D333 Study Guide

Ctrl + click HERE **for Supplemental Resources**
(If the links are not working, all the videos and quiz resources can be found under "course search" on your course page.)

<mark>Section 1</mark>
This section overviews the course layout.

<mark>Section 2</mark>
In this section, three competencies are covered across four modules. This section of the course contains Modules 1, 2, and 3, as follows:
- **Module 1: An Overview of Ethics**
- **Module 2: Introduction to Ethical Frameworks**
- **Module 3: Professional Ethics**
- **Module 4: Cyberattacks and Cybersecurity**

Module 1	An Overview of Ethics

From *Computing and Technology Ethics*: *Engaging Through Science Fiction*, Chapter 1

1. Define the following terms:
- Normative statement
- Descriptive statement
- Ethical framework

2. Why is fostering good business ethics (also known as **Corporate Social Responsibility** or **CSR**) important?

3. What are **three basic/perennial** problems in ethics discussed in the chapter?

4. Explain the misconception about ethics and self-interest described in the chapter. How does the chapter argue against this view?

5. What trends have increased the likelihood of unethical behavior?

6. What trends have increased the risk that information technology will be used in an unethical manner?

7. What is the "invisibility factor" of computing technologies, as described by James Moor? List the three issues stemming from this factor.

8. According to the chapter, what three specific changes have been brought about by computer technologies? Briefly describe each.

9. Why does the chapter argue that computing professionals have a particular responsibility to consider ethical issues?

10. Identify two advantages of using stories/science fiction to examine ethical issues, as discussed in the chapter.

12. Define the following term:
   - Moral imagination

15. What does the chapter say about the role of professional societies in articulating ethical norms for a field?

16. What is the Hippocratic Oath, and how does it serve as an example of a professional code of ethics?

Module 2	Introduction to Ethical Frameworks

From *Computing and Technology Ethics*: *Engaging Through Science Fiction*, Chapter 2

1. Define the following terms:
  - Habitus
  - Practical wisdom
  - Heuristics of fear

2. What are the four main ethical frameworks discussed in detail in the chapter? Briefly describe the core focus of each.

3. How does virtue ethics differ from deontology and utilitarianism in its approach to ethical decision-making?

4. Explain the concept of "finding the mean" in virtue ethics. How does it relate to practical wisdom?

5. What is the principle of utility in utilitarianism? What are some challenges in applying this principle?

6. How does communitarianism view the relationship between individuals and their communities? How does this differ from other frameworks?

7. What is the "invisibility factor" in computing technologies, as described by James Moor? List the three issues stemming from this factor.

9. What is preference utilitarianism, and how does it differ from classical utilitarianism?

10. What are the main criticisms of traditional ethical frameworks that led to the development of responsibility ethics?

11. How does feminist ethics differ in its approach to ethical reasoning compared to traditional frameworks?

12. What is the Capability Approach, and how does it evaluate individual actions and social policies?

13. What is emotional labor, and why is it an important concept in feminist ethics?

14. How does the chapter suggest that studying multiple ethical frameworks can benefit our understanding and application of ethics?

Module 3	Ethics for IT Workers and IT Users

From *Computing and Technology Ethics*: *Engaging Through Science Fiction*, Chapter 6 (NOT CHAPTER 3!)

Define the following terms:
- Profession
- Conflict of interest
- Licensing
- Certification

What are the core characteristics of a profession?

Identify three functions or purposes of codes of ethics.

What are the three utilitarian approaches to ethical decision-making?

What are the three approaches based on respect for persons?

How does the ACM Code of Ethics address the issue of privacy?

What is the difference between **preventive ethics** and **aspirational ethics** in professional codes?

Explain two ways that professional societies interact with laws and regulations.

How does the IEEE Code of Ethics address the issue of discrimination?

Describe the concept of moral imagination and its importance in ethical decision-making.

What is the SECEPP, and what is its purpose?

How do the ACM and IEEE codes of ethics address the issue of professional development?

Explain the concept of policy vacuums in relation to technology and ethics.

What are the seven principles outlined by the ACM for designing and deploying algorithms to maximize transparency and accountability?

Module 4	Cyber Attacks and Cybersecurity

From *Ethics in Information Technology*, Chapter 3
(NOT *COMPUTING AND TECHNOLOGY ETHICS*!! Move to Cengage.)

