

11*12

WHAT STUDENTS NEED TO KNOW ABOUT FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

A Resource Guide for Grade 11/12 Teachers



Ann Cavoukian, Ph.D.

Information and Privacy Commissioner of Ontario, Canada

September 2011

WHAT STUDENTS NEED TO KNOW ABOUT FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

A Resource Guide for Grade 11*12 Teachers

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario, Canada
September 2011

ACKNOWLEDGMENTS

Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario,
gratefully acknowledges the work of:

Sandra Mateus, Teacher, *Peel District School Board*

Bernadette Hattar, Teacher, *Peel District School Board*

Bob Spence, Communications Co-ordinator, *IPC*

Sandra Kahale, Communications, *IPC*

Vance Lockton, Policy Department, *IPC*

in researching and writing this extensively revised and updated edition,
and all those who worked on earlier editions.

PREFACE

The Information and Privacy Commissioner of Ontario (IPC) provides an active outreach program to help increase the awareness and understanding of two very important public values: **open government** and **protection of privacy**. As part of this outreach program, the IPC has developed an elementary and secondary school program: ***What Students Need to Know about Freedom of Information and Protection of Privacy***.

What Students Need to Know provides an opportunity for students and teachers to discuss access to government-held information and protection of privacy as important public values, and how these values are reflected in our relationships with governments.

The program is focused on introducing to or reviewing with students the importance of these two values, and how they are relevant to their lives.

A Resource for Grade 11*12 Teachers is an extensively revised and updated version of the IPC's 2004 Grade 11*12 Teacher's Guide. It contains four units which may be completed one at a time or in combination. The units have been designed to engage students' interests, generate questions, and stimulate group discussion of privacy protection and open government.

This version has been revised to be consistent with the course profiles funded by the Ontario Ministry of Education. New to this version is a Fishbone overview of each unit. Teachers are encouraged to examine the overview and then use, modify or adapt the units and their activities to suit their students' needs.

TABLE OF CONTENTS

	PAGE
Resource Overview	1
Unit Overviews	3
Curriculum Expectations	9
Unit 1 Introduction to the IPC, Freedom of Information and Protection of Privacy	18
1.1 PowerPoint Presentation Outline: <i>Introduction to the IPC, Freedom of Information and Protection of Privacy</i>	
1.2 Handout: <i>Privacy is Your Right</i> Web Quest	
1.3 <i>Exit Ticket</i>	
1.4 Assessment: <i>Teacher Anecdotal Recording Sheet</i>	
Unit 2 Personal Information and Privacy Matters	32
2.1 Handout: <i>Who is Watching?</i> Placemat	
2.2 Handout: <i>Privacy Quiz</i>	
2.3 Teacher Answer Key: <i>Privacy Quiz</i>	
2.4 Handout: <i>A Day in the Life of a Student</i>	
2.5 Slide/Overhead: <i>Defining Invasion of Privacy</i>	
2.6 Handout: Case Studies: <i>Privacy at Risk</i>	
2.7 Teacher Answer Key: Case Studies: <i>Privacy at Risk</i>	
2.8 Handout: Final Task: <i>If you wanted to know...What if you're a victim of identity theft or your credit/bank card is lost or stolen?</i>	
2.9 Final Task: Teacher Answer Key: <i>If you wanted to know...What if you're a victim of identity theft or your credit/bank card is lost or stolen?</i>	
Unit 3 Using the Web: Internet Privacy	48
3.1 Handout: Reference Check: <i>Is Your Boss Watching? Privacy and Your Facebook Profile</i>	
3.2 Slide/Overhead: <i>The 5 Ps</i>	

- 3.3 Handout: *Video Worksheet – Online Privacy*
- 3.4 Handout: *Mini-Debates: Social Networking*
- 3.5 Handout: *Mini-Debates: Self-Reflection*
- 3.6 Handout: *Analysing Current Issues Related to Web Privacy*
- 3.7 Article: *Facebook fakers prey on students*
- 3.8 Article: *Spy chief's wife puts him on Facebook; Head of M16 learns millions have access to family details*
- 3.9 Article: *Identity theft among Canada's fastest-growing crimes; In recent years, reports have soared 500 per cent*
- 3.10 Article: *Privacy rights when using employer-provided computers*
- 3.11 Article: *The Perils of Facebook; Beware of consequences of baring your soul, or other things, online*
- 3.12 Handout: *Culminating Task: Staying Safe Online, Public Information Poster*
- 3.13 Culminating Task Evaluation Rubric

Unit 4 Open Government and Freedom of Information Matters

72

- 4.1 Handout: *Your Right to Access Information* Web Quest
 - 4.2 Teacher Answer Key: *Your Right to Access Information* Web Quest
 - 4.3 Handout: *Freedom of Information Quiz*
 - 4.4 Slide/Overhead: *Teacher Answer Key: Freedom of Information Quiz*
 - 4.5 Handout: *Analysing Political Cartoons: Democracy vs. Dictatorship*
 - 4.6 Handout: *Comparing Access to Information*
 - 4.7 Handout: *Venn Diagram*
 - 4.8 Handout: *Analysing Access to Information Cases*
 - 4.9 Article: *Freedom of Information request uncovers diagnostic errors*
 - 4.10 Article: *Public kept from 20 per cent of Elton John concert tickets*
 - 4.11 Article: *DineSafe cuts rate of sickness; Food-related illness cases have plunged 30% since Star exposed violations in city's eateries*
 - 4.12 Article: *Daycare Parents Triumph*
 - 4.13 Handout: *Government Transparency Please!*
 - 4.14 Handout: *Culminating Task: Listen Up! – Rant Writing*
 - 4.15 Culminating Task, Evaluation Rubric
- Copy of Teacher Anecdotal Recording Sheet (**See Unit 1, Appendix 1.4**)

Resources

107

RESOURCE OVERVIEW

The four units included in this Information and Privacy Commissioner of Ontario resource were created to meet *several* expectations of senior courses outlined in the Ontario Ministry of Education Curriculum documents for Grades 11 and 12.

Grades: 11-12

Course Type: Open, College, University

Senior Courses:

- Media Studies, Grade 11, Open, EMS30;
- Canadian Politics and Citizenship, Grade 11, Open, CPC30;
- Understanding Canadian Law, Grade 11, University/College Preparation, CLU3M;
- Canadian and International Law, Grade 12, University Preparation, CLU4U

Essential Skills

Through extensive research, Human Resources and Skills Development Canada (HRSDC) and other national and international agencies have identified and validated key literacy and Essential Skills needed for work, learning, and life. The skills are used in virtually all occupations and throughout daily life in different forms and at different levels of complexity. The key literacy and Essential Skills are *reading text, document use, numeracy, writing, oral communication, working with others, thinking skills, computer use, and continuous learning*. These Essential Skills, as described by HRSDC, are included in the Teaching/Learning strategies provided in this resource.

For more information on Essential Skills, visit the HRSDC website: (<http://www.hrsdc.gc.ca/eng/workplaceskills/LES/index.shtml>).

UNITS: TITLES AND TIMES

UNIT 1	Introduction to the IPC, Freedom of Information and Protection of Privacy	180 minutes
UNIT 2	Personal Information and Privacy Matters	375 minutes
UNIT 3	Using the Web: Internet Privacy	600 minutes
UNIT 4	Open Government and Freedom of Information Matters	1005 minutes

UNIT OVERVIEWS

UNIT 1: INTRODUCTION TO THE IPC, FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

Description and Purpose

The purpose of this unit is to introduce the Office of the Information and Privacy Commissioner of Ontario and the Commissioner's mandate to ensure *access to government information* for, and the *protection of privacy* of, the citizens of Ontario. The unit will provide students with an understanding of the terms *personal information* and *privacy protection*. Students will learn about the purpose and role of the IPC and the legislation that pertains to individuals' right of access to government-held information and the protection of privacy. In addition, students will learn about the current Information and Privacy Commissioner of Ontario. Teachers are free to select either activity in the unit to achieve the purpose of the unit.

UNIT 1	EXPECTATIONS (OVERALL AND SPECIFIC)	ASSESSMENT STRATEGIES/TASKS	ESSENTIAL SKILLS
Introduction to the IPC, Freedom of Information and Protection of Privacy	<p>Overall Expectations: DMV.03 PIV.01 RFV.01, RFV.03* LIV.01*, LIV.03* HTV.03</p> <p>Specific Expectations: DM3.02, DM3.03 PI1.01, PI1.02, PI1.04 RF1.02, RF3.07 LI1.02*, LI3.01* HT3.02 RF3.02, RF3.04</p> <p>*Please note: coded expectations meet the requirements for both the CLU3M and CLU4U courses.</p>	<p>Note-taking Internet Research Reflection Exit Ticket Teacher Anecdotal Recording Sheet</p>	<p>Reading Text Writing Thinking Skills Oral Communication Computer Use Document Use Working With Others Continuous Learning</p>

Appendices

- 1.1 PowerPoint Presentation Outline: *Introduction to the IPC, Freedom of Information and Protection of Privacy*;
- 1.2 Handout: *Privacy is Your Right* Web Quest;
- 1.3 *Exit Ticket*;
- 1.4 Assessment: *Teacher Anecdotal Recording Sheet*.

UNIT 2: PERSONAL INFORMATION AND PRIVACY MATTERS

Description and Purpose

The purpose of this unit is to increase students' awareness of the risks involved in giving out one's personal information. The unit will provide students with an understanding of personal and private information. Students will explain how personal information is collected during daily activities and how that information can be used. They will learn about the various types of invasion of privacy and understand what to do in a situation where their personal information has been compromised.

ACTIVITY 2	EXPECTATIONS (OVERALL AND SPECIFIC)	ASSESSMENT STRATEGIES/TASKS	ESSENTIAL SKILLS
Personal Information and Privacy Matters	<p>Overall Expectations: MSV.02 RFV.01*, RFV.03* LIV.02*, LIV.03*</p> <p>Specific Expectations: MS2.02, MS2.04 RF1.02*, RF1.03, RF3.02, RF3.04 LI2.01*, LI2.02*, LI2.03*, LI3.01, LI3.02</p> <p>*Please note: coded expectations meet the requirements for both the CLU3M and CLU4U courses.</p>	<p>Note-taking Internet Use Reflection Discussion Analysing Sharing Critical Thinking Teacher Anecdotal Recording Sheet</p>	<p>Reading Text Writing Thinking Skills Oral Communication Computer Use Document Use Working With Others Continuous Learning</p>

Appendices

- 2.1 Handout: *Who is Watching?* Placemat;
- 2.2 Handout: *Privacy Quiz*;
- 2.3 Teacher Answer Key: *Privacy Quiz*;
- 2.4 Handout: *A Day in the Life of a Student*;
- 2.5 Slide/Overhead: *Defining Invasion of Privacy*;
- 2.6 Handout: Case Studies: *Privacy at Risk*;
- 2.7 Teacher Answer Key: Case Studies: *Privacy at Risk*;
- 2.8 Handout: Final Task: *If you wanted to know...What if you're a victim of identity theft or your credit/bank card is lost or stolen?*
- 2.9 Final Task: Teacher Answer Key: *If you wanted to know...What if you're a victim of identity theft or your credit/bank card is lost or stolen?*

UNIT 3: USING THE WEB: INTERNET PRIVACY

Description and Purpose

The purpose of this unit is to increase students' awareness of privacy as it relates to using the Web. Students will be able to identify areas of risk that pose a threat to Web users. They will explore areas of concern related to privacy through an IPC tip sheet, MTV video, online and print articles. Students will assess and discuss current issues, analyse their impact on society and think creatively to formulate solutions. In the culminating task, students will use their knowledge to research Internet privacy risk to create a public information poster that will be used to increase the school community's awareness.

