**Revision Test**

***First Semester: 1436 / 1437 - 2015 / 2016***

**Question 3: Answer the following questions:**

Chapter: 5

1. **Do you agree with Judith Jarvis Thomson that every “privacy right” violation is a violation of another right? Explain your position.**

I think it is true that every privacy violation constitutes another violation of the same degree. If a person took a picture of a picture you own and started to distribute this picture then that person has committed a privacy violation and property violation as well. Privacy rights are about some of our basic rights we have to protect ourselves and the things we hold dear.

1. **Describe three modern information technology devices and how they may be used to decrease privacy.**
* Bluetooth can be used to decrease privacy as once you turn your Bluetooth then other people can connect to your phone and with a bit of hacking can see the content of your device.
* Camera can be used to decrease privacy as other people start filming you and take images of you.
* NFC technology is similar to Bluetooth as well as it allow some devices to connect over short range allowing some to see the content of devices as well.
1. **Describe the Facebook Beacon service and explain why it raised privacy complaints after it was introduced.**

**In November 2007, Facebook announced Beacon, “a core element of the Facebook Ads system for connecting businesses with users and targeting advertising to the audiences they want”**

Facebook's decision to make their Beacon system opt-out infuriated many Facebook users, who didn't even know Beacon existed until it had revealed information they thought was private.

1. **Give two examples of how organizations are applying the techniques of data mining to information contained in social networks.**
2. Cell phone companies are using data mining on social networks to identify “influencers" and offer them incentives to keep them loyal.
3. Police are using data mining on social networks to identify where big parties are happening and deploy officers accordingly.
4. Banks are using data mining to evaluate the riskiness of loans.

Chapter: 6

1. **Choose one of the following pieces of federal legislation and explain how it limits the amount of information private entities can collect from individuals:**
	1. **Employee Polygraph Protection Act**

The Employee Polygraph Protection Act helps jobs applicants and company employees maintain their privacy by making it illegal for companies to require polygraph tests as a condition of employment (except for a few types of job). The EPPA also makes it illegal for companies to give polygraph tests to current employees, with a few exceptions. The most significant loophole of the Employee Polygraph Protection Act is that it does not apply to federal, state, or local government agencies.

* 1. **Children’s Online Privacy Protection Act**

The purpose of the Children's Online Privacy Protection Act is to reduce the amount of personal information gathered from children using the Internet.

* 1. **Genetic Information Nondiscrimination Act**

The two principal purposes of the Genetic Information Nondiscrimination Act are:

* Prevent health insurance companies and health plan administrators from using genetic information when making decisions about “coverage, rates, or preexisting conditions”.
* Prohibit most employers from taking genetic information into account when making decisions related to the terms of employment (e.g., hiring, firing, and promotions).
1. **Relate the Fourth Amendment to the United States Constitution to the definition of privacy elaborated in the book.**

The Fourth Amendment to the U.S. Constitution protects people from unreasonable searches and seizures of their property by law enforcement authorities.

1. **In what ways does the USA PATRIOT Act represent a challenge to the Fourth Amendment to the U.S. Constitution?**

Despite language in the Patriot Act to the contrary, civil libertarians are concerned that law enforcement agencies may use their new powers to reduce the rights of law-abiding Americans, particularly those rights expressed in the First and Fourth Amendments to the United States Constitution.

Critics maintain that other provisions of the Patriot Act undermine the right against unreasonable searches and seizures guaranteed by the Fourth Amendment:

* By revealing the URLs of Web sites visited by a suspect, a pen register is a much more powerful surveillance tool on the Internet than it is on a telephone network. The Patriot Act allows police to install Internet pen registers without demonstrating probable cause that the suspect is engaged in a criminal activity.
* Court orders authorizing roving surveillance do not “particularly describe the place to be searched.”
* It allows law enforcement agencies, under certain circumstances, to search homes and seize evidence without first serving a search warrant.
* It allows the FBI to obtain—without showing probable cause—a warrant authorizing the seizure of business, medical, educational, and library records of suspects.
1. **What are the principal limitations of the Privacy Act of 1974?**

The Privacy Act has the following principal limitations:

* The Privacy Act applies only to government databases.

