UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)

Academic Year 2017 – 3rd Year Examination – Semester 5

IT5105: Professional Issues in IT

10th June, 2017

(TWO HOUR)

To be completed by the candidate

BIT Examination Index No: .....

Important Instructions:

- The duration of the paper is **2 (two) hour**.
- The medium of instruction and questions is English.
- This paper has **4 questions** and **16 pages**.
- **Answer all questions.** All questions **do** carry similar marks.
- **Write your answers** in English using the space provided **in this question paper**.
- Do not tear off any part of this answer book.
- Under no circumstances may this book, used or unused, be removed from the Examination Hall by a candidate.
- Note that questions appear on both sides of the paper.
  If a page is not printed, please inform the supervisor immediately.

Questions Answered

Indicate by a cross (×), (e.g. [×]) the numbers of the questions answered.

	Question numbers				
To be completed by the candidate by marking a cross (×).	1	2	3	4	
To be completed by the examiners:					

Case Study

Google Collects Unprotected Wireless Network Information

Google's Street View maps allow users to zoom into a location on a map and view actual images of houses, shops, buildings, pavements, fields, parked cars and anything else that can be photographed from the vantage point of a slow-moving vehicle. Google gradually expanded to most U.S. cities and then to other cities around the world. In August 2009, Google began collecting data for Street View in several German cities. Germany, however, has stricter privacy laws than other countries, and prohibits the photographing of private property and people unless they are engaged in a public event, such as a sports event. As a result, Google had to work closely with the country's Data Protection Agency in order to comply with German laws in the hopes of getting its Street View service for Germany online by the end of 2010.

In April 2010, a startling admission by Google provoked public outrage in Germany and around the world. It resulted in government probes in numerous countries, as well as several class action lawsuits in the United States. In response to queries by Germany's Data Protection Agency, Google acknowledged on April 27 that, in addition to taking snapshots, its cars were also sniffing out unprotected wireless network information. Google reported, however, that it was only collecting service set identifier (SSID) data— such as the network name—and the media access control (MAC) address—the unique number given to wireless network devices. Google's geo-location services could use this data to more accurately pinpoint the location of a person utilizing a mobile device, such as a smartphone. The company insisted that it was not collecting or storing payload data (the actual data sent over the network).The German Federal Commissioner for the Data Protection Agency was horrified and requested that Google stop collecting data immediately. Additionally, the German authorities asked to audit the data Google had collected. Google agreed to hand over its code to a third party, the security consulting firm Stroz Friedberg. Nine days later there came another admission: Google had in fact been collecting and storing payload data. However, Google insisted that it had only collected fragmented data and made no use of this data. A few days later, Germany announced that it was launching a criminal investigation. Other European nations quickly opened investigations of their own. By early June, six class action lawsuits claiming that Google had violated federal wiretapping laws had been filed in the United States. In its defense, Google argued that collecting unencrypted payload data is not a violation of federal laws. Google explained that in order to locate wireless hotspots, it used a passive scanning technique, which had picked up payload data by mistake. The company used open source Kismet wireless scanning software that was customized by a Google engineer in 2006. Google insisted that the project's managers were unaware that the software had been programmed to collect payload data when they launched the project. Finally, Google argued that the data it collected was fragmented—not only was the car moving, but it was changing channels five times per second. However, a civil lawsuit claimed that Google filed a patent for its wireless network scanning system in November 2008 that revealed that Google's system could more accurately locate a router's location—giving Google the ability to identify the street address of the router. The more data collected by the scanning system, the lawsuit contended, the higher the confidence level Google would have in its calculated location of the wireless hotspot. In the fall of 2010, the U.S. Federal Trade Commission (FTC) ended its investigation, deciding not to take action or impose fines. The FTC recognized that Google had taken steps to amend the situation by ceasing to collect the payload data and hiring a new director of privacy. However by that time, 30 states had opened investigations into the matter. During the course of these and other investigations, Google turned over the data it had collected to external regulators. On October 22, the company announced that not all of the payload data it had collected was fragmentary. It had in fact collected entire email messages, URLs, and passwords. In November, the U.S. Federal Communications Commission announced that it was looking into whether Google had violated the federal Communications Act. Some analysts believe that Google's behavior follows a trend in the Internet industry: Push the boundaries of privacy issues; apologize, and then push again once the scandal dies down. If this is the case, Google will have to decide, as the possible fines and other penalties accrue, whether this strategy pays off.

Ref 2: Ethics in Information Technology George W. Reynolds Fourth Edition pages 133-134

Use the above case study to answer Question 1.