ACTIVITY 3	EXPECTATIONS (OVERALL AND SPECIFIC)	ASSESSMENT STRATEGIES/TASKS	ESSENTIAL SKILLS
Using the Web: Internet Privacy	<p>Overall Expectations: MSV.02, PMV.01 PIV.01, PIV.03 LIV.01*, LIV.02*, LIV.03*</p> <p>Specific Expectations: MS2.02, MS2.04, MS2.05 PM1.01, PM1.03, PM1.04 PI1.01, PI1.02, PI1.03, PI1.04 PI3.01, PI3.02, PI3.03 LI1.01*, LI1.02*, LI1.03*, LI1.04*, LI1.05* LI2.01*, LI2.02*, LI2.03* LI3.01*, LI3.02*</p> <p>*Please note: coded expectations meet the requirements for both the CLU3M and CLU4U courses.</p>	Note-taking Internet Use Reflection Discussion Analysing Sharing Critical Thinking Self-reflection Teacher Anecdotal Recording Sheet	Reading Text Writing Thinking Skills Oral Communication Computer Use Document Use Working With Others Continuous Learning

Appendices

- 3.1 Handout: Reference Check: *Is Your Boss Watching? Privacy and Your Facebook Profile*;
- 3.2 Slide/Overhead: *The 5 Ps*;
- 3.3 Handout: *Video Worksheet – Online Privacy*;
- 3.4 Handout: *Mini-Debates: Social Networking*;
- 3.5 Handout: *Mini-Debates: Self-Reflection*;
- 3.6 Handout: *Analysing Current Issues Related to Web Privacy*;
- 3.7 Article: *Facebook fakers prey on students*;
- 3.8 Article: *Spy chief's wife puts him on Facebook; Head of M16 learns millions have access to family details*;
- 3.9 Article: *Identity theft among Canada's fastest-growing crimes; In recent years, reports have soared 500 per cent*;
- 3.10 Article: *Privacy rights when using employer-provided computers*;
- 3.11 Article: *The Perils of Facebook; Beware of consequences of baring your soul, or other things, online*;
- 3.12 Handout: Culminating Task: *Staying Safe Online Public Information Poster*;
- 3.13 Culminating Task Evaluation Rubric.

UNIT 4: OPEN GOVERNMENT AND FREEDOM OF INFORMATION MATTERS

Description and Purpose

The purpose of this unit is two-fold: to deepen students' understanding of freedom of information legislation and its connection to the principles of a democracy, and to allow students to apply some of the features inherent in a democracy – active citizenship and participation. In this unit, students will review the features of a democracy and compare them to other types of government with respect to accessing personal and government information. They will read and analyse a variety of articles and opinion pieces, with a focus on the effectiveness of the legislation in ensuring government accountability and the development and/or support of authors' arguments. They will also demonstrate active citizenship by developing, supporting and presenting their opinions through written and oral communication.

CULMINATING ACTIVITY	EXPECTATIONS (OVERALL AND SPECIFIC)	ASSESSMENT STRATEGIES/TASKS	ESSENTIAL SKILLS
Open Government and Freedom of Information Matters	<p>Overall Expectations: MSV.01, MSV.02 PMV.01 CDV.01, CDV.02 DMV.02, DMV.03 PIV.01, PIV.03 RFV.01*, RFV.03* HTV.03, HTV.04</p> <p>Specific Expectations: MS1.02, MS2.02, MS2.04 PM1.01, PM1.03, PM1.04 CD1.01, CD2.01, CD2.04 DM2.03, DM3.02, DM3.03 PI1.01, PI1.02, PI1.03, PI1.04 PI3.01, PI3.02, PI3.03 RF1.02*, RF3.01, RF3.02, RF3.04 HT3.02, HT3.03, HT4.03</p> <p>*Please note: coded expectations meet the requirements for either CLU3M or CLU4U courses.</p>	<p>Note-taking Reflection Discussion Organizing Information Venn Diagram PMI Chart Analysing Issues Critical Thinking Teacher Anecdotal Recording Sheet</p>	<p>Reading Text Writing Thinking Skills Oral Communication Computer Use Document Use Working With Others Continuous Learning</p>

Appendices

- 4.1 Handout: *Your Right to Access Information Web Quest*;
- 4.2 Teacher Answer Key: *Your Right to Access Information Web Quest*;
- 4.3 Handout: *Freedom of Information Quiz*;
- 4.4 Slide/Overhead: *Teacher Answer Key: Freedom of Information Quiz*;
- 4.5 Handout: *Analysing Political Cartoons: Democracy vs. Dictatorship*;
- 4.6 Handout: *Comparing Access to Information*;
- 4.7 Handout: *Venn Diagram*;
- 4.8 Handout: *Analysing Access to Information Cases*;
- 4.9 Article: *Freedom of Information request uncovers diagnostic errors*;
- 4.10 Article: *Public kept from 20 per cent of Elton John concert tickets*;

- 4.11 Article: *DineSafe cuts rate of sickness; Food-related illness cases have plunged 30% since Star exposed violations in city's eateries*;
 - 4.12 Article: *Daycare Parents Triumph*;
 - 4.13 Handout: *Government Transparency Please!*;
 - 4.14 Handout: *Culminating Task: Listen Up! – Rant Writing*;
 - 4.15 Culminating Task, Evaluation Rubric;
- Copy of Teacher Anecdotal Recording Sheet (**See Unit 1, Appendix 1.4**).

CURRICULUM EXPECTATIONS

The units in this guide will assist teachers in meeting the following coded overall and specific expectations in the Ontario Ministry of Education courses listed below. For more information, please visit: <http://www.edu.gov.on.ca/eng/curriculum/secondary/>.

MEDIA STUDIES, GRADE 11, OPEN, EMS30

STRAND	OVERALL EXPECTATIONS	SPECIFIC EXPECTATIONS
Media and Society	<p>Understanding Media Perspectives MSV.01 – analyse and critique media representations of people issues, values, and behaviours;</p> <p>Understanding the Impact of Media on Society MSV.02 – analyse and evaluate the impact of media on society.</p>	<p>Current Issues MS1.02 – analyse media representations of current, social, political, and cultural issues and events, and explain how the representations might affect the audience’s interpretation of the issues;</p> <p>Health and Relationships MS2.02 – analyse the impact of the media and of communication technologies on health, relationships and interpersonal communications;</p> <p>Privacy MS2.04 – examine the ways in which the media and communication technologies can infringe on the privacy rights of individuals, and how consideration of those rights affects the behaviours of the media industry;</p> <p>Effects of Using Media Technology MS2.05 – explain how people use media and communication technologies in their personal and working lives and identify some of the effects of those technologies.</p>
Producing and Reflecting on Media Texts	<p>Producing Media Texts PMV.01 – create a variety of media texts for different audiences and purposes using effective forms, codes, conventions, and techniques.</p>	<p>Purpose and Audience PM1.01 – create media texts for different purposes and audiences;</p> <p>Using Media Conventions and Techniques PM1.03 – select and use the conventions and techniques of a particular form to produce media texts;</p> <p>Language and Point of View PM1.04 – select and use the appropriate level of language, tone, and point of view when creating media texts for specific purposes and audiences.</p>

CANADIAN POLITICS AND CITIZENSHIP, GRADE 11, OPEN, CPC30

STRAND	OVERALL EXPECTATIONS	SPECIFIC EXPECTATIONS
Citizenship, Democracy, and Participation	<p>CDV.01 – describe the key features of citizenship and democracy;</p> <p>CDV.02 – evaluate the influence of various forms of citizen action on public policy.</p>	<p>Principles of Democracy</p> <p>CD1.01 – explain the importance of democratic principles such as political equality; majority rule; minority representation; responsible government; representation by population; decision making for the common good; the rule of law; and universal human rights, freedoms, and responsibilities;</p> <p>Active Citizenship</p> <p>CD2.01 – identify opportunities for citizens to participate in governmental and non-governmental political decision-making at the community, municipal, provincial, federal, and international levels;</p> <p>CD2.04 – apply the techniques of democratic participation to a political question under investigation.</p>
Decision-Making Systems and Processes	<p>DMV.02 – evaluate the role and influence of key participants in Canadian government decision-making;</p> <p>DMV.03 – describe the extent to which political and economic systems and institutions meet people’s needs and promote the common good.</p>	<p>Key Roles in Decision-Making</p> <p>DM2.03 – explain the role in government decision-making of unelected key players;</p> <p>Making Decisions for the Common Good</p> <p>DM3.02 – identify the types of decisions made by government that are critical for protecting individual rights and promoting the common good;</p> <p>DM3.03 – explain how the Canadian Charter of Rights and Freedoms has influenced decisions in a variety of areas.</p>
Methods of Political Inquiry and Communication	<p>PIV.01 – use methods of political science inquiry to locate, gather, evaluate, and organize information from a variety of sources;</p> <p>PIV.03 – communicate knowledge, opinions, and interpretations about events, issues, and trends relating to politics and citizenship, using a variety of forms of communication.</p>	<p>Research</p> <p>PI1.01 – formulate questions that lead to a deeper understanding of a political issue and an awareness of the different ways in which the issue can be approached;</p> <p>PI1.02 – collect data from a range of media and information sources;</p> <p>PI1.03 – evaluate the credibility of sources and information;</p> <p>PI1.04 – organize research findings, using a variety of methods and forms;</p> <p>Communication</p> <p>PI3.01 – express ideas, understandings, arguments, and conclusions, as appropriate for different audiences and purposes, using a variety of styles and forms;</p> <p>PI3.02 – use an accepted form of documentation to acknowledge all sources of information, including electronic sources;</p> <p>PI3.03 – use appropriate terminology to communicate political concepts, opinions, and arguments.</p>

