PRIVACY ISSUES

Definition:

Privacy: It is the degree at which the data and information about the individuals and groups can be collected, stored and disseminated in a confidential way.

Information Collected at E-commerce sites

1. Personally identifiable information (PII): Data that can be used to identify, locate, or contact an individual.

2. Anonymous information: Demographic and behavioral information that does not include any personal identifiers.

3. Almost all e-commerce companies collect PII and use cookies to track click stream behavior.

4. Profiling: Creation of digital images that characterize online individual and group behavior.

5. Anonymous profiles: Identify people as belonging to highly specific and targeted groups.

6. Personal profiles: Add personal identifiers.

7. Advertising networks can:
   - Track both consumer behavior and browsing behavior on the Web.
   - Dynamically adjust what the user sees on screen.
   - Build and refresh high-resolution data images or behavior profiles of consumers.

- **Sources of information to collect personal data:**
- 1. Questionnaires in web site self-registration: Customers are asked to type in their private information, such as name, address, phone, e-mail address, or even interests and hobbies in order receive needed information, or to play a game, or to receive a password to participate in a lottery. This information may be collected for planning the business, sold to a third party, and used in an inappropriate manner.
- 2. Cookies: It is a piece of information that allows a web site to record users' preferences, interest, and surfing pattern across HTTP connections. Most leading browsers, including MS-IE, support cookies.
- The solution for this is: 1. Delete cookie files stored in their computers. 2. Use of anti-cookie software that filters to either block or allow cookies at a user's command.

Privacy policies in areas of concern

I. Data collection:

1. Data should be collected on individuals only to accomplish a legitimate business objectives.

2. Data should be adequate, relevant, and not excessive in relation to the business objective.

3. Individuals must give their consent before data pertaining to them can be gathered.

II. Data accuracy:

1. Sensitive data gathered on individuals should be verified before it is entered into the database.

2. Data should be accurate and, where and when necessary, kept current.

3. The file should be made available so the individual can ensure that the data are correct.

4. If there is disagreement about the accuracy of the data, the individual's version should be noted and included with any disclosure of the file.

III. Data confidentiality:

1. Computer security procedures should be implemented to provide reasonable assurance against unauthorized disclosure of data. They should include physical, technical, and administrative security measures.

2. Third parties should not be given access to data without the individual's knowledge or permission, except as required by law.

3. Disclosures of data, other than the most routine, should be noted and maintained for as long as the data are maintained.

4. Data should not be disclosed for reasons incompatible with the business objective for which they are collected.

TECHNOLOGICAL PROTECTIONS FOR ONLINE PRIVACY

TCHNOLOGY	PRODUCTS	PROTECTION
1. Secure e-mail	Ziplip, SafeMessage.com	E-mail and document encryption
2. Anonymous remailers	WWW Anonymous Remailer	Send e-mail without trace
3. Anonymous surfing	Freedom, Anonymizer.com	Surf without a trace
4. Cookie managers	CookieCrusher; Magic Cookie Monster	Prevents client computer from accepting cookies
5. Disk/file erasing programs	FileWiper, Eraser, DiskVac	Completely erases hard drive and floppy files
6. Policy generators	OECD Privacy Policy Generator	Automates the development of an OECD privacy compliance policy
7. Privacy Policy Reader	P3P	Software for automating the communication of privacy policies to users.