New Research
Canadian Privacy Breaches

Tracy Ann Kosa, Privacy Impact Assessment Specialist

SecTor 2008
Illuminating the Black Art of Security
October 7-8, 2008

Agenda / Overview

- **Defining Privacy**
- **Regulatory Environment**
  - Legislation
  - Office of the Privacy Commissioner of Canada
  - Privacy Breaches
- **Research**
  - Hypothesis
  - Methodology
  - Results
  - Next Steps

Defining Privacy

- **3 Dimensions of Privacy:**
  - Territorial
  - Physical
  - Informational

Informational Privacy

- **"Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others"**

(Westin 1967)

Personal Information

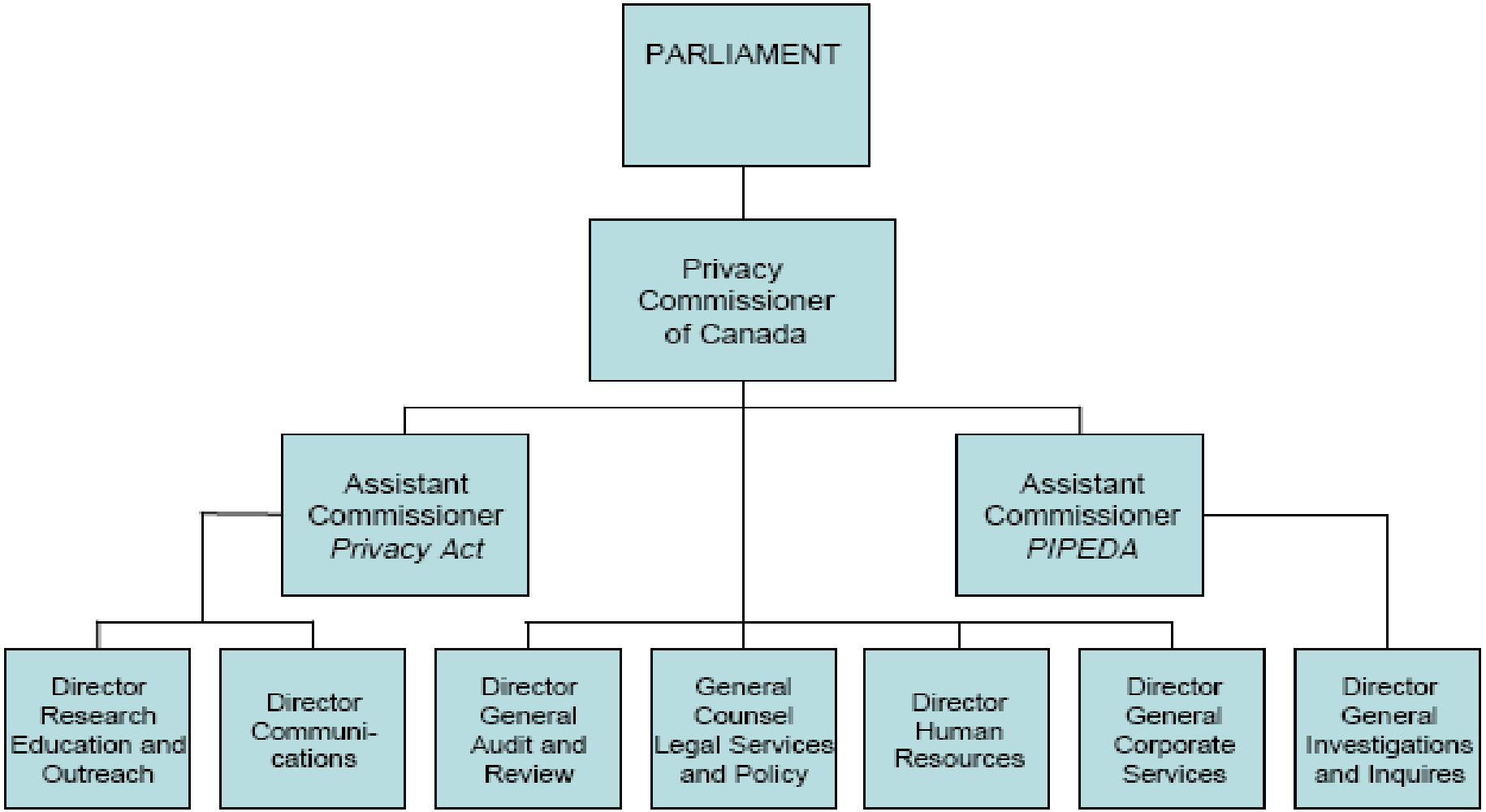
- **Any information concerning the personal or material circumstances of an identified or identifiable person**

