

# Canada's new privacy laws ...

... and how you can  
benefit from them!



## APSGroup

Your privacy and security management partner

# Topics to Cover

---

- Current Environment
- Overview of privacy legislation
- Fair Information Practices
- Key Compliance Issues
- Privacy Safeguards
- Steps to Compliance and Beyond
- The Privacy Payoff

---

“You have zero privacy  
anyway. Get over it.”

Scott McNealy, CEO Sun Microsystems,  
1999, when asked about efforts to  
combat the tracking of Internet users

# Current Environment

---

“175 Million E-mail  
Addresses for  
\$220 U.S.”

“**17,000 names, addresses and  
driver’s licence info were stolen from  
UC Berkeley’s library – UC waits 3  
months to notify individuals**”

“27 million employees  
under constant  
surveillance”

“**Security breach  
at Equifax opens  
1,400 Canadians  
to possible  
identity theft**”

“Exxon Valdez of  
data leaks: personal  
information of  
180,000 customers of  
Co-operators Life”

“Bank of Montreal  
servers offered on eBay  
– sensitive customer  
info included”

“Canada Customs and Revenue Agency break-in -  
theft of information about 120,000 Canadians,  
including social insurance numbers...”

# Identity Theft Complaints

---



- Identity theft cost Canadians over \$21.5M in losses in 2003 – up from \$8.5M in 2002.
- Nearly \$2M in BC alone!

Source: PhoneBusters.com

# Technology Fuels Privacy Concerns

---

- Caller ID



- Surveillance cameras

- Web bugs

- Cell phone locators

- Telematics / GPS in cars

- Airline passenger database

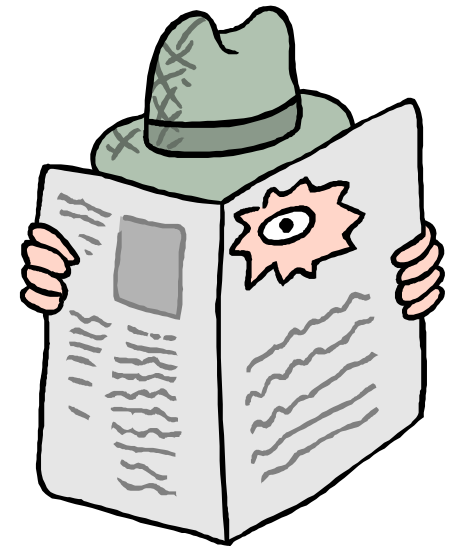
- Biometrics

And much, much more...

# What about your own privacy?

---

- Have you ever shopped on-line?
- Do you use credit cards?
- Do you have a mobile phone?
- Do you drive a car?
- Do you use a loyalty card?
- Do you rent videos?
- Do you use a security card to access your office?
- Do you use an ATM card?
- Do you subscribe to magazines?
- Do you use the Internet?
- Do you recycle paper?



# How Do Consumers React?

---

- 84% of Internet users are **concerned** about businesses getting personal information about them
- 24% of Internet users have provided a **fake name** or personal information to avoid giving a Web site real information



'Trust and Privacy Online' survey, conducted by the Pew Internet and American Life Project, Aug. 2000



# How Do Consumers React?

---

2 out of 3 web shoppers surveyed deliberately chose not to buy goods from an online retailer because of privacy concerns.



IDC "Online Consumer Internet Privacy Survey 2000"

# Privacy Violators – How to Punish?

---

Percent who think privacy violators should be punished

94%

## Suitable punishments:

Public blacklisting of site

30%

Site should be shut down

26%

Company should pay fine

27%

Owners should go to prison

11%



Source: Aug. 2000 survey 'Trust and Privacy Online', conducted by the Pew Internet and American Life Project

# Topics to Cover

---

- Current Environment
- Overview of privacy legislation
- Fair Information Practices
- Key Compliance Issues
- Privacy Safeguards
- Steps to Compliance and Beyond
- The Privacy Payoff

# Government Response

---

## Canada

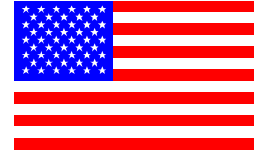


- PIPEDA – Federal legislation
- BC Personal Info. Protection Act
- Alberta PIPA similar to BC
- Quebec – since 1994
- Ontario – not passed

# Government Response

---

## USA



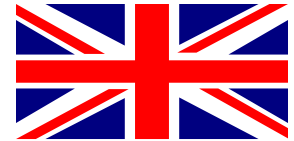
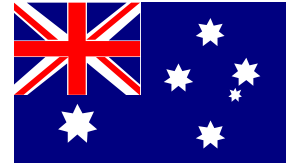
- 228 separate pieces of legislation
- Gramm-Leach-Bliley for financial services industry
- HIPAA for healthcare industry
- Children's Internet Protection Act
- California legislation on notification of breaches has global implications
- Patriot Act can ignore most of above