Topic: The Threat Landscape
Define a Zero-day exploit.

Explain several reasons why computer incidents are so prevalent (p. 86-87)?

What are some common reasons mentioned for computer exploits?

Complete the perpetrator table.
Using the descriptions shared on the table, identify the types of computer perpetrators noted in the reading (p. 88).

Perpetrator Type	Description
	Someone who violates computer or Internet security maliciously or for illegal personal gain (in contrast to a white hat hacker who is someone who has been hired by an organization to test the security of its information systems).
	An employee or contractor who attempts to gain financially or disrupt a company's information systems and business operations.

	Someone who attacks a computer system or network for financial gain.
	Someone who attempts to destroy the infrastructure components of governments, financial institutions, and other corporations.
	An individual who causes problems, steals data, and corrupts systems.

Topic: Types of Exploits
Define the following terms.
    Ransomware
    Virus
    Worm
    Trojan Horse

What is it called when a threat combines various types of exploits and vulnerabilities in one payload?

Answer the following questions about spam.

    In states where it is legal to spam, what are the usual requirements?

    How common is spam?

Define the following attacks and terms (p.93-96).
    DDos Attack
    Botnet
    Rootkit
    APT
    Spear Phishing
    Smishing

Identify the large federal agency with a budget of almost $65 billion whose goal is to provide for a "safer, more secure America, which is resilient against terrorism and other potential threats." (p. 98)

Topic: Federal Laws for Prosecuting Computer Attacks

Complete the table of Federal Laws. These laws were enacted to address computer

crimes (p. 100).

Law	Subject Area
	Address fraud and related activities in association with computers including access, transmission, password trafficking, and threats.
	Covers false claims regarding unauthorized use of credit cards.
	Focuses on unlawful access to stored communications to obtain, alter, or prevent unauthorized access to electronic communication while it is in electronic storage.
	Defines cyberterrorism and associated penalties.

Topic: CIA Triad (p.100)

Identify are the three components of the CIA triad:

1.
2.
3.

Describe a layered solution that can help prevent or minimize an attack.

How can an organization implement a CIA security strategy (p. 101)?

Define the following terms (102-103).
  Risk-Assessment
  Reasonable Assurance
  Disaster Recovery Plan
  Business Continuity Plan

What does a good security policy do (p. 104)?

What should a good security audit do?

Complete the table of Regulatory Standards Compliance. In addition to the requirement to comply with your own security program, you may also be required to comply with external security standards (p.106).

Act or Standard	Subject Matter
	Requires financial institutions in the United States to assist U.S. government agencies in

	detecting and preventing money laundering.
	Makes certain payments to foreign officials and other foreign persons illegal and requires companies to maintain accurate records
	Governs the collection, disclosure, and protection of consumers' nonpublic personal information or personally identifiable information
	Regulates the use and disclosure of an individual's health information
	Provides a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information
	Protects shareholders and the general public from accounting errors and fraudulent practices in the enterprise

Topic: Implementing CIA at the Network Level (p.108)

Develop an example of one type of authentication method.

Explain how a next-generation firewall (NGFW) is different from a standard firewall.

Explain the following two encryption terms (p. 109):
Encryption Key-
Triple Layer Security (TLS)-

How does an intrusion detection system work (p. 111)?

Topic: Implementing CIA at the End-User Level (p.113)

Identify the several components of a good security education for employees.

What does most antivirus software scan for?

Topic: Response to Cyberattack (p.115)

Why might a company try to conceal information about a data breach to it's customers?

Explain the importance of activity logs surrounding a data breach or other security

incident.

What must the IT security group do before it begins eradication efforts for cyberattack?

Identify at least 3 key elements that should be included in the formal incident following a cyberattack (p. 116):
a.
b.
c.

What is a MSSP and what does it do (p.117)?

Explain the role of a computer forensics team.

<mark>Section 3</mark>

In this section, one competency is covered across three modules. This section of the course contains Modules 4, 5, and 6, as follows:
- Module 5: Privacy
- Module 6: Freedom of Expression
- Module 7: Intellectual Property

Module 5	Privacy

From *Ethics in Information Technology*, Chapter 4
(NOT *COMPUTING AND TECHNOLOGY ETHICS*!! Move to Cengage.)

