CO6: Evaluate the process of how surveillance is subpoenaed.

CO7: Evaluate the process of privacy violations.

CO8: Analyze how privacy violations are implemented.

Outline

Week 1: Introduction to Surveillance Methods and Legislation

Learning Outcomes

1. In the Handbook of Surveillance Technologies reading, you will observe the multiple devices and forms of surveillance. Furthermore, the evolution of the digital forms of surveillance becoming law will be observed.
2. An observation of the previous policies of surveillance will be observed in the lecture.
3. Via the readings and the lecture, the legal policies and implementations will be observed.

Required Readings

- Privacy at Risk: The New Government Surveillance and the Fourth Amendment – Chapters 1 and 2
- Handbook of Surveillance Technologies – Chapter 1

Assignments

- Week One Forum - Introductions and Surveillance Techniques
- Lab - CompTIA (Network +) Assisted Lab 16: Configure Syslog – Lab

Recommended Optional Reading
Recommended Media

Week 2: Surveillance and Human Rights

Learning Outcomes

1. While reading The Electronic Surveillance Manual for Procedures and Case Law along with Chapter 26 of The Routledge Handbook on Exterritorial Human Rights Obligations, you will observe and generate possible scenarios and processes of surveillance, and its data, being subpoenaed.
2. An observation of the Foreign Intelligence Surveillance Act Title 50 will provide how policy violations can occur in foreign sectors
3. Via the reading and lab, you will observe how privacy violations are implemented, which can be intentional or unintentional

Required Readings

- The Routledge Handbook on Extraterritorial Human Rights Obligations - Chapter 26
- The DoD Policy Chart - Foreign Intelligence Surveillance Act Title 50
- The Electronic Surveillance Manual for Procedures and Case Law – Affidavit for Electronic Communications (pages 90 – 99)

Assignments

- Week Two Forum – How do we assure we are adhering to human rights when implementing our surveillance tactics?

- Lab – CompTIA Security+ Assisted Lab 30: Acquiring Digital Forensics Evidence

Recommended Optional Reading

- Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework – Chapter 3
- Understanding Privacy Violations in Big Data Systems

Recommended Media

Week 3: Surveillance via IoT

Learning Outcomes

1. In the Security Risk Management for the Internet of Things reading for the week, learners will observe current surveillance methods of Internet of Things devices.
2. Throughout the Security Risk Management for the Internet of Things reading for the week, obtain information regarding how and why government agencies can implement more surveillance methods than organizations in the private sector.
3. Observe how EULAs allow forms of data surveillance could be collected amongst Internet of Things devices

Required Readings

- Security Risk Management for the Internet of Things - Chapter 2
- Beyond the EULA: Improving consent for data mining

Assignments

- Week Two Forum - What surveillance techniques are being utilized via IoT and what are companies legally allowed to do with the data they mine from your IoT device(s)?
- Midterm Exam

Recommended Optional Reading
Recommended Media

Week 4: Determining the Audio Surveillance needs of an Organization

---

Learning Outcomes

1. In the Handbook of Surveillance Technologies reading, you will observe the multiple devices and forms of audio surveillance. Furthermore, the evolution of audio surveillance from analog to digital as well as from wired means to wireless means will be observed.
2. An observation of the past policies of audio surveillance will be observed in the lecture notes and reading.
3. Via the readings and the lecture, the legal policies of how and when audio surveillance is appropriate will be observed.

Required Readings

- Handbook of Surveillance Technologies – Chapter 2

Assignments

- Week Four Forum - With the vast number of common categories of audio surveillance, which methods do you perceive to be the most beneficial to your organization of choice and why do you perceive your audio surveillance method to be the most beneficial?

Recommended Optional Reading
Recommended Media

Week 5: Cryptography and Decoding Methods

Learning Outcomes

1. In the Handbook of Surveillance Technologies reading, you will observe forms of cryptographic surveillance. Furthermore, you will observe how to generate and decipher forms of cryptography once the surveillance evidence has been obtained.
2. An observation of unsolved cryptographic surveillance will be observed in the lecture notes and reading, and how these unsolved cryptographic means have altered our surveillance tactics.
3. Via the readings and the lecture notes, you will determine how and when cryptography methods of surveillance are appropriate in a legal setting, such as when it is relevant to a felony-charged crime.

