Advanced Topics on Legal and Ethical Issues in IS

Dr. Arafat Awajan

CH. Three
Privacy and Security

Example

- Two programmers at the city of Chicago's computer center began matching the tape files from the city's different data processing applications on name and ID.
- They discovered
  - High paid city employers had unpaid parking fines
  - Some employees are listed in the files of alcoholic and drug abuse program
- Where are the problems?

Introduction

- Privacy was a sensitive issue long before the advent of computers
- Concerns have been magnified by the use of computer databases that make it easy to compile a dossier about an individual from many different data source
- The internet makes it easy for new data to be collected and added to databases and then accessed.
- Computer based technologies: satellites, telephone, fax, emails, …

Introduction

- Computers based technology
  - High digitalization of information
  - Increasing bandwidth
  - Declining costs
  - Easy to be used (anywhere, anytime)
  - Greater public awareness
- Results
  - Amount of information is increasing
  - Demand for information is increasing
  - Access information is easier

Privacy and Anonymity

- One of the earliest computer ethics topics to attract the public interest was privacy
- Creating large databases of information about citizens (census data, tax records, military service records, welfare records, and so on) and assign a personal identification number to every citizen, it will be easy to gather all the data about each citizen under the corresponding ID number
- Computer technology and Privacy
  - No guarantee to be respected
  - Rules, laws and regulation are needed

Privacy and Anonymity

- Anonymity is the absence of identity
- Privacy is a human value that consists of four elements:
  - Solitude: the right to be alone without disturbance
  - Anonymity: the right to have no public personal identity
  - Intimacy: the right not to be monitored
  - Reserve: the right to control one's personal information including their dissemination
- It is the core of human dignity and autonomy

Privacy Violations

- Intrusion:
  - invasion of the privacy by wrongful entry, seizing and acquiring possession of the property of others.
  - Sophisticated network scanning and spying software makes that no personal information on any computer on any network is safe
  - Examples:
    - STARR
    - FreeWhacker
    - PC Activity MOnitor

Privacy Violations

◻ Misuse of Information
  - Information is not collected only to be stored
  - It has value
  - It is used
  - How??
  - Is it used for legitimate reason??
  - Problem: when it is used for unauthorized purposes

Privacy Violations

◻ Interception of Information
  - It is unauthorized access to private information by accessing private communication between two or more parties.
  - From the source, from the destination or from the communication channels used

◻ Information Matching
  - Matching information about individuals form different sources
  - Problems?? Outdated data, timing, errors, …
  - Legal?? Ethical?? Where are the limits??

Privacy Protection

□ Technical Measures
  ■ Use of software and technically based safeguards
  ■ Information gathering policies
    ▫ Which information
    ▫ Privacy policy
  ■ Educating users and consumers to carry out self regulation
    Activity: discuss a such self regulation
  ■ Use Encryption:
    → Problem: strong encryption was viewed as a threat to national security

Privacy Protection

□ Legal Measures
  ■ Enacting laws by the national legislatures
  ■ Regulations and measures in the companies
  ■ Examples form the USA
    ▫ Consumer protection
    ▫ Children's Online Privacy protection
    ▫ Privacy act
    ▫ Electronic Fund Transfer Act

Privacy Protection

- Example from the European Union
  - Limited collection of personal data.
  - Data must be up-to-date and destroyed when no longer needed.
  - Consent for sharing data is required.
  - Sensitive data (e.g. religion) can only be provided with consent.
  - Notify consumers about the collection and intended purpose of data.
  - Restricted access and sharing of criminal convictions.
- Contractual Measures
  - Which information is to be published or disseminated,

Email Privacy

- Some companies consider e-mail more private than others.
- E-mail is entirely private, like the telephone and the mail. Employees have to feel that you trust them and that you're not looking over their shoulders. employees' work environment is more secure and they will be more productive if they think their privacy is protected.
- Other companies consider that e-mail uses the company equipment and time, they assert their right to check that it is being used properly.

Email Privacy

- Sending private e-mail uses company time. This can be regarded as a type of theft from the employer.
- E-mail can be used to steal from the company in more direct ways:
  - breach of contract,
  - slander,
  - invasion of privacy.
  - stealing trade secrets
- Many companies have a policy that the company can monitor e-mail messages.
- IBM Federal Express, American Airlines, and Pacific Bell have strict policies against use of computers for personal purposes.

Cryptography

- Cryptography
  - Definition:
    - Hiding data in plain sight.
  - Terms:
    - Plaintext: Original, readable message or data.
    - Cyphertext: Modified, unreadable message or data.
    - Encryption: The act of converting plaintext into cyphertext.
    - Decryption: The act of reverting cyphertext back to readable, plaintext.

Cryptography

- Public Key Cryptography
  - How it works:
    - User creates a mathematically-related key pair (public and private keys).
    - Public keys are shared publicly; private keys are kept secret.
    - Public keys are used to encrypt message or data.
    - Private keys are used to decrypt message or data.
  - Benefits:
    - No secret keys need be shared or transmitted.
    - Very secure.

Cryptography

- Encryption
  - Used by:
    - Military personnel.
    - Financial institutions.
    - Human-rights activists.
    - Government agencies.
    - Anyone wanting to keep messages or data private.

Cryptography

- Steganography
    - Definition:
        - Hiding data so that its existence is not known.
    - Examples:
        - Digital watermarks.
        - Hiding text in image files.
    - Used by:
        - Military,
        - Publishers,
        - Anyone wishing to hide messages or data.