Topic: Privacy Protection and the Law

What is the right of privacy, and what is the basis for protecting personal privacy under the law? (p.136)

Identify at least 3 systems that gather data about individuals? (p. 137)

Define the following terms.
   Right of Privacy

Information Privacy

Topic: Privacy Laws, Applications, and Court Rulings

Complete the table below by identifying the applicable Law or Act (p. 139). Use this to review the patterns and changes in legislation relating to privacy. While you do not need to memorize these, you will want to be familiar with them and notice how they affect one another and change over time due to political and environmental circumstances.

Law or Act	Year	Impact
Financial Data		
	1970	Regulates the operations of credit reporting bureaus, including how they collect, store, and use credit information. This act is enforced by the U.S. Federal Trade Commission.
	1978	Protects the records of financial institution customers from unauthorized scrutiny by the federal government.
	1999	Also known as the Financial Services Modernization Act of 1999. Includes three key rules that affect personal privacy: Financial privacy (collection and disclosure guidelines), Safeguards (data security plan), and Pretexting rules.
	2003	Allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies. The act helped establish the National Fraud Alert system to help prevent identity theft.
Health Data		
	1996	Designed to improve the portability and continuity of health insurance coverage; to reduce fraud, waste, and abuse in health insurance and healthcare delivery; and to simplify the administration of health insurance.
	2009	Included strong privacy provisions for electronic health records (EHRs), including banning the sale of health information, promoting the use of audit trails and encryption, and providing rights of access for patients. Individuals whose health information has been exposed be notified within 60 days after discovery of a data breach.
Children's Data		
	1974	Assigns certain rights to parents regarding their

		children's educational records. Includes rights to access, request, amend school records; along with file complaints for disclosure violations.
	1998	Any website that caters to children must offer comprehensive privacy policies, notify parents or guardians about its data collection practices, and receive parental consent before collecting any personal information from children under 13 years of age.
Surveillance		
	1968	Allows state and federal law enforcement officials to use wiretapping and electronic eavesdropping, but only under strict limitations. Under this act, a warrant must be obtained from a judge to conduct a wiretap.
	1978	Describes procedures for the electronic surveillance and collection of foreign intelligence information in communications between foreign powers and the agents of foreign powers. Requires the government to obtain a court order before it can intentionally target a U.S. person.
	1981	Identifies various U.S. governmental intelligence-gathering agencies and defines what information can be collected, retained, and disseminated by these agencies. These agencies are allowed to collect information, including messages, obtained during lawful foreign investigations.
	1986	Deals with three main issues: the protection of communications while in transfer from sender to receiver; the protection of communications held in electronic storage; and the prohibition of devices from recording dialing, routing, addressing, and signaling information without a search warrant. Under this act, the FBI director may issue a National Security Letter (NSL) to an Internet service provider to provide various data and records about a service subscriber.
	1994	Required the telecommunications industry to build tools into its products that federal investigators could use, with a court order, to eavesdrop on conversations and intercept electronic communications.
		(Terrorist attacks of September 11, 2001)
	2001	It gave sweeping new powers to both domestic law enforcement and U.S. international intelligence agencies, including increasing the ability of law enforcement

		agencies to search telephone, email, medical, financial, and other records. It also eased restrictions on foreign intelligence gathering in the United States.
	2004	Congress amended the FISA to authorize intelligence gathering on individuals not affiliated with any known terrorist organization (so-called lone wolves).
	2008	Grants NSA expanded authority to collect, without court-approved warrants, international communications as they flow through U.S. telecommunications network equipment and facilities. The targets of the warrantless eavesdropping had to be "reasonably believed" to be outside the United States.
		(Edward Snowden leaks NSA secrets)
	2015	Act terminated the bulk collection of telephone metadata by the NSA. Instead, telecommunications providers are now required to hold the data and respond to NSA queries on the data. The act also restored authorization for roving wiretaps.
Fair Information Practices		
	1980	Often held up as the model for ethical treatment of consumer data. These guidelines are composed of the eight principles: collection limitation, data quality, purpose, use limitation, safeguards, openness, individual participation, and accountability.
	1995	Requires any company doing business within the borders of the countries comprising the European Union (EU) to implement a set of privacy directives on the fair and appropriate use of information.
	2018	Strengthens data protection for individuals within the EU by addressing the export of personal data outside the EU, enabling citizens to see and correct their personal data, and ensure data protection consistency across the EU.
Access to Government Records		
	1966	Grants citizens the right to access certain information and records of federal, state, and local governments upon request. Enables journalists and the public to acquire information that the government is reluctant to release.
	1974	A code of fair information practices that sets rules for the collection, maintenance, use, and dissemination of

		personal data that is kept in systems of records by federal agencies. It also prohibits U.S. government agencies from hiding any personal data keeping system.

