

# Fair Information Practices

Simson L. Garfinkel



# The "Bad People" problem

- The world is filled with bad people.
- You can't put them all in jail.



# Evidence of "bad people"

- Decreasing inventory at stores
  - Shoplifting?
  - Employee theft?
- Merchandise purchased with "lost" credit cards
  - Perhaps the card was stolen
  - Perhaps the card wasn't stolen



# More Evidence...

- Money borrowed and not repaid
- Faked insurance claims
- Forged checks



# Solution to the "bad person" problem

- Make a list of the bad people.
- Don't do business with anybody on the list.



# Examples of Solution...

- Retail Credit Company (1899-)

- List of people "known" not to repay their debts

- Medical Information Bureau (est. 1902)

- List of people with "known" medical problems

- Chicago-area merchants (1950s)

- List of "known" shoplifters



# Typical Credit Report

- "Retired Army Lieutenant Colonel"

- "A rather wild-tempered, unreasonably, and uncouth person....

- "who abused his rank and wasn't considered a well-adjusted person.

- "He was known to roam the reservation at Ft. Hood and shoot cattle belonging to ranchers who had leased the grazing land from the Army."

- —Hearings on the Retail Credit Company, 1968



# Credit reports of the 1960s

- Contained information that was hearsay or just plain wrong.
- Records confused between individuals.
- No "statute of limitations" on the information.
- People frequently prohibited from seeing their own records.



# Fair Credit Reporting Act, 1970

- Right to see your credit report.
- Right to challenge incorrect information.
- Information automatically removed from report after 7 years
  - 10 years for Bankruptcy.
- Right to know who accesses your report.
- Right to a free credit report if you are denied credit.



# Code of Fair Information Practice (HEW, 1973)

## #1

- There must be no personal data record-keeping systems whose very existence is secret.



## CFIP #2

- There must be a way for a person to find out what information about the person is in a record and how it is used.



# CIFP #3

- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.



# CFIP #4

- There must be a way for a person to correct or amend a record of identifiable information about the person.



# CFIP #5

- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.



# CFIP in Short

- No Secret databanks
- You are allowed to see your own record
- Information obtained for one purpose can't be used for another without consent.
- Ways for correcting or amending information.
- Prevention of misuse.



## CIFP, cont.

- Good ideas --- matches what we believe.
- Never passed into law.
- Adopted in Europe.



# 1980 OECD Guidelines

- "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"
- Collection Limitation Principle
  - "obtained by lawful and fair means"
  - "with the knowledge or consent" where appropriate
- Data Quality Principle
  - Data should be relevant and kept up-to-date.



# 1980 OECD Guidelines, Cont.

## • Purpose Specification Principle

- Purpose specified before the data is collected.

## • Use Limitation Principle

- Not be used for purposes other than originally intended except
  - With the consent of the data subject
  - By the authority of law.



# 1980 OECD Guidelines, Cont.

## • Security Safeguards Principle

- "Reasonable security safeguards" to prevent loss, unauthorized access, destruction, use, modification or disclosure of data.

## • Openness Principle

- Clearly stated practices and policies.
- No secret databases.



# 1980 OECD Guidelines, Cont.

## • Individual Participation Principle

- Individuals have the right to see their own records.
- Right to challenge and demand correction or erasure.
  - (note Steve Ross story!)

## • Accountability Principle

- "A data controller should be accountable for complying with measures which give effect to the principles stated above."



# 1995 CSA "Privacy Standard"

- 1. Accountability
- 2. Identifying Purposes
- 3. Consent
- 4. Limiting Collection
- 5. Limiting Use, Disclosure, and Retention
- 6. Accuracy
- 7. Safeguards
- 8. Openness
- 9. Individual Access
- 10. Challenging Compliance

