Course: Professional Issues in Information Technology

Week 6: Ethical Dilemmas (PAPA)

Lecturer: Martha Gichuki

Lecture learning outcomes

At the end of this lecture, the learner should be able to:

1. Define Ethical Dilemma
2. Describe the aspects of Ethical dilemmas: - Privacy, Accuracy, Property, Access (PAPA)
3. Identify a process for analyzing ethical dilemmas
4. Describe Transborder Data Flows

1.1 Introduction to Ethical Dilemmas (PAPA)

1.1.1 **Privacy**

- ✓ Issues to do with disclosure about a person and their interactions.
- ✓ Important privacy issues include: - data breaches, electronic discovery, consumer profiling, workplace monitoring, and advanced surveillance technology.[1]
- ✓ The common good may push towards using information to uncover socially and economically damaging situations e.g. data stores that indicate criminal activities.
- ✓ ***Dilemma - Solve conflict of privacy and accessibility***
- ✓ In the United States privacy law, the control of one's personal data a property right.
- ✓ Individuals can voluntarily transfer or sell their property rights to a firm interested in its use or even to government, as long as they deem the terms and conditions to be fair.[2]
- ✓ The European approach is different and treats individuals' data as a liberty right that cannot be given up, even voluntarily.[3]

[1] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 151
[2] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 361
[3] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 148

1.1.2 Accuracy

- ✓ Issues to do with achieving informational accuracy.
- ✓ Automation of systems (speed) at the expense of occasional errors.
- ✓ Manual systems are also prone to human error
- ✓ Example - erroneous credit authorization causing economic damage
- ✓ Example - a billing software error generating high bills leading to disconnection of amenities causing social/economic damage.
- ✓ ***Dilemma – conflict of automation and systems failure/error***

1.1.3 Property

- ✓ Question of ownership of information and its communication channels.
- ✓ Organizations store data and information about their interactions with others e.g. customers, suppliers, employees etc.
- ✓ ***Dilemma - who has the rights of information ownership and how can communal ownership be mediated in a morally just way?***

1.1.4 Access

- ✓ Issues to do with ability to access Information and Communications Technology (ICT)
- ✓ **Digital divide –** describes the gap between those who can access ICT e.g. smartphones, personal computers, and the Internet and those who cannot.
- ✓ This gap must be bridged since people need to use the information provided by the Internet to manage their careers, retirement, health, and safety.
- ✓ Clearly, health, crime, and other emergencies could be resolved more quickly if people in trouble had easy access to a communications network.[4]
- ✓ Access to ICT enhances learning and provides educational and economic opportunities.
- ✓ ***Dilemma – How do we bridge the digital divide gap?***

These dilemmas call for the establishment of a Corporate Code of conduct or code of ethics

- ✓ A code of ethics is a statement that highlights an organization's key ethical issues, stating the important values and principles to the organization.

[4] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 306

- ✓ A formal, written statement about the organization mission, values, and employee behavioural guiding principles.[5]
- ✓ An organization's code of ethics is meant for all employees; managers, directors, officers etc. and it focuses on ethical areas related to their role in the organization.
- ✓ It offers employees guidance on ethical issues, provides mechanisms for reporting unethical conduct to foster a culture of honesty and accountability within the organization.[6]
- ✓ An effective code of ethics ensures that employees abide by the law, follow necessary regulations, and behave ethically at all times.[7]

2.1 Ethical Issues affecting Data Transfers

2.1.1 Transborder Data Flows (TBDF)

- ✓ These occur when a **computer in one country is accessed by, or transmits data to, a computer in another country.** Transfer of computerized data across national borders.
- ✓ As data is transferred, it is **stored and processed outside the originating country**.
- ✓ Ideally, TBDFs need strong regulation, but, since many countries' economies are supported by TBDFs, local legislation prohibiting information access may be by-passed.