Topic: Key Privacy and Anonymity Issues (p.158)

Identify and explain at least three common ways businesses may use a person's cookie information:

   1.
   2.
   3.

About how much does a data breach cost a company per record? (p. 159)

What act makes identity theft illegal and punishable up to 15 years of imprisonment?

Topic: Electronic Discovery (p.162)

Explain an electronic discovery and what types of information it might include.

What might a litigation hold prevent?

How might predictive coding assist in an e-discovery? What issues might arise from this?

Topic: Workplace Monitoring (p.163)

What are some examples of cyber loafing?

It is estimated that cyberloafing costs U.S. business as much as $___ billion a year.

Explain why a business may want to monitor its employees and if they are legally allowed to.

What type of employee information and data are frequently tracked?

Topic: Advanced Surveillance Technology (p.165)

Complete the following table. In the second column, describe the types of data collected by each of the following terms:

Type	What data do they capture?
Camera Surveillance	
Vehicle Event Data Recorder (EDR)	
Stalking Apps	

Module 6	Freedom of Expression

From *Ethics in Information Technology*, Chapter 5
(NOT *COMPUTING AND TECHNOLOGY ETHICS*!! Move to Cengage.)

Topic: 1st Amendment Rights

What is the basic for the protection of freedom of expression?

The Supreme Court has held that the following types of speech are not protected by the First Amendment and may be forbidden by the government: (p. 188)

Explain one of the three questions that can be used to determine if speech is considered obscene:

Define the following terms.
- ☐ Defamation
- ☐ Slander
- ☐ Libel

Topic: Freedom of Expression- Key Issues

What important freedom of expression issues relate to the use of information technology?

Complete the following access table by identifying the key legislation in column one (pp. 190-192).

Law or Ruling	Year	Description
	1996	Title V of the Telecommunications Act, aimed at

		protecting children from pornography. Penalties include fines and imprisonment.
	1998	States that "whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor…" is subject to fines and/or imprisonment.
	2004	Declared COPA was unconstitutional and could not be used to shelter children from pornographic materials.

What then can be used by households to protect children from explicit websites while still allowing open access to media by adults? (p.192)

Explain at least two ways a government may censor a website (p.195).

Identify the top three countries with the largest populations of internet users (p.196):
1.
2.
3.
What is a SLAPP? (p.197)

Identify one court case where the US protected the right of anonymity. (p.198)

Define the following terms.
- ☐ Doxing
- ☐ Anonymous remailer service
- ☐ John Doe Lawsuit
- ☐ Hate Speech

Module 7	**Intellectual Property**

**From *Ethics in Information Technology*, Chapter 6
(NOT *COMPUTING AND TECHNOLOGY ETHICS*!! Move to Cengage.)**

Topic: What is Intellectual Property

What does the term intellectual property encompass?

What measures can organizations take to protect their intellectual property?

Define the following terms. (p. 225)
- ☐ Intellectual property
- ☐ Copyright

How long does the current copyright term protect authors?

Explain the four factors that should be considered when determining whether a copyrighted work is prohibited by the fair use doctrine. (p. 226)
1.
2.
3.
4.

What must be proven to validate a software claim of copywrite infringement? (p. 227)

What act created the position of Intellectual Property Enforcement Coordinator within the Executive Office of the President, while also increasing enforcement and penalties for infringement? (p. 228)

International trade in counterfeit and pirated goods could have accounted for as much as $____ billion or 2.5 percent of world trade in 2013.

In **WTO TRIPS Agreement** table, the second column lists the key terms of the agreement. In the first column, enter the form of intellectual property that is protected. (p. 229)

Form of Intellectual Property	Key Term of Agreement
	Computer programs are protected as literary works. Authors of computer programs and producers of sound recordings have the right to prohibit the commercial rental of their works to the public.
	Patent protection is available for any invention—whether a product or process—in all fields of technology without discrimination, subject to the normal tests of novelty,

		inventiveness, and industrial applicability.
		These have commercial value must be protected against breach of confidence and other acts that are contrary to honest commercial practices. Steps must have been taken to keep it secret.