(1) (i) Individuals must reveal much of their personal financial data in order to take advantage of the wide range of financial products and services available, including credit cards, current and savings accounts, loans, payroll direct deposit, and brokerage accounts. To access many of these financial products and services, individuals must use a personal login name, password, account number, or PIN. The inadvertent loss or disclosure of this personal financial data carries a high risk of loss of privacy and potential financial loss. There are a number of federal laws in US that provide protection for personal financial data, Gramm–Leach–Bliley Act (GLBA) is one of them.

(a). Name the three rules that are included in GLBA.

(3 marks)

ANSWER IN THIS BOX

1.Financial Privacy Rule,

2.Safeguards Rule,

3.Pretexting Rule

Answer: Ref 2 - Pages 139,140

(b) Of the three rules, explain the rule that deals with collection and disclosure of personal financial information by financial organizations.

(10 marks)

ANSWER IN THIS BOX

Financial Privacy Rule—This rule **established mandatory guidelines** for the collection and disclosure of personal financial information by financial organizations. Under this provision, financial institutions **must provide a privacy notice to each consumer that explains what data** about the consumer is gathered, **with whom that data is shared**, **how the data is used**, and **how the data is protected**. The notice must also **explain the consumer's right to opt out—to refuse to give the institution the right to collect and share personal data with unaffiliated parties.** Anytime the privacy policy is changed, the consumer must be contacted again and given the right to opt out. The privacy notice **must be provided to the consumer at the time the consumer relationship is formed** and once **each year thereafter**. **Customers who take no action automatically opt in and give financial institutions the right to share personal data**, such as annual earnings, net worth, employers, personal investment information, loan amounts and Social Security numbers, to other financial institutions.

Ref 2 - Pages 139,140

(ii) European Union Data Protection Directive (1998) - The European Union Data Protection Directive requires any company doing business within the borders of 15 western European nations to implement a set of privacy directives on the fair and appropriate use of information. Basically, this directive requires member countries to ensure that data transferred to non–European Union (EU) countries is protected. It also bars the export of data to countries that do not have data privacy protection standards comparable to the EU's. Summarize the seven European data privacy principles.

(7 marks)

ANSWER IN THIS BOX

• Notice—Tell all customers what is done with their information.

• Choice—Give customers a way to opt out of marketing.

• Onward transfer—When data is transferred to suppliers or other business partners, companies must observe the notice and choice principles mentioned above and require all recipients of such data to provide at least the same level of protection for such data.

• Access—Give customers access to their information.

• Security—Protect customer information from unauthorized access.

• Data integrity—Ensure that information is accurate and relevant.

• Enforcement—independently enforces the privacy policy.

Answer: Ref 2 - Pages 150

(iii) The phrases & statements given in Column 1 & Column 2 are associated with security & privacy of personal data. Correctly match the contents of a cell in Column A with the contents of a cell in Column B.

(5 marks)

	Column 1		Column 2
A	Personal financial data	P	is an attempt to steal personal identity data by tricking users into entering information on a counterfeit Web site. Spoofed emails lead consumers to counterfeit Web sites designed to trick them into divulging personal data.
B	Identity Theft	Q	is keystroke-logging software downloaded to users' computers without the knowledge or consent of the user. It is often marketed as a spouse monitor, child monitor, or surveillance tool. This software creates a record of the keystrokes entered on the computer, enabling the capture of account usernames, passwords, credit card numbers, and other sensitive information.
C	Spyware	R	may include login name, password, account number, or PIN.
D	HIPAA	S	is 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.
E	Phishing	T	occurs when someone steals key pieces of personal information to impersonate a person. This information may include such data as name, address, date of birth, Social Security number/National ID, passport number, driver's license number, and mother's maiden name.

ANSWER IN THIS BOX

A & R,

B &T,

C & Q,

D & S,

E & P

Answer: Ref 2 – Page 150 (Personal financial data) , 155 (Identity Theft), 158 (Spyware), 140 (HIPAA), 158 (Phishing)

(2) (i) What are the key characteristics that distinguish professionals from other kinds of workers***?***

(3 marks)

ANSWER IN THIS BOX

1. they require advanced training and experience,

2. they must exercise discretion and judgment in the course of their work,

3. their work cannot be standardized.

Answer: Ref 2 - Page 40

(ii) Define what ethics mean.

(2 marks)

ANSWER IN THIS BOX

Definition of Ethics - ethics describes standards or codes of behaviour expected of an individual by a group (nation, organization, profession) to which an individual belongs.