# Government Response

---

## Outside North America

- UK, European Union, Australia, Singapore and many other countries are well ahead of Canada
- Most require equivalent privacy laws to do international business where personal information is shared



# Legal Situation in Canada - PIPEDA

---

- Personal Information Protection and Electronic Documents Act
  - Came into force on Jan 1, 2001 for **federally regulated companies**, such as banks and airlines
  - As of January 1, 2004, **all** organizations, individuals, associations, partnerships and trade unions are covered IF they collect, use or disclose personal information in the course of commercial activities.
  - Provincial legislation must be '**substantially similar**' to PIPEDA otherwise PIPEDA applies
- “PIPEDA creates an enforceable right to privacy for individuals” – Canadian Institute of Chartered Accountants

# Legal Situation in BC - PIPA

---

- BC Personal Information Protection Act took effect Jan 1, 2004
- Covers ALL organizations, including non-profits and trade unions, associations
- Covers customers, employees, donors, volunteers, contractors, suppliers and members





# PIPA Exclusions

---

- Business contact information (business card details)
- Information captured by PIPEDA (trans-border transfers)
- Public body or information under FOIPP
- Personal or domestic uses
- Journalistic, artistic, literary uses
- The Courts
- Work product information



# PIPA and Employee Information

---

- May collect, use and disclose employee personal information for **reasonable purposes** that are necessary to establish, manage or terminate the employment relationship **without consent** as long as employee is **notified**
- Some limited exceptions to notification (e.g. for medical emergency, investigation)



# PIPA Grandfather Clause

---

- Organizations do not have to 're-collect' personal information they already hold
- BUT, may only use and disclose for purposes that are reasonable and consistent with original purposes when collected
- All other protections will apply (e.g. security, new uses, right of access)



# PIPA Enforcement

---

- BC Privacy Commissioner may make orders and will name offenders
- Fines up to **\$100,000** for non-compliance



- [www.mser.gov.bc.ca/foi\\_pop/Privacy](http://www.mser.gov.bc.ca/foi_pop/Privacy)  
or call PIPA Hotline at 250-356-1851

# What is Personal Information?

---

- Personal Information is “information about an identifiable individual” that includes any factual or subjective information, recorded or not, in any form. Examples:
  - Name, ID number, income, blood type
  - Evaluations, comments, social status or disciplinary actions
  - Employee files, credit records, loan records
- Sensitive Information
  - Medical / health conditions
  - Financial information
  - Racial or ethnic origins, sexual preferences
  - Political or religious beliefs




# Topics to Cover

---

- Current Environment
- Overview of privacy legislation
- **Fair Information Practices**
- Key Compliance Issues
- Privacy Safeguards
- Steps to Compliance and Beyond
- The Privacy Payoff

# Fair Information Practices

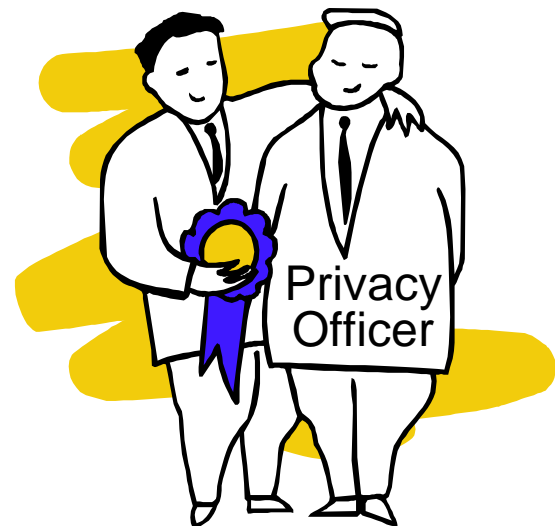
---

- 
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

# 1. Accountability

---

An organization is responsible for personal information under its control and shall designate an individual or individuals who are **accountable** for the organization's compliance with the following principles.





## 2. Identifying Purposes

---

The **purposes** for which personal information is collected shall be identified by the organization at or before the time the information is collected.