UNDERSTANDING CANADIAN LAW, GRADE 11, UNIVERSITY/COLLEGE PREPARATION, CLU3M

STRAND	OVERALL EXPECTATIONS	SPECIFIC EXPECTATIONS
Rights and Freedoms	<p>RFV.01 – describe the sources of rights and freedoms in Canada and explain how particular rights and freedoms may conflict;</p> <p>RFV.03 – describe the rights and freedoms enshrined in Canadian law and explain how they are interpreted, how they may be limited, and how they are enforced in Canada and in Ontario.</p>	<p>Rights and Freedoms</p> <p>RF1.02 – explain key concepts associated with human rights;</p> <p>RF1.03 – analyse situations in which rights and freedoms may compete or conflict.</p> <p>Human Rights Legislation in Canada and in Ontario</p> <p>RF3.07 – describe procedures for hearing complaints about human rights violations.</p>
Methods of Legal Inquiry and Communication	<p>LIV.01 – use appropriate research methods to gather, organize, and evaluate and synthesize information;</p> <p>LIV.02 – apply the steps in the process of legal interpretation and analysis;</p> <p>LIV.03 – explain, discuss, and interpret legal issues using a variety of formats and forms of communication.</p>	<p>Research</p> <p>L11.01 – formulate questions that lead to a deeper understanding of a legal issue;</p> <p>L11.02 – conduct research on legal topics, using traditional and non-traditional sources of information;</p> <p>L11.03 – evaluate the credibility of sources and information by checking for logical errors, accuracy, and underlying assumptions, including prejudices, biases, stereotyping, or a lack of substantiation or statements, arguments, and opinions;</p> <p>L11.04 – classify and clarify information, using organizers, graphs, charts, and diagrams;</p> <p>L11.05 – compile summary notes in a variety of forms and for a variety of purposes.</p> <p>Interpretation and Analysis</p> <p>L12.01 – distinguish among opinions, facts, and arguments in sources;</p> <p>L12.02 – draw conclusions based on analysis of information gathered through research and awareness of diverse legal interpretations;</p> <p>L12.03 – apply and analytical/inquiry method to juridical questions.</p> <p>Communication</p> <p>L13.01 – express opinions, ideas, arguments and conclusions, as appropriate for different audiences and purposes using a variety of styles and forms, as well as visual supports;</p> <p>L13.02 – use an accepted form of documentation to document all information sources, including electronic sources.</p>

CANADIAN AND INTERNATIONAL LAW, GRADE 12, UNIVERSITY PREPARATION, CLU4U

STRAND	OVERALL EXPECTATIONS	SPECIFIC EXPECTATIONS
Heritage	<p>HTV.03 – describe the relationship between law and societal values;</p> <p>HTV.04 – assess the influence of individual and collective action on the evolution of law.</p>	<p>Law and Society</p> <p>HT3.02 – analyse how society uses law to express its values;</p> <p>HT3.03 – analyse contemporary events and issues that demonstrate a possible conflict between the law and societal values.</p> <p>Law Reform</p> <p>HT4.03 – assess the power of the individual citizen to change or modify our laws and determine under what circumstances individuals have a responsibility to seek legal reform.</p>
Rights and Freedoms	<p>RFV.01 – describe the historical development of human rights legislation in Canada;</p> <p>RFV.03 – explain the rights and responsibilities of individuals under the Canadian Charter of Rights and Freedoms.</p>	<p>Human Rights in Canada</p> <p>RF1.02 – evaluate the protections provided by federal and provincial human rights legislation.</p> <p>The Canadian Charter of Rights and Freedoms</p> <p>RF3.01 – explain what is meant by entrenching rights in a written constitution;</p> <p>RF3.02 – analyse how rights and freedoms are protected under the Charter of Rights and Freedoms;</p> <p>RF3.04 – explain how citizens can exercise their rights under the Charter.</p>
Methods of Legal Inquiry and Communication	<p>LIV.01 – use appropriate research methods to gather, organize, and evaluate and synthesize information;</p> <p>LIV.02 – apply the steps in the process of legal interpretation and analysis;</p> <p>LIV.03 – explain, discuss, and interpret legal issues using a variety of formats and forms of communication.</p>	<p>Research</p> <p>LI1.01 – formulate questions that lead to a deeper understanding of a legal issue;</p> <p>LI1.02 – conduct research on legal topics, using traditional and non-traditional sources of information;</p> <p>LI1.03 – evaluate the credibility of sources and information by checking for logical errors, accuracy, and underlying assumptions, including prejudices, biases, stereotyping, or a lack of substantiation or statements, arguments, and opinions;</p> <p>LI1.04 – classify and clarify information, using organizers, graphs, charts, and diagrams;</p> <p>LI1.05 – compile summary notes in a variety of forms and for a variety of purposes.</p> <p>Interpretation and Analysis</p> <p>LI2.01 – distinguish among opinions, facts, and arguments in sources;</p> <p>LI2.02 – draw conclusions based on analysis of information gathered through research and awareness of diverse legal interpretations;</p> <p>LI2.03 – apply an analytical/inquiry method to legal issues.</p> <p>Communication</p> <p>LI3.01 – express opinions, ideas, arguments and conclusions, as appropriate for different audiences and purposes using a variety of styles and forms, as well as visual supports;</p> <p>LI3.02 – use an accepted form of documentation to document all information sources, including electronic sources.</p>

TEACHING/LEARNING STRATEGIES

Lesson Design

The lesson format used in this resource is consistent with the Peel District School Board's three-part lesson design. The three phases of the lesson are explained below:

Minds On

- connect the content to prior learning;
- set the context for students.

Action

- guided practice – application of concept with guidance from peers and/or teacher, and provides opportunities for assessment and instruction;
- independent application of the concept – provides opportunities for assessment and/or evaluation.

Consolidate/Debrief

- summary of learning;
- connection to other concepts;
- often combined with reflection, which is ongoing throughout the lesson;
- provides opportunities for assessment and/or evaluation.

ASSESSMENT AND EVALUATION OF STUDENT LEARNING

Varied forms of assessment and evaluation have been employed in the development of this resource. It is expected by the Ontario Ministry of Education that teachers use both formative and summative evaluation to identify clearly the strengths and weaknesses of each student. Consequently, there are various assessment and evaluation strategies in each activity that provide students with opportunities to demonstrate expectations. The activities included are designed to assess a student's understanding of new concepts and the ability to apply them in written, oral, and/or visual forms. Each unit's culminating task has been designed to be consistent with the Ontario Ministry of Education's four categories: *Knowledge/Understanding, Thinking/Inquiry, Communication, and Application*. Each category is further divided into levels of achievement, which explain what students need to achieve/produce in order to be classified within that level. The accepted provincial standard is Level 3. To develop fair and meaningful assessment and evaluation instruments, teachers must be familiar with each category and strand.

RESOURCES

Information and Privacy Commissioner of Ontario Website

The IPC website (www.ipc.on.ca) serves as a research and information tool. It is updated regularly and includes:

- information about the IPC's role and answers to frequently asked questions about access and privacy;
- educational resources, including the *What Students Need to Know about Freedom of Information and the Protection of Privacy* program, health privacy publications, presentations, and speeches given by IPC staff;
- annual reports;
- links to the text of the provincial and municipal *Freedom of Information and Protection of Privacy Acts*, as well as plain language summaries;
- IPC orders, investigation reports and judicial reviews;

- IPC publications such as policy papers; health privacy papers and the *If You Wanted to Know* series; and
- links to other access and privacy websites in Canada and around the world.

Privacy by Design

As well as the original website, the IPC has a second website, www.privacybydesign.ca, devoted to *Privacy by Design (PbD)*. *PbD* is a concept that was developed by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, back in the 90's, to address the ever-growing and systemic effects of *information and communication technologies*, and of large-scale networked data systems.

A landmark resolution by Commissioner Cavoukian was approved by International Data Protection and Privacy Commissioners in Jerusalem on October 29, 2010, at their annual conference. The resolution – co-sponsored by Commissioners from three different continents – recognizes Commissioner Cavoukian's concept of *Privacy by Design* – which ensures that privacy is embedded into new technologies and business practices, right from the outset – as an “essential component of fundamental privacy protection.”

ADDITIONAL RESOURCES

Internet

Canadian Legal Information Institute – <http://www.canlii.org/>;

Media Awareness Network – www.media-awareness.ca;

myprivacy.mychoice.mylife – <http://www.youthprivacy.ca/en/index.html>;

Office of the Privacy Commissioner of Canada – http://www.priv.gc.ca/index_e.cfm;

Office of the Information Commissioner of Canada – <http://www.oic-ci.gc.ca/eng/>; and

Ontario History and Social Sciences Teachers' Association (OHASSTA) – www.ohassta.org.

INTERNATIONALLY RECOGNIZED PRIVACY PRINCIPLES

In 1980, the Organization for Economic Co-operation and Development (OECD) developed a set of principles to ensure the fair treatment and handling of personal information collected by organizations. These principles are known as the Code of Fair Information Practices, and they form the basis of virtually all privacy legislation throughout the world.

The principles include the following:

- Only the information that is really needed should be collected;
- Where possible, it should be collected directly from the individual to whom it pertains (the data subject);
- The data subject should be told why the information is needed;
- The information should be used only for the intended purpose;
- The information should not be used for other (secondary) purposes without the data subject's consent; and
- The data subject should be given the opportunity to see his/her personal information and correct it if it's wrong.

FREEDOM OF INFORMATION LEGISLATION IN CANADA

Freedom of information legislation in Canada gives members of the public a statutory right of access to government-held records. These laws operate in accordance with the general principles that:

- information should be available to the public;
- necessary exemptions to the right of access should be limited and specific; and
- decisions on the disclosure of government information should be reviewed independently of government.

The right of access to government records reflects an extremely important public value in mature democratic countries – it means that government is prepared to be open and accountable to its citizens.

PROTECTION OF PRIVACY LEGISLATION IN CANADA

Privacy protection legislation in Canada reflects the OECD's Code of Fair Information Practices. The legislation includes rules the government must follow in order to protect an individual's right to privacy. These include:

- the right of access to one's own personal information, and the corresponding right to correct inaccurate personal information;
- the right to an independent review of any access decision;
- regulations governing the collection, retention, use, disclosure, and disposal of government-held personal information; and
- the right to complain to an independent oversight body if anyone feels that these regulations have been breached.

Privacy protection is extremely important, especially in the computer age where technology can have a profound impact on the collection, use, and disclosure of personal information, as well as issues of storage and security. Without these rules and regulations, governments would have the power to infringe upon and control the lives of their citizens.

FEDERAL LEGISLATION

Privacy Act – Privacy Commissioner of Canada

The *Privacy Act* came into effect on July 1, 1983, replacing some limited personal information rights set out in Part IV of the *Canadian Human Rights Act*.