Required Readings

- Handbook of Surveillance Technologies – Chapter 17
- The Zodiac Killer Ciphers

Assignments

- Week Five Forum – Discuss the well-known cryptography tactics that have not been resolved, such as the Zodiac Killer
- Lab – Download the cryptographic text file and discover the cryptographic format that is being used to hide the “message inside of the message.” After the cryptographic format is discovered, decipher the hidden message

Recommended Optional Reading

- Handbook of Surveillance Technologies – Chapter 12

Recommended Media

Week 6: Behavior Differences of Employees regarding Organizational Surveillance

---

Learning Outcomes

1. An observation as to how organizations have and have not utilized surveillance methods regarding employee compliance.
2. Determine the logicalities of how organizational surveillance methods can be utilized for reprimanding employee non-compliance.
3. Review and analyze if and how employee reprimanding is justified via organizational surveillance methods.

Required Readings

- A Self-Fulfilling Cycle of Coercive Surveillance: Workers’ Invisibility Practices and Managerial Justification

Assignments

- Week Six Forum – Discuss the impacts of organizational surveillance and employee compliance and stress

Recommended Optional Reading
Recommended Media

Week 7: Computer Surveillance

Learning Outcomes

1. Observe the information that can be obtained through various forms of computer surveillance.
2. Review the privacy rights associated with computer users and computer surveillance.
3. Discover how privacy violations can be implemented via computer surveillance.

Required Readings

- Handbook of Surveillance Technologies – Chapter 18

Assignments

- Lab – CompTIA Security+ Assisted Lab 12: Configuring a System for Auditing Policies

Recommended Optional Reading
Recommended Media

Week 8: Biometrics

Learning Outcomes

1. Observe the various forms and implementations of biometric surveillance.
2. Discover the methods and polices of biometric surveillance.
3. Analyze the validity of biometric surveillance in organizations in government sectors.

Required Readings

- Handbook of Surveillance Technologies – Chapter 13

Assignments

- Week Eight Forum – Describe the benefits and disadvantages of using biometrics for a form of security surveillance
- Final Exam

Recommended Optional Reading
Recommended Media

Evaluation

Discussions	25%
Assignments and Labs	50%
Exams	25%

Grading:

Name	Grade %
Discussions	25.00%
W1 Discussion: Introductions and Surveillance Techniques	3.57%
W2 Discussion: Surveillance and Human Rights	3.57%
W3 Discussion: Surveillance via IoT	3.57%

W4 Discussion: Determining the Surveillance Needs of an Organization	3.57%
W5 Discussion: Cryptography and Decoding Methods	3.57%
W6 Discussion: Behavior Differences of Employees Regarding Organizational	3.57%
W8 Discussion: Biometrics	3.57%
Assignments	50.00%
W1: CompTIA Network Lab: Configure Syslog	12.50%
W2: CompTIA Security Lab: Acquiring Digital Forensics Evidence	12.50%
W5: Hackthissite.org Cryptography Lab	12.50%
W7: CompTIA Security Lab - Configuring a System for Auditing Policies	12.50%
Exams	25.00%
Midterm Exam (Written Response)	12.50%
Final Exam (Written Response)	12.50%

Materials

Book Title: Handbook of Surveillance Technologies - eBook available in the APUS Online Library

Author: Taylor & Petersen

Publication Info: Routledge Lib

ISBN: 9781439873151

Book Title: Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework

Author: Brumfield, C & Haugli, B.

Publication Info: Wiley

ISBN: 978119816287

Book Title: Privacy at Risk: The New Government Surveillance and the Fourth Amendment

Author: Slobogin, C

Publication Info: The University of Chicago Press

ISBN: 9780226762838

Book Title: Handbook of Surveillance Technologies

Author: Petersen, J. K.

Publication Info: CRC Press

ISBN: 9781439873151

Book Title: The Routledge Handbook on Extraterritorial Human Rights Obligations

Authors: Gibney, M., Turkelli, G. E., Krajewski, M. & Vandenhole, W.