Regulatory Environment

- **Office of the Privacy Commissioner**

- **Legislation**
  - Public versus Private Sector
  - Industry Specifics
  - PIPEDA v. PHIPA

Office of the Privacy Commissioner

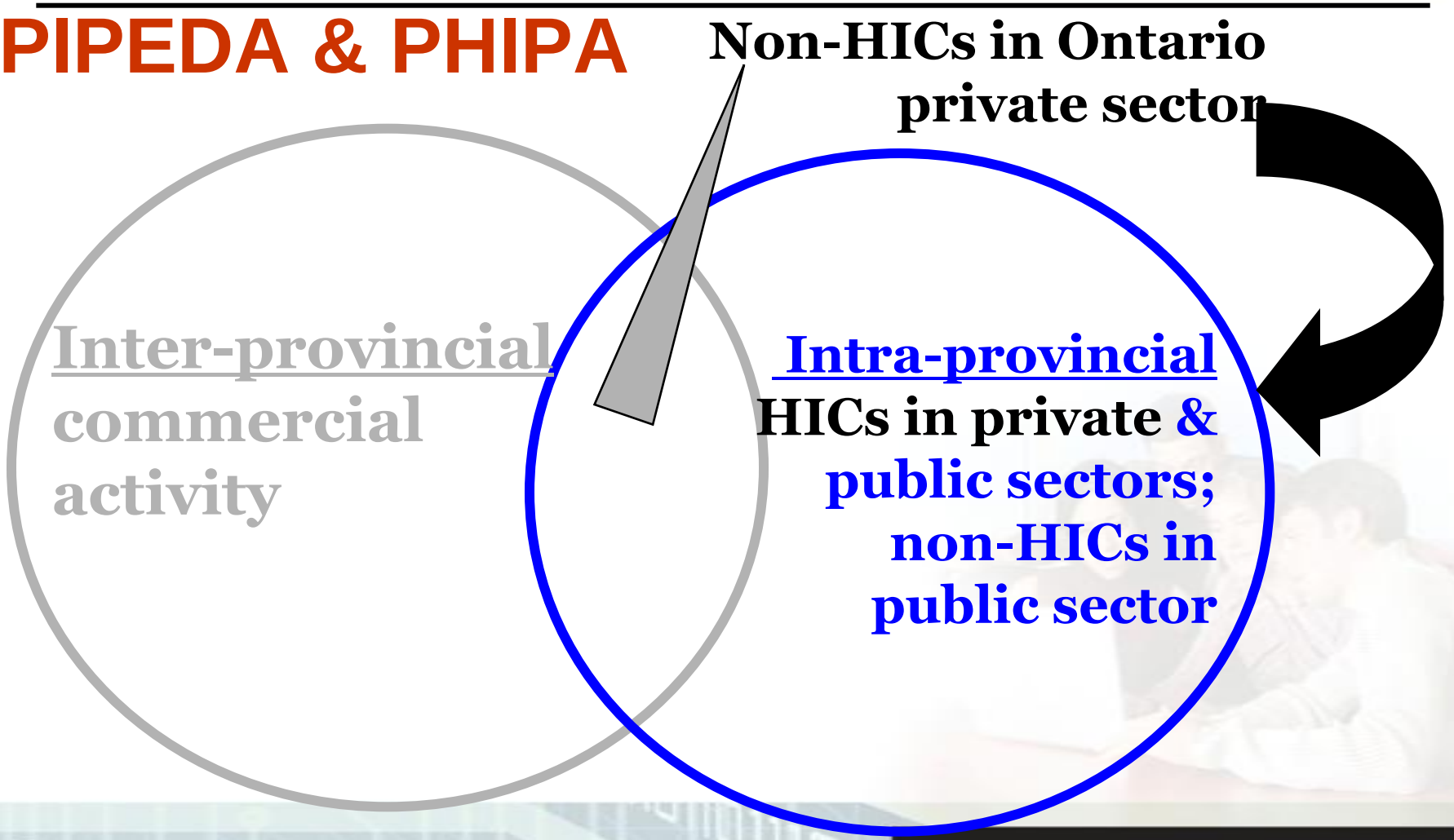


Office of the Privacy Commissioner

- **Independent office that oversees Canada's private sector privacy law**
- ***PIPEDA* applies to all personal data that flows across provincial or national borders, in the course of commercial transactions involving organizations subject to the Act or to substantially similar legislation.**

- **Roles:**
  - Investigating Complaints (PIPEDA s.11) in the private sector – except Quebec, BC & Alberta, and Ontario in respect of PHI
    - *Negotiation, persuasion, mediation and conciliation*
  - Conducting Audits (PIPEDA s.18), Pursuing Court Action
  - Public Reporting, Advocacy, Research and Public Awareness
- **Powers:**
  - Summon witnesses, administer oaths and compel the production of evidence.
  - Taking matters to Federal Court (to seek a court order)

PIPEDA & PHIPA



Office of the Privacy Commissioner Plans & Priorities 2008-2009

- **The four priority privacy issues areas are:**
  - information technology
  - national security
  - identity integrity and protection
  - genetic information

PIPEDA Audits

- **PIPEDA s.18**
  - Mandate to conduct audits of the personal information management practices in the private sector where there is reasonable grounds to believe there is noncompliance with *PIPEDA*

Office of the Privacy Commissioner Plans & Priorities, 2008-2009

- **"At the time of preparing this report, no new audits are planned in the private sector under Section 18 of the *PIPEDA*. We will be further developing and applying a process for selecting *PIPEDA* audits based on reasonable grounds."**

