Ethical and Legal Issues in Data Management

Richard Holowczak

Baruch College, CUNY

Richard.Holowczak@baruch.cuny.edu

Portions of this presentation were adapted from the textbook:
Business Database Systems by Connolly, Begg and Holowczak. Addison-Wesley Publishing Company, USA. 2008.
and from the article:
"Database Administrator's Code of Ethics" by Brian Carr.
RMOUG SQL UPDATE: The Magazine For the Rocky Mountain Oracle Users Group
Vol 56. Fall 2009.

Objectives

- Define ethical and legal issues in information technology
- Distinguish between legal and ethical issues and situations data/database administrators face
- Explore how regulations place additional requirements and responsibilities on data/database administrators

Business Environment

- Organizations have to answer tough questions about the conduct and character of their employees and the manner in which they collect and use data
  - eCommerce
  - Social Media
  - Telecommunications
  - Finance
  - Government
- At the same time, we need to develop knowledge of what constitutes professional and non-professional behavior

Trends in data collection

- The "Grand Bargain" of consumer data:
  - Turn over your personal data in exchange for free (or cheap) services
  - e.g., Google, Facebook, YouTube, Twitter, Instagram, etc.
- The "Internet of Things" (IoT) produces the "Data of Things"
- Governments, etc.
- Result: A relative handful of organizations control vast amounts of valuable data

Ethics definitions

- 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

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

Examples

- Which of the following are Legal? Ethical?
  - Your current professor looking at your grades in prior courses
  - Students looking at the salaries of their professors
  - Photocopying a business textbook
  - A systems administrator viewing personal files and browsing histories of their users *
  - A database administrator querying the Customer database to identify a potential love interest

* Adapted from: "Ethical issues for IT security professionals" by Deb Shinder. Computerworld. Aug 2, 2005
https://www.computerworld.com/article/2557944/security0/ethical-issues-for-it-security-professionals.html

Ethical behavior in information technology

- Systems Administrators and Database Administrators: Generally can access and manipulate any and all data
- A survey conducted by TechRepublic (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

Securities and Exchange Commission (SEC) Regulation National Market System (NMS)

- Concerns activities that appear ethical but are in fact illegal
- Presents an 'order protection rule' under which an activity that is acceptable to one facet of the investment community was deemed illegal under the new regulation
- Impact: financial services firms are required to collect detailed market data to demonstrate that a better price was indeed not available at the time the trade was executed

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
- Impact: Security and auditing of financial data and has implications on data collection, processing, security and reporting both internally and externally to the organization
- Concerns establishment of internal controls - A set of rules an organization adopts to ensure policies and procedures are not violated, data is properly secured and reliable, and operations can be carried out efficiently

The Health Insurance Portability and Accountability Act (HIPPA)

- Administered by Health and Human Services in US and affects providers of healthcare and health insurance.
- Five main provisions of 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 EU General Data Protection Regulation (GDPR) (EU) 2016/679 Effective May, 2018

Formerly: The European Union (EU) Directive on Data Protection of 1995

- "The protection of natural persons in relation to the processing of personal data is a fundamental right. … the Treaty on the Functioning of the European Union (TFEU) provide that **everyone has the right to the protection of personal data concerning him or her**.
- The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular **their right to the protection of personal data**.
- (32) **Consent** should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her...
- (49) The processing of personal data to **the extent strictly necessary** and proportionate for the purposes of **ensuring** network and information **security**...
- (65) A data subject should have the right to have personal data concerning him or her rectified and a '**right to be forgotten**'
- (148) In order to strengthen the enforcement of the rules of this Regulation, **penalties including administrative fines** should be imposed for any infringement of this Regulation…
- https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

The UK Data Protection Act of 1998

Presents eight data protection principles -

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.

International banking – BASEL II Accords

- Presents policies and framework that must be enacted into law in each country and monitored by national regulators.

- Framework presents three main 'pillars' -
  - *Minimum capital requirements*
  - *Supervisory review process*
  - *Market discipline*

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

Developing a Code of Ethics

- Frameworks:
  - Common Good: Welfare of the community
  - Utilitarian: Do the most good/least harm e.g. Hippocratic oath
  - Rights: Respecting the moral rights of others
  - Equality: Fairness for all
  - Virtues: e.g., Aristotle's cardinal virtues: Prudence, Courage, Temperance, Justice
- Author Brian Carr offers the following suggestions for a DBA Code of Ethics based on Aristotle's cardinal virtues

"A Framework for Ethical Decision Making". Markkula Center for Applied Ethics. Santa Clara University. August 1, 2015. https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/a-framework-for-ethical-decision-making/

DBA Code of Ethics

- **Principle 1 - Prudence** - the ability to judge between actions with regard to appropriate actions at a given time
- A DBA should:
  - Seek counsel
  - Examine facts
  - Consider the general norms of society
- **Principle 2 – Justice** – To act in Fairness or Righteousness
- A DBA should:
  - Respect the rights and dignity of all
  - Promote the well being of all

Adapted from "Database Administrator's Code of Ethics" by Brian Carr. RMOUG SQL UPDATE: The Magazine For the Rocky Mountain Oracle Users Group Vol 56. Fall 2009. Page 16-18.
http://www.rmoug.org/wp-content/uploads/News-Letters/fall09Web.pdf

DBA Code of Ethics

- **Principle 3 – Temperance** – To act with restraint, self-control and discretion
- A DBA should:
  - Consider carefully how to treat confidential data
- **Principle 4 – Courage** – The ability to confront fear, uncertainty and intimidation
- A DBA should:
  - Honor all commitments
  - Keep constituents advised of all issues
  - Provide complete information

Adapted from "Database Administrator's Code of Ethics" by Brian Carr. RMOUG SQL UPDATE: The Magazine For the Rocky Mountain Oracle Users Group Vol 56. Fall 2009. Page 16-18.
http://www.rmoug.org/wp-content/uploads/News-Letters/fall09Web.pdf

DBA Code of Ethics

- **Principle 5 – Responsibility** – Control and accountability for systems
- A DBA should:
  - Take responsibility for systems they are entrusted with
  - Be accountable for any events occurring on their systems
- **Principle 6 – Trustworthy** – Credible and worthy of trust
- A DBA should:
  - Do their best and keep their word
  - Follow through on their commitments

Adapted from "Database Administrator's Code of Ethics" by Brian Carr. RMOUG SQL UPDATE: The Magazine For the Rocky Mountain Oracle Users Group Vol 56. Fall 2009. Page 16-18.
http://www.rmoug.org/wp-content/uploads/News-Letters/fall09Web.pdf