University of Pittsburgh

School of Information Sciences

College in High School

2019-2020

Cybersecurity and the Law

INFSCI 0014

3 Credits

Description: Computers, the Internet, and mobile information technologies have become routine elements of our daily lives. The percentage of our social, professional, and political discourse mediated by information systems increases each year. Critical infrastructure likewise follows suit, with financial, healthcare, energy and other utilities leveraging the Internet to increase both capability and efficiency. In the physical world, we publish rules (laws) to govern our interactions with one another. These rules tell us what behaviors are permissible and what responsibilities we have to one another. In cyberspace, where these rules exist – and what they require – are less clear. This course explores questions surrounding how we "govern" cyberspace in the context of cybersecurity and privacy issues. We will examine a series of examples, both real-world and hypothetical, to investigate what policy "tools" are in-place, available, and *should be available* to address Internet security and privacy issues.

Prerequisite: None. Neither a technical nor a legal background is required or expected.

Grading: There is no final examination in this course. The Term Paper or Project is in lieu of a final examination. Students will be graded on a combination of participation (in-class and through the course website/blog), short response papers, and a term paper or project.

Textbook: Required readings will be provided by the instructor. Students are expected to have completed all required readings in advanced for the class for which they are posted.

The following topics are covered in the University of Pittsburgh INFSCI 0014 course:

1. **Social Networks**
   - Privacy
   - Security
   - Policing
2. **Virtual Communities**
3. **Online behavioral advertising/data aggregation**
   - Google
   - Network Advertising Initiative
   - Interactive Advertising Bureau
4. **Mobile devices/location services/context-aware computing**
5. **Financial network security/identity theft**
6. **Privacy and security of health information**
   - HIPAA
7. **Critical infrastructure issues**
   - Energy grids
   - Nuclear power controls
8. **Cyber investigations**
   - Criminal and civil
   - E-Discovery issues
9. **Trans-national issues**
10. **Electronic privacy and security in the employment context**
11. **Responsibilities of "network" operators**
    - Google
    - Microsoft
    - Verizon
    - AT&T

Learning Objectives:
Students will:

- Recognize terminology related to "cyberspace," with emphasis on terms and concepts pertinent to the application of computerization within the criminal justice system
- Examine the historical development of law enforcement community efforts to police unlawful use of computer-related technology
- Identify and assess impacts that cyber-technology-related security issues have had on past, present and future aspects of criminal justice systems and societies
- Examine key provisions of the United States Constitution—with special emphasis on The Bill of Rights—which serve as both statutory and philosophical foundations for the U.S. criminal justice system in combatting cybercrimes and apprehending and prosecuting cybercriminals
- Identify ethical challenges faced by law enforcement individuals and organizations working in cyber-technology areas
- Recognize the particular attributes of various computer-based economic systems and how those systems facilitate fraud and other criminal acts by those with criminal intent
- Evaluate efforts undertaken by the Legislative and Executive branches of both state and federal governments to detect and thwart crimes facilitated by computers and/or crimes solely made possible by computer usage
- Investigate and assess changes in domestic and global laws and legal procedures that are likely to occur in the near future, as criminal justice systems work to avert cyber-technology breaches and to hold cyber-technology criminals accountable via civil and criminal measures

Course Structure: The course will be organized into (approximately) eleven topical areas. A preliminary list of these areas is provided above. Students will be expected to stay up-to-date with the current topics list as maintained on the course website. Each cluster (generally) will comprise two classes, one focusing on technical issues and one focusing on legal/policy issues.

Assignments: Students will be graded on a combination of participation (in-class and through the course website/blog), short response papers, and a term paper or project. Specifically:

Class Participation (discretionary): Class participation includes both: 1) participation during class meetings; and 2) active participation in discussion on the course website/discussion boards, if required. Additionally, as the subject matter of this course is actively evolving, students will be expected to read a "newspaper of record" (e.g., the Washington Post) to keep abreast of current events to facilitate class discussion. In the "Information Age" several valid alternatives to print-based newspapers exist. As such, leading online news sources (e.g., cnn.com) may fulfill this requirement.

Individual Response Papers (50%): students will prepare two individual response papers over the course of the semester. The first paper will be approximately 3-5 pages in length and the second paper will be approximately 6-10 pages in length. Both papers will tie in to current class discussions and/or current events.

Term Paper or Project (50%): The term paper or project will give students the opportunity to explore the cybersecurity regulatory issues surrounding a current (or projected) information system or product.

Academic Integrity: All College in High School teachers, students, and their parents/guardians are required to review and be familiar with the University of Pittsburgh's Academic Integrity Policy located online at www.as.pitt.edu/fac/policies/academic-integrity.

Grades: Grade criteria in the high school course may differ slightly from University of Pittsburgh standards. A CHS student could receive two course grades: one for high school and one for the University transcript. In most cases the grades are the same. These grading standards are explained at the beginning of each course.

Transfer Credit: University of Pittsburgh grades earned in CHS courses appear on an official University of Pittsburgh transcript, and the course credits are likely to be eligible for transfer to other colleges and universities. Students are encouraged to contact potential colleges and universities in advance to ensure their CHS credits would be accepted. If students decide to attend any University of Pittsburgh campuses, the University of Pittsburgh grade earned in the course will count toward the student grade point average at the University. At the University of Pittsburgh, the CHS course supersedes any equivalent AP credit.

Drops and Withdrawals: Students should monitor progress in a course. CHS teacher can obtain a Course Drop/Withdrawal Request form from the CHS office or Aspire. The form must be completed by the student, teacher and parent/guardian and returned to teacher by deadlines listed. Dropping and withdrawing from the CHS course has no effect on enrollment in the high school credits for the course.