



UNIVERSITY OF TECHNOLOGY SYDNEY

(32557) ENABLING ENTERPRISE INFORMATION SYSTEMS

---

# **Ethics, Privacy and Information security**

---

*by Team Super*

Seoyoon Kim (25388442) [Group leader]

Jin Lee (25388733)

Ariel Manueke (25207919)

Nonthawat Praisompong (25233750)

March 15, 2024

## Contents

<b>1</b>	<b>Question 1</b>	<b>1</b>
1.1	Ethical approaches with scenarios . . . . .	1
1.1.1	Scenario 1: The Rights Approach . . . . .	1
1.1.2	Scenario 2: The Utilitarian Approach . . . . .	1
<b>2</b>	<b>Question 2</b>	<b>3</b>
2.1	The ACS Code of Professional Ethics, Conduct and Complaints . . . . .	3
<b>3</b>	<b>Question 3</b>	<b>4</b>
3.1	Understanding and Preventing Phishing Attacks . . . . .	4
<b>4</b>	<b>Question 4</b>	<b>5</b>
4.1	How Scammers Infiltrate Our Precious Data . . . . .	5
4.1.1	Impersonation Scams . . . . .	5
4.1.2	Product and Service Scams . . . . .	5
4.2	How To Realise New Scammers' Tricks is Crucial . . . . .	5

## **1 Question 1**

### **1.1 Ethical approaches with scenarios**

#### **1.1.1 Scenario 1: The Rights Approach**

In our view, under the rights approach, monitoring internet browsing by supervisors is ethically contentious because it infringes on an individual's right to privacy. While employers may have legitimate interests in ensuring productive use of work time and protecting company assets, these interests must be balanced against employee's rights.

For example, if your company only monitors websites accessed using company equipment to ensure that employees do not visit harmful or inappropriate content that could threaten company security, and this is clearly communicated and agreed to by employees, the monitoring may be considered ethical under the rights approach. Furthermore, if the monitoring is explicitly stated in the employment contract, the employee was provided with information about the kind of monitoring, why it is necessary, and how the information collected will be used, and the employee agreed to work under these conditions, then it would be ethical. However, if a supervisor tracks an employee's personal email or social media activity without a policy or notice, it violates the employee's right to privacy and is clearly unethical because such monitoring violates an individual's rights without informed consent.

Therefore, from the perspective of rights approach, the ethics of monitoring internet browsing by managers should be based on the rights of employees, especially privacy and informed consent. The importance of respecting rights and ethical business practices, as emphasized in "Business Ethics: A Stakeholder and Issues Management Approach" requires a nuanced approach to managing stakeholder interests while respecting individual rights (Weiss, 2014). This monitoring must be respected and transparent, and employers must find the proper balance between legitimate business interests and protecting employees' fundamental rights.

#### **1.1.2 Scenario 2: The Utilitarian Approach**

Utilitarianism emphasizes the maximization of overall happiness and satisfaction resulting from actions. According to this ethical philosophy, the design of information systems should aim to exert a positive influence on as many individuals as possible. Consider a scenario in which a system preferentially displays male candidates over female ones to enhance recruitment efficiency. Although this might initially increase the company's productivity through faster hiring processes, it would likely exacerbate gender-based discrimination in the long term, thereby intensifying societal inequalities and detracting from widespread happiness.

Moreover, within the IT industry, a recruitment system that prioritizes white applicants over Black applicants can deepen existing racial disparities, undermining diversity and innovation and causing detrimental long-term effects on both the company and society at large. From a utilitarian perspective, such a system would negatively impact the well-being of the majority, and therefore, the design requirements of this information system would be deemed unfavorable.

The “Ethics in Information Technology” explores the application of utilitarian principles in the realm of technological decision-making that has implications for individuals and society. He argues that the utilitarian approach necessitates a comprehensive assessment of the overall outcomes of these decisions and their impact on the well-being of all stakeholders involved (Reynolds, 2018). Similarly, the “The Handbook of Information and Computer Ethics”, highlights the necessity of assessing the wide-reaching societal impacts of technological choices, advocating for a thorough evaluation that considers long-term societal welfare (Himma and Tavani, 2008).

In conclusion, aligning with utilitarian ethics, the design of information systems should extend beyond short-term efficiency gains and consider the long-term consequences for society. By avoiding discrimination and offering equal opportunities to all candidates, such designs are expected to promote collective well-being and support the creation of an equitable and innovative community.

