Course: Professional Issues in Information Technology

Week 3: Law, Ethics and the Concept of Privacy

Lecturer: Martha Gichuki

Lecture learning outcomes

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

1. Define Legal and Ethical issues
2. Describe the concept of privacy
3. Describe basic Internet Security issues specifically those affecting E-Commerce Sites

1.1 Legal Issues and Ethical Issues

- Ethics is the branch of philosophy that deals with what is considered to be right or wrong.
- What is unethical in one culture may be perfectly acceptable in another culture but not always
- Some of the legal and ethical issues include privacy & intellectual property rights
- In this lecture we look at privacy issue

1.1.1 Basic Ethical Concepts…

- ***Accountability*** means that individuals, organizations, and societies should be held accountable to others for the consequences of their actions
- ***Liability*** is a feature of political systems in which a body of law is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations
- Due process is a feature of law-governed societies and refers to a process in which laws are known and understood.[1]
- Appeal to higher authorities to ensure that laws have been applied correctly is possible

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

1.1.2 The Concept of Privacy -

What is Privacy?

- Privacy is the moral right of individuals to be left alone, free from surveillance or interference or unreasonable personal intrusions from other individuals or organizations, including the state.[2]
- Loss of this right seems a necessary evil for technology to evolve, in other words, with the advancement of technology; it becomes easier for one to lose private and confidential details to unauthorized parties.[3]
- Presently, no laws govern the privacy of individuals on the internet. The internet provides easy access to public information. It also enables marketers to track anything bought using database technology, i.e., data warehouses and data mining technologies.
- This in turn allows them to profile customers and send them customized offers for goods and services they are most likely to buy.
- Complication arise when these organization start selling your profile to other marketing organizations against your wish.[4]

1.1.3 Information Privacy

Information privacy includes two claims: -

i. That certain information should not be collected at all by governments or business firms

ii. The right of individuals to control the use of whatever information that is collected about them

1.1.4 The Concept of Privacy – Informed Consent

- Informed consent is consent given with knowledge of all material facts needed to make a rational decision

a) ***Opt-in*** requires an affirmative action by the consumer to allow collection and use of consumer information

b) ***Opt-out*** **-** the default is to collect information unless the consumer takes an affirmative action to prevent the collection of data

[2] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 135
[3] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 142
[4] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 154

1.1.5 Privacy, Secrecy & Confidentiality

- Privacy refers to keeping personal information to oneself and under self-control
- The desire to be free from intrusion.
- Privacy differs from secrecy and confidentiality in a number of ways.
- Privacy rights do not apply where free disclosure of information relevant to the workings of government is needed.
- Privacy entails personal freedom and control, and it provides individual protection.

Secrecy

- Secrecy is a functional concept, requiring an agreement on the part of those who are party to some information to not share it with others.
- It generally does not require (or seek) the sanction of society, merely the commitment of those who share the information.

Confidentiality

- Confidentiality is a more formal and social concept.
- Confidentiality deals with a set of rules that govern the use of information held by institutions about individuals and the conditions under which that information can be shared.

2.1 Three Aspects of Privacy

a) Information in own possession

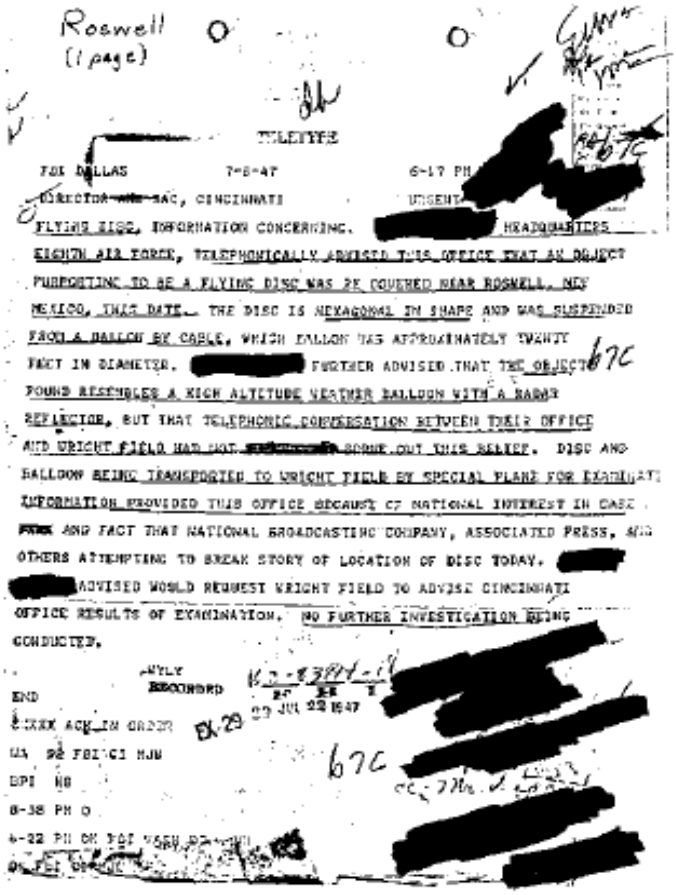
- ✓ Consider information in one's own possession, in the sense of its protection from observation, and perhaps tampering, by others.
- ✓ Data that is stored and transmitted by computer systems is potentially very vulnerable, compared to papers that are locked in filing cabinet
- ✓ The pace of technology change is so rapid that it often renders existing privacy laws obsolete.
- ✓ For example, tampering with surface mail is criminal offence in most countries, whereas the legal status of electronic mail messages is less clear.

