Chapter 25 Ethics and Impact of Computing

Content

Annex 1 – CODE OF CONDUCT

Syllabus Learning Outcomes

3.4 Social, Ethical, Legal and Economic Issues

Understand the importance of ethics in the conduct of Computing professionals and the impact of Computing in different real-life situations.

3.4.1 Understand the code of ethics (conduct) of a Computing professional. 3.4.2 Describe the impact of computing on lifestyle and workplace for social and economic developments.

3.4.3 Discuss the social, ethical, legal and economic issues of computing and technology.

1 Ethics

Ethics is a set of rules of behaviour based on ideas of what is morally good and bad and what is morally right and wrong. Every society has its rules about whether certain issues are ethical or not. As the use of computers becomes more widespread in every aspect of our lives, discussions in computer ethics have reached a somewhat common consensus.

The consensus can be represented in the Ten Commandments of Computing Ethics: 1) Thou shalt not use a computer to harm other people.
2) Thou shalt not interfere with other people's computer work
3) Thou shalt not snoop around in other people's files
4) Thou shalt not use a computer to steal
5) Thou shalt not use a computer to bear false witness
6) Thou shalt not use or copy software for which you have not paid
7) Thou shalt not use other people's computer resources without authorization 8) Thou shalt not appropriate other people's intellectual output
9) Thou shalt think about the social consequences of the program you write 10) Thou shall use a computer in ways that show consideration and respect

For a more detailed explanation of each of the ten commandments, please visit: https://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics
https://www.youtube.com/watch?v=ASm-2t31Ptg

2 The Professionalism of Computing Professionals

Computing professionals includes hardware designers, software engineers, database administrators, system analysts, and computer scientists. Today, with more adaptations of technology into our daily life, the scope of computing professionals also increase. No matter

what their particular specialisation is, any professional person is expected to act ethically.

In Singapore, the Singapore Computing Society (SCS) has a code of conduct that gives guidance under four rules:

- act at all times with **integrity**
- accept **full responsibility** for their work
- always aim to increase their **competence**
- act with **professionalism** to enhance the prestige of the profession and the Society

For more details, refer to Annex 1

3 Ethical Issues

Ethical issues involve examining the moral dilemmas and ethical considerations arising from the use of computing and technology such as data privacy and security, surveillance, intellectual property rights (e.g., copyright, patents), digital rights management, ethical considerations in artificial intelligence and machine learning algorithms, and the ethical implications of emerging technologies like biometrics and autonomous systems.

Example: Use of Facial Recognition Technology for Surveillance

Facial recognition technology has advanced significantly in recent years and is increasingly being deployed for various purposes, including surveillance by governments, law enforcement agencies, and private companies. While facial recognition offers potential benefits such as enhanced security and convenience, its widespread use raises serious ethical concerns regarding privacy and civil liberties. There are fears that unchecked surveillance through facial recognition systems could erode individuals' right to privacy and lead to too much surveillance. Moreover, there are concerns about the accuracy and bias of facial recognition algorithms, particularly regarding their disproportionate misidentification of individuals from minority groups. Ethical considerations must be carefully weighed against the potential benefits of facial recognition technology, and robust regulatory frameworks are needed to ensure its responsible and ethical use.

4 Legal Issues

Legal issues are issues where a law has been passed by a government. While you are not expected to learn the details of all the Acts listed, you may be asked to consider the issues in the legal context.

One thing to note is that as technology develops rapidly, laws often become outdated rapidly. Many acts are introduced/amended in response to current events. For example, the Electronic Transactions Act was recently amended in 2021. The new Copyright Act which was passed in Parliament in September 2021, came into force on 21 November 2021.

You may find the summary of regulations on the IMDA's website:
https://www.imda.gov.sg/Regulations-and-Licences/Regulations

● **Personal Data Protection Act**

This has been discussed in Chapter 24 Data Management.

● **Copyright Act**

The Copyright Act strengthens creators' and performers' rights by granting default ownership of certain commissioned works to creators and performers, unless stated otherwise in the contract. Additionally, it mandates clear identification of creators or performers when using or distributing their works in public, including on online platforms. The Act also introduces exceptions to copyright owners' rights, allowing lawful use of copyrighted works for computational data analysis and educational purposes without seeking explicit permission, as long as proper attribution is

provided. These changes aim to balance the interests of creators and the public, fostering innovation, education, and recognition in the digital age.
More details can be found at
https://www.ipos.gov.sg/news/press-releases/ViewDetails/commencement-of-the-copyright-act