Type of data transmitted in TBDFs

The type of information transmitted determines the rules applied to TBDF.

a) **Personal Data**

- ✓ This is the **most sensitive type of data** and it includes **plane reservations, medical or criminal records, and credit card billings.**
- ✓ Individuals are concerned about the erosion of privacy of data concerning their health for fear of intrusions into their health by employers, schools, insurance firms, law enforcement agencies, and even marketing firms looking to promote their products and services.[8]
- ✓ Most countries enforce some protection against unauthorized processing of sensitive personal data.

[5] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 15

[6] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 15

[7] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 15

[8] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 138

b) **Business Data**

- ✓ This data allows financial and **business transactions to be conducted and contracts to be executed**.
- ✓ This is a major source of profit and governments need to regulate them since they tax these profits or to protect domestic industries.[9]
- ✓ Example - banking community has created the **Society for Worldwide Interbank Financial Telecommunications (SWIFT)** which provides **Electronic Fund Transfer (EFT)** services through a steadily expanding network of systems.

c) **Technical Data**

- ✓ Technical or scientific data includes **weather forecasting, geological exploration, market research, product specifications and experimental results**.
- ✓ This information has both economic and strategic importance, and is usually central to any transfer of technology arrangement.
- ✓ Some of this information is now gathered by remote **sensing satellites**.

d) **Organizational Data**

- ✓ Organizational data is sometimes called "**operational data**" as it relates to the administrative functions or decisions of organizations, usually between **a corporation and its subsidiaries, foreign distributors, or licensees.**
- ✓ These are regulated for not only the protection of personnel records and their personal information, but also for political or economic reasons.

2.1.2 Types of Data Flows

I. **One-Way Flows**:

- ✓ These flows either consolidates information (E.g. the headquarters in country B gathers all information from subsidiary offices such as that in country A.) or distributes information, where a centralized operation distributes data to several subsidiary organizations from sources in other countries.

II. **Two-Way Flows**:

- ✓ Two-way transfers of data occur for two reasons: lack of processing capacity in the home country; or, where databases are shared internationally (such as a credit reporting agency).

[9] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 135

2.1.3 Why the need for regulation?

i. **Privacy**

- ✓ ICT has enabled collection and storage of personal information that can easily be transferred within and between countries causing concern its usage and effects on individual. This has led to many countries to ***passing privacy legislation to protect the privacy of their people.***[10]

ii. **Security**

- ✓ Many countries have introduced legislation to ensure that *national security is not threatened by excessive reliance on and use of TBDFs.*
- ✓ National data stored and processed outside the country may bring the fear that data may become inaccessible in a time of political confrontation.

iii. **Sovereignty of nations**

- ✓ This is a nation's ***ability to protect its political autonomy and cultural integrity*****.**
- ✓ Nations may feel the threat of data moving via communications technology, outside the state and becoming a target of espionage which is a sovereignty threat.

iv. **Economies of nations**

- ✓ Data-processing operations can have significant economic consequences for nations
- ✓ These operations could create high paying technical jobs in the data-processing countries.
- ✓ TBDFs are national economic indicators since the show the balance between trade and employment. Creating barriers to TBDFs is a driving force as nations pursue economic advantage.[11]

2.1.4 Types of regulation possible

- ✓ There are many legislative and administrative practices restricting how TBDFs are regulated.
- ✓ Effective regulation targets the **nature of data transferred or access to telecommunications technology** used in the transfer.

1. ***Regulation of Data***

- ✓ Some countries require that 'domestic' information and transactions be processed in the home country before transmission.

2. ***Regulation of Communications Technology***

- ✓ Countries can impose regulations to control communication e.g. a requirement to have a single Internet portal in the country to have control over TBDFs to and from the country.

[10] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 148
[11] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 148

2.1.5 Methods of regulation

a) **National Regulation**

✓ Focuses transfer of personal data across borders and whether the legislation has an extra-territorial protection effect (should be clear in the legislation wording) e.g. If data is collected in one country and transferred to another, citizens in the country of origin have no protection under destination country's laws, unless by extension (legislation wording is key)

b) **International Agreements**

✓ International communities encourage **free and open trade between nations through a number of international agreements but none of the agreements** created is a **treaty** meaning the agreements are not binding under international customary law.

