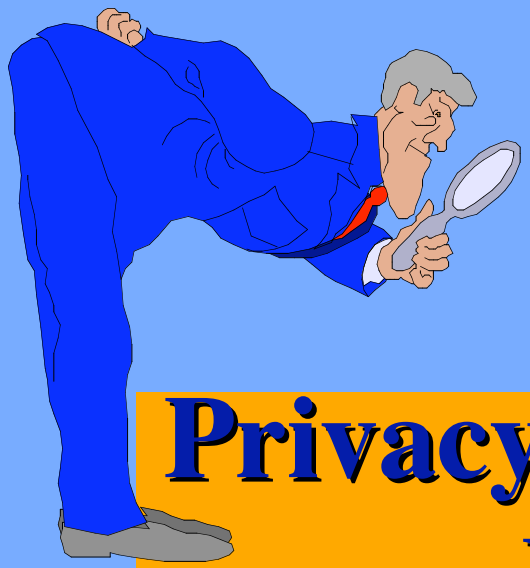


Privacy in a Networked World: Privacy for Sale?

CSci 110

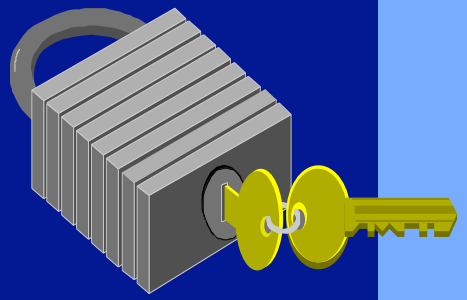
Summer 2002

Prof. C.D. Martin

Code of Fair Information Practices

Notion of Data "Stewardship"

- Ownership of data
- Notice
- Choice - opt-in versus opt-out
- Access
- Security / Integrity of Data



Still voluntary, not regulated!

Discussion Issue: The "great debate" over opt-in/ opt-out

- **Opt-in - you choose to have your data used:**

Check here if you want to be on our mailing list[X]

Check here if you want to be on our mailing list[ ]

- **Opt-out - your data is used unless you specify otherwise**

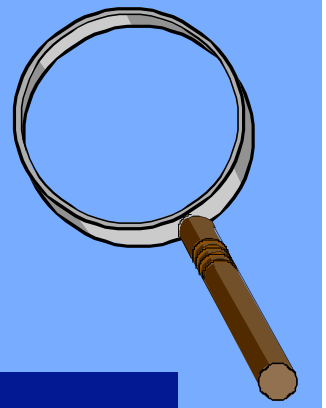
Check here if you don't want to be on our mailing list[ ]

Check here if you don't want to be on our mailing list[X]

- **Pros and cons?**

European Union

http://www.privacy.org/pi/intl_orgs/ec/eudp.html



- Data Directive
- Effective October 1995
- Requires any country that trades with the EU must protect any personal information of citizens of any member country involved in the transaction
- US had to negotiate a “safe harbor” agreement- US companies had to agree to abide by safe harbor principles in all transactions
- Certified by US Dept of Commerce

Canada's New Privacy Act

- Personal Information Protection and Electronic Documents Act (PIPEDA)

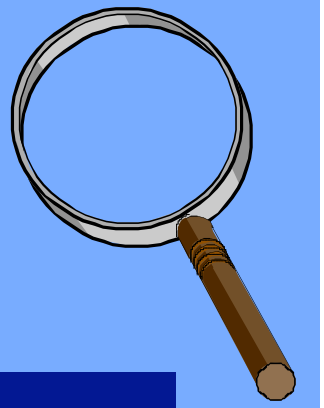
http://www.davis.ca/topart/personal_information_protection_.htm

- Implemented January 2001.
- One of the main purposes of PIPEDA is to
- protect personal information held by the private sector.
- Government data already protected by the Privacy Act and Privacy Commissioner.
- Enacted under pressure from EU.

Under PIPEDA, orgs must:

1. Designate an individual who is accountable for compliance with PIPEDA.
2. Explain to that person the purposes for information is being collected; must obtain that person's consent before collecting, using or disclosing the information.
3. Must not collect more information than is necessary to achieve stated purposes.
4. Must destroy the personal information once it is no longer needed to achieve stated purpose.
5. Ensure the personal information is accurate/ complete. must be given access to that information; must also change any inaccurate and incomplete information.
6. Must protect all personal information. The level of security required depends upon the sensitivity of the information.
7. Must make policies and practices regarding management of personal information available upon request.