# 3. Consent

---

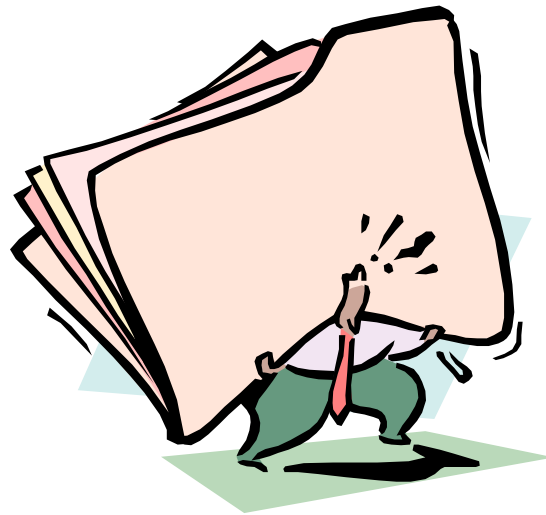
The **knowledge** and **consent** of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.



## 4. Limiting Collection

---

The collection of personal information shall be **limited** to that which is **necessary** for the purposes identified by the organization. Information shall be collected by **fair** and **lawful** means.

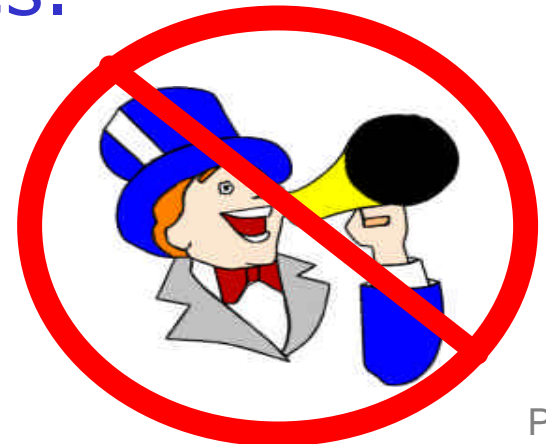


## 5. Limiting Use, Disclosure & Retention

---

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law.

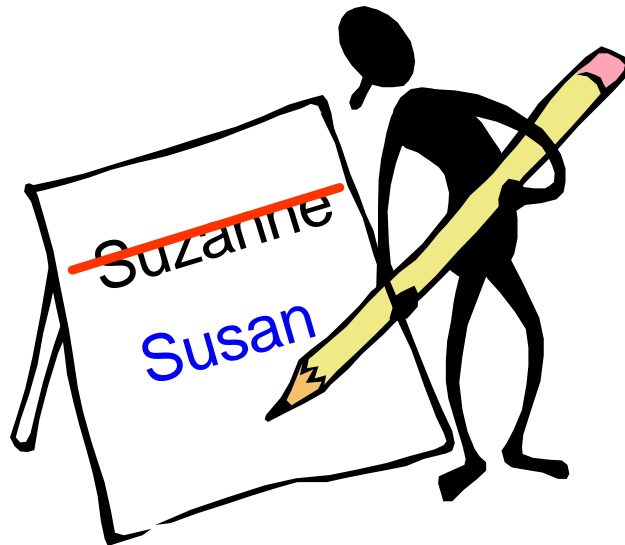
Personal information shall be retained only as long as necessary for fulfilment of those purposes.



## 6. Accuracy

---

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.



# 7. Safeguards

---

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.



## 8. Openness

---

An organization shall make **readily available** to individuals specific information about its policies and practices relating to the management of personal information.



### APS Group Privacy Policy

1. Our Commitment
2. Privacy Practices
3. Website and E-Commerce
4. Contact Information

## 9. Individual Access

---

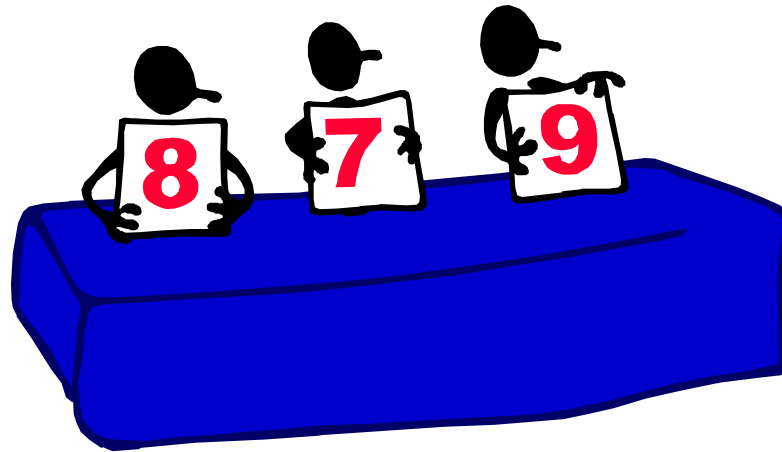
Upon request, an individual shall be **informed** of the existence, use and disclosure of his or her personal information and shall be given **access** to that information. An individual shall be able to **challenge** the accuracy and completeness of the information and have it **amended** as appropriate.



# 10. Challenging Compliance

---

An individual shall be able to address a **challenge** concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.