Far more information is held in private databases, which are excluded.

This is an enormous loophole, because government agencies can purchase information from private organizations that have the data they want.

* The Privacy Act only covers records indexed by a personal identifier.

Records about individuals that are not indexed by name or another identifying number are excluded. For example, a former IRS agent tried to gain access to a file containing derogatory information about himself, but the judge ruled he did not have a right to see the file, since it was indexed under the name of another IRS employee.

* No one in the federal government is in charge of enforcing the provisions of the Privacy Act.

Federal agencies have taken it upon themselves to determine which databases they can exempt. The IRS has exempted its database containing the names of taxpayers it is investigating. The Department of Justice has announced that the FBI does not have to ensure the reliability of the data in its NCIC databases.

* The Privacy Act allows one agency to share records with another agency as long as they are for a “routine use.”

Each agency is able to decide for itself what “routine use” means. The Department of Justice has encouraged agencies to define “routine use” as broadly as possible.

Although the Privacy Act applies only to government databases, Congress has passed legislation regulating how some private institutions manage databases containing sensitive information about individuals, and these laws put into effect many of the principles of the Code of Fair Information Practices. In the remainder of this section, we survey some of the most influential of these laws.

1. **Choose one of the following pieces of legislation and explain how it restricts the dissemination of personal information that organizations have collected.**
	1. **Family Education Rights and Privacy Act**

The Family Education Rights and Privacy Act give students 18 years old and older the right to review their educational records. It also gives them the right to request changes to records containing errors. Students may prevent others from accessing these records without permission, except under certain circumstances. If a student is less than 18 years old, these rights are held by the student's parents or guardians.

* 1. **Video Privacy Protection Act**

The Video Privacy Protection Act enhances privacy by making it illegal for videotape service providers to disclose rental records without the consent of the customer. The law also requires stores to destroy information about who rented what within a year of when the information is no longer needed for the purposes of the original transaction.

* 1. **Health Insurance Portability and Accountability Act**

The Health Insurance Portability and Accountability Act limit how doctors, hospitals, pharmacies, and insurance companies can use medical information collected from patients. The regulations forbid health care providers from releasing information to life insurance companies, banks, or other businesses without specific signed authorization from the person being treated. Health care providers must provide their patients with a notice describing how they use the information they gather. Patients have the right to see their medical records and request corrections to errors they find in those records.

Chapter: 7

1. **Explain how the meaning of the word “hacker” changed between the 1950s and the 1990s.**

In the 1950s the term “hacker" referred to an inquisitive and creative person able to make systems do new things. When digital computers became available, the use of the term shifted to include software virtuosos as well as hardware experts. After people began breaking into government and corporate computer networks in the 1980s -1990s, the everyday meaning of the word shifted.

1. **Briefly relate the story of the Firesheep extension to the Firefox browser. What capability did Firesheep provide its users? What happened after Firesheep was released? Was Eric Butler wrong to release Firesheep to the public?**

Firesheep makes it easy for a Firefox user to sidejack open Web sessions. The user starts the Firefox browswer, connects to an open WiFi network, and clicks on a button called “Start Capturing.”

When someone using the network visits an insecure Web site that Firesheep knows about, the user’s name and photo are displayed in a sidebar, along with the name of the Web site he is connected to, such as Amazon.

Butler wrote: “The attack that Firesheep demonstrates is easy to do using tools that have been available for years. Criminals already knew this, and I reject the notion that something like Firesheep turns otherwise innocent people evil”.

1. **Explain the similarities and differences between computer viruses and computer worms.**
* A virus is a piece of self-replicating code contained inside another program, called the host.
* A worm is a self-contained program that is capable of automatically propagating through a computer network by exploiting security holes.
1. **What is a cyber-attack? Give two examples of politically motivated cyber-attacks since 2007.**

A **cyber-attack** is a “computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or information resident on it”. A cyber-attack is an attack from one computer to another that attempts to disable the target computer or steal information from it.