US: Online Privacy Alliance (OPA)

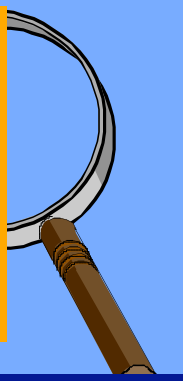


- Voluntary membership of US corporations
- Agree to a set of privacy principles
- All commercial web sites must have a Policy Policy
- See http://www.privacyalliance.org/

OPA Privacy Guidelines

1. Adoption and Implementation of a Privacy Policy – easy to understand
2. Notice and Disclosure
   - How data will be used
3. Choice/Consent
   - opt-out; opt-in
4. Data Security
   – protect from loss, misuse
5. Data Quality and Access
   - accurate, complete, timely, correctable

OECD Transborder Data Flow Guidelines / US safe harbor

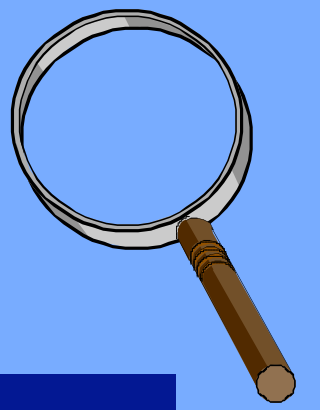


http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-en.HTM

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle
- *Implemented , validated, insured nationally*

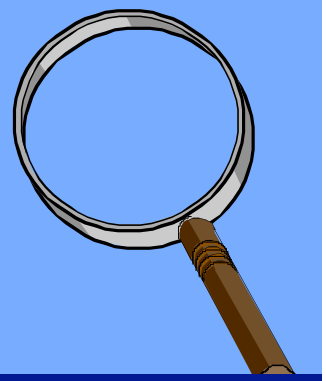
http://www.exports.gov/safeharbor/sh_overview.html

Discussion



- Which approach is better?
  - EU and Canada - Privacy Commission, Data Directive
  - US - voluntary, self-regulation
- Is there another way?

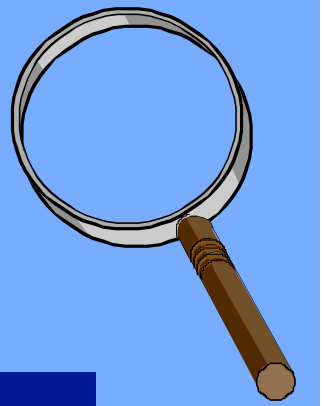
COPPA provisions



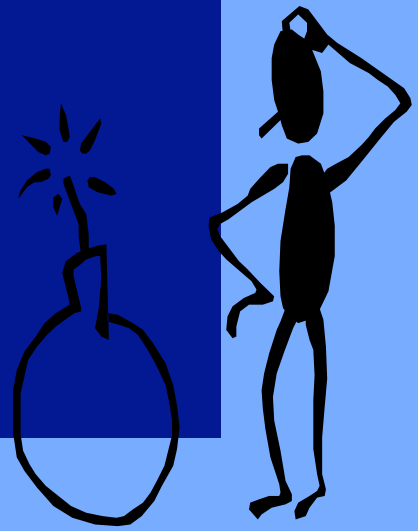
http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm

- Who: commercial Web site or an online service directed to children under 13 that collects personal information from children
- What: applies to individually identifiable information about a child that is collected online – name, address
- Required: privacy notice and policy, direct notification of parents, verifiable parental consent, use of data by third parties, access verification

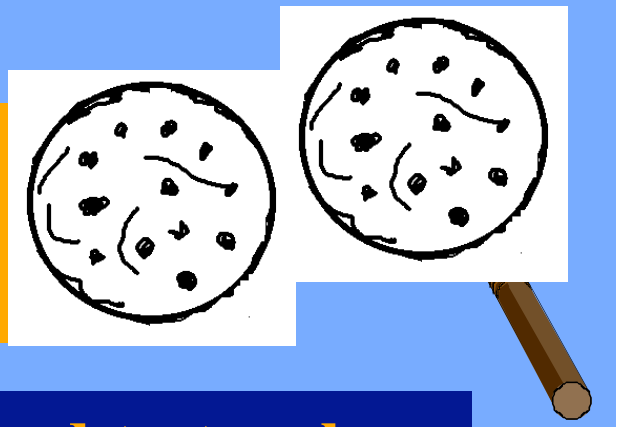
Privacy Implications of the Internet



- Email spamming - practice
- Electronic cookies - technical
- Web bugs - technical
- Identity theft - fraud
- Data mining and profiling
- Customized marketing