/ ● **Computer Misuse Act**

The Computer Misuse Act aims to protect computer material against unauthorized access or modification and prevent abuse of the national digital identity service. It defines various terms related to computer usage, such as "computer," "damage," "data," and "program," and outlines what constitutes unauthorized access or modification of computer material. The Act prohibits unauthorized interception of computer functions and provides penalties for such offenses. Additionally, it establishes provisions for securing access to computer programs or data and specifies circumstances under which access is considered unauthorized.
More details can be found at
https://sso.agc.gov.sg/Act/CMA1993

● **Cybersecurity Act**

The Cybersecurity Act establishes a comprehensive legal framework to enhance national cybersecurity in Singapore. It aims to achieve four key objectives: strengthening the protection of Critical Information Infrastructure (CII) against cyber-attacks by designating sectors and clarifying obligations for CII owners; authorizing the Cyber Security Agency (CSA) to prevent and respond to cybersecurity threats and incidents; establishing a framework for sharing

cybersecurity information to enhance prevention and response capabilities; and implementing a light-touch licensing framework for cybersecurity service providers, initially focusing on penetration testing and managed security operations center (SOC) monitoring to ensure the security of sensitive information and foster a robust cybersecurity ecosystem.

More details can be found at
https://www.csa.gov.sg/Legislation/Cybersecurity-Act

Example: Compliance with Personal Data Protection Act (PDPA)

The PDPA is a comprehensive data protection law enacted in Singapore to safeguard the privacy and personal data. It imposes strict requirements on organizations regarding the collection, processing, and storage of personal data, as well as the rights of individuals over their data. Non compliance with PDPA can result in severe financial penalties for organizations, highlighting the importance of legal compliance in the digital age. To adhere to PDPA regulations, organisations must implement robust data protection measures, obtain explicit consent from individuals for data processing activities, provide transparency about data practices, and ensure the security and integrity of personal data. Compliance with PDPA not only mitigates legal risks but also fosters trust and confidence among consumers regarding the handling of their personal information.

5 Social Issues

Social issues are factors that influence the beliefs attitudes and actions of people within society. There are elements of computer use that have a cultural impact in that they can change our attitudes, beliefs, and actions.

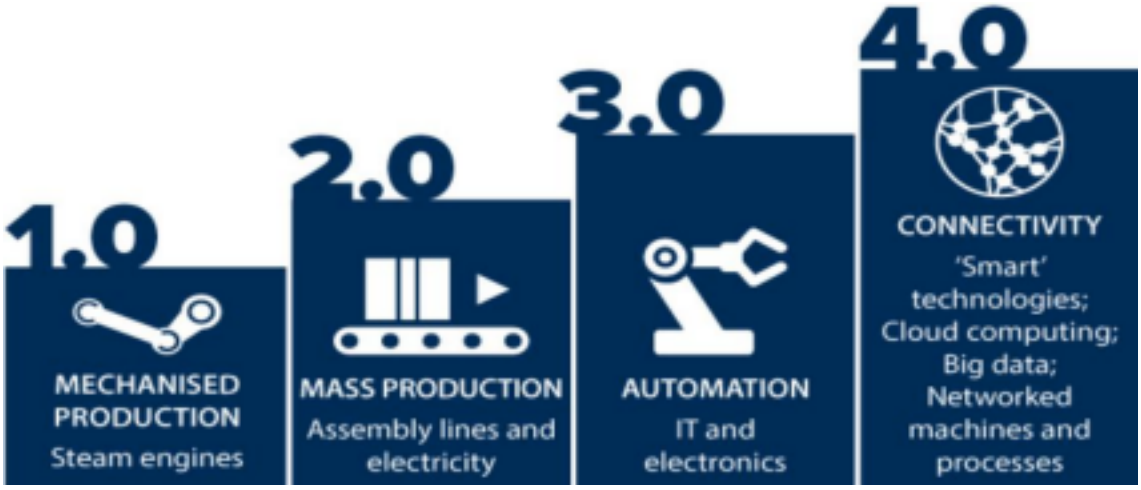
Topics under this category might include the impact of social media on communication patterns, the digital divide (inequality in access to technology), online communities, privacy concerns in social networks, and the effects of technology on mental health and well-being.

Example: Impact of Social Media on Mental Health

Social media platforms like Facebook, Instagram, and Twitter have become integral parts of modern society, enabling people to connect and share information instantaneously. However, there is growing concern about the negative impact of excessive social media use on mental health. Research suggests that constant exposure to curated images and unrealistic standards of beauty on platforms like Instagram can contribute to feelings of inadequacy and low self esteem, particularly among young users. Moreover, the addictive nature of social media, characterized by endless scrolling and seeking validation through likes and comments, can lead to anxiety and depression. Additionally, cyberbullying and online harassment are prevalent issues that can have severe consequences on the mental well-being of individuals. Therefore, it is crucial to consider strategies for promoting healthier online behaviours and fostering positive digital experiences to mitigate these negative social impacts.