# Topics to Cover

---

- Current Environment
- Overview of privacy legislation
- Fair Information Practices
- **Key Compliance Issues**
- Privacy Safeguards
- Steps to Compliance and Beyond
- The Privacy Payoff

# Key Compliance Issues

---

- Purpose
  - What is a reasonable business purpose and who decides?
  - Secondary uses
- Consent
  - Express or implied
  - Opt-in vs. opt-out
  - Tracking of consent
- Access
  - Developing cost-effective procedures and safeguards

# Key Compliance Issues – Cont.

---

- Employee information
  - Monitoring / surveillance
  - Access to personnel files
- Third party relationships
  - Who is accountable?
- Safeguards
  - How much is enough?

# Topics to Cover

---

- Current Environment
- Overview of privacy legislation
- Fair Information Practices
- Key Compliance Issues
- **Privacy Safeguards**
- Steps to Compliance and Beyond
- The Privacy Payoff

# Start at the Beginning

---

- Deal with privacy and security issues at the beginning rather than forcing it in at the end!
  - Business case
  - Project planning & feasibility studies
  - Development and testing
  - Change management
- Make privacy impact assessments part of business cases and feasibility studies

# Privacy Impact Assessments

---

Ask the questions....

- Why is this information being collected?
- Who will use this information?
- How will the information be used?

Assessment should occur during  
business case or project planning

# Computer-Use Policy

---

## Key Elements of Policy

- Establishing no expectation of privacy
- Protecting sensitive information
- Monitoring use of proprietary assets
- Improper employee use
- Allowable employee uses
- Disciplinary action
- Employee acknowledgement of policy

Source: GAO's analysis of recommended computer-use policies.



# Supporting Players

---

- Other corporate policies should support or reference privacy and security efforts
  - Provide guidance to employees, business partners, contractors, etc.
  - Set expectations and avoid confusion
  - Provide guidance on who to contact and how to raise privacy / security related concerns

# Information Management

---

- Corporate records management
- Data inventory and classification
  - What information is collected and available
  - How & where information is collected
  - Why is it collected
  - Who sees it and when
  - How sensitive is it
  - Consent requirements (to collect or release)
  - Retention and destruction

# Information Management

---

- Potential benefits
  - Helps decide level of protection needed for data combinations
  - Streamline collection processes
    - Which sources are most current
    - Which sources are most accurate
    - Avoid duplication of efforts
  - Eliminate unnecessary data
    - Reduce storage requirements & costs
    - Can't lose what you don't have!

# Protection by Default

---

- Protect everything as a default
  - Don't rely on vendor default settings
  - Only allow access by authorized users for authorized business purposes
  - Easier to grant access than try to figure out if information has inadvertently been left "in the open"
  - Propagate same levels of security if file is moved or copied
- Don't forget to protect any back-up and log files as well!

# Everyone's Unique

---

- An important precept is accountability
- Each person accessing information in your charge should have a unique user identification (user-id)
  - Easier to assign individual access privileges
  - Easier to assign temporary access privileges
  - Easier to rescind individual privileges
  - Track access to address accountability

# Origins

---

- Limit access based on location
  - inside your trusted network
  - outside your trusted network
    - dial-up, dedicated line, or VPN
    - wireless
    - over the Internet
- Limit access by date and time

# Beyond Passwords

---

- Access to your information systems should at *minimum* require a unique user identifier & password in combination
- Remote access should consider using additional multi-factor authentication
- Extremely sensitive information might also require additional authentication
- Consider encryption when storing or transmitting extremely sensitive information.

# Beyond Passwords

---

- Don't allow "remembering" of passwords by programs at log-in
- Don't hardcode passwords in scripts
- Files on laptops should be encrypted
  - Better still, do not allow sensitive files on laptops, etc.



# Keeping Track

---

- Knowing what has happened to data or information is integral to privacy and security efforts
- Privacy & disclosure breaches are rarely committed by changing information, usually only access is involved
- Most systems only track changes to data; many don't even track changes!