Office of the Privacy Commissioner Plans & Priorities, 2008-2009

The following two tables present the financial and human resources of the OPC over the next three fiscal years.

Financial Resources (planned)

2008-2009	2009-2010	2010-2011
$18,979, 000	$18,997,000	$19,001,000

Human Resources (planned)

2008-2009	2009-2010	2010-2011
150 FTEs*	150 FTEs	150 FTEs

* FTE: Full-Time Equivalent

1.8 Departmental Planned Spending and Full-Time Equivalents

($000)	Forecast Spending 2007–2008	Planned Spending 2008–2009	Planned Spending 2009–2010	Planned Spending 2010–2011
Compliance Activities	10,084	9,675	9,672	9,672
Research & Analysis	4,606	4,386	4,385	4,385
Public Outreach	3,656	3,766	3,785	3,785
Total Planned Spending	**18,346**	**17,827**	**17,842**	**17,842**
Adjustments				
Implementation of the *Federal Accountability Act*	1,365	1,152	1,155	1,159
Total Planned Spending	$19,711	$18,979	$18,997	$19,001
Full Time Equivalents	154	150	150	150

Office of the Privacy Commissioner Plans & Priorities, 2008-2009

The amounts under "Adjustments" include resources that will be required for new responsibilities related to the implementation of the *Federal Accountability Act (FedAA)*; namely the creation of an office to manage access to information and privacy requests and additional privacy investigators to handle new organizations that are now subject to the *Privacy Act*. Funds for the implementation of the *FedAA* within the OPC have been earmarked within the Government of Canada fiscal framework. However, final spending plans will only be determined once a detailed business case has been prepared and submitted to the Parliamentary Panel on the Funding of Officers of Parliament and subsequently approved by Treasury Board ministers.