The federal Privacy Commissioner has oversight responsibilities for all federal government departments and agencies. She reviews decisions of the government regarding access to one's own personal information, and investigates complaints about breaches of the statutory rules and regulations regarding privacy. (Visit http://www.priv.gc.ca/index_e.cfm for more specific details.)

Access to Information Act – Information Commissioner of Canada

The *Access to Information Act* also came into effect on July 1, 1983.

The federal Information Commissioner has corresponding oversight responsibilities for freedom of information requests within the federal public sector. She reviews decisions of the government regarding access to government-held records, ensuring that any exemption claims are defensible, that searches for all relevant records are thorough, and that fees charges are reasonable. (Visit <http://www.oic-ci.gc.ca/eng/> for more specific details.)

PROVINCIAL LEGISLATION

All provinces and territories in Canada have freedom of information and protection of privacy laws. All of these laws reflect the same public values of open government and protection of personal privacy, although coverage and powers vary from province to province. In each of the provinces, the legislation covers both provincial and municipal government organizations. In each of the three territories, the legislation covers territorial government organizations (as of early 2011). There is an independent official with oversight responsibilities in each jurisdiction. Sometimes this is a provincial Ombudsman with the authority to recommend and persuade; in others, like Ontario, this person is a Commissioner with the power to order the disclosure of records.

PRIVATE SECTOR

The underlying value of freedom of information law – public accountability through open government – has no application in the private sector. However, the value of privacy protection exists no matter what organization holds personal information.

On January 1, 2001, the federal *Personal Information Protection and Electronic Documents Act* came into force. The immediate impact was the extension of privacy protection to the federally regulated private sector and to the transjurisdictional (cross-border) flow of personal information for commercial purposes. On January 1, 2004, the law expanded to cover provincially regulated enterprises in the seven provinces (and all three territories) that had not enacted very similar legislation. Three provinces, British Columbia, Alberta and Quebec, brought in their own privacy laws covering provincially regulated enterprises.

Unit One - Overview of Unit Activities “Introduction to the IPC, Freedom of Information and Protection of Privacy”

ACTIVITY ONE: What Students Need to Know
Introductory PowerPoint
75 minutes
 Students will begin the unit by viewing a PowerPoint that introduces the laws governing freedom of information and the protection of privacy. They will learn the purpose and role of the Office of the Information and Privacy Commissioner of Ontario.

ACTIVITY TWO: Privacy is Your Right
Web Quest
75 minutes
 Students will visit the IPC website and complete a Web Quest to learn about the laws governing freedom of information and protection of privacy in Ontario. They will learn about the purpose and role of the Office of the Information and Privacy Commissioner of Ontario.

Activity 1
Subtasks

- b) Note-taking
- a) Viewing PowerPoint presentation

Activity 2
Subtasks

- b) Answering Web Quest questions
- a) Locating information online

Exit Ticket – 30 minutes
 Students complete the questions on an Exit Ticket to assess their understanding in the unit and to identify concepts that require clarification.

GUIDING QUESTIONS:
 What is meant by the terms “*personal information*” and “*privacy protection*?”
 Who is Ontario’s current Information and Privacy Commissioner?
 What is the role of the Information and Privacy Commissioner of Ontario?
 Which legislation pertains to freedom of information and protection of privacy in Ontario?

UNIT 1

Introduction to the IPC, Freedom of Information and Protection of Privacy

Time | 180 minutes

Description and Purpose

The purpose of this unit is to introduce the Office of the Information and Privacy Commissioner of Ontario and the Commissioner’s mandate to ensure *access to government information* for, and the *protection of privacy* of, the citizens of Ontario. The unit will provide students with an understanding of the terms *personal information* and *privacy protection*. Students will learn about the purpose and role of the IPC and the legislation that pertains to individuals’ right of access to government-held information and the protection of privacy. In addition, students will learn about the current Information and Privacy Commissioner of Ontario. Teachers are free to select either activity in the unit to achieve the purpose of the unit.

Guiding Questions

What is meant by the terms “personal information” and “privacy protection?”

Who is Ontario’s current Information and Privacy Commissioner?

What is the role of the Information and Privacy Commissioner of Ontario?

Which legislation pertains to freedom of information and protection of privacy in Ontario?

Prior Knowledge and Skills

- Note-taking;
- Literacy;
- Computer and Internet literacy;
- Discussing and sharing ideas as a class;
- Critical thinking;
- Reflecting.

Planning Notes/Preparation

- Reserve an LCD projector and computer;
- A copy of the PowerPoint presentation: *An Introduction to the IPC and Freedom of Information and Protection of Privacy*;
- Photocopy appropriate Appendices for students;
- Reserve a computer lab (or have students access the website at home).

Materials List

- Copies of *What Students Need to Know* introductory PowerPoint slides (**Appendix 1.1**);
- Copies of *Privacy is Your Right* Web Quest (**Appendix 1.2**);
- Copies of the Culminating task: *Exit Ticket* (**Appendix 1.3**);
- Copies of the *Teacher Anecdotal Recording Sheet* (**Appendix 1.4**).

TEACHING/LEARNING STRATEGIES

ACTIVITY	MINDS ON	ACTION	CONSOLIDATION AND DEBRIEF
1	<p>After setting up and starting the introductory PowerPoint presentation, ask students, “What do the terms privacy and freedom of information mean to you?”</p> <p>“Who and/or what protects your rights to these?”</p> <p>“Why are these rights important?”</p>	<p>Students will follow along with <i>What Students Need to Know</i> introductory PowerPoint slides (Appendix 1.1) that accompany the presentation. They are to make additional notes in the spaces provided, asking appropriate questions and responding.</p>	<p><i>Students will complete the Exit Ticket (Appendix 1.3) to assess their own understanding of key concepts in the PowerPoint presentation and to identify areas that require clarification.</i></p> <p>The teacher should answer any questions raised by the students regarding the purpose and role of the IPC and the legislation the Commissioner oversees.</p>
2	<p>Ask students “What do the terms privacy and freedom of information mean?”</p> <p>“Who and/or what protects your rights to these?”</p> <p>“Why are these rights so important?”</p> <p>Indicate to students that the website they will be exploring will help them expand on these questions.</p>	<p>Students are to access the IPC’s website at www.ipc.on.ca and complete the <i>Your Right to Privacy</i> Web Quest (Appendix 1.2) to learn more about the purpose and role of the IPC and the legislation that protects the privacy of individuals in Ontario.</p>	<p><i>Students will complete the Exit Ticket (Appendix 1.3) to assess their own understanding of key concepts from the Web Quest and to identify areas that require clarification.</i></p> <p>The teacher should conclude the activity by answering questions raised by the students regarding the purpose and role of the IPC and the legislation the Commissioner oversees.</p>

Assessment and Evaluation of Student Learning

- assess students’ understanding on the *Exit Ticket*;
- assess students’ ability to contribute to class discussion using the *Teacher Anecdotal Recording Sheet*.

Professional Resources

Spence, Bob. ***Opening the door: Access to government records.***

PowerPoint presentation to media students, October 2010.

http://www.ipc.on.ca/site_documents/10-20-2010-Mohawk-students.ppt

“About Us.” Information and Privacy Commissioner of Ontario

<http://www.ipc.on.ca/english/About-Us/>

Information and Privacy Commissioner of Ontario Website:

<http://www.ipc.on.ca/english/Home-Page/>

Access to Information under Ontario’s Access and Privacy Acts brochure

Your Privacy and Ontario’s Information and Privacy Commissioner brochure

The Personal Health Information Protection Act and Your Privacy brochure

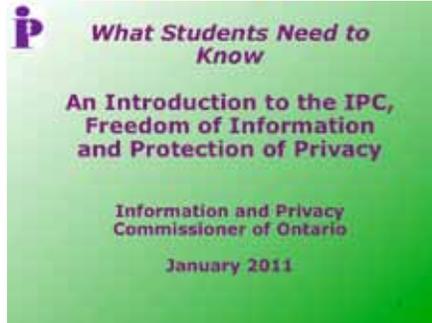
IPC’s *Privacy by Design* website: <http://www.privacybydesign.ca/>

ACTIVITY 1:

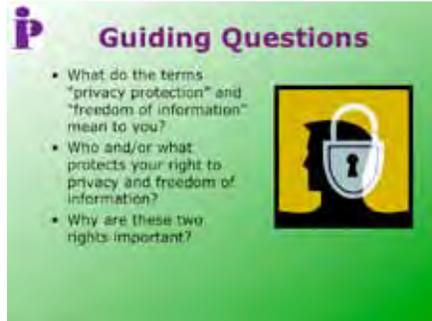
WHAT STUDENTS NEED TO KNOW

INTRODUCTORY POWERPOINT

SLIDE 1



SLIDE 2



SLIDE 3



SLIDE 4



SLIDE 5

iP **Defining Privacy**

Privacy is a fundamental human right.
What does this mean?

SLIDE 6

iP **Key Terms**

- "Privacy" involves control over the collection, use and disclosure of personal information.
- "Personal information" is any information that is about you or can identify you.
- Can you think of any examples of "personal information?"

SLIDE 7

iP **Key Terms (Cont'd)**

Freedom of information (FOI), or "access to information" refers to:

- public access to general records relating to the activities of government – ranging from administration and operations to legislation and policy to ensure accountability and transparency of government activities;
- access to records of your own *personal* information that government offices may hold.

SLIDE 8

iP **II. History of Fair Information Practices**

Illustrations from the Ages

PREHISTORIC TIMES 19th century
 20th century 21st century

SLIDE 9

iP **Internationally Recognized Privacy Principles**

- In 1980, the Organization for Economic Co-operation and Development (OECD) developed voluntary Guidelines on the Protection of privacy and Transborder Flows of Personal Data.
- They have served as the blueprint for the development of national privacy laws.

SLIDE 10

iP **OECD Principles**

- Only necessary information should be collected;
- Where possible, it should be collected directly from the individual to whom it pertains (the data subject);
- The data subject should be told why the information is needed;

SLIDE 11

iP **OECD Principles (Cont'd)**

- The information should be used only for the intended purpose;
- The information should not be used for other (secondary) purposes without the data subject's consent; and
- The data subject should be given the opportunity to see and correct his/her personal information if it's incorrect.

SLIDE 12

iP **Global Privacy Standard**

- Created in 2006
- Goal: create a single instrument for businesses and technology companies to evaluate their privacy enhancing practices.