6 Economic Issues

Modern industry has seen great advances since its earliest iteration at the beginning of the industrial revolution in the 18th century. This has changed the pace of the economic growth of many countries. On the individual level, it creates many different jobs.



5

VJC/H2Computing/9569

The First Industrial Revolution used water and steam power to mechanise production. The Second used electric power to create mass production. The Third used electronics and information technology to automate production. Now a Fourth Industrial Revolution is building on the Third, the digital revolution that has been occurring since the middle of the last century. It is characterised by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.

To find out more: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution what-it-means-and-how-to-respond/

With the advancement of computer and technology, economica issues may arise involving the role of technology in shaping economic sectors (e.g., e-commerce, digital marketing), job displacement and automation, the digital economy, economic inequalities exacerbated by technological advancements, the economics of software development and licensing, and the economic benefits and costs of implementing new technologies.

Example: Automation's Impact on Employment in the Retail Sector

The widespread adoption of automation technologies, such as robotics, artificial intelligence, and machine learning, has led to concerns about job displacement and the future of work. While automation can increase efficiency, productivity, and economic growth, it also has the potential to disrupt labour markets and displace workers in certain industries, particularly those involving routine and repetitive tasks. This phenomenon has sparked debates about the need for reskilling and upskilling programs to prepare workers for jobs in emerging fields, the role of government policies in mitigating the negative impacts of automation on employment, and the potential for

income inequality to widen as a result of technological advancements.

7 AI Ethics & Governance (Enrichment for now…)

The rapid advances in AI tools and technologies, and the increasing deployment and embedding of such tools in apps or solutions push the need for a Body of Knowledge (BoK).

It is, therefore, vital to building stakeholder confidence in AI. That can happen if solution providers and deploying organisations ensure the responsible use of AI to manage different risks in AI deployment.

Moreover, such organisations will also have to take measures to align internal policies, structures and processes with relevant accountability-based practices in data management and protection

The Body of Knowledge (BoK) is based on the Infocomm Media Development Authority's (IMDA) Model AI Governance Framework and it is tailored for practical issues related to human safety, fairness and the prevailing approaches to privacy, data governance and general ethical values.

Through this initiative, the AI Ethics and Governance Toolkit has been formulated. It provides an overview of AI governance issues and explores a risk-based approach to deploying AI. This Toolkit can be immensely useful for tech and non-tech professionals to understand the ethical issues surrounding AI.

For access to the Toolkit, please view

https://files-scs-prod.s3-ap-southeast 1.amazonaws.com/public/uploads/200721016+SCS+Booklet+6+Nov.pdf

For more information on BoK, please visit
- https://www.scs.org.sg/ai-ethics-bok
- https://ai-ethics-bok.scs.org.sg/

8 Conclusion

Ultimately, it is undeniable that advances in computing and technology have impacted our lives greatly and are here to stay for the foreseeable future. It brings along with its benefits as well as risks. What matters is that we must learn to embrace the limitless possibilities that it brings and learn to manage the risks.

Annex 1 – CODE OF CONDUCT

https://www.scs.org.sg/membership/code-of-conduct

SCS members will:
- act at all times with **integrity**
- accept full **responsibility** for their work
- always aim to increase their **competence**
- act with **professionalism** to enhance the prestige of the profession and the Society

Integrity

SCS members will act at all times with integrity. They will:
- not lay claim to a level of competence that they do not possess
- act with complete discretion when entrusted with confidential information ● be impartial when giving advice and will disclose any relevant personal interests ● give credit for work done by others where credit is due

Full Responsibility

SCS members will accept full responsibility for their work. They will:
- carry out their assignments in a professional manner
- adhere to their employers' or client's standards and guidelines

- indicate to their employers or clients the consequences to be expected if their professional judgement is overruled

Competence

SCS members will always aim to increase their competence. They will:

- continue to upgrade their knowledge and skills, and be aware of relevant development in the technology they are involved in
- provide opportunity and encouragement for professional development and advancement to fellow professionals and aspirants to the profession
- extend public knowledge, understanding and appreciation of information technology and to oppose false or deceptive statements related to information technology of which they are aware

Professionalism

SCS members will act with professionalism to enhance the prestige of the profession and the Society. They will:

- uphold and improve the professional standards of the Society through participation in their formulation, establishment and enforcement
- not seek personal advantage to the detriment of the Society
- not speak on behalf of the Society without proper authority
- not slander the professional reputation of any other person
- use their special knowledge and skill for the advancement of human welfare