Research – Background

- **Enforcement of PIPEDA is complaint driven, findings are published**
- **Privacy 'Breaches'**
  - Not all privacy breaches are a violation of PIPEDA and not all violations of PIPEDA are privacy breaches
- **Existing OPC Analysis:**
  - PIPEDA complaints by type
  - PIPEDA complaints by sector
  - PIPEDA complaints by outcome

Research – Outline

- **Hypothesis**
  - One of the reasons that private sector organizations do not implement privacy is because of the lack of a framework for decision-making

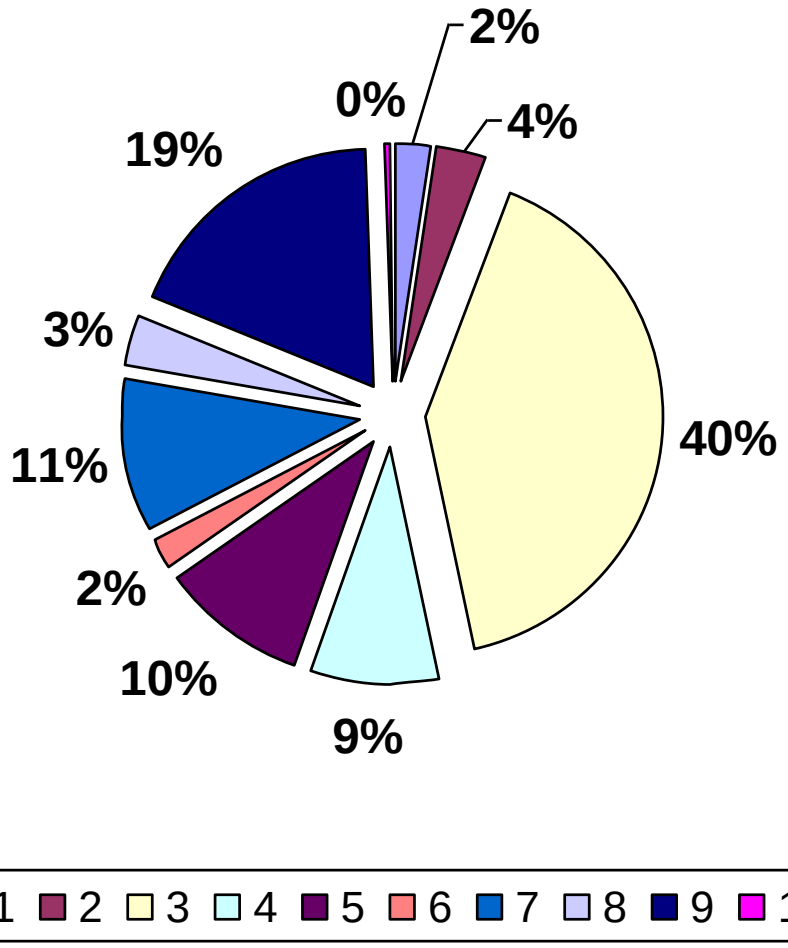
- **Research Question**
  - How can privacy be prioritized for implementation purposes?

- **Methodology**
  - PIPEDA is the private sector privacy legislation, OPC is the regulatory body administering the Act. The published findings could be examined by legislative requirement to provide an indicator of importance.