SLIDE 13

Global Privacy Standard Principles:

1. Consent
2. Accountability
3. Purposes
4. Collection Limitation – Data Minimization
5. Use, Retention, Disclosure Limitation

SLIDE 14

Global Privacy Standard Principles (Cont'd)

6. Accuracy
7. Security
8. Openness
9. Access
10. Compliance

SLIDE 15

III. About the IPC/ Ontario

SLIDE 16

Mandate and Role

- The Information and Privacy Commissioner is appointed by the Ontario Legislative Assembly and is independent of the government of the day.
- The Commissioner's mandate includes overseeing the access and privacy provisions of these Acts:
 - Freedom of Information and Protection of Privacy Act (FIPPA);
 - Municipal Freedom of Information and Protection of Privacy Act (MFIPPA); and
 - Personal Health Information Protection Act (PHIPA).

SLIDE 17

iP **Mandate and Role (Cont'd)**

The Commissioner is responsible for:

- Investigating privacy complaints;
- Resolving appeals, including those involving refusals to provide access to information;
- Ensuring that government organizations and health information custodians comply with the access and privacy provisions of the Acts;
- Educating the public about access and privacy issues;
- Conducting research to promote understanding of privacy and access issues.

SLIDE 18

iP **The Acts**

The role of the Information and Privacy Commissioner/Ontario (IPC) is set out in **three** statutes (The Acts):

1. the *Freedom of Information and Protection of Privacy Act (1988) - FIPPA*;
2. the *Municipal Freedom of Information and Protection of Privacy Act (1991)- MFIPPA*; and
3. the *Personal Health Information Protection Act (2004) - PHIPA*.

SLIDE 19

iP **What do the Acts cover?**

The two public sector Acts (*FIPPA* and *MFIPPA*) provide the public with a right of access to information held by the government in accordance with the following principles :

- Information should be available to the public;
- Exemptions to the right to access should be **limited and specific**; and
- Decisions on the disclosure of government information should be reviewed independently of government.

SLIDE 20

iP **What do the Acts cover? (Cont'd)**

- The other key purposes of these two public sector Acts are:
 - to protect the personal information held by *government* organizations and;
 - to provide individuals with a right of access to their **own** personal information.

SLIDE 21

What organizations are covered by the public-sector Acts?

- **FIPPA (the provincial Act)**
 - Provincial ministries;
 - Most provincial agencies, boards and commissions;
 - Community colleges;
 - Universities;
 - Hospitals - as of January 1, 2012;
- **MFIPPA (the municipal Act)**
 - Municipalities;
 - Police boards;
 - School boards;
 - Boards of health, transit commissions and most other local boards.

SLIDE 22

Personal Health Information Protection Act, 2004

- This is Ontario's health privacy legislation;
- It governs the manner in which personal health information may be collected, used and disclosed within the health care system

SLIDE 23

For more information,
Visit:
www.ipc.on.ca

ACTIVITY 2:

PRIVACY is your **RIGHT**

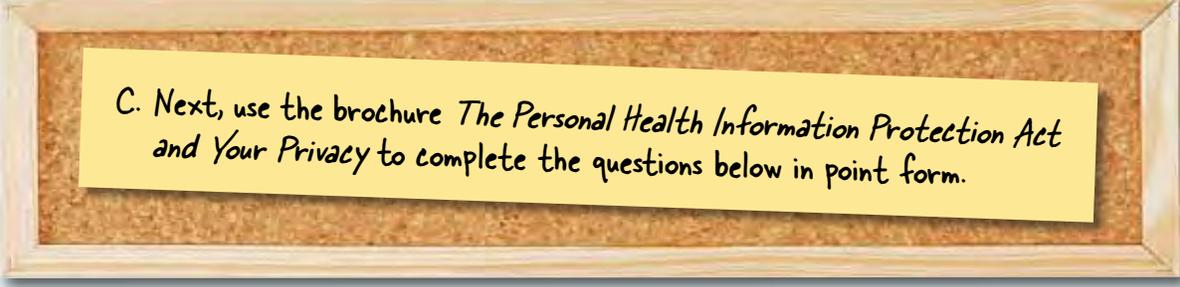
Student: _____



A. Visit the Information and Privacy Commissioner of Ontario website at www.ipe.on.ca.

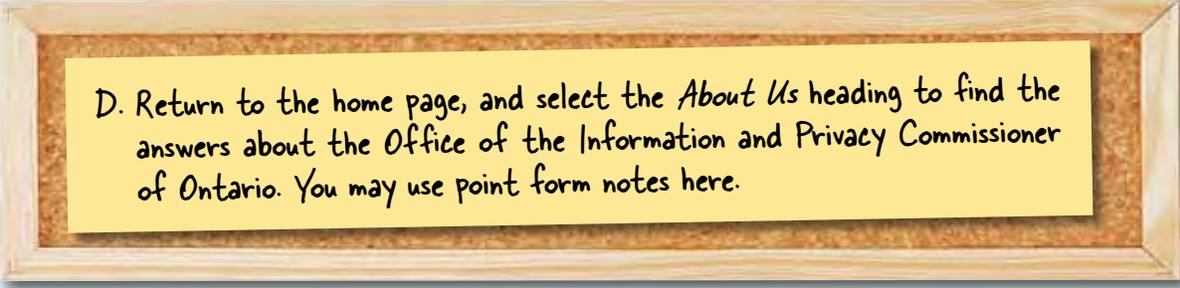
B. Click on the "Privacy" heading and select the "For the Public" subsections. Read the information in the subsections focusing on the brochure *Your Privacy and Ontario's Information and Privacy Commissioner* to answer the following questions. You may use point form here.

1. Which two *Acts* help to protect your personal information held by provincial and local government organizations?
 - a.
 - b.
2. To which organizations does the provincial *Act* apply? The municipal *Act*?
3. What is meant by "personal information?" Provide examples.
4. How do government organizations obtain information about me?
5. How do the *Acts* protect my personal information?
6. Who has access to my personal information?
7. How do I request correction of my personal information?



C. Next, use the brochure *The Personal Health Information Protection Act and Your Privacy* to complete the questions below in point form.

8. What is the *Personal Health Information Protection Act*?
9. What is considered personal health information?
10. As a patient, do I have the right to see my personal health information?
11. What do I do if I have a complaint?



D. Return to the home page, and select the *About Us* heading to find the answers about the *Office of the Information and Privacy Commissioner of Ontario*. You may use point form notes here.

12. Who is the present Information and Privacy Commissioner of Ontario? When was he/she first appointed?
13. List two of the awards or recognition received by the Information and Privacy Commissioner.
 -
 -
14. Under its statutory mandate, what are the key roles of the IPC?

ACTIVITY 3:



EXIT TICKET

Reflecting on what you have learned thus far, please complete the following statements:

<p>Two new things that I have learned:</p> <p>1.</p> <p>2.</p>	<p>One thing I want to learn more about is:</p> <p>1.</p>
<p>The concept or idea that I found the most challenging to understand is:</p>	<p>Privacy and Freedom of Information Laws are important because...</p>

TEACHER ANECDOTAL RECORDING SHEET

Student: _____

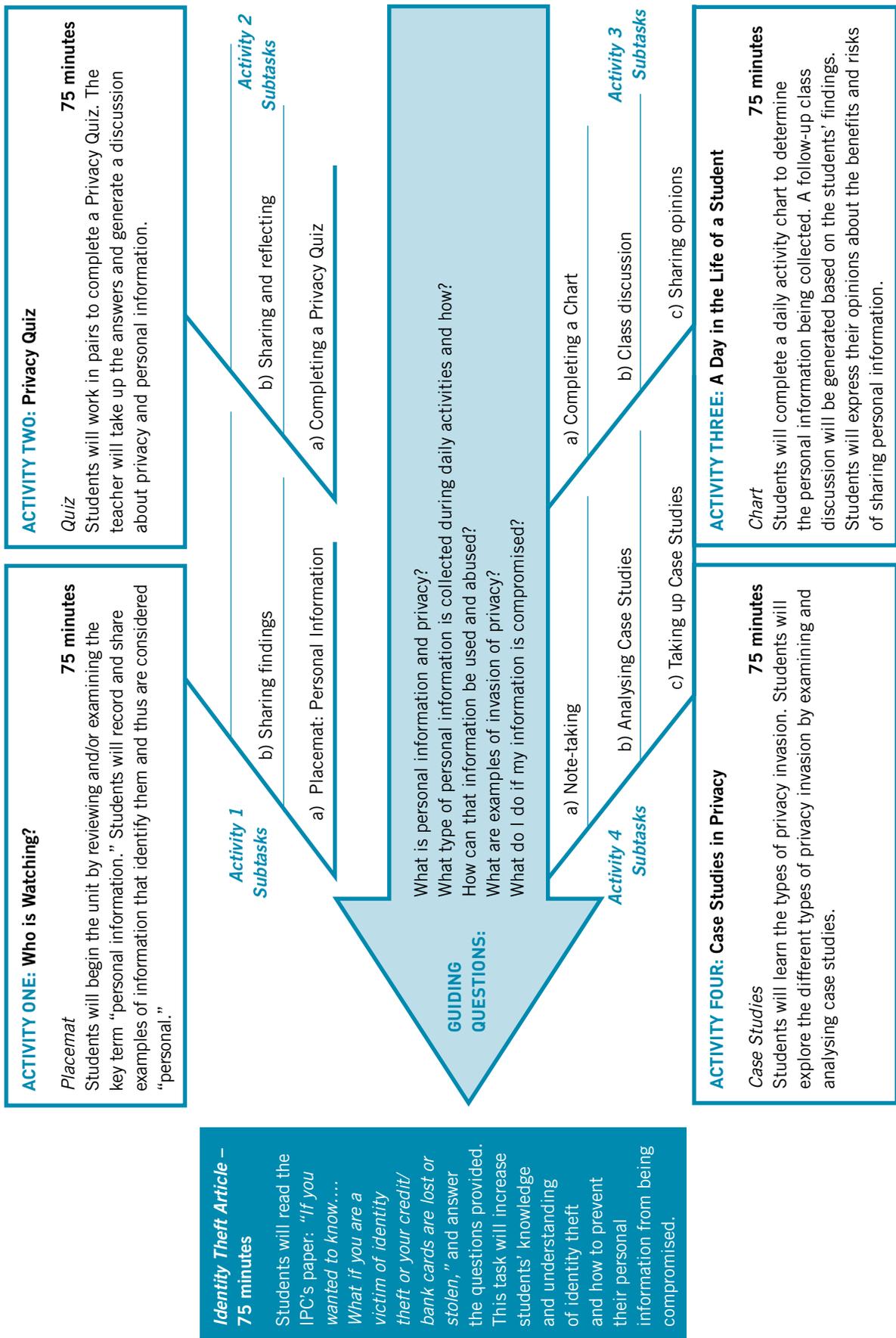
Scale: 1=seldom 2=occasionally 3=frequently 4=regularly

Performance Task

Scale

<input type="checkbox"/> communicates ideas clearly and effectively	1	2	3	4
<input type="checkbox"/> demonstrates orally an understanding of the content	1	2	3	4
<input type="checkbox"/> shows respect for the ideas of others	1	2	3	4
<input type="checkbox"/> listens without interrupting	1	2	3	4
<input type="checkbox"/> contributes to discussions	1	2	3	4
<input type="checkbox"/> asks appropriate questions	1	2	3	4
<input type="checkbox"/> carries out assignments independently; completes them on time	1	2	3	4
<input type="checkbox"/> works effectively in a small group	1	2	3	4

Unit Two - Overview of Unit Activities “Personal Information and Privacy Matters”



Identity Theft Article – 75 minutes
 Students will read the IPC’s paper: “If you wanted to know.... What if you are a victim of identity theft or your credit/ bank cards are lost or stolen,” and answer the questions provided. This task will increase students’ knowledge and understanding of identity theft and how to prevent their personal information from being compromised.

