Privacy and Data Protection Issues for UCLA

Christine Borgman, Professor
Information Studies
Privacy & data protection issues

Privacy is fundamental to democracy
- freedom of speech, freedom to read
- academic freedom

Privacy requires data protection
- organizational responsibility for student records (e.g., FERPA), faculty& staff records
- risks of data misuse (e.g., identity theft)
- chilling effect on communication if speech is not protected, if people think that what they are saying and reading is being tracked
Privacy practices are evolutionary

- **print records:**
  - physical controls: locks, keys, signing authority
  - records held by controlling agency (e.g., registrar, library)
  - record-specific laws and policies (e.g. FERPA, state laws on access to library circ data)

- **electronic records:**
  - electronic controls: encryption, passwords, firewalls
  - records of multiple types may be held by central agency
  - institutional policies and practices required
BASIC PRINCIPLES OF NATIONAL APPLICATION.

**Collection Limitation Principle**
7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

**Data Quality Principle**
8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
Privacy principles-OECD 1980-2

**Purpose Specification Principle**

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

**Use Limitation Principle**

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.
Privacy principles-OECD 1980-3

Security Safeguards Principle
11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle
12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
Privacy principles-OECD 1980-4

Individual Participation Principle

13. An individual should have the right:
   a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b) to have communicated to him, data relating to him
      1. within a reasonable time;
         * at a charge, if any, that is not excessive;
         * in a reasonable manner; and
         * in a form that is readily intelligible to him;

      2. c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
         d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
Privacy principles-OECD 1980-5

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.
UCLA- where are we now?

- A wide array of personal data are being collected via BruinCard and other means.
- Basic OECD privacy principles are not in place.
  - Individuals on whom data are being collected lack basic knowledge of what is being collected, by whom, for what purposes, for whose access, and the retention and destruction cycles for these data.
  - Individuals do not have rights (or do not know about them) to access or correct these data.
- Many individuals are reluctant to obtain a BruinCard or participate in other university electronic records systems (e.g., electronic voting, academic personnel systems) w/o privacy and data protection principles in place.
UCLA - further concerns

- Identity fraud (#1 white collar crime in the U.S.) occurs mainly through insider access to personal data.
- The more data aggregated in one ID card, the more valuable it becomes.
- The risk for abuse, and the liability incurred, increase with the amount of data collected and aggregated.
- System administrators (some of whom are student workers) may have access to email transaction records, content, and other unencrypted records.
Sample Issues to be addressed by system designers and review panels

- What data are being collected? What are the specific uses and justifications for each data element?
- How long is each data element and each transaction retained? When are data destroyed? How is destruction assured?
- What are the criteria to determine when data should be aggregated in one system or ID card and when data should be isolated?
- What audit trails need to be in place? Who has access to the audit trails? What rights do individuals have to their audit trails? How can the privacy of the data in the audit trails be assured?
- What is an acceptable level of risk and liability for each data element collected, and each type of transaction?
- What are the criteria for encrypting data within databases?
- What are the criteria to determine “need to know”? What data, what purposes, what audit trails to determine abuse?
Proposal to ITPB / UCLA

- Establish university privacy and data protection policies based on OECD guidelines
- Establish privacy and data protection board to oversee implementation of policies and to review all new data collection plans
- Membership of the board to include
  - Representatives from agencies that do major data collection
    - Finance, registrar, library, other
  - Representatives from constituencies on whom data are being collected
    - Students, faculty, staff, public
  - Additional members
    - external privacy / data protection expert?
    - at large members?
Further contributions today

- Susan Abeles, Financial Services, on BruinCard privacy and data protection
- Janice Koyama, Interim University Librarian, on library practices
Appendix: Examples of best practices

- OECD template provides a framework for institutional practices
- Practices vary by organization; no single “best practices” model exists
- List that follows was assembled by Ruchika Agrawal of the Electronic Privacy Information Center, paraphrased from Peter Wayner's "Translucent Databases"
examples from Wayner -1

(1) Encryption: keep data secure with one-way functions and encryption
(2) Ignorance: data is scrambled (or encrypted) by the user's computer before it travels over the network
(3) Minimization: collect/keep the minimum amount of data necessary
(4) Misdirection: add fake data into the mix (only the legitimate user can spot the real data)
examples from Wayner -2

(5) Stunt data: replace data with encrypted items that can protect the real data while still looking like the real information
(6) Equivalence: obscure sensitive information by replacing it with a similar value that is functionally equivalent (e.g. instead of date-of-birth, why not just yes/no for is of legal voting age?)
(7) Quantization: reduce the precision of numbers of values
(8) Security: even if invaders find all the passwords to all of the access levels, the raw data should be encrypted or scrambled so even if you gain access to the system, you won't gain access to the data.

(9) OS Independence: "All of the major operating systems are insecure." Hence the raw data should be encrypted or scrambled so even if you gain access to the system, you won't gain access to the data.