Publication Info: Routledge

ISBN: 9781003090014

Book Title: Security Risk Management for the Internet of Things

Authors: Soldatos, J

Publication Info: NOW

ISBN: 9781680836837

Course Guidelines

Phasellus eros sopien, lacinia eget veut vitae, viverro finibus neque Donec vulputate (empor erat id laoreet Nunc commodo ornare justo, sit omet ultrices magna pharetro quis Ut oc nunc in metus fermentum pellentesque eel quia leo. Fusce sodales diam eel tempor posuere ougue nsus ullamcorper quom, id vehiculo libero ante oc ipsum, Donec vitae purus magna Curobitur semper dui quis risus pretium finibus Phosellus non magna consectetur, foucibus magno et, ullamcorper eros. Ut oc nunc in metus fermentum pellentesque eel quia leo. Fusce sodoles, diom eel tempor posuere, ougue risus ullomcorper quom, id vehiculo libero ante oc ipsum. Donec vitae purus magna. Curobitur semper dui quia risus pretium finibus. Phasellus non magna consectetur, faucibus magno et, ullomcocper eros. lacinia eget velit vitae, vrvecro finibus neque Donec vulputote tempor erot id looreet Nunc commodo ornare ‘usto, sit omet ultrices magno phoretro quis. Ut oc nunc in metus fermentum pellentesque eel quis leo. Fusce sodoles, diom eel tempor posuere, ougue risus ullomcocper quom, id vehiculo libero ante oc ipsum, Donec vitae purus magno. Curobitur semper dui quia risus pretium finibus. Phasellus non magno consectetur, foucibus magno et, ullamcorper ecos. Phosellus eros sopien, lacinia eget veut vitae, viverra finibus neque Donec vulputote tempor erot id looreet Nunc commodo ornare justo, sit omet ultrices magno phoretro quis Ut oc nunc in metus fermentum pellentesque eel quia leo. Fusce sodoles, diom eel tempor posuer ougue nsus ullomcorpec quom, id vehicula libero ante oc ipsum. Donec vitae purus magno Curabitur semper dui quis risus pretium finibus Phosellus non magno consectetur, foucibus magno et, ullomcorpec eros.

Communications

Student Communication

To reach the instructor, please communicate through the MyClassroom email function accessible from the Classlist of the Course Tools menu, where the instructor and students email addresses are listed, or via the Office 365 tool on the Course homepage.

- In emails to instructors, it’s important to note the specific course in which you are enrolled. The name of the course is at the top center of all pages.
- Students and instructors communicate in Discussion posts and other learning activities.
- All interactions should follow APUS guidelines, as noted in the Student Handbook, and maintain a professional, courteous tone.
- Students should review writing for spelling and grammar.
- Tips on Using the Office 365 Email Tool

Instructor Communication

The instructor will post announcements on communications preferences involving email and Instant Messaging and any changes in the class schedule or activities.

- Instructors will periodically post information on the expectations of students and will provide feedback on assignments, Discussion posts, quizzes, and exams.
- Instructors will generally acknowledge student communications within 24 hours and respond within 48 hours, except in unusual circumstances (e.g., illness).
- The APUS standard for grading of all assessments (assignments, Discussions, quizzes, exams) is five days or fewer from the due date.
- Final course grades are submitted by faculty no later than seven days after the end date of the course or the end of the extension period.

University Policies

Consult the Student Handbook for processes and policies at APUS. Notable policies:

- Drop/Withdrawal Policy
- Extension Requests
- Academic Probation
- Appeals
- Academic Dishonesty / Plagiarism
- Disability Accommodations
- Student Deadlines
- Video Conference Policy

Mission

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.

Minimum Technology Requirements

- Please consult the catalog for the minimum hardware and software required for undergraduate and graduate courses.
- Although students are encouraged to use the Pulse mobile app with any course, please note that not all course work can be completed via a mobile device.

Disclaimers

- Please note that course content – and, thus, the syllabus – may change between when a student registers for a course and when the course starts.

- Course content may vary from the syllabus' schedule to meet the needs of a particular group.