ACTIVITY ONE: Who is Watching?
Placemat
 75 minutes
 Students will begin the unit by reviewing and/or examining the key term “personal information.” Students will record and share examples of information that identify them and thus are considered “personal.”

Activity 1 Subtasks
 a) Placemat: Personal Information
 b) Sharing findings

ACTIVITY TWO: Privacy Quiz
Quiz
 75 minutes
 Students will work in pairs to complete a Privacy Quiz. The teacher will take up the answers and generate a discussion about privacy and personal information.

Activity 2 Subtasks
 a) Completing a Privacy Quiz
 b) Sharing and reflecting

GUIDING QUESTIONS:
 What is personal information and privacy?
 What type of personal information is collected during daily activities and how?
 How can that information be used and abused?
 What are examples of invasion of privacy?
 What do I do if my information is compromised?

Activity 4 Subtasks
 a) Note-taking
 b) Analysing Case Studies
 c) Taking up Case Studies

Activity 3 Subtasks
 a) Completing a Chart
 b) Class discussion
 c) Sharing opinions

ACTIVITY FOUR: Case Studies in Privacy
Case Studies
 75 minutes
 Students will learn the types of privacy invasion. Students will explore the different types of privacy invasion by examining and analysing case studies.

ACTIVITY THREE: A Day in the Life of a Student
Chart
 75 minutes
 Students will complete a daily activity chart to determine the personal information being collected. A follow-up class discussion will be generated based on the students’ findings. Students will express their opinions about the benefits and risks of sharing personal information.

UNIT 2

Personal Information and Privacy Matters

Time | 375 minutes

Description and Purpose

The purpose of this unit is to increase students' awareness of the risks involved in giving out one's personal information. The unit will provide students with an understanding of personal and private information. Students will explain how personal information is collected during daily activities and how that information can be used. They will learn about the various types of invasion of privacy and understand what to do in a situation where their personal information has been compromised.

Guiding Questions

What is personal information and privacy?

What type of personal information is collected during daily activities and how?

How can that information be used and abused?

What are examples of invasion of privacy?

What do I do if my information is compromised?

Prior Knowledge and Skills

- Placemat strategy;
- Organizing information;
- Teamwork;
- Critical Thinking;
- Literacy.

Planning Notes/Preparation

- Teachers arrange the class into groups of four for activity one;
- Arrange class into groups of two for activity four;
- Provide sufficient copies of the handouts for each activity;
- Reserve a lab to access IPC article for culminating task.

Materials List

- Placemat: *Who is Watching?* (**Appendix 2.1**);
- Handout: *Privacy Quiz* (**Appendix 2.2**);
- Teacher Answer Key: *Privacy Quiz* (**Appendix 2.3**);
- Handout: *A Day in the Life of a Student* (**Appendix 2.4**);
- Slide/Overhead copy of *Defining Invasion of Privacy* (**Appendix 2.5**);
- Handout: Case Studies: *Privacy at Risk* (**Appendix 2.6**);
- Teacher Answer Key: Case Studies: *Privacy at Risk* (**Appendix 2.7**);
- Handout: Final Task: “*If you wanted to know...What if you’re a victim of identity theft or your credit/bank cards are lost or stolen?*” (**Appendix 2.8**);
- Final Task Teacher Answer Key: “*If you wanted to know...What if you’re a victim of identity theft or your credit/bank cards are lost or stolen?*” (**Appendix 2.9**).

TEACHING/LEARNING STRATEGIES

ACTIVITY	MINDS ON	ACTION	CONSOLIDATION AND DEBRIEF
1	<p>Ask students, “<i>What is personal/private information?</i>”</p> <p>Teacher records response(s) on the board. Then teacher leads students into placemat activity.</p> <p>If students are not familiar with the placemat learning strategy, teacher will need to review the strategy.</p>	<p>Teachers will distribute copies of <i>Who is Watching?</i> placemat (Appendix 2.1).</p> <p>Students will brainstorm - in groups of four - examples of information that identifies them and is considered to be personal or private.</p>	<p>Ask students, “<i>Which information would you be comfortable sharing with strangers, and which would you want to keep private?</i>”</p> <p>“<i>Why?</i>”</p>
2	<p>Show students the Rick Mercer Report spoof, “<i>Personal Information Blowout</i>” found at www.youtube.com/mercerreport#p/search/1/jRSIXk4jeDc (Season Five: 16 October 2007).</p> <p>Ask students, “<i>What privacy risk does this clip make reference to?</i>”</p>	<p>Teacher will distribute <i>Privacy Quiz</i> (Appendix 2.2). Have students complete the True and False questions on privacy.</p>	<p>Teacher will provide the answers to the quiz using the Teacher Answer Key: <i>Privacy Quiz</i> (Appendix 2.3).</p>
3	<p>Teacher asks students, “<i>You go to a nightclub with your friends. What information might be collected while you are at the nightclub?</i>”</p> <p>Sample answers:</p> <ul style="list-style-type: none"> - Driver’s licence; - Phone number; - Etc. 	<p>Distribute copies of <i>A Day in the Life of a Student</i> (Appendix 2.4). Students complete the chart to identify and analyse the type of monitoring taking place and personal information being collected during their daily activities.</p>	<p>Ask students, “<i>What type of monitoring did this activity show and what does it tell us about our day-to-day privacy?</i>”</p> <p>“<i>What are the benefits and risks involved with sharing this information?</i>”</p>
4	<p>Display slide/overhead transparency <i>Defining Invasion of Privacy</i> (Appendix 2.5) to record the types of privacy invasion.</p>	<p>In groups of two, have students analyse Case Studies: <i>Privacy at Risk</i> (Appendix 2.6) to determine the type of privacy invasion. Students will present their answers to the class. Verify their responses with Answer Key - Case Studies: <i>Privacy at Risk</i> (Appendix 2.7).</p>	<p>To review, ask students, “<i>What are some of the ways in which your personal information may be compromised?</i>”</p> <p>“<i>What are some strategies to prevent these types of invasion of privacy from occurring?</i>”</p>
Final Task	<p>Students will read the IPC’s article, “<i>If you wanted to know... What if you’re a victim of identity theft or your credit/bank cards are lost or stolen?</i>” found at: http://www.ipc.on.ca/images/Resources/identitytheft.pdf.</p>	<p>Students will answer questions on the handout <i>Final Task</i> (Appendix 2.8). Teacher may collect the answers for evaluation.</p>	<p>Provide students with the answers from the Final Task Teacher Answer Key: (Appendix 2.9).</p>

Assessment and Evaluation of Student Learning

- assess students' understanding of the key terms and concepts of personal information and privacy;
- assess students' ability to contribute to class discussion using the *Teacher Anecdotal Recording Sheet* (included in **Unit 1, Appendix 1.4**);
- evaluate students' responses in the Unit Final Task.

Professional Resources

"If you wanted to know...What if you're a victim of identity theft or your credit/bank cards are lost or stolen?"

Information and Privacy Commissioner of Ontario. December 2008

<http://www.ipc.on.ca/images/Resources/identitytheft.pdf>

In Your I - <http://www.idtrail.org/InYourI/en/teacher/introduction.html>

Media Awareness Network. - <http://media-awareness.ca/english/index.cfm>

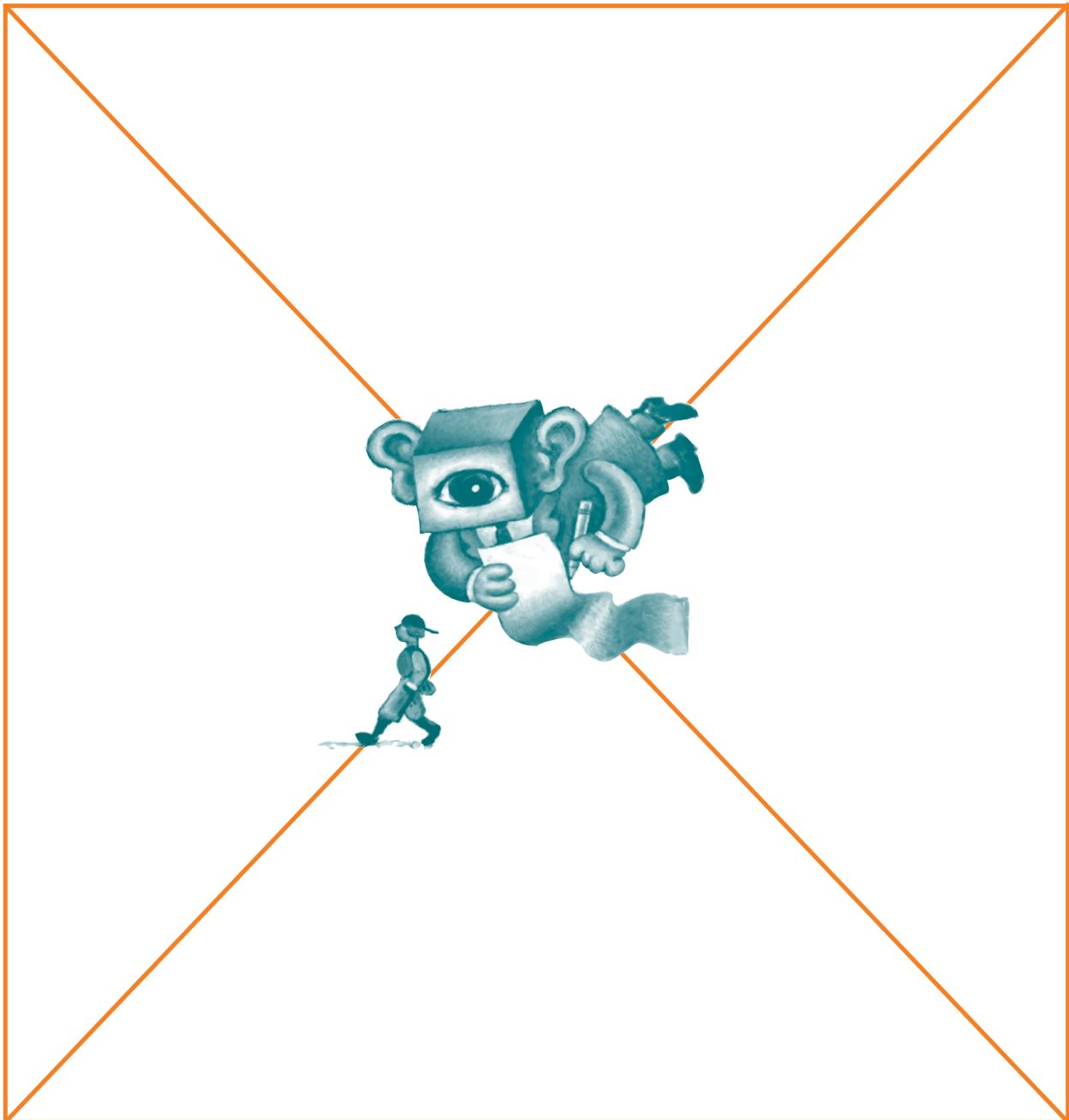
"Personal Information Blowout." *Rick Mercer Report* spoof. Season Five: 16 October 2007

www.youtube.com/mercerreport#p/search/1/jRSIXk4jeDc

ACTIVITY 1:

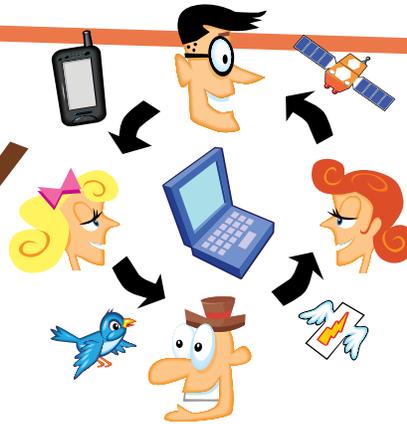
WHO IS WATCHING?

In a group of four, individually record examples of what you think is “personal or private information” on the placemat below. Then, as a group, decide what these examples have in common.



ACTIVITY 2:

PRIVACY QUIZ



Circle T for True or F for False,
based on your knowledge of privacy.

- | | | |
|---|---|--|
| T | F | 1. When a company asks you for personal information, it is safe to assume that it has a good reason for doing so. |
| T | F | 2. The first thing you should do if you receive an abusive message online is delete it. |
| T | F | 3. There are multiple ways that your activities online can be tracked. |
| T | F | 4. Any organization can refuse to provide a service unless you give it the personal information it seeks from you. |
| T | F | 5. A teacher is allowed to search you for drugs or weapons. |
| T | F | 6. You don't have to worry about information that appears about you, or is posted by you, online; eventually, it will disappear. |
| T | F | 7. Anyone who works in a hospital, pharmacy or doctor's office can access your health information for any reason. |
| T | F | 8. If you've never had a credit card or bank loan, there's no reason to check your credit report. |
| T | F | 9. It's okay to create a Facebook account for your pre-teen brother or sister, reporting their age as 14. |
| T | F | 10. You can be suspended from school for something you post online, even if you do it at home on your own computer. |
| T | F | 11. Once a company has your personal information, it can do whatever it wants to with that information. |
| T | F | 12. As long as you don't tell anyone your password for an account, no one can discover what it is. |
| T | F | 13. Privacy policies are too long and too difficult to read – it's not worth the effort of looking these up. |

TEACHER ANSWER KEY: PRIVACY QUIZ

- (1) **False.** You should not give information to anyone unless you know **why** they want it and **what** they plan to do with it, unless you are required, by law, to do so.
- (2) **False.** WiredSafety and the IPC teach a three-step response to online abuse or cyberbullying: *Stop, Block, and Tell Someone*. First, you need to “Stop” – don’t respond right away, take a moment to calm down. Next, you should “Block” the cyberbully, or limit your communications to those you trust. Finally, “Tell Someone” – let a trusted person know what is happening. This is why it is important not to delete the messages; it is better to be able to prove exactly what was said.
- (3) **True.** Currently, the best known means of tracking are advertising cookies. However, there are other ways of tracking you across websites, including your IP address, cookies placed to keep you logged in to Facebook or other sites, and something called “browser fingerprinting,” which can occur if your browser configuration is rare or unique.
- (4) **False.** The federal *Personal Information Protection and Electronic Documents Act* requires organizations to supply individuals with a service even if they refuse consent to collect, use or disclose their personal information, **unless** that information is required to fulfil the explicitly specified and legitimate purpose.
- (5) **True.** A teacher or principal has the authority under Ontario’s Education Act to conduct a search where there are reasonable grounds to believe that a school rule has been violated and the evidence of the breach will be found on the student.
- (6) **False.** While some content may disappear, you should not depend on this happening. If information online is indexed by one or more search engines or is stored by the Internet Archive’s Wayback Machine, it can be found later by those who know how. Material might also be copied, saved or redistributed by other people, or even appear in an online news site.

However, if there is material online you’d like to have taken down (particularly if it is offensive or harmful material about you posted by another person), there are steps you can take. First, ask the person who posted the information to take it down. Alternatively, politely ask the webmaster of the site to remove the information, explaining why. Once you have done this, you can also ask Google or other search engines to remove it from their results (though, given time, this will happen automatically). Some companies, such as Reputation Defender, will also provide this service for a fee. Finally, if you can’t get the material down, try to control your online reputation by posting positive information, or explaining why the “negative” material is wrong – let people see you the way you want to be seen.

- (7) **False.** The *Personal Health Information Protection Act* strictly defines the circumstances under which your health information can be used or disclosed. Here is a link to that Act: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm.

(8) **False.** Identity theft can happen to anyone – even teenagers. Similar to your online reputation, you should periodically check your financial reputation, and take steps to correct any inaccuracies. Checking your credit report is not difficult – you can get a free copy by writing to one of the credit bureaus. (Contact information for the bureaus is provided in the IPC paper, *If you wanted to know... What if you're a victim of identity theft or your credit/bank card is lost or stolen*, which is the focus of another lesson in this unit.)

(9) **False.** This would violate a number of Facebook's terms of service. Specifically, you are not permitted to create an account for anyone else (without permission), and you are not allowed to provide false personal information. Facebook does not permit anyone under the age of 13 to open an account.

In general, the consequence for creating a false account is that the account will be deleted if discovered. However, if you create a false account and use it for malicious purposes (to harm the person whose name you are using, or someone else), there may be further repercussions involving either your school or the police.

(10) **True.** Your actions online, particularly when they are harmful to others, are not consequence-free. Again, threats, malicious comments and other forms of cyberbullying do not need to take place on school property to warrant the involvement of teachers, principals, or even police.

(11) **False.** The federal *Personal Information Protection and Electronic Documents Act (PIPEDA)* generally requires private sector organizations to obtain consent when they collect, use or disclose personal information and to collect, use and disclose it only for purposes that are stated and reasonable. (There are exemptions from these requirements for some purposes, such as journalistic and literary purposes.)

(12) **False.** If you use common passwords (such as “1234” or “LetMeIn”), or a password associated with you (such as your pet's name), your password might be discovered through simple guesswork. Dictionary words are harder to guess, but can be discovered by a “brute force” search by a computer in a matter of hours. That is why it is important that you use strong passwords – combinations of letters and symbols that are at least eight characters long. For instance, you could use the phrase, “My birthday is October 21 and I'm 17,” as “MbiO21&I17.”

(13) **False.** Some privacy policies are indeed very long, and written in “legal-ese” – which can make them difficult to comprehend. However, there is a broad range of important information that can be included in these policies, raising red flags or reassuring you. A company might note, for example, that it owns any information uploaded to the site, and will reuse it as it chooses – or that it will never use the information for any other purpose than what it was collected for, without your permission.. As well, many companies have started to make their privacy policies much more understandable, in order to attract or keep customers. If you are not comfortable with the way a company presents this important information to you (or with the policies themselves), say so, or consider other companies. Staying informed is the best way of staying in control of your personal information.

ACTIVITY 4:

DEFINING INVASION OF PRIVACY



A) IDENTITY THEFT

Theft of personal information can be the starting point to a range of crimes – from financial fraud and forgery to abuse of government programs.

Examples of identity fraud include:

- the use of stolen credit cards or credit card numbers;
- fraudulently obtaining money, loans, finance and credit;
- fraudulently obtaining benefits, pensions, or entitlements;
- evading the payment of taxes, levies or other debts.



B) DEBIT AND CREDIT CARD FRAUD

Fraud committed using a credit card or debit card as a fraudulent source. Credit card fraud can happen several ways:

- Your card could be lost or stolen and used to purchase goods and services;
- A criminal could obtain your card number and expiry date and use this information to manufacture a counterfeit card;
- You could inadvertently provide your card number and expiry date to a criminal over the phone or Internet.



C) STALKERS AND HARASSMENT

“Stalker” is used to describe someone that follows or observes (a person) persistently, especially out of obsession or derangement. “Harassment” is to trouble persistently or incessantly with repeated annoyances, threats, or demands.



D) SHARING OR SELLING PERSONAL INFORMATION TO DIRECT MARKETERS

The term used to describe when private companies sell or share a customer’s personal information (such as name, address, phone number, age, interests, etc.) to a third party without the customer’s consent.

Sources:

<http://www.business.mcmaster.ca/IDTDefinition/defining/idfraudTCF.htm>
[http:// www.cba.ca](http://www.cba.ca)
<http://legal-dictionary.thefreedictionary.com/>

ACTIVITY 4:

CASE STUDIES: PRIVACY AT RISK?

Privacy is about control over your own information. If control is in the hands of someone other than you, your privacy can be lost. Once your privacy is lost, it is very difficult to get it back or repair any resulting damage.

Identify the *type of abuse* of personal information in the space below each scenario, and explain your choice. Choose from the following: identity theft, debit and credit card fraud, stalkers and harassment, and sharing or selling personal information to direct marketers.



1. A man, using someone's stolen birth certificate and SIN card, obtained a driver's licence from the provincial government. He then used these three pieces of ID to open fraudulent bank accounts and proceeded to steal more than \$170,000 from several banks.

2. A reporter got a call from Canadian Tire because his application for a Canadian Tire credit card seemed suspicious. It turned out someone else had filled out the application. If the application had been approved, the criminal could have racked up purchases on the card, in the reporter's name. The person had also tried to apply for a MasterCard. These actions could have damaged the reporter's personal credit rating.

3. In an Interac scam, the cashier at a store "double-swiped" the shopper's debit card, once on the store's machine and then again to enter the data from the magnetic stripe on her own computer under the counter. Then, by watching the shopper closely, the cashier learned his PIN number. This made it possible to duplicate the debit card and access the shopper's bank account.