3.1 What are the objectives of Data protection Acts?

i. To protect personal fundamental rights especially the right to privacy with respect to the processing of personal data
ii. To give legal rights to data subjects (individuals whose data is held by others)
iii. Appoint information commissioner(s) whose roles are; compile and maintain a register of data controllers (persons who hold personal data of others), serving notices to those who contravene the act and ensure that requests for information from data subjects to data controllers are honored

3.1.1 Key principles of the Data Protection Act (1990).

1. Data to be used for the specific **purposes for which it was collected**.
2. Data **must not be disclosed to other parties without the consent of the individual** whom it is about, but for exceptions like prevention or detection of crime. Other parties should not obtain this personal data without authorization.
3. **Individuals have a right of access information held about them**, but for certain exceptions e.g. information held for the prevention or detection of crime
4. Personal information **may not be kept for longer than necessary**.
5. Personal information **may not be transmitted** outside unless with the consent of the individual or adequate protection is in place.
6. All entities that process personal information **must register with the Information Commissioner**. And organizations should only do minimal processing meant for domestic use.[12]

[12] . Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 147, 148

7. Entities holding personal information should have **adequate security measures in place** e.g. technical measures like firewalls and organizational measures like adequate staff training.
8. Data subjects have the **right to make changes to wrong information** held about them[13]

To enforce principles of good practice, the following rules apply while processing personal data. Personal data should be: -

i. fairly and lawfully processed
ii. processed for limited purposes;
iii. adequate, relevant and not excessive;
iv. accurate;
v. stored only for necessary periods;
vi. processed in accordance with the data subject's rights;
vii. secure;
viii. adequately protected while in transit across borders.[14]

3.1.2 DATA SUBJECT RIGHTS

1. ***Right of subject access:*** The data subject should know what data is held about them, for what purpose and the recipient of that data
2. ***Right to prevent processing:*** A data subject can serve a notice to the data controller requiring them not to process data, if it can cause damage or distress to them and others.
3. ***Right to rectification and erasure:*** Data subjects may apply for a court order requiring inaccurate data relating to them to be rectified or erased
4. ***Right to compensation:*** A data subject who suffers damage or distress is entitled to compensation if the data controller is unable to prove that they took reasonable care

[13] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 148
[14] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 147

3.1.4 Basic tenets of the European Union Data Protection Directive (1995):

- ✓ ***Notice of Data Collection-*** Individuals have the right to know that their personal data is being collected, and the purpose of the collection
- ✓ ***Informed Consent (choice)*** **-** Individuals have the right to choose not to have their personal data collected.
- ✓ ***Use of the collected information*** – Individuals have the right to know how personal data will be used and the right to restrict its use.
- ✓ ***Security*** – Individuals have the right to know the measures implemented by organizations to protect personal data be they technical or organizational.
- ✓ ***Correction*** **-** An individual has the right to challenge the accuracy of the data and to provide corrected data or require for erasure.
- ✓ ***Legal relief*** **-** An individual has the right to seek legal enforcement through appropriate channels to protect privacy rights[15]

Content Covered in Week 6: Ethical Dilemmas

In this lecture, we have covered the following: -

1. Defined Ethical Dilemma
2. Described the aspects of Ethical dilemmas: - Privacy, Accuracy, Property, Access (PAPA)
3. Identified a process for analyzing ethical dilemmas
4. Described Transborder Data Flows

Course Text Books

1. Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005)
2. Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA.* (2011)
3. Computers in Society: Privacy, Ethics and the Internet. George, J.F. *Pearson Prentice Hall, New Jersey.* (2004)
4. Cyber-ethics: Morality and Law in Cyberspace, 5th ed., Spinello, R.A. *Jones & Bartlett, Burlington, Mass., USA.* (2013)
5. Contemporary Issues in Ethics and Information Technology. *Schultz, R.A. IRM Press, USA.* (2005)

[15] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 147 & 148