## **2 Question 2**

### **2.1 The ACS Code of Professional Ethics, Conduct and Complaints**

ACS has three fundamental values in its professional ethics code in its latest publication (Australian Computer Society, 2023). First is honesty, to create a healthy work environment where members need to have open and honest personalities, including holding the truth, not purposely distorting facts, and keeping silent when any misconduct occurs regarding their employers and position. The second value is trustworthiness, upholding dignity as an ICT professional, including having responsibility regarding results, practicing integrity, learning proactively, maintaining company secrets, good communication, know knowing your limits in authority. Last is respect, which aims to support a safe working environment. Members have respect for others, including respect, support, and treat everyone equally regarding their personal, work, and intellectual property rights. Members also have to respect their profession, including having and sharing knowledge in their field, encouraging and supporting other ICT professionals, and contributing to enhancing and advancing the development of information technology.

- **Path:** Home/Menu/ACS/Ethics-Conduct\_Education\_&\_Complaints/Professional\_Ethic, Conduct\_&\_Complaints
- **Word Count:** 150

### **3 Question 3**

#### **3.1 Understanding and Preventing Phishing Attacks**

This video explains phishing, a sophisticated cyberattack aimed at stealing user data through deceptive social engineering tactics. It vividly illustrates the attack with a compelling example of a fake email, supposedly from the U.S. Department of Justice, showing how attackers meticulously create a sense of urgency to compromise personal information. Phishing often involves clever impersonation of authoritative figures or major brands, and exploiting current events to deceive users effectively. The consequences include significant financial loss and identity theft. To guard against phishing, the video strongly recommends vigilance, manual entry of web addresses, not sharing personal details online, and using secure email gateways. It stresses the importance of contacting authorities and securing accounts if attacked, highlighting awareness and prevention as key defenses against these scams.

For a detailed exploration of phishing scams and prevention techniques, refer to the following video resource:

- **Title:** How To Recognize and Avoid Phishing Scams — Explained - YouTube
- **Video Length:** 8:54
- **URL:** <https://www.youtube.com/watch?v=Yz0PnAkeRiI>
- **Word count:** 99

## **4 Question 4**

### **4.1 How Scammers Infiltrate Our Precious Data**

According to the Australian Competition & Consumer Commission (2023), the scammer has devised a new trick or storytelling for stealing personal information. Scammers improve their capability to exploit benefits from technology, products, services, and occurring events to deceive victims into believing that they are real (Australian Competition and Consumer Commission, 2023). In this assignment, we consider impersonation and product and service scams as a discussion topic.

#### **4.1.1 Impersonation Scams**

The scammers develop new methods for deceiving victims that the trusted organisations contact, such as police, banks, and well-known businesses, including the government, and disguise as a victim's relative or family member (Australian Competition and Consumer Commission, 2023). Scammers trick you with different mediums, such as email or messages designed for victims to easily give them precious information (Australian Competition and Consumer Commission, 2023). Moreover, scammers adopt technology to disguise their calls and messages as they come from legitimate phone numbers.

#### **4.1.2 Product and Service Scams**

Scammers pretend to be buyers or sellers by using fake websites or verifying retailers to offer products and services that cannot be real (Australian Competition and Consumer Commission, 2023). Furthermore, they trick victims into using logos of reliable sources such as the Australian Business Number (ABN), which are difficult to check (Australian Competition and Consumer Commission, 2023). Also, sending fake invoices or bills confuses victims, in the worst case, they end up paying for scammer bills instead of real ones

### **4.2 How To Realise New Scammers' Tricks is Crucial**

Based on the advancement of privacy, only the data owner can access data such as bank accounts and credit card numbers, including personal details. Scammer always develops new methods to deceive customers that they are staff from reliable companies. When customers permit them only once, scammers will access and exploit personal data, which causes unbelievable disadvantages to victims without consent.

## References

Australian Competition and Consumer Commission (2023). The little black book of scams.  
<https://www.accc.gov.au/about-us/publications/the-little-black-book-of-scams>

Australian Computer Society (2023). *ACS Code of Professional Ethics*.  
<https://www.acs.org.au/memberships/professional-ethics-conduct-and-complaints.html>

Himma, K. E. and Tavani, H. T. (2008). *The Handbook of Information and Computer Ethics* John Wiley Sons, Inc.  
[https://search.lib.uts.edu.au/permalink/61UTS\\_INST/1v2k6o8/alma991006728260405671](https://search.lib.uts.edu.au/permalink/61UTS_INST/1v2k6o8/alma991006728260405671)

Reynolds, G. (2018). *Ethics in Information Technology (6th ed)*. Cengage Learning.  
[https://search.lib.uts.edu.au/permalink/61UTS\\_INST/19joism/alma991006933969805671](https://search.lib.uts.edu.au/permalink/61UTS_INST/19joism/alma991006933969805671)

Weiss, J. W. (2014). *Business ethics: A stakeholder and issues management approach (6th ed)*. Berrett-Koehler Publishers, Inc.  
[https://search.lib.uts.edu.au/permalink/61UTS\\_INST/1v2k6o8/alma991006740178305671](https://search.lib.uts.edu.au/permalink/61UTS_INST/1v2k6o8/alma991006740178305671)