Professional, Legal, and Ethical Issues in Data Management

QMUL EECS Database Lecture
Thomas Roelleke & Tony Stockman

Objectives

- How to define ethical and legal issues in information technology.
- How to distinguish between legal and ethical issues and situations data/database administrators face.
- How new regulations are placing additional requirements and responsibilities on data/database administrators.
- How legislation such as the Sarbanes-Oxley Act impact data/database administration functions.
- Intellectual property (IP) issues related to IT and data/database administration.

Legal and ethical issues and database systems

- Organizations increasingly find themselves having to answer tough questions about the conduct and character of their employees and the manner in which their activities are carried out.
- At the same time, we need to develop knowledge of what constitutes professional and non-professional behavior.

Ethics in the context of information technology

- Ethics - A set of principles of right conduct or a theory or a system of moral values.
- Can consider ethical behavior as “doing what is right” according to the standards of society. This, of course, begs the question “of whose society” as what might be considered ethical behavior in one culture (country, religion, and ethnicity) might not be so in another.

Difference between ethical and legal behavior

- Laws can be considered as simply enforcing certain ethical behaviors. This leads to two familiar ideas: what is ethical is legal and what is unethical is illegal.
- Consider
  - Is all unethical behavior illegal?
  - Is all ethical behavior legal?
- Ethical codes of practice help determine whether specific laws should be introduced. Ethics fills the gap between the time when technology creates new problems and the time when laws are introduced.

Ethical behavior in information technology

- A survey conducted by TechRepublic, an IT oriented web portal maintained by CNET Networks (techrepublic.com), reported that 57% of the IT workers polled indicated they had been asked to do something 'unethical' by their supervisors (Thornberry, 2002).
- Examples include installing unlicensed software, accessing personal information, and divulging trade secrets.

Legislation and its impact on the IT function

- Securities and Exchange Commission (SEC) Regulation National Market System (NMS)
- The Sarbanes-Oxley Act, COBIT, and COSO
- The Health Insurance Portability and Accountability Act
- The European Union (EU) Directive on Data Protection of 1995
- The United Kingdom's Data Protection Act of 1998
- International banking – BASEL II Accords
- …

The Sarbanes-Oxley Act, COBIT, and COSO

- Result of major ***financial frauds*** allegedly carried out within companies such as Enron, WorldCom, Parmalat, and others.
- US and European governments presented legislation to tighten requirements on how companies form their board of directors, interact with auditors, and report their financial statements.

The Health Insurance Portability and Accountability Act

- Administered by Health and Human Services in US and affects providers of healthcare and health insurance.
- Five main provisions of the Act includes:
  - Privacy of ***patient information***
  - Standardizing electronic health/medical records and transactions between health care organizations
  - Establishing a nationally recognized identifier for employees to be used by all employee health plans
  - Standards for the security of patient data and transactions involving this data
  - Need for a nationally recognized identifier for healthcare organizations and individual providers

The United Kingdom's ***Data Protection Act*** of 1998

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless it is consented to or 'necessary'. The conditions under which processing is considered necessary are explicitly listed in Schedule 2 and Schedule 3 of the Act.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

GDPR

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

https://www.eugdpr.org/key-changes.html

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Implementation date: 25th May 2018

GDPR: Penalties and Consent

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).

Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, ...

GDPR: Lawful basis for processing

Data may not be processed unless there is at least one lawful basis to do so:

1. The data subject has given consent to the processing of personal data for one or more specific purposes.

2. Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.

3. Processing is necessary for compliance with a legal obligation to which the controller is subject.

4. Processing is necessary to protect the vital interests of the data subject or of another natural person.

5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular if the data subject is a child.

Establishing a culture of legal and ethical data stewardship

- Senior managers such as board members, presidents, Chief Information Officers (CIOs), and data administrators are increasingly finding themselves liable for any violations of these laws.

- Steps to consider include
  - Develop an organization-wide policy for legal and ethical behavior.
  - Professional organizations and codes of ethics.

Intellectual Property (IP)

- Important that data and database administrators as well as business analysts and software developers recognize and understand the issues surrounding IP both to ensure that their ideas can be protected and to ensure that other people's rights are not infringed.
- IP is the product of human creativity in the industrial, scientific, literary, and artistic fields.

Intellectual Property (IP)

- Covers inventions, inventive ideas, designs, patents and patent applications, discoveries, improvements, trademarks, designs and design rights (registered and unregistered), written work (including computer software) and know-how devised, developed, or written by an individual or set of individuals.

- Two types of IP:
  - Background IP – IP that exists before an activity takes place.
  - Foreground IP - IP that is generated during an activity.

Intellectual Property (IP)

- Patents - provides an exclusive (legal) right for a set period of time to make, use, sell or import an invention.
- Patents are granted by a government when an individual or organization can demonstrate:
  - the invention is ***new***;
  - the invention is in some way ***useful***;
  - the invention involves an ***inventive*** step.

Intellectual Property (IP)

- ***Copyright*** - provides an exclusive (legal) right for a set period of time to reproduce and distribute a literary, musical, audiovisual, or other 'work' of authorship.
- ***Trademark*** - provides an exclusive (legal) right to use a word, symbol, image, sound, or some other distinction element that identifies the source of origin in connection with certain goods or services another make, use, sell, or import an invention.

Intellectual Property Rights (IPR)

- Why important to consider?
  - To understand your own right or your organization's right as a producer of original ideas and works;
  - To recognize the value of original works;
  - To understand the procedures for protecting and exploiting such work;
  - To know the legal measures that can be used to defend against the illegal use of such work;
  - To be fair and sensible about legitimate use of your work for non-profit purposes.

Intellectual Property Rights (IPR)

- Issues related specifically to IPR and software include –
  - Software and patentability
  - Software and copyright
    - Commercial software (perpetual use),
    - Commercial software (annual fee),
    - Shareware,
    - Freeware.

Intellectual Property Rights (IPR)

- Consideration must also be paid to data that an organization collects, processes, and possibly shares with its trading partners.
- In conjunction with senior management and legal counsel, data administrators must define and enforce policies that govern when data can be shared and in what ways it can be used within the organization.

Summary / Learning Outcomes

- Awareness for ethical and legal issues in data management/preocssing
- Difference between ethics and legal structures
- “Data” Protection Acts: protect data and people/citizens
  - Main principles of the 98 data protection act (UK)
    - https://en.wikipedia.org/wiki/Data_Protection_Act_1998
  - Main principles of the GDPR, EU reg from 2016, implementation May 2018
- IP: Protect original work
  - Patents, Copyright, Trademark