In the **Digital Millennium Copyright Act** (DCMA), enter the name of the title section in the second column to match the appropriate description. (p. 230)

Title	Name	Description
1		This section implements the WIPO treaties by making certain technical amendments to the U.S. law to provide appropriate references and links to the treaties. It also creates two new prohibitions, one on circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information. Adds penalties for violation.
2		This section enables website operators that allow users to post content on their website (e.g., music, video, and pictures) to avoid copyright infringement liability if certain "safe harbor" provisions are followed.
3		This section permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer. The new copy cannot be used in any other manner and must be destroyed immediately after the maintenance or repair is completed.
4		This section adds language to the Copyright Act confirming the Copyright Office's authority to continue to perform the policy and international functions that it has carried out for decades under its existing general authority.
5		This section creates a new form of protection for the original design of vessel hulls

Since DMCA does not directly govern copying, what does it do instead?

Define the following terms. (p.232)
- ☐ Utility Patent
- ☐ Design Patent
- ☐ Prior Art

The U.S. Supreme Court has ruled that three classes of items cannot be patented (p. 233):
1.
2.
3.

If a court determines that the infringement is intentional, it can award up to ___ times the amount of the damages claimed by the patent holder.

Under the Leahy-Smith America Invents Act, the U.S. patent system changed from a "first-to-invent" to a _____ system effective from March 16, 2013. (p.234)

Topic: Trade Secrets

Explain how trade secret laws protect more technology worldwide than patent laws do. (p. 236)

In the **Trade Secret Laws** table, identify the law in column 1 that is described in column 2.

Act	Description
	Defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by, persons who can obtain economic value from its disclosure or use, and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."
	An act passed in 1996 to help law enforcement agencies pursue economic espionage. It imposes penalties of up to $10 million and 15 years in prison for the theft of trade secrets.
	An act passed in 2016 that amended the Economic Espionage Act to create a federal civil remedy for trade secret misappropriation.

Define the following terms. (p. 238)
- ☐ Nondisclosure Clause
- ☐ Noncomplete Agreement

Topic: Current Intellectual Property Issues
Define the following terms. (p. 240-242))
- ☐ Plagiarism
- ☐ Reverse Engineering

Identify one argument for and one argument against reverse engineering.

Explain the reasoning behind why firms or individual developers create open source code, even though they do not receive money for it. (p. 244)

Contrast competitive espionage from industrial espionage. (p. 245)

Explain what is covered by a trademark and who it protects. (p.247)

When might nominal fair use apply?

What does a cybersquatter typically hope to gain? (P. 248)

<mark>Section 4</mark>
In this section, one competency is covered across three modules. This section of the course contains Modules 7, 8, and 9, as follows:
- Module 8: Ethical Decisions in Software Development
- Module 9: The Impact of Information Technology on Society
- Module 10: Social Media

Module 8	Ethical Decisions in Software Development

**From *Ethics in Information Technology*, Chapter 7
(NOT *COMPUTING AND TECHNOLOGY ETHICS*!! Move to Cengage.)**

Topic: Software Quality and Why It Is Important

Explain quality management and state it's primary objective. (p. 266)

Identify and explain at least three factors that can contribute to poor-quality software. (p.267)

    1.

    2.

    3.

Fill in the blank. A _____ is a set of interrelated components (including hardware, software, databases, networks, people, and procedures) that collects and processes data and disseminates the output. (p. 269)

Explain what a DSS is and how it may be used by a company. (p. 269)

Compare the terms product liability and strict liability. (p. 270)

What must be proven in a breach of warranty claim?

