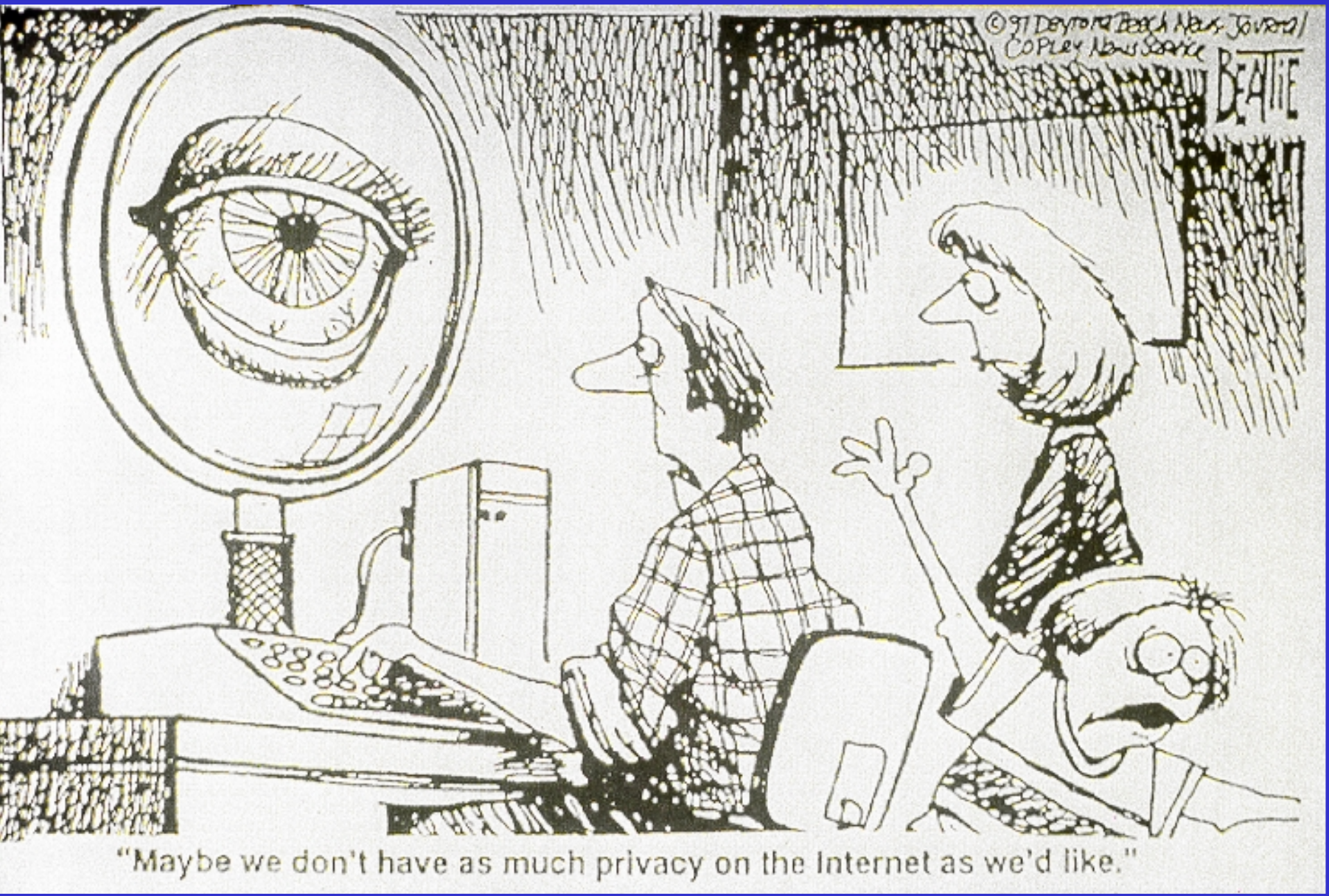
Privacy Overview

Christine Varney

Hogan & Hartson L.L.P.



"Maybe we don't have as much privacy on the Internet as we'd like."

PRIVACY—The Ability to Control Who Knows What About You, When They Know It, and What They Can Do With That Knowledge.

- Data is easy and inexpensive to gather, store, analyze, transmit, and reuse.
- More use of the Internet means more data about more interactions in forms that are more readily accessible to a wider circle of data users.
- Digital information is inherently global; it respects no boundaries.

Privacy and Electronic Commerce on the Internet

- Over 90 million Americans use the Internet on a regular basis
- 92% of Internet users are concerned about the misuse of their personal information
- 85% believe that it is “absolutely essential” or “very important” that a site display a privacy policy before they provide personal information or purchase online

Source: IBM Multi-National Consumer Privacy Survey, October 1999

Privacy Concerns and Impact

- Consumers are most concerned about
  - security of sensitive information
  - sharing of personal information
- Concerned consumers shop less
  - 61% of Internet users have refused to make a purchase online at some time because of privacy fears
  - 48% of consumers who are “very concerned” about privacy don’t shop online

  Source: Forrester Research, The Privacy Best Practice, Sept. 1999
- By 2002, privacy concerns could account for $18 billion in lost revenue

  Source: Jupiter Communications, August 1999; IBM-Harris Multi-National Consumer Privacy Survey, Jan. 2000

Privacy = Trust

- Privacy/Data Collection
- Integrity/Authentication
- Security/Encryption
- Recourse/Liability