# Keeping Track

---

- Comprehensive logging capabilities
  - read only or browse access
  - update / modify
  - create / delete
  - failed access attempts
- Log records should show at minimum
  - date and time of access
  - user-id
  - some details of record being accessed
  - access type

# Gone but Not Forgotten

---

- Deleting file does not mean information it contained is no longer available
- Recovery tools readily available
- Possible courses of action
  - Encrypt file several times before “deleting”
  - Use a good quality “shredder” program
  - Physically shred or destroy media

# Gone but Not Forgotten

---

- And don't forget about other data...
  - back-up copies
  - PCs being replaced, sold or re-cycled
  - PDAs, laptops, cell-phones, etc.
  - hard drives being replaced
  - floppy diskettes
  - CDs and DVDs
  - voice mail systems
  - access cards and badges

# Paper Trails

---

- Printed reports need to be handled with the same diligence as computer files.
- Keep track of where reports with sensitive or confidential data are distributed
  - Review reports to see if really needed
  - Limit distribution of sensitive reports
  - Provide lockable cabinets for report storage

# Threats From Within

---

“The greatest security asset, and the greatest security risk”

- Background Checks
- Confidentiality and Disclosure
- Monitoring and Surveillance
- Subcontractors

# Get it in Writing

---

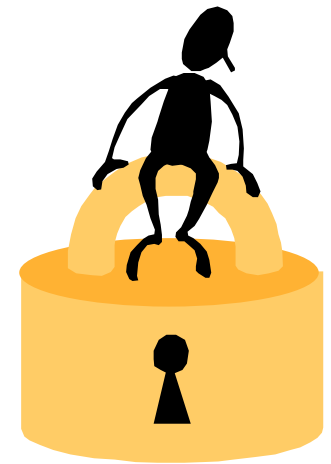
- Make sure business partners align with your privacy and security efforts
- Adherence to your organization's IT privacy and security policy / practices should be included in:
  - confidentiality agreements
  - contracts and service agreements
  - non-disclosure agreements
  - outsourcing agreement
  - termination agreements
- Ensure you have the right to audit their practices

# Privacy Enhancing Technologies

---

## Definition

- “Protocols, standards, and tools that directly assist in protecting privacy, minimizing the collection of personally identifiable information, and when possible, eliminating the collection of personally identifiable information.”



Electronic Privacy Information Center



# Topics to Cover

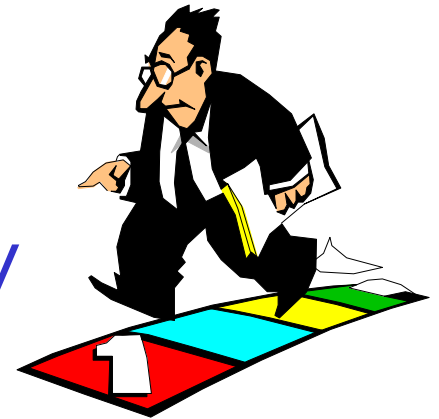
---

- Current Environment
- Overview of privacy legislation
- Fair Information Practices
- Key Compliance Issues
- Privacy Safeguards
- Steps to Compliance and Beyond
- The Privacy Payoff

# Steps to Privacy Management

---

1. Establish accountability
  - Role of the CPO
  - Models being used
2. Conduct a privacy opportunity and risk assessment
  - Inventory of collection practices
  - Consider opportunities, not just risks!
3. Develop your privacy policy
  - Consult with key stakeholders, including customers!
  - Aim to go beyond compliance to best practice
4. Prepare a plan for implementation



# Inventory of privacy practices

---

- What information is collected?
- What are the sources?
- Why is it collected?
- How is it used?
- Where is it stored?
- Who can see it?
- How is it disposed of?
- What security measures are in place?



# Where do you collect info?

---

- Point-Of-Purchase
- Customer Service Numbers
- Kiosks
- Contests
- E-Mail
- Telephone/Voice Mail
- Surveys
- Video Cameras
- Audio Tapes
- Marketing Lists
- Loyalty Programs
- Delivery Services
- Warranties
- Bankruptcies
- Returns
- Application Forms
- Order Forms
- Web Sites
- Bulletin Boards
- Chat Rooms
- Call Centres

Source: **How to Conduct a Privacy Audit**  
Ministry of Management Services website

# Simple Classification Scheme

<b>Info item</b>	<b>Sens. (H/M/L)</b>	<b>Req. / Opt.</b>	<b>Intended Uses</b>	<b>Used By</b>	<b>How do we collect?</b>	<b>Resp. dept.</b>
Name & Address	M	R	Order taking Account Contact Mailings	Accounts Marketing Order Desk Shipping	Phone Website	Accounts
Age	H	O	Seniors discount	Order Desk	Phone	Accounts
Phone Number	H	R	Order or account problems	Customer service		Accounts
Credit Card #	H	O	Credit card orders	Order Desk Accounts	Phone Website	Accounts

# Assess opportunities, not just risks!

---

- Customer profile
  - Do you know their privacy preferences?
  - Expectations may depend on geographic location
- Value proposition
  - Is the exchange of value clear and compelling?
  - Are there incentives for accuracy?
- Trust proposition
  - Is your message easy to find?
  - Why should they trust you?