Topic: Strategies for Developing Quality Software

Explain the two types of popular software development methodologies from the reading: (p.272-273)

    1. Waterfall System

    2. Agile

In the **Software Testing** table, identify the type of testing in column 1 that is described in column 2. (p. 276)

Test Type	Description

	A type of dynamic testing that involves viewing the software unit as a device that has expected input and output behaviors but whose internal workings are unknown (a black box).
	A type of dynamic testing that treats the software unit as a device that has expected input and output behaviors but whose internal workings, unlike the unit in black-box testing, are known.
	A software-testing technique in which software is tested without actually executing the code. It consists of two steps—review and static analysis.
	A software-testing technique that involves testing individual components of code (subroutines, modules, and programs) to verify that each unit performs as intended.
	Software testing done after successful unit testing, where the software units are combined into an integrated subsystem that undergoes rigorous testing to ensure that the linkages among the various subsystems work successfully.
	Software testing done after successful integration testing, where the various subsystems are combined to test the entire system as a complete entity.
	Software testing done independently by trained end users to ensure the system operates as expected.

What are Capability Maturity Model Integration (CMMI) models? (p.277)

Describe the five levels of maturity described CMMI

1. Initial	
2. Managed	
3. Defined	
4. Quantitatively Managed	
5. Optimizing	

Define the following terms. (p. 279-280)
- ☐ Safety-Critical System
- ☐ System Safety Engineer
- ☐ Annualization Loss Expectancy (ALE)
- ☐ Risk Management

Identify the five strategies for addressing a particular risk? (p.281)
- **1.**
- **2.**
- **3.**
- **4.**
- **5.**

Fill in the blank. Reliability and safety are two different system characteristics. _____ has to do with the capability of the system to continue to perform; _____ has to do with the ability of the system to perform in a safe manner. (p.282)

Describe the ISO 9001 family of standards guide. (p. 283)

Explain Failure Mode and Effects Analysis (FMEA).

Module 9	The Impact of Information Technology on Society

From *Ethics in Information Technology*, Chapter 8
(NOT *COMPUTING AND TECHNOLOGY ETHICS*!! Move to Cengage.)

Describe what might be included in a patient's electronic health record (EHR). (p. 300)

What does the Health Information Technology for Economic and Clinical Health Act

(HITECH) do?

Explain labor productivity and key factors related to improving it. (p. 303)

Topic: IT and Workplace Automation (p.306)

According to the reading, about how much of human work could be automated using existing technology? (p.306)

Identify types of work activities lease suited for automation.

In the **Artificial Intelligence** table, identify the type of AI in column 1 that is described in column 2.(p. 307-309)

AI Type	Description
	A type of artificial intelligence (AI), involves computer programs that can learn some task and improve their performance with experience.
	A branch of engineering that involves the development and manufacture of mechanical or computer devices that can perform tasks that require a high degree of precision or that are tedious or hazardous for human beings, such as painting cars or making precision welds.
	An aspect of artificial intelligence that involves technology that allows computers to understand, analyze, manipulate, and/or generate "natural" languages, such as English.
	A software-testing technique that involves testing individual components of code (subroutines, modules, and programs) to verify that each unit performs as intended.

What are the three major components of machine learning? (p. 307)

Identify some of the major improvements made by IT to the healthcare industry. (p.311)

Contrast the how an electronic medical record is different from a personal health record. (p. 312)

Explain Health Information Exchange (HIE) and its benefits.

Define the following terms. (p. 312-314)
- ☐ Clinical Decision Support (CDS)
- ☐ Computerized Provider Order Entry (CPOE)
- ☐ Telehealth

Identify the three basic forms of telemedicine: (p.314)
1.
2.
3.

Module 10	Social Media

**From *Ethics in Information Technology*, Chapter 9
(NOT *COMPUTING AND TECHNOLOGY ETHICS*!! Move to Cengage.)**

Explain the meaning of social media and what it includes. (p.330)

Topic: Social Networking Platforms (p.331)
How do individuals use social networks?

What are some practical business uses of social networking?

Topic: Business Applications of Social Media
Identify some business-oriented social networking platforms. (p.333)

Describe social media marketing. (p. 335)

Explain the following four types of social media marketing and it benefit to a business:
1. Organic Media Marketing

2. Paid Media Marketing

3. Earned Media

4. Viral Marketing

Topic: Social Networking Ethical Issues (p. 339)
Define the following types of cyber abuse:
☐ Cyberharassment
☐ Cyberstalking

Describe at least one way the law protects against cyberstalking.

What does SORNA stand for?