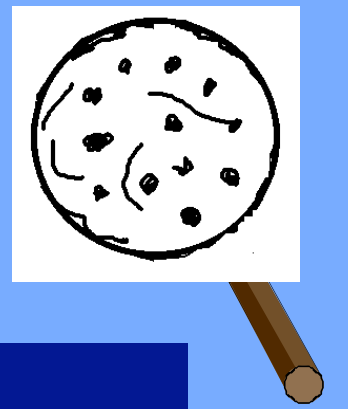


Electronic Cookies



- **Electronic tracking mechanism used to track user progress through a web site.**
- **Session Cookies:** used during a unique user online session and do not exist after the session ends. Is often a way to authenticate a valid user of a service.
- **Persistent Cookies:** remain on user's computer's hard drive after a user session is ended. The site can check for these cookies if the user returns to that website; can remember previous selections.

Pros and Cons of Cookies



- Can be a convenience to the user to prevent certain pop-ups from reappearing, such as license agreements
- Allows personalized marketing
- Can be a sneaky tracking mechanism to do profiling of user
- Should users always be given the choice to accept or block cookies?
- Should they always be informed?

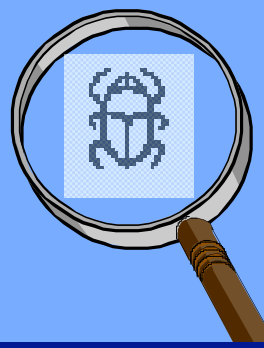
Web Bugs

- The use java script clear Gif image requests on Web pages.
- Widespread practice commonly associated with application service provider (ASP) services that are performing outsourced administrative functions on behalf of web site operators. These functions include measuring traffic, verifying advertising revenue and payment amounts and providing back up for the administration of web sites' affiliate programs.

The Privacy Problem with Web Bugs

- Almost all Web bugs in use today are invisible, so their tracking function is hidden to consumers.
- Their use of Web bugs is almost never disclosed in the privacy policies.
- Privacy issues: May be collecting information that could be related to an individual consumer.

Principles for Using Web Bugs (Privacy Foundation)



1) A “Web bug” should a visible icon.

2) Visible icon should identify the name of the company and be labeled to say it is a "tracker", “spotlight", or "sensor" device.

3) By clicking on the icon, a user should see a description of the purpose of the Web bug,

   (i) what data is collected with the Web bug,

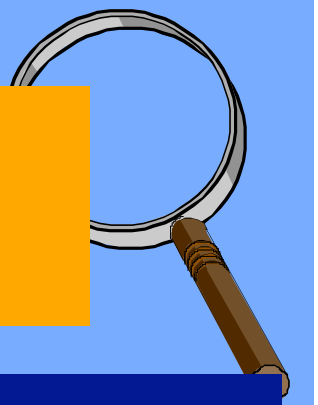
   (ii) how the data is used after it is collected

   (ii) what company or companies receive the data,

   (iii) what other data the Web bug is combined with

   (iv) if a cookie is associated with the Web bug or not.

More Principles - Web Bugs



4) Internet users “should be able to "OPT-OUT" from any data collection being done by the Web bug” from the “Web bug” disclosure page.

5) “Web bugs” should not be used to collect information from sensitive Web pages, such as those