Research – Step 1 & Step 2

- **Raw Data Analysis**
  - Step 1: PIPEDA Schedule 1, 10 Principles
    - *Which principles have more findings / complaints?*
  - Step 2: PIPEDA Schedule 1, 46 Sub-Principles
    - *Which sub-principles have more findings / complaints?*

Findings by Legislative Requirement
PIPEDA Schedule 1



Research – Step 1, Results

- **PIPEDA Schedule 1, 10 Principles**
  - Which principles have more findings / complaints?
    1. *S.4.3: Consent Requirements*
    2. *S.4.9: Individual Access Requirements*
    3. *S.4.7: Requirements for Safeguards*
    4. *S.4.5: Requirements Limiting Use, Disclosure & Retention*
    5. *S.4.4: Requirements Limiting Collection*
    6. *S.4.2: Purpose Identification Requirements*
    7. *S.4.8: Openness Requirements*
    8. *S.4.1: Accountability Requirements*
    9. *S.4.6: Accuracy Requirements*
    10. *S.4.10: Requirements for Challenging Complaints*

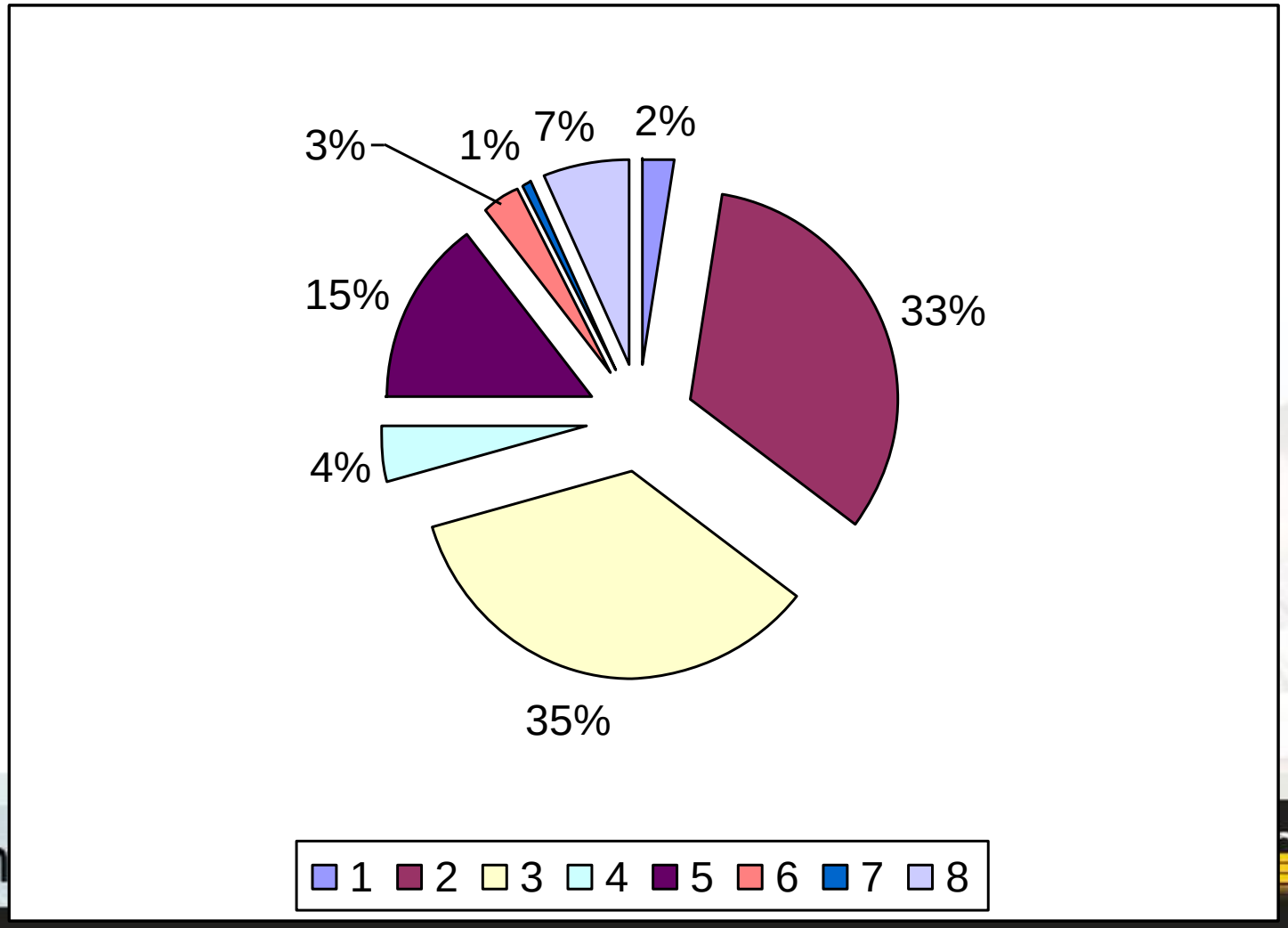
Research – Step 1, Results

- **Top three areas for findings / complaints:**
  - Consent Requirements (s.4.3.)
  - Individual Access Requirements (s.4.9.)
  - Requirements for Safeguards (s.4.7.)

The Top 3: #1 Consent

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

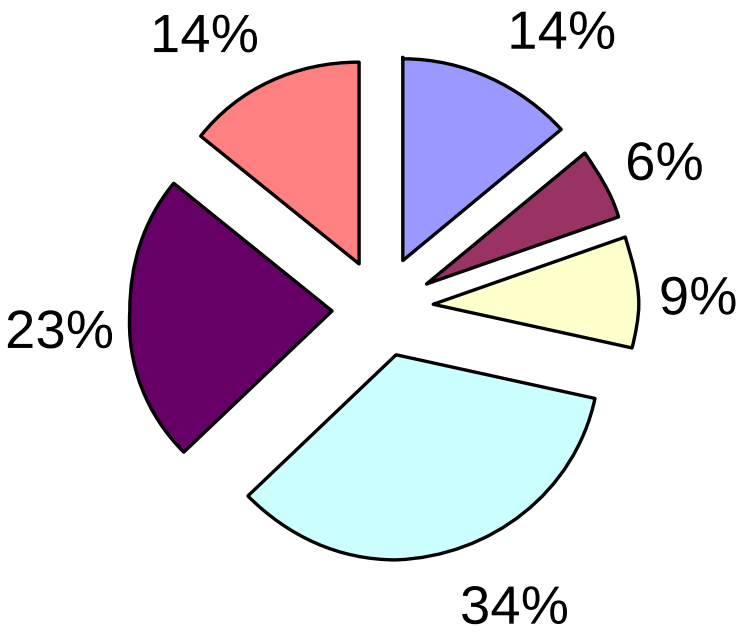
#1 Consent (184 Findings)