Fill in the blank. The First Amendment of the U.S. Constitution protects the right of freedom of expression from government interference; however, it does not prohibit free speech interference by _____. (p.344)

SECTION 5

In this section, four competencies are covered across two modules. This section of the course contains Modules 10 and 11, as follows:

- Module 11: Ethics of IT Organizations
- Module 12: AI Ethics and Appendix A: A Brief Introduction to Morality

Module 11	Ethics of IT Organizations

From *Ethics in Information Technology*, Chapter 10
(NOT *COMPUTING AND TECHNOLOGY ETHICS*!! Move to Cengage.)

Topic: Use of Contingent Workers (p. 360)
Define the following types of contingent working:
☐ Temporary Staffing
☐ Employee Leasing
☐ Professional Employer Organization

In a gig economy, how might an individual make a profit? (p.361)

Identify at least one benefit and one draw back to being employed as an independent contractor. (p. 362)

Describe at least two benefits to a business when they hire contingent workers. (p.363)

Describe at least one disadvantage to a business hiring contingent workers.

Topic: H-1B Workers (p. 366)
Explain what an H-1B visa is.

How long can an individual work in US as an H-1B employee?

What would an individual need to do to transition from a temporary H-1B employee to full-time US resident?

Identify at least one disadvantage to a business relying heavily on H-1B employees?

Topic: Outsourcing
Explain the difference between outsourcing and offshore outsourcing. (p. 372)

What is outsourcing so common in the IT field?

Identify one pro and one con to offshoring. (p.373)

What can improve the chances that offshoring will be successful? (p374)

What does a successful Statement on Standards for Attestation Engagements (SSAR) demonstrate?

Topic: Whistle-Blowing
Define the term whistle-blowing and explain who might be behind it. (p.375)

Explain two common legal provisions from the reading that are associated with whistle-blowing: (p.376)
     1. False Claims Act
     2. Qui tam

Identify the eight steps behind an effective whistle-blowing process:

1.
2.
3.
4.
5.
6.
7.
8.

Explain what green computing refers to. (p.381)

What are the goals of green computing?

What does EPEAT do?

Module 12	AI Ethics

> From *Computing and Technology Ethics*: *Engaging Through Science Fiction*, Chapter 3.4, Chapter 4.4.
> (*NOT CENGAGE*)
> ALSO, the video linked below:

https://westerngovernorsuniversity.sharepoint.com/:u:/r/sites/D333Supplemental
Resources/Things%20to%20watch/AI%20Bias.url?csf=1&web=1&e=ijbdG2

1. Define the following terms:
 - Bias
 - Selection bias
 - Cognitive bias
 - Ethics washing

2. What are **three examples** of automated decision-making systems that have been shown to reproduce subjective bias in harmful ways?

3. Explain the concept of "**weblining**" and how it relates to historical discriminatory practices.

4. How can big data analytics unintentionally reproduce existing patterns of bias and discrimination?

5. Describe **three ways** in which computing and large data systems can promote

positive social change, according to Abebe et al.

6. What did the study by Cowgill et al. reveal about the sources of bias in AI systems?

7. Why is it problematic to view data as value-neutral in the context of automated decision-making systems?

8. What is the **General Data Protection Regulation (GDPR)**, and how does it aim to address issues of bias in algorithmic decision-making?

9. Explain the concept of using computing as a diagnostic tool for addressing bias.

10. What are **two positive outcomes** of using large, automated decision-making systems, as mentioned in the chapter?

Topic: Understanding Bias & Fairness (Video)

WATCH AT THIS LINK:

https://lrps.wgu.edu/provision/295566175

Identify and explain the three core components of AI Trust: (4:11)
1.
2.
3.

List the five defined measurements of performance (5:49).

List the five defined measurements of operations (5:49).

List the five defined measurements of ethics (5:49).

Explain the following common sources of bias (9:50):
    ☐ Skewed Sample
    ☐ Limited Features
    ☐ Tainted Examples
    ☐ Sample Size
    ☐ Proxies

What are four suggestions are made for tackling AI bias? (17:48)
1. Identify-
2. Select-
3. Build-
4. Mitigate-

Explain the following bias mitigation techniques (27:22):
  ☐ Pre-processing
  ☐ In-processing
  ☐ Post-processing

Topic: A Brief Introduction to Morality (Appendix A)

Complete the table by describing the following ethical theories.

Theory	Description
Deontology	
Consequentialism/ Utilitarianism	
Virtue Ethics	
Relativism	

SECTION 6

Course summary and completion notice.