Answer: Ref 2 - Page 4

(iii) Distinguish among Morals, Ethics & Law

(5 marks)

ANSWER IN THIS BOX

Morals: One's personal beliefs about right and wrong (1 mark)

Ethics: Standards or codes of behaviour expected of an individual by a group to which an individual belongs (nation, organization, profession) (2 marks)

Law: System of rules that tells us what we can and cannot do, Laws are enforced by a set of institutions (the police, courts, law-making bodies) (2 marks)

Answer: (Morals) Ref 2 - Page 4, (ethics) Ref 2 - Page 3, (Law) Ref 2 - Page 5

Consider the following description to answer part (iv).

ACM and the IEEE-CS in their code of ethics, in accordance with their commitment to the health, safety and welfare of the public, have stipulated that software engineers shall adhere to the following Eight Principles:

1. PUBLIC - Software engineers shall act consistently with the public interest.
2. CLIENT AND EMPLOYER - Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
3. PRODUCT - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
4. JUDGMENT - Software engineers shall maintain integrity and independence in their professional judgment.
5. MANAGEMENT - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
6. PROFESSION - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
7. COLLEAGUES - Software engineers shall be fair to and supportive of their colleagues.
8. SELF - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

(iv) There are many clauses under each principle. The following Column A contains some of the clauses of the ACM/IEEE-CS code of ethics. Correctly identify the Principle to which each clause belong to
and write the name of the Principle in Column B.

(6 marks)

Example 1 – PUBLIC

	Column A - Clauses	**Column B - Principle**
1.	Accept full responsibility for their own work.	PUBLIC
2.	Ensure adequate testing, debugging, and review of software and related documents on which they work.	
3.	Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.	
4.	Offer fair and just remuneration.	
5.	Not promote their own interest at the expense of the profession, client or employer.	
6.	Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.	
7.	Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.	

ANSWER IN THIS BOX

	Column A - Clauses	Column B - Principle
1.	Accept full responsibility for their own work.	PUBLIC
2.	Ensure adequate testing, debugging, and review of software and related documents on which they work.	PRODUCT
3.	Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.	PUBLIC
4.	Offer fair and just remuneration.	MANAGEMENT
5.	Not promote their own interest at the expense of the profession, client or employer.	PROFESSION
6.	Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.	SELF
7.	Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.	CLIENT AND EMPLOYER

Answer: Ref 2 – Pages 447 - 451

(v). Organizations have five good reasons for creating an environment that encourages employees to act ethically. Name these 5 reasons.

(5 marks)

ANSWER IN THIS BOX

(1) to gain the goodwill of the community,

(2) to create an organization that operates consistently,

(3) to foster good business practices,

(4) to protect the organization and its employees from legal action, and

(5) to avoid unfavorable publicity

(or any other acceptable answer.)

Answer: Ref 2 – Page 7

(vi) Philosophers have developed many approaches to ethical decision making. Four common philosophies are the virtue ethics approach, the utilitarian approach, the fairness approach, and the common good approach. Describe the basis of the Common good approach and outline its problems.

(4 marks)

ANSWER IN THIS BOX

The Common good approach is based on the two principles of working together for common

set of values and goals and implementing systems that benefit all people. (2 marks)

Problems associated with it are: Consensus is difficult and Some people are required to bear

greater costs than others.(2 marks)

Answer Ref 2 – Page 21

(3) (i) What does discrimination mean?

(2 marks)

ANSWER IN THIS BOX

Discrimination means treating one person or one group of people less/more favourably than another

on the grounds of personal characteristics.

Answer: Ref 3 - Page 136

(ii) Name six factors on which people can be discriminated upon?

(3 marks)

ANSWER IN THIS BOX

Any 6 of the following:

Race, color, national origin, ancestry, sex, sexual orientation, gender/sexual identity or

expression, marital status, creed, religion, age, disability, veteran's status, or political ideology.

Answer: Ref 3 - Page 136

(iii) What would you describe as harassment at workplace?

(2 marks)

ANSWER IN THIS BOX

In the workplace, harassment involves persistent attacks or abuse and can range from shouting

to racial slurs to crank calling (or any other acceptable answer)

Answer: Lecture Notes VLE

(iv) What are some of the key ethical issues associated with the use of social networking Web sites?

(2 marks)

ANSWER IN THIS BOX

Cyberbullying, Cyberstalking, Sexual predators, Uploading inappropriate material (or any other

acceptable answer.)

Answer: Ref 2 – Pages 364 – 369

(v) How do social network web sites help in advertising? Name 5 different advertising strategies used in the social network web sites.

(7 marks)

ANSWER IN THIS BOX

Social network advertising enables advertisers to generate a conversation with viewers of their ads and to target ads to reach people with the desired demographic characteristics.