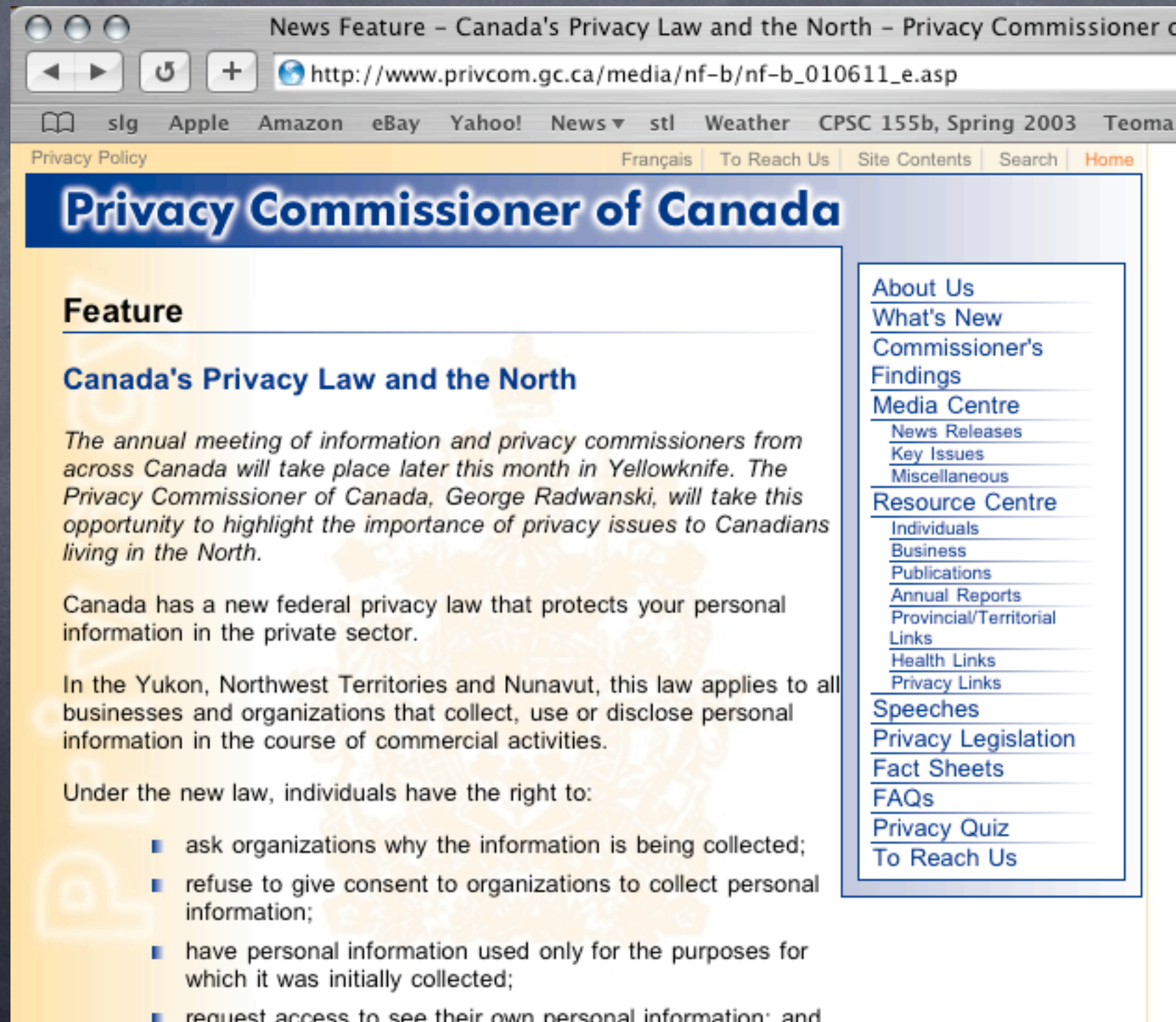


# 1999: Canada "C6"

- Comprehensive privacy law applies to both public and private sector
- National businesses, banks, etc
- Medical records, prescriptions and insurance records (January 1, 2002)
- Law extends to all commercial activity in Canada (January 1, 2004)



# What really makes C6 work...



The screenshot shows a web browser window with the title "News Feature – Canada's Privacy Law and the North – Privacy Commissioner of Canada". The address bar shows the URL "http://www.privcom.gc.ca/media/nf-b/nf-b\_010611\_e.asp". The browser's toolbar includes links to "slg", "Apple", "Amazon", "eBay", "Yahoo!", "News", "stl", "Weather", "CPSC 155b, Spring 2003", and "Teoma". The website's navigation bar includes "Privacy Policy", "Français", "To Reach Us", "Site Contents", "Search", and "Home". The main heading is "Privacy Commissioner of Canada". The "Feature" section is titled "Canada's Privacy Law and the North" and contains the following text:

*The annual meeting of information and privacy commissioners from across Canada will take place later this month in Yellowknife. The Privacy Commissioner of Canada, George Radwanski, will take this opportunity to highlight the importance of privacy issues to Canadians living in the North.*

Canada has a new federal privacy law that protects your personal information in the private sector.