# Assess opportunities, not just risks!

---

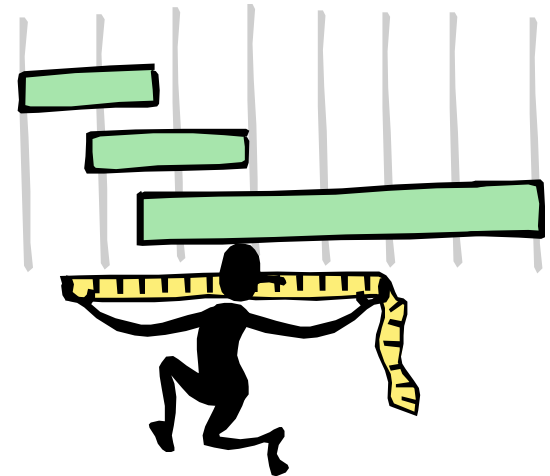
- Competitor Analysis
- Marketing Messages
  - Communicating your trustworthiness
- Brand Alignment
  - Consistency of privacy approach with other brand values
- Information Management
  - Do you know what your information costs are?
- Strategic Partners
  - Privacy is a global phenomenon



# Elements of your Implementation Plan

---

- Develop supporting procedures, forms and systems
  - Consent
  - Inquiries
  - Individual access
  - Complaint handling
  - Security measures
- Enable technical safeguards
- Revise third party contracts
- Train staff, contractors and volunteers
- Provide information to your customers in various media





# Topics to Cover

---

- Current Environment
- Overview of privacy legislation
- Fair Information Practices
- Key Compliance Issues
- Privacy Safeguards
- Steps to Compliance and Beyond
- The Privacy Payoff

# Privacy as a Competitive Edge

---

- 47% of US firms with privacy officials surveyed recognize privacy as a competitive edge issue with consumers where they want to play a leadership role
- Senior management supports a proactive, 'leadership-oriented' privacy policy.

Source: Privacy and American Business

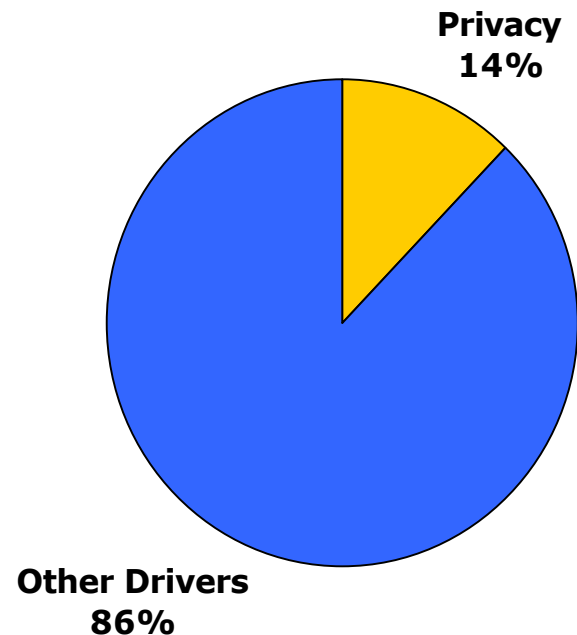
# Privacy Brand Valuation

---

For Royal Bank of Canada, privacy accounts for an estimated **14%** of overall Brand Value!

## PRIVACY VS. BRAND VALUE

CAN \$679 M



Source: Privacy Payoff, by Ann Cavoukian, Information and Privacy Commissioner of Ontario