**Examples of politically motivated cyber-attacks:**

* The Estonian government decided to relocate the controversial statue from downtown Tallinn to a Russian military cemetery in the suburbs. They knew the relocation would be hugely unpopular with the Russians. In fact, the Russian government had warned that removing the statue would be “disastrous for Estonians”. The police were prepared for violence, and although ethnic Russians rioted for two nights after the statue was moved, the damage was limited.
* The government also expected an attack on its cyber infrastructure. Sure enough, an attack came, but its magnitude was greater than anything expected by the government’s Internet security group. DDoS attacks from nearly a million computers targeted Estonian government ministries and all of Estonia’s major commercial banks, telecommunications companies, and media outlets. To combat the attacks, much of Estonia’s Internet was made inaccessible to computers outside the country, and on May 10, Estonia’s largest bank had to suspend online services for an hour.

**The examples in short:**

* Cyber attack on Estonia in 2007 destroyed the websites of Estonian organizations like banks, parliament, minister’s newspapers and broadcasters.
* Georgia DDoS attack on twitter, Facebook, and Google. The attack was an effort to block political bloggers. Nobody took responsibility of the attack but it coincided with the War between Russia and Georgia over South Ossetia.

Chapter: 8

1. **For each of the following kinds of errors, define the error type and give an actual occurrence of an error of that type: data-entry error, data-retrieval error, software bug.**
* A **data-entry error** is an error resulting from incorrect data being entered into a computer system.
* The data-entry errors caused the voting system to work incorrectly.
* A **data-retrieval error** is an error resulting from the output of a computer system being misunderstood.
* The data-retrieval error caused the criminal justice system to perform incorrectly.
* A **software bug** that causes one computer to fail will cause both computers to fail.
1. **Explain the mistakes that led to the failure of the Patriot missile system.**
* A system designed for one purpose was used for another purpose.
* There was an error in storing or converting a data value.
1. **Explain the mistakes that led to the failure of the AT&T long-distance network.**
* A line of code became a single point of failure.
1. **Explain the error that caused NASA’s Mars Climate Orbiter to crash.**
* There was an error in storing or converting a data value.
1. **What evidence is there that software quality is improving?**

There is evidence that the field of software engineering is becoming more mature (Figure 8.10).



**Figure 8.10** Research by the Standish Group reveals that the success rate of IT projects in 2009 was twice that of 1994. Today, about one-third of software projects are completed on time and on budget.

1. **Explain how computer simulations are validated.**

You can validate a computer simulation by compare its predicted result with the actual result found by doing the experiment in the real world. For example, you can use a computer simulation to predict what happens when you drive a Nissan Leaf into a wall at 35 miles per hour. Then you can drive a real Nissan Leaf into a wall at 35 miles per hour and compare the predicted results with the actual results. Another way to validate a computer simulation is to take its prediction to an expert and ask the expert if the prediction is accurate.

1. **Explain why the courts reached different conclusions about the validity of software licenses in Step-Saver Data Systems v. Wyse Technology and The Software Link and Mortenson v. Timberline Software.**

The significance of the court's ruling in Step-Saver Data Systems v. Wyse Technology and The Software Link was that the purchase order, the invoice, and the oral statements constituted the contract, not the software license agreement.

The significance of the court's ruling in Mortenson v. Timberline Software was that the licensing agreement limited the consequential damages that Mortenson could recover from Timberline, even though Timberline knew there was a bug in the program and had not told Mortenson.

Chapter: 9

1. **Why is good judgment required in order to use the Software Engineering Code of Ethics effectively?**
* Temper all technical judgments by the need to support and maintain human values.
* Only endorse documents either prepared under their supervision or within their areas of competence and with which they are in agreement.
* Maintain professional objectivity with respect to any software or related documents they are asked to evaluate.
* Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.
* Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.
* Refuse to participate, as members or advisors, in a private, governmental or professional body concerned with software related issues, in which they, their employers or their clients have undisclosed potential conflicts of interest.
1. **What is virtue ethics? How does virtue ethics relate to the Software Engineering Code of Ethics and Professional Practice?**

Virtue ethics is the ethical theory that holds the right thing to in a particular circumstance is what a person of high moral character would do in that situation.