Privacy and Fair Information Practices

- **NOTICE, about how personal information collected online is used;**
- **CHOICE, about whether and how that personal information will be used;**
- **SECURITY, so that personal information is protected from unauthorized use; and**
- **ACCESS, so that consumers can ensure the accuracy of their personal information.**

What's Government Doing

- FTC Privacy Initiative
  - Workshops; Surveys and Reports; Enforcement
- Congress Passed and Pending Legislation
  - HIPAA; COPPA; GLB
- State Attorneys General
  - Task Force; NAAG Committee; Enforcement Actions
- Private Class Actions
  - DoubleClick; Yahoo; RealNetworks; Amazon

COPPA

- Operators of commercial websites directed to children (under 13) that collect personal information, or that knowingly collect such information from children
- Companies on whose behalf these websites collect the information
- Collection of anonymous information does not trigger the Act

Operator Obligations

- Give parents notice of information practices
- Obtain verifiable parental consent before collecting, using, disclosing information
- Provide reasonable parental access to information
- Provide parent opportunity to halt further use and/or further collection of information
- Collect only what is reasonably necessary
- Maintain confidentiality of information

Gramm-Leach-Biliey (G-L-B) Financial Services Modernization Act of 1999

- Financial institutions must provide customers with notice and certain opt-out by JULY 1, 2001
- Financial institutions include businesses engaged in various financial activities (leasing, financing, tax preparations, credit counseling, investment advice)
- Consumers, who are not customers, may be entitled to notice and opt-out
- Key issue of affiliate sharing

Health Insurance Portability and Accountability Act of 1996

- Adds Part C, Administrative Simplification to Title XI of the Social Security Act
- Section 264(c) establishes Secretarial authority regarding medical privacy
- Establishes penalties for violations

Administrative Simplification

1. Standard formats to enable electronic data exchange (Aug. 17, 2000)
2. Code sets (Aug. 17, 2000)
3. Unique identifiers (provider, employer, plan, individual)
4. Security standards
5. Electronic signature
6. Privacy (Dec. 28, 2000)

The Scope Of The European Data Protection Directive

- Applies to the processing of personal data
  - "processing" is defined as any set of operations, whether or not by automatic means, including collection, recording, organization, storage and use
  - "personal data" is defined as any information relating to an identified or identifiable natural person

The Scope Of The European Data Protection Directive

- Covers both electronic and manual data if the latter is part of a filing system
- Encompasses employee, corporate and customer data
- Contains exemptions for the processing of data for journalistic purposes

Data Transfer

- Transfer of personal data to countries outside the EU may take place only if the third country in question ensures an adequate level of protection
  - Non-personal data, i.e., data that is stripped of all identifying elements, may be transferred outside the EU
  - Data may be transferred outside the EU if the data subject unambiguously consents to the transfer
  - Limited derogations exist

Transfer According To Contracts

- The terms of a contracts can ensure "adequate protections" by laying out data controller obligations and data subjects rights similar to those in the Directive
  - The European Commission is in the process of drafting a model contract that provides such protections
  - The Bush Administration has stated that the proposed terms of the model contract are "unduly burdensome"
  - Parties may draft their own contracts, but such contracts should be approved by the local data protection authority
  - It is very difficult to provide for third party rights in such contracts – which is required for the enforcement of a data subject's rights

Achieving Adequate Protections In The US – Safe Harbor

- **Companies that sign up with the Department of Commerce and adhere to the Safe Harbor Principles may freely transfer data between the US and the EU**

Safe Harbor Principles

- **The Safe Harbor Principles are similar to the protections required by the Directive. They require an organization to provide the following:**
  - **Notice - an organization must notify individuals about the purposes for which it collects and uses information about them, provide contact information, list the types of third parties to which it discloses information and the choices and means for limiting disclosure**

Safe Harbor Principles

- **The Safe Harbor Principles are similar to the protections required by the Directive. They require an organization to provide the following:**
  - **Choice - an organization must give individuals the opportunity to choose (opt-out) whether their personal information will be disclosed to third parties or used for purposes other than for which it was collected; sensitive information requires an affirmative opt-in**

Safe Harbor Principles

- **Onward transfer - an organization must apply the notice and choice principles to onward transfer and may make the transfer only if the organization to which the data is to be disclosed adheres to Safe Harbor or is subject to the Directive or another adequacy finding**
- **Access - individuals must have access to personal information about them and be able to correct, amend or delete that information**

Safe Harbor Principles

- **Security - organizations must take precautions to protect data against loss, misuse or unauthorized access**
- **Data integrity - personal information must be relevant for the purposes for which it is to be used and organizations must take reasonable steps to ensure data is reliable, accurate, complete and current**

Safe Harbor Principles

- **Enforcement - there must be a readily available and affordable independent recourse mechanism for individuals, procedures for adherence to the Safe Harbor principles and sanctions for failure to comply**

Safe Harbor Enforcement

- The FTC has committed to reviewing an organization's compliance with Safe Harbor under Section 5 of the FTC Act
  - Once a company registers under Safe Harbor, any failure to comply with it's principles is considered an unfair and deceptive act
  - Only entities subject to the FTC Act are eligible for Safe Harbor
    - Excludes financial institutions

Enforcement Of The Directive

- Provides for an individual right of judicial remedy for breach of rights guaranteed by the Directive
- Although the Directive provides only for a civil right of compensation, some Member States allow criminal prosecution of data protection violators