(i) intended for children

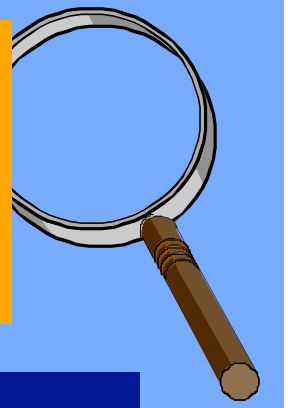
(ii) about medical issues

(iii) about financial and job matters

(iv) about sexual issues

Identity Theft

http://www.consumer.gov/idtheft/

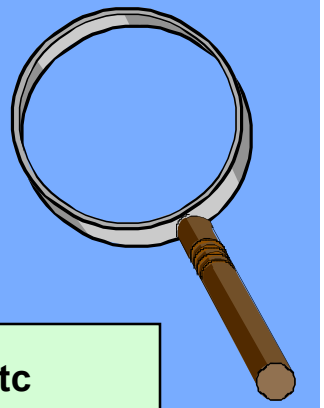


- Open a new credit card account, using your name, date of birth, and Social Security number, and don't pay the bill!
- Call your credit card issuer and, pretending to be you, change the mailing address on your credit card account.
- Establish cellular phone service in your name – don't pay the bill!
- Open a bank account in your name and write bad checks on that account.

Rationale for a Usable, Robust Web Site Privacy Policy

- It is a key part of reputation, brand, public image
- An important aspect of articulating data policy for internal as well as for external audiences
- Make it easy to understand and use.
- Make it easy to extend or change in the future.
- Facilitate compliance with privacy seal programs such as BBBOnline and TrustE.

Layout of a Model Web-based Privacy Policy



1. Home page - Intro

   * Commitment to privacy
   * Participation in any privacy initiatives
   *Participation in privacy seal programs(links)

2. Link to a set of Privacy Principles

3. Link to privacy policies
   * web site
   * other products, services

4. Link to FAQ's

5. Link to list of all policy changes with dates

6. Link to full contact info

2. Privacy Principles to cover:

Data Collection
Notice, esp. PII
Choice
Security
Access to help

3. Privacy Policy – web site

Use template
notice, choice, access
security
Includes info on cookies
Outbound links

3c, d, etc Others as needed

3b. Privacy Policy- Products, services

Use template – notice,choice, access, security

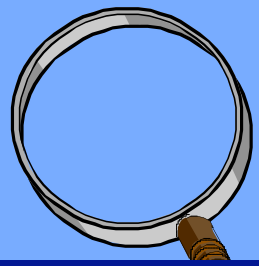
4. FAQ's

5. Changes to Privacy Policy

Date of each change and brief description of change

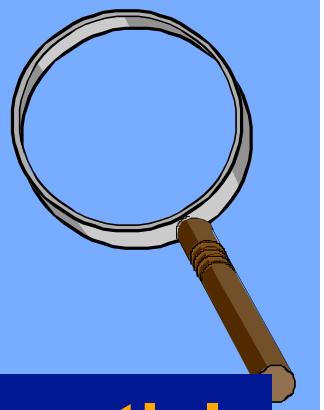
6. Contact info

EX: Intro to a Privacy Policy



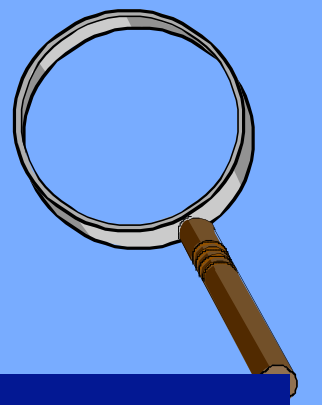
- As an information service provider, GeoTrust is the steward of many different types of enterprise data. We take the responsibility of protecting the security and, when appropriate, the confidentiality, of that data very seriously. Protecting your personal privacy is also very important to us. We hope that the following statement will help you to understand how GeoTrust collects, uses and safeguards the information you provide to us through this web site as well as through our other products and services.
- GeoTrust participates in and supports industry and government efforts to identify and resolve privacy issues. We actively participate in the Online Privacy Alliance, an industry-based non-profit organization committed to the protection of consumer privacy on the Internet. We are regularly involved in hearings convened by Federal agencies and by Congress to debate privacy and data usage issues.

Example: GeoTrust's 10 Privacy Principles



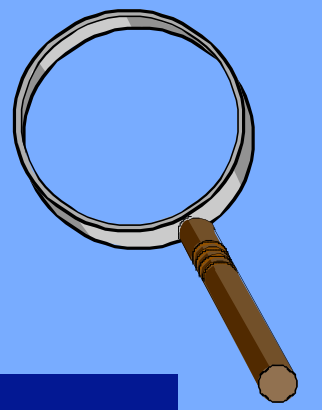
1. We collect only information that is essential to providing good service to customers and users.
2. We inform users about what data is collected and how it will be used.
3. We allow users to choose how their self-disclosed data will be used.
5. We use information security safeguards.
6. We are responsive to requests for explanation about our data use and policies.