The Top 3: #2 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.**

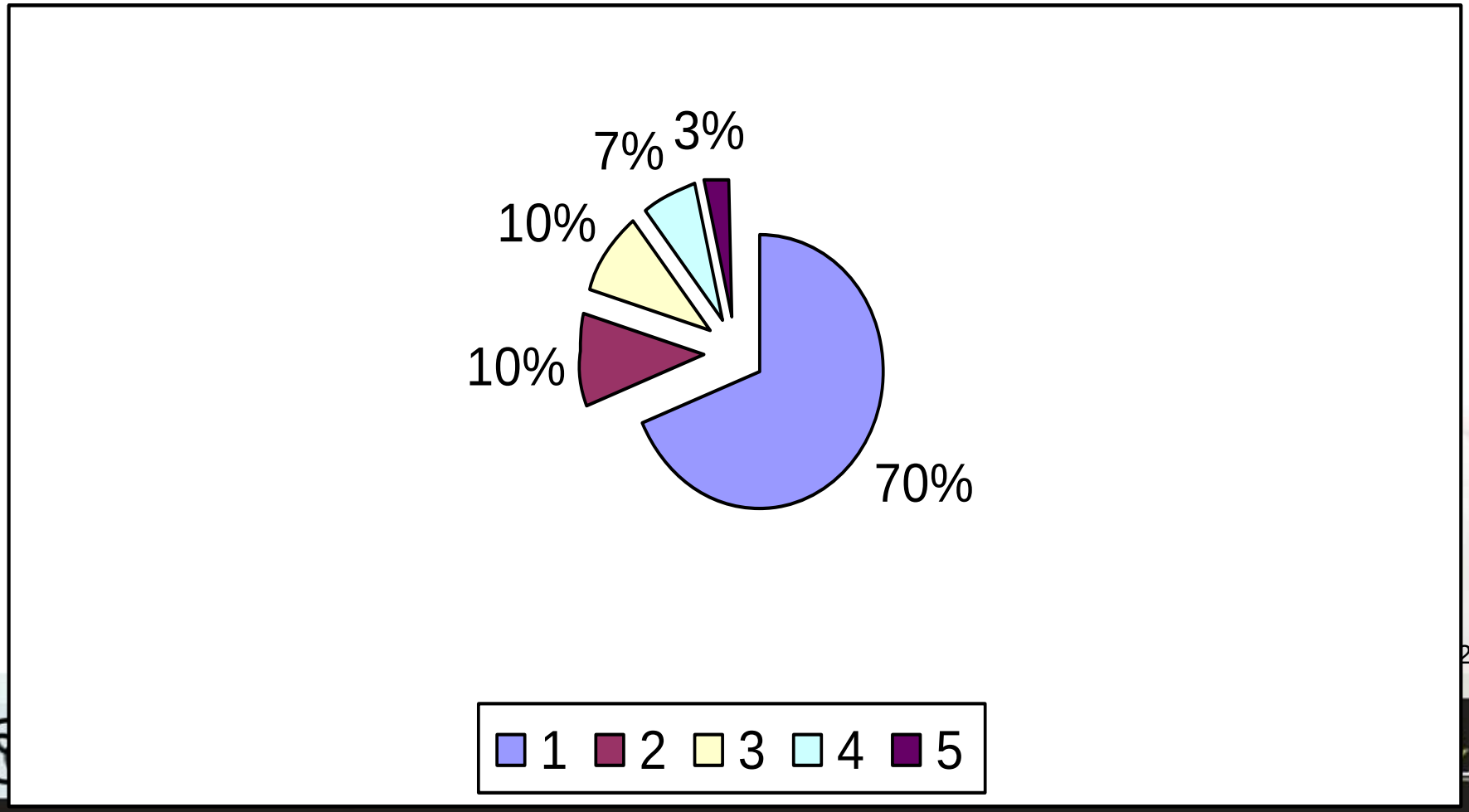
#2 Individual Access (84 Findings)



The Top 3: #3 Safeguards

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

#3 Safeguards (48 Findings)



The Next Layer: Top Five Under the Top Three

- **PIPEDA s.4.3.3.**
  - An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

The Next Layer: Top Five Under the Top Three

- **PIPEDA s.4.3.2.**
  - The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

The Next Layer: Top Five Under the Top Three

- **PIPEDA s.4.7.1.**
  - The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

The Next Layer:
Top Five Under the Top Three

- **PIPEDA s.4.3.5.**
  - In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

The Next Layer: Top Five Under the Top Three

- **PIPEDA s.4.1.3.**
  - An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Next Steps

- **Map the research results against the privacy design requirements**
- **Use the map to guide decision making on accountabilities, business process and technology requirements**

Sneak Preview

- **Detailed privacy requirement (sub-principle) with the most findings: consent is limited to that required to fulfill the explicitly specified, and legitimate purposes of collection (s.4.3.3.)**

- **Corresponding privacy design requirements for the system are:**
  - Ability to manage individual consent preferences
  - Ability to serve consent statement to individual prior to collection
  - Ability to support updated consent statements when notice of collection changes

Tracy Ann Kosa
Privacy Impact Assessment Specialist
PIA Development Service
Office of the Chief Information and Privacy Officer
Ministry of Government Services

(416) 212-1136
tracy.kosa@ontario.ca