There are several social network advertising strategies, including

1) direct advertising,

2) advertising using an individual's network of friends,

3).indirect advertising through social networking groups,

4).advertising via company-owned social networking Web sites, and

5). viral marketing

(or any other acceptable answer)

Answer: Ref 2 – Page 358

(vi) Name 4 factors that have caused a dramatic increase in the number, variety and impact of security incidents in computer systems.

(4 marks)

ANSWER IN THIS BOX

Increasing complexity, higher computer user expectations, expanding and changing systems, and increased reliance on software with known vulnerabilities have caused a dramatic increase in the number, variety and impact of security incidents (***or any other acceptable answer.)***

Answer: Ref 2 - Page 86

(vii) What is the key to prevent a computer security incident?

(2 marks)

ANSWER IN THIS BOX

The key to prevention of a computer security incident is to implement a layered security solution to make computer break-ins so difficult that an attacker eventually gives up,

(or any other acceptable answer)

Answer: Ref 2 – Page 107

(viii) What actions must be taken in response to a security incident?

(3 marks)

ANSWER IN THIS BOX

If an intrusion occurs, there must be a clear reaction plan that addresses notification, evidence protection, activity log maintenance, containment, eradication, and recovery,

(or any other acceptable answer)

Answer: Ref 2 – Page 103

(4) (i) What is meant by the digital divide?

(2 marks)

ANSWER IN THIS BOX

Digital divide is the gap between those who have ("information haves") and those who do not have ("information have-nots") computers and access to cybertechnology.

Answer: Ref 1 – Page 304

(ii) Identify five initiatives that have been developed to make web content more accessible by disabled people.

(5 marks)

ANSWER IN THIS BOX

a). Web applications that include more graphics and images that can serve as universal symbols (can be used by persons who cannot read English too).

b). Software used in speech synthesizers and screen magnifiers that will benefit people with visual, hearing, physical, cognitive, and neurological disabilities.

c). Web browsers and other types of software that retrieve and render Web content.

d). Agents designed to conform and communicate with other technologies, especially "assistive technologies "such as screen readers (which perform a function similar to Braille applications in offline contexts).

e). Voice-recognition technology designed to assist disabled persons who are unable to use keyboards will ultimately also benefit nondisabled persons with low literacy skills.

Answer: Ref 1 – Page 310-312

(iii) How has cybertechnology transformed the nature of work especially with regard to job displacement?

(4 marks)

ANSWER IN THIS BOX

a) Job displacement is often associated with automation. (1 mark)

b) Developments in robotics have also caused job displacement. Robots, equipped with motor abilities that enable them to manipulate objects can be programmed to perform tasks that are either routine or mundane for humans or considered hazardous to humans. (2 marks)

c) Sophisticated programs called expert systems threaten many professional jobs.(1 mark)

Answer: Ref 1 – Page 325

(iv) Many organizations offer telework or remote work opportunities to their employees. Outline 5 advantages and 5 disadvantages of teleworking for organizations.

(10 marks)

ANSWER IN THIS BOX

Answer (any 5 from the 2 columns)

Advantages	Disadvantages
1. As more employees telework, there is less need for office and parking space; this can lead to lower costs.	1. Allowing teleworkers to access organizational data and systems from remote sites creates potential security issues.
2. Allowing employees to telework can improve morale and reduce turnover.	2. Informal, spontaneous meetings become more difficult if not impossible.
3. Telework allows for the continuity of business operations in the event of a local or national disaster.	3. Managers may have a harder time monitoring the quality and quantity of the work performed by teleworkers, wondering, for instance, if they really "put in a full day".
4. The opportunity to telework can be seen as an additional perk that can help in recruiting.	4. Increased planning is required by managers to accommodate and include teleworkers.
5. There may be an actual gain in worker Productivity.	5. There are additional costs associated with providing equipment, services and support for people who work away from the office.
6. Telework can decrease an organization's carbon footprint by reducing daily commuting.	6. Telework increases the potential for lost or stolen Equipment.

Answer: ***Ref 2 – Page 322***

(v) Outline the differences between "white hat" and "black hat" hackers.

(4 marks)

ANSWER IN THIS BOX

- Black-hat hackers, violate computer security for personal gain (such as stealing credit card numbers or harvesting personal data for sale to identity thieves)
- For pure maliciousness (such as creating a botnet and using that botnet to perform DDOS attacks against websites they do not like.)
- Black hats fit the widely-held stereotype that hackers are criminals performing illegal activities for personal gain and attacking others. They are the computer criminals.
- **W**hite-hat hackers are the opposite of the black-hat hackers. They are the "ethical hackers," experts in compromising computer security systems who use their abilities for good, ethical and legal purposes rather than bad, unethical and criminal purposes.

Answer: Ref 2 - Pages 125-126

****