Example: GeoTrust's 10 Privacy Principles(cont)



7. We hold our employees responsible for our privacy principles.
8. We provide these privacy principles to our business partners.
9. We comply with all applicable privacy laws and regulations wherever GeoTrus does business.
10. We undergo regularly scheduled independent audits of our privacy policies and practices to ensure that we are in compliance with our stated policies.

4 Ways to Privacy Protection

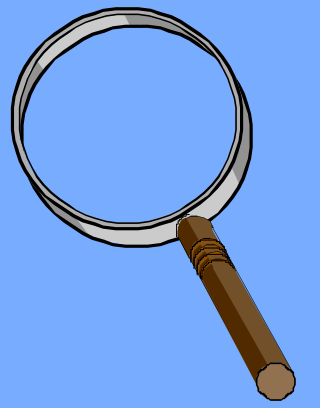


- Norms and practices of society
- Laws and regulations
- Marketplace solutions - voluntary self-regulation
- Code - technical solution

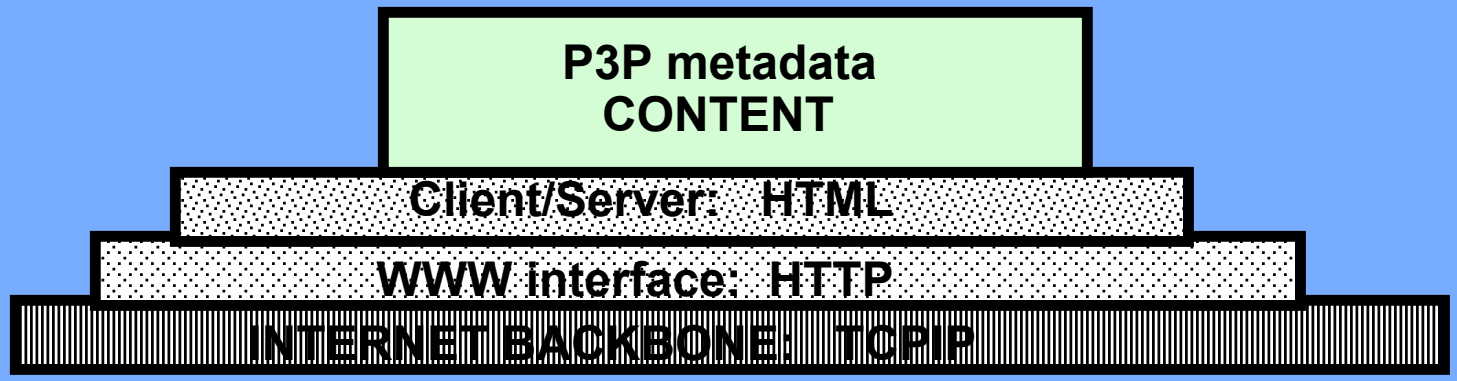
W3C Founding Principles

- Technology can be used to provide safe access to the internet
- Technology can be used to protect users from unreliable, unwanted, offensive or illegal information as well as from hackers, viruses, unwanted intrusion, invasion of privacy, and electronic fraud.
- W3C sets up working groups to establish technical standards and data exchange protocols to be used by others to develop systems to accomplish the above.

P3P: Platform for Privacy Preferences and Practices



Web Architecture



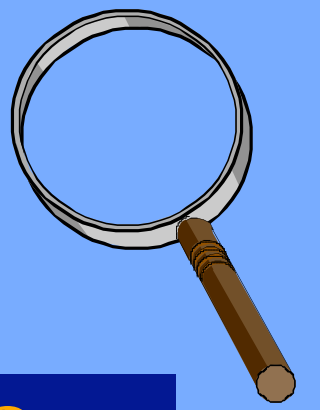
P3P: A "Code" Solution

- P3P - enables an agreed upon protocol for the expression of privacy preferences and privacy practices - allows an agreement of what data is to be exchanged

"privacy assistant - users can be informed, in control, simplify, state their privacy preferences." privacy for sale?

- OPS (Open Profiling System) - secure storage, transport, control of user data - allows secure exchange of data

Brave New World Since 9/11



Will Privacy be the final victim?

- Biometrics identification systems
- Video cameras
- National Identity Card
- A nation of vigilant “watchers”
- Random searches