# Consumer Attitudes Towards Privacy

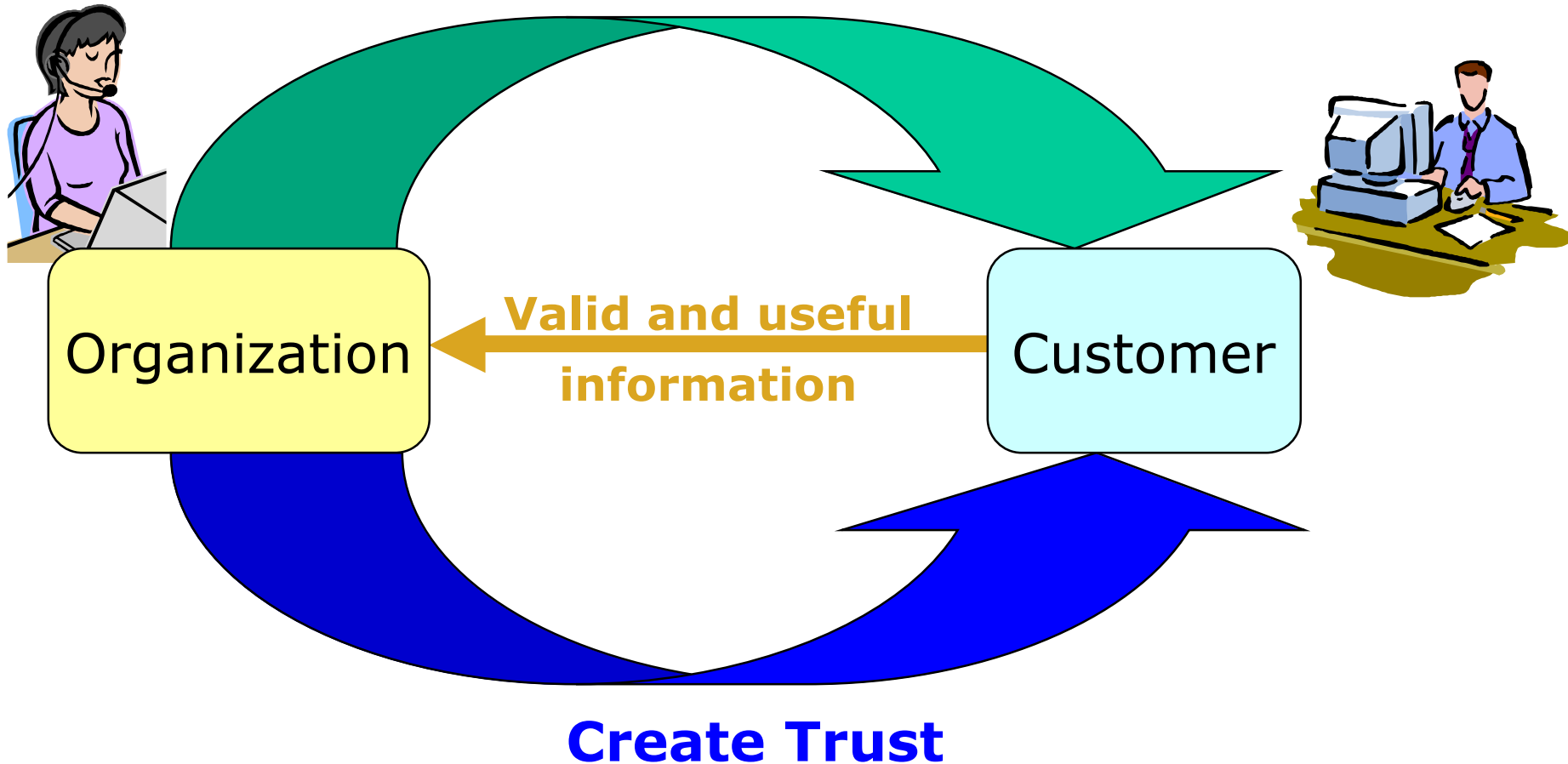
---

	<u>1990s</u>	<u>Nov/2001</u>
Privacy unconcerned	20%	8%
Privacy pragmatists	55%	58%
Privacy fundamentalists	25%	34%

**Source:** 2001 US Survey of 1,500 Americans  
“Privacy On and Off the Internet: What Consumers Want”  
conducted by Harris Interactive for Privacy and American Business

# The Privacy Exchange

**Provide Value**



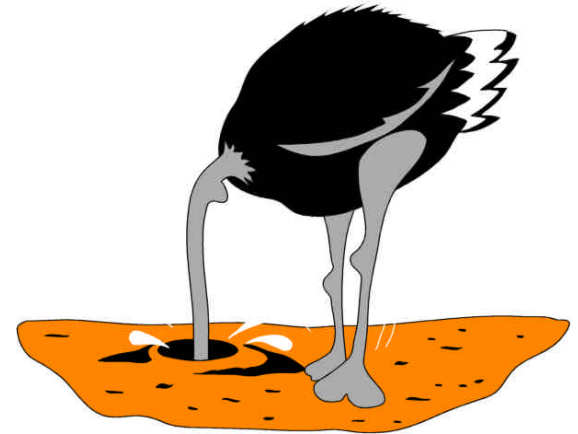
# Business Strategic Questions

---

- Complying with the letter of the legislation?

OR

- Having a proactive privacy strategy to take a leadership role with consumers?



