

Information Ethics

CIS 381

Sources

- Baase, S. (1997) A Gift of Fire. Prentice-Hall.
- Spinello, R. (1997) Case Studies in Information and Computer Ethics. Prentice-Hall.

Outline

- Context
- Critical Areas
 - Acquisition
 - Access
 - Stewardship

Dialog

Hello!!
I am PersonA, doing my Master's degree
I am doing my thesis in web usage mining
under Dr.Persona.
I need some server logs for my thesis.
So, when could be a good time to meet you
regarding this.

Have you conducted an ethical analysis that
would convince me your activities are
"reasonable?"

i'm requesting the server logs purely for my
research work only. i assure you that i
would not misuse or do any nasty things
with the requested details. if you still feel
that i might do some unethical work, you
can contact my professor(Dr. Persona)
under whom i'm working.
please do give me an appointment so that i
can explain you my work.

It has nothing to do with nasty or misuse. It has to do with understanding what you are doing, and the consequences of what you do.

**I am doing my thesis is web usage mining.
In my thesis i have to analyse the server logs by applying one of the data mining techniques on these logs.
By analysing these logs i can track the users.
The analysis will give me:What are the pages which are most frequently visited, what are the pages(i.e.,the path) which users most frequently follow etc..**

Problem(s)

- For those charged with managing and controlling information, IT proposes interesting and difficult problems.**

Challenge

- The increased availability, mobility, and value of information creates a special responsibility to maximize benefits and prevent misuse.

Critical Areas

- acquisition
- access
- stewardship

Acquisition

- Useful data is now collected, stored, manipulated (transformed), and accessed quite economically.

Transformation

- Data is captured in electronic format then compiled and structured. This can be thought of as a value-added process where new meaning can be derived from the data.

Example

- Otis Elevator began to compile information on elevator reliability and performance. Such data would be shared with managers, service personnel, and product designers.

Lions, Tigers, and Bears, Oh My!

- Corporate counsel feared having such information would put the company in jeopardy if sued for an elevator related accident.

Strategy

- A corporate data policy must consider what types of data should be collected and compiled into useful information. Careful review of how such information may be used both internally and externally is required.

Dilemmas

- Does the opportunity to create information imply an obligation to do so when it is related to safety issues?
- Does data collection imply a responsibility to analyze the data in search of patterns which may suggest risks to employees, customers, and/or society in general?

Access

- Information stored digitally is easily accessed and shared.

Issues

- Access issues point to the difficulty of defining and protecting privacy. Policies are required that help define what data is available either internally or externally.

Personal Information

- A growing segment of the economy depends on the secondary use of personal information.

Example

- DMVs in most states sell personal data collected on drivers to direct marketers.

Strategy

- A corporate data policy must determine the parameters and protocol for information sharing.

Stewardship

- Stewardship implies custodial responsibility. This suggests taking care of the "property" entrusted to you. Responsibility in the information domain many include timeliness, accuracy, and security.

Obligations

- Verification of Accuracy
- Prevention of unauthorized access
- Control over data recombination

Computer Matching

- Computer matching is a form of data recombination. The idea is to take information in one database and combine it with data in another.

Example

- The IRS matches income records against lifestyle databases.

Fair Information Practices

- There should be no systems whose existence is secret.
- There should be a way for a person to find out what data about him or her are in the system and how they are used.
- Information obtained for one purpose should not be used for another without the person's consent.
- There should be a way for a person to correct errors in his or her files.
- Any organization creating, maintaining, using, or distributing personal data is responsible for the reliability and security of the data.