b) Information possessed by others

- Consider information concerning an individual which is in the possession of others;
- The individual does not possess the information, but it is considered personal and hence in some sense 'theirs'.
- The concern with this aspect of privacy is the potential misuse of information.
- The data subject (the person whose information is held by another individual or organization) may have no idea what information is stored about them, or who is using it.
- A person or company may be prejudiced by incorrect information, without even being aware that data has been accessed

c) Information shared across borders (Trans-border Data flows)

- A trans-border Data Flow (TDF) occurs when a computer in one country is accessed by or transmits data to a computer in another country.
- This type of data could be personal e.g. patient medical history, or public e.g. business transactional data
- Local legislation that prohibits access to information may be dodged and therefore, Trans- Border Data Flows should be strongly regulated.
- However, the economies of many countries are supported by this trading of information between countries.



Roswell
(1 page)

TELETYPE

FBI DALLAS 7-8-47 6-17 PM
DIRECTOR AND SAC, CINCINNATI URGENT

FLYING DISC, INFORMATION CONCERNING. [redacted] HEADQUARTERS EIGHTH AIR FORCE, TELEPHONICALLY ADVISED THIS OFFICE THAT AN OBJECT PURPORTING TO BE A FLYING DISC WAS RECOVERED NEAR ROSWELL, NEW MEXICO, THIS DATE. THE DISC IS HEXAGONAL IN SHAPE AND WAS SUSPENDED FROM A BALLOON BY CABLE, WHICH BALLOON WAS APPROXIMATELY TWENTY FEET IN DIAMETER. [redacted] FURTHER ADVISED THAT THE OBJECT FOUND RESEMBLES A HIGH ALTITUDE WEATHER BALLOON WITH A RADAR REFLECTOR, BUT THAT TELEPHONIC CONVERSATION BETWEEN THEIR OFFICE AND WRIGHT FIELD HAD NOT [redacted] BORNE OUT THIS BELIEF. DISC AND BALLOON BEING TRANSPORTED TO WRIGHT FIELD BY SPECIAL PLANE FOR EXAMINATION. INFORMATION PROVIDED THIS OFFICE BECAUSE OF NATIONAL INTEREST IN CASE AND FACT THAT NATIONAL BROADCASTING COMPANY, ASSOCIATED PRESS, AND OTHERS ATTEMPTING TO BREAK STORY OF LOCATION OF DISC TODAY. [redacted] ADVISED WOULD REQUEST WRIGHT FIELD TO ADVISE CINCINNATI OFFICE RESULTS OF EXAMINATION. NO FURTHER INVESTIGATION BEING CONDUCTED.

END

[redacted]

67C

FIGURE 4-1 Response to FOIA request for information about the 1947 Roswell incident
Source Line: http://vault.fbi.gov/Roswell UFO/Roswell UFO Part 1 of 1/view

A tampered document

Source: *Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 149*

3.1 Basic Security Issues -

What are the concerns of the user?

a) Is the web server owned and operated by a legitimate company?

b) Does the web page and forms contain malicious / dangerous code or content?

c) Will the web server distribute information provided by the user to some unauthorized third party?

What are the concerns of the company?

a) Will users attempt to break into the web server or alter the pages and content?

b) Will the users try to disrupt the server so that it is unavailable to others - Denial of Service (DoS) attacks

What are the concerns of the users and the company?

a) Is the network connection free from eavesdropping by a third party "listening in" on the line?

b) Is the information sent back and forth between the server and the user's browser being altered?

3.1.1 Cyber attacks

- A cyberattack is a malicious and deliberate attempt by an individual or organization to break into the information system of another individual or organization.[5]
- The attacker normally seeks some type of benefit from disrupting the victim's network.
- Cybercrime has increased over the years due to the benefit attackers get from vulnerable business systems usually in form of ransom
- Cyber attacks are initiated with hidden motives and some attackers look to destroy systems and data.
- Cyber-attacks include
    - Malware (malicious software),
    - Phishing (sending fraudulent communication e.g. emails,
    - Denial of Service attacks (DoS)
    - Man-in-the-middle attack (eavesdropping) etc.[6]

[5] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 346
[6] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 81-96

3.1.2 Internet Security - Why are cyber-attacks are on the rise?

i. Systems' security and systems' ease of use are opposing one another

ii. Security is taking a back seat due to market pressures

iii. Security of an E-Commerce site depends on the security of the Internet as a whole yet the Internet has no security guarantee to individuals or organizations[7]

iv. Many security vulnerabilities are mushrooming

v. Common applications are now compromising security[8]

Organizations and business people engaging in E-Commerce need guidelines as to what behaviors are reasonable under any given set of circumstances.

Review Questions

1. Outline two examples of cyber crimes and describes at least two groups of individuals who may be behind the offenses.
2. List down five factors which have given rise to cyber-attacks.
3. Discuss the following basic security issues:
    a) from the user's perspective
    b) from the company's perspective
    c) from both users and company's perspective

[7] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 87-88
[8] Ethics in Information Technology, 4th ed. Reynolds, G. Course Technology, Boston, USA. (2011) Pg. 84-86

Content Covered in Week 3: Law, Ethics and the Concept of Privacy

1. Legal and Ethical issues
2. The concept of privacy, secrecy and confidentiality
3. Basic Internet Security issues specifically those affecting E-Commerce Sites e.g. Cyber attacks

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)