# Famous Quotes Revisited

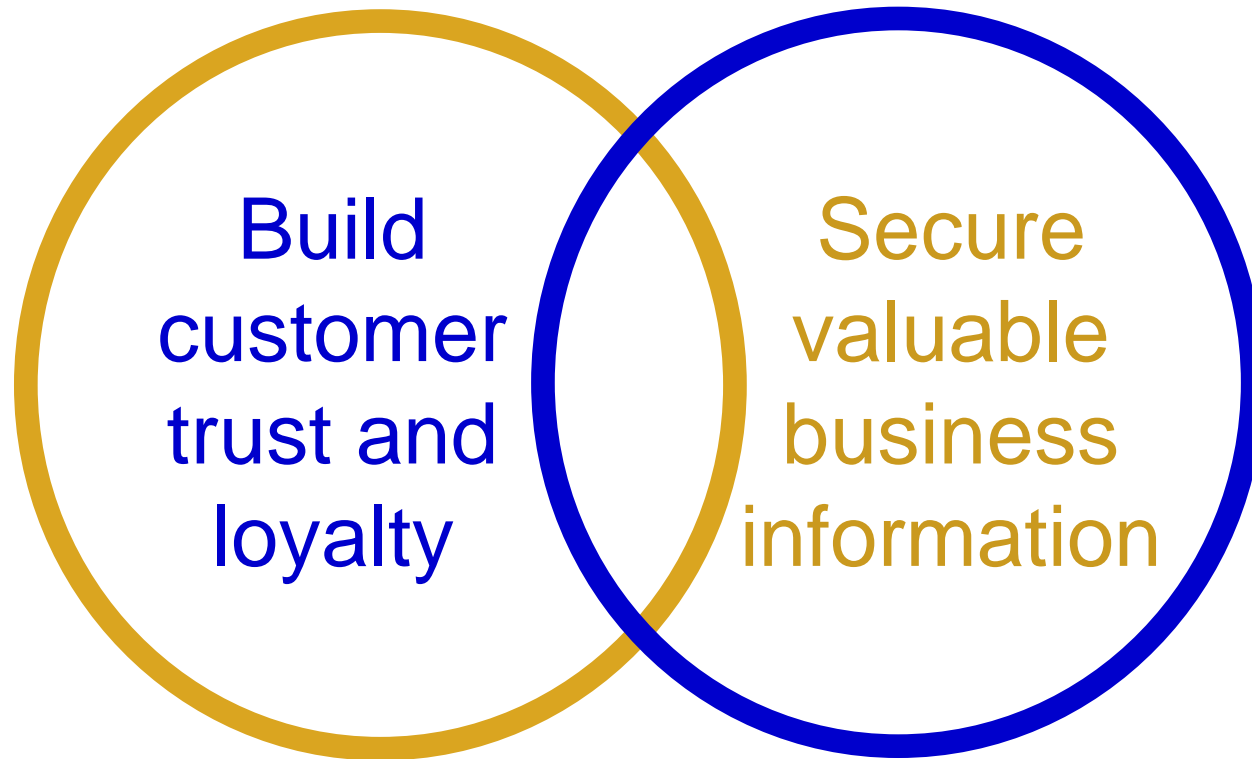
---

*"Trust is the real currency of the Internet. Squander what you have and you'll find out how hard it can be to get more."*

Scott McNealy, 2001

# Business Imperatives

---



Applied **Privacy** & **Security** Group

**APS**Group



# Who is APSGroup?

---

- Consulting and advisory firm specializing in privacy and information security
- Experienced business and technology consultants – 20+ years of experience each. Big firm expertise without the overheads.
- Accredited in information security, accounting, information systems audit, disaster recovery planning and management consultancy.
- Knowledgeable - we keep abreast of information privacy and security developments through research, conferences and regular contacts with other experts in the field.
- Independent of any vendors so we can offer unbiased product assessments.
- Local expertise - in Vancouver, Surrey and Victoria. We are convenient and accessible.

# Privacy Service Offerings

---

- Privacy Opportunity and Risk Assessment
  - Quick snapshot of critical risks
  - Helps you focus your compliance efforts
  - Identifies opportunities to attract customers and cut costs
- Privacy Policy Development
- Privacy Expert on Call
  - Cost-effective way for small and medium-sized businesses to get expert assistance as needed
- Privacy Awareness Training
  - Seminars at convenient hours
  - Customized on-site training sessions

# Security Services

---

- Security management
  - Integrated risk management framework
  - Structured workshop approach
  - Appropriate and cost-effective controls
- Security Training / Awareness
  - Turn your weakest link into your strongest assets
  - Customized on-site training sessions

# Business Continuity Planning

---

- Could your business survive a natural or man-made disaster? Are you relying on luck?
- We can help you with:
  - Risk evaluation
  - Business impact analysis
  - Realistic and cost-effective strategy
  - Recovery plans
  - A compelling case for action
  - Implementation assistance

For more information, to request a presentation to your organization or for assistance with conducting an Opportunity and Risk Assessment or Privacy Impact Assessment, please contact us:

Susan Johnson      1.604.833.9358

Bob Tremonti      1.604.986.4930

John Glover      1.250.888.6564

OR

Information@APS-Group.com

Please visit our website at: <http://www.APS-Group.com>

Seminars and self-assessment tools are also available.