In the Yukon, Northwest Territories and Nunavut, this law applies to all businesses and organizations that collect, use or disclose personal information in the course of commercial activities.

Under the new law, individuals have the right to:

- ask organizations why the information is being collected;
- refuse to give consent to organizations to collect personal information;
- have personal information used only for the purposes for which it was initially collected;
- request access to see their own personal information; and

The right sidebar contains a list of links: "About Us", "What's New", "Commissioner's Findings", "Media Centre" (with sub-links "News Releases", "Key Issues", "Miscellaneous"), "Resource Centre" (with sub-links "Individuals", "Business", "Publications", "Annual Reports", "Provincial/Territorial Links", "Health Links", "Privacy Links"), "Speeches", "Privacy Legislation", "Fact Sheets", "FAQs", "Privacy Quiz", and "To Reach Us".



# Approaches to Privacy Enforcement

## • Governmental Standards

- Enforcement by regulatory agencies, states, etc.
- Enforcement through litigation

## • Industry Standards

- "Codes of conduct"
- Limited enforcement through licensing
  - TRUSTe didn't throw out Microsoft
- Enforcement through "market forces"
- Limited enforcement from government

## • Unregulated Market

- Caveat emptor



"Video Rental Records have better protection than medical records."

- This was true in 1990
- No Longer



Robert Bork





# "Privacy" in the US, Last Few Years

## • Some Legislation

- HIPAA — Health Insurance Portability and Accountability Act (1996)
- COPPA — Children's Online Privacy Protection Act (1998)
- GLB — Gramm-Leach-Bliley Act of 1999  
(Final rule, May 24, 2000)
- Sarbanes-Oxley Act of 2002

## • "Voluntary" Standards

- Payment Card Industry Data Security Requirements



# HIPAA - 1996\*

## • Key Provisions:

- Largely about health insurance portability, not about privacy
- Privacy mandates are largely about security:
  - Firewalls, anti-virus, etc.
  - Designate a privacy officer
  - Post privacy policy
  - Require outsourcing companies to protect information.
  - Access to health information; procedures for correcting errors.
- Enforced by the States (unfunded mandate); HHS enforces in "extreme cases."

(\*privacy rule passed 2002)



# COPPA (1998)

## • Key Provisions:

- Applies to online collection information on children under 13
- Requires "verifiable parental consent"
  - Very hard in most cases; letter, fax or phone call
  - Some exceptions — one time response to "homework help"
- Privacy notice must be posted on website

• <http://www.ftc.gov/opa/1999/9910/childfinal.htm>



# GLB (2000)

- Consumers must be informed of privacy policies
  - Initial notice
  - Annual notice
  - Mostly ignored!
- Consumers must have a chance to "opt-out"
  - Many different ways to "opt-out"



# California SB 1386:

- Applies to all agencies, persons or businesses that conduct business in California.
- Must notify CA residents if personal information is acquired by an unauthorized person.
- Excludes "encrypted" information.



# S.2201

## The "Missed Opportunity?"

- Online Privacy originally an FTC initiative
  - 1995-1999: Heavy push for industry self-regulation
  - 1998: Industry fails with children; Congress passes COPPA.
  - 2000: FTC admits that self-regulation failed; recommends legislation.
- FTC's Recommendations:
  - Notice
  - Choice
  - Access
  - Security



## S.2201 (cont.)

- Notice, Access, Choice and Security
- Mandatory opt-in for "sensitive" info:
  - Race, income, sexual preference
- Mandatory opt-out for other information:
  - Name, email address, purchase history
  - Opt-out for Collection and sharing
- National law that preempts state laws.
- Right to sue for security breaches.



# Trust Marks "Trust Us."

- Original plan was to have minimal standards
- Today, they mandate that Companies Follow their privacy policies