A person obtains high moral character by possessing many virtues. A person possesses a virtue by repeatedly practicing that virtue.

1. **Why is it usually difficult to assign moral responsibility for computer system failures to a particular individual? What are the implications for the organizations that create these systems?**

Because Moral responsibility is not exclusive, people cannot pass the buck by saying. It is implement causal responsibility.

1. **What is whistleblowing? What harms does it cause? What benefits does it provide? Why is whistleblowing rare?**

Whistleblowing occurs when an organization is involved in an activity that is fraudulent or a threat to public safety, and a member of that organization reveals information about this activity to someone outside the organization.

Harms of Whistleblowing: Whistleblowing usually ruins the career of the whistleblower and causes turmoil within the organization. The public relations damage caused the organization may harm it for years to come.

Possible benefits of Whistleblowing: Whistleblowing may keep people from being hurt, or it may prevent the public from being defrauded. Whistleblowing may discourage other companies from engaging in activities that defraud or harm the public.

**Whistleblowers are rare because it is a near suicidal vocation and everyone else is too scared to help. And if your Whistleblowing involves the world of war and spying, they will try to set you up on false charges… and not just sack you but destroy you.**

Chapter: 10

1. **Define the term “globalization” and explain how advances in information technology have stimulated globalization.**

**Globalization** refers to the process of creating a worldwide network of businesses and markets.

The rapidly decreasing cost of information technology has made globalization possible. The cost of computing is dropped by 99.99 percent between 1975 and 1995. The cost of an international telephone call from New York to London is dropped by 99 percent between 1930 and 1996. Companies have made extensive use of low-cost information technology to coordinate operations distributed around the planet.

1. **Describe recent events that provide evidence of globalization.**
* Globalization increases competition among multiple possible providers of the same product. Competition ensures that higher-quality products are sold at the best possible prices. Consumers get better prices when each area produces the goods or services it does best: corn in Kansas, automobiles in Ontario, semiconductors in Singapore, and so on. When prices are lower, the real purchasing power of consumers is higher. Hence, globalization increases everyone’s standard of living.
* People in poorer countries deserve jobs, too. When they gain employment, their prosperity increases.
* Every example in the past century of a poor country becoming more prosperous has been the result of that country producing goods for the world market rather than trying for self-sufficiency.
* Creating jobs around the world reduces unrest and leads to more stability. Countries with interdependent economies are less likely to go to war with each other.
1. **What is “the digital divide?” Describe the two fundamentally different dimensions of the digital divide.**

The **digital divide** refers to the situation where some people have access to modern information technology while others do not.

There are two fundamental of digital divide which are in the following:

* The **global divide** refers to the disparity in Internet access between more industrialized and less industrialized nations.
* The **social divide** refers to the difference in access between the rich and poor within a particular country.
1. **Describe the two models of technological diffusion and explain how technological optimists (and technological pessimists) to predict the future of “the digital divide” use them.**
* In the **normalization model** (Figure 10.10a), group A begins to adopt the technology first, followed by group B, and finally group C. However, at some point nearly everyone in all three groups is using the new technology.



* **Stratification model** (Figure 10.10b), the order of adoption is the same. However, in this model the eventual number of people in group C who adopt the technology is lower than the number of adoptees in group A. The percentage of people in group B who adopt the technology is somewhere between the levels of the other two groups.

Technological optimists believe the global adoption of information technology will follow the normalization model. Information technology will make the world a better place by reducing poverty in developing countries. Creating opportunities elsewhere will reduce the number of people trying to immigrate into the United States.

Technological pessimists believe information technology adoption will follow the stratification model, leading to a permanent condition of “haves” and “have nots.” Information technology will only exacerbate existing inequalities between rich and poor nations and between rich and poor people within each nation.