4. An actress in the United States was killed by an obsessive stalker, who had obtained her home address by hiring a private investigator. The investigator used a Department of Motor Vehicles licence database to find her address.

5. A woman received a 12-page letter from a stranger. He knew her birthday, the fact that she was divorced, the kind of soap she used in the shower, her favourite magazines, and many other details about her life. It turned out he was a convicted rapist, and one of his jobs at the prison was entering data from consumer surveys. The woman had sent in a completed questionnaire in order to get the free samples and coupons promised by the company. She had assumed her information would be kept confidential by company employees.

6. A woman returned home from a stay in hospital, where she had been diagnosed with cancer. The next day she received a phone solicitation from a local funeral home; the funeral home asked for her by name, even though she had an unlisted number. After much pressing, the salesperson admitted that he had been given her number by someone from the hospital.

7. Do you have an example? Add it here.

Source: Adapted from and used with the permission of the Office of the Information and Privacy Commissioner for Alberta

ACTIVITY 4: TEACHER KEY FOR CASE STUDIES: *PRIVACY AT RISK?*

1. Identity theft;
2. Debit and credit card fraud;
3. Debit and credit card fraud;
4. Sharing or selling personal information to marketers without consent;
5. Sharing or selling personal information to marketers without consent;
6. Stalkers and harassment.

Source: Adapted from and used with the permission of the Office of the Information & Privacy Commissioner for Alberta

FINAL TASK:

**“If you wanted to know...
What if you’re a victim of
identity theft or your
credit/bank cards are lost
or stolen?”**



Visit the website below to view the IPC article, *“If you wanted to know ...What if you are a victim of identity theft or your debit/bank cards are lost or stolen?”* Read the article and answer the following questions in your notes. Be prepared to submit your responses to your teacher for evaluation.

<http://www.ipc.on.ca/images/Resources/identitytheft.pdf>

1. How does one verify if impersonation has occurred?
2. What is a credit bureau?
3. What is a credit report?
4. How long does information remain on your credit report?
5. What is a credit score?
6. How many credit bureaus are there in Ontario?
7. What is the process to request a credit report?
8. What should you do if you discover you are a victim of identity theft?
9. What should you do if your credit or bank cards are lost or stolen?
10. How do I avoid becoming a victim of identity theft?

MARK: /10

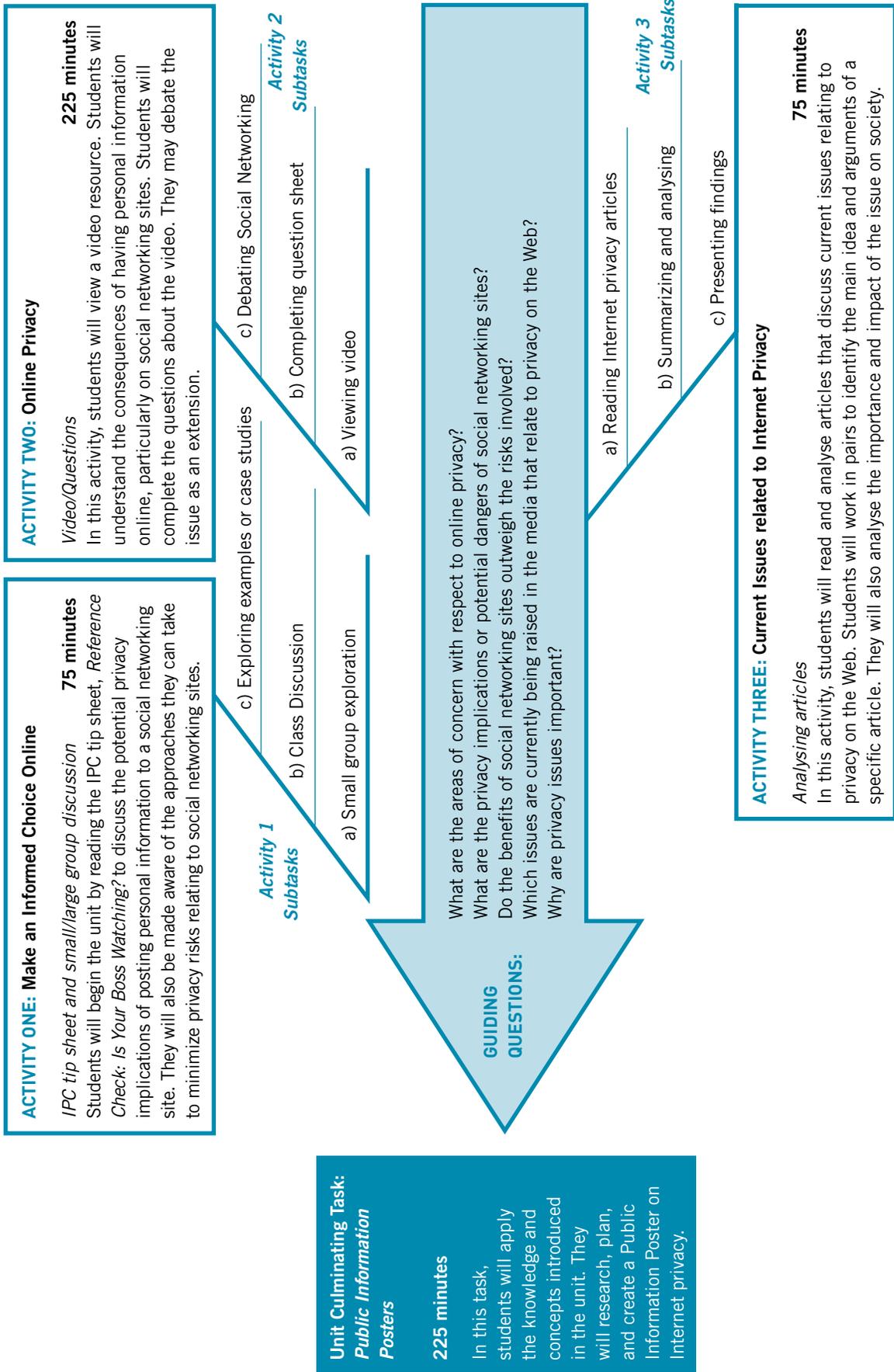
**FINAL TASK:
TEACHER ANSWER KEY:**

“If you wanted to know.... What if you’re a victim of identity theft or your credit/bank cards are lost or stolen?”

- 1. How does one verify if impersonation has occurred?**
 - Contact a credit bureau to check your credit report for fraudulent activity.
- 2. What is a credit bureau?**
 - A credit-reporting agency is a private institution which serves retailers and other credit grantors by providing them with information about your credit record.
- 3. What is a credit report?**
 - A credit report is a profile of how you pay your financial obligations. It is created when you first borrow money or apply for credit. If you make your payments on time, or miss a payment, or if you have gone over your credit limit, this information will be on your record.
- 4. How long does information remain on your credit report?**
 - Six years.
- 5. What is a credit score?**
 - A credit score, not part of your report, is a mathematical formula that translates the information in your credit report into a three digit number that lenders use to make decisions. The higher your credit score, the more likely you are to be approved for loans or credit and receive favourable rates.
- 6. How many credit bureaus are in Ontario?**
 - There are three credit bureaus: Equifax Canada, TransUnion Canada, and Experian Canada.
- 7. What is the process to request a credit report?**
 - You can request your reports free of charge, via mail or phone, or for a fee via the Internet.
- 8. What should you do if you discover you are a victim of identity theft?**
 - Immediately report this to the police. Cancel all existing credit cards, accounts, passwords and personal identification numbers (PINs) and explain why. Close accounts that you know, or believe have been tampered with or opened fraudulently.
- 9. What should you do if your credit or bank cards are lost or stolen?**
 - Call your credit grantors immediately upon discovering that your cards are missing. Most will have round-the-clock service phone numbers for emergencies. Write down the name of each person you speak with.
- 10. How do I avoid becoming a victim of identity theft?**
 - Pay attention to your billing cycles;
 - Review bills and statements on a regular basis;
 - Monitor account balances and activity;
 - Shred all personal records and financial statements;
 - Obtain a separate credit card (with the lowest credit limit available) that will be dedicated to online purchases only.

Unit Three - Overview of Unit Activities

“Using the Web: Internet Privacy”



UNIT 3

Using the Web: Internet Privacy

Time | 600 minutes

Description and Purpose

The purpose of this unit is to increase students' awareness of privacy as it relates to using the Web. Students will be able to identify areas of risk that pose a threat to Web users. They will explore areas of concern related to privacy through an IPC tip sheet, MTV video, online and print articles. Students will assess and discuss current issues, analyse their impact on society and think creatively to formulate solutions. In the culminating task, students will use their knowledge to research Internet privacy risk to create a public information poster that will be used to increase the school community's awareness.

Guiding Questions

What are the areas of concern with respect to online privacy?

What are the privacy implications or potential dangers of social networking sites?

Do the benefits of social networking sites outweigh the risks involved?

Which issues are currently being raised in the media that relate to privacy on the Web?

Why are privacy issues important?

Prior Knowledge and Skills

- Organizing information;
- Computer literacy skills;
- Reading skills;
- Teamwork skills;
- Listening skills;
- Critical thinking skills;
- Summarizing;

- Working with others;
- Self-reflection;
- Research skills and proper documentation of sources.

Planning Notes/Preparation

- Arrange students into groups of four for activity one;
- Arrange students into groups of two for activity three;
- Arrange students in groups of two for culminating task;
- Book an LCD with a DVD player to watch the short MTV video;
- Book a lab for students with Web access to complete culminating task;
- Provide sufficient copies of handouts for each activity.

Materials List

- Handout: *Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile*; **Appendix 3.1**);
- Slide/Overhead: *The 5 P's* (**Appendix 3.2**);
- Handout: *Video Worksheet – Online Privacy* (**Appendix 3.3**);
- Handout: *Mini-Debates: Social Networking* (**Appendix 3.4**);
- Handout: *Mini-Debates: Self-Reflection* (**Appendix 3.5**);
- Handout: *Analysing Current Issues Related to Web Privacy* (**Appendix 3.6**);
- Article: *Facebook fakers prey on students* (**Appendix 3.7**);
- Article: *Spy chief's wife puts him on Facebook; Head of M16 learns millions have access to family details* (**Appendix 3.8**);
- Article: *Identity theft among Canada's fastest-growing crimes; In recent years, reports have soared 500 per cent* (**Appendix 3.9**);
- Article: *Privacy rights when using employer-provided computers* (**Appendix 3.10**);
- Article: *The Perils of Facebook; Beware of consequences of baring your soul, or other things, online* (**Appendix 3.11**);
- Handout: *Culminating Task: Staying Safe Online Public Information Poster* (**Appendix 3.12**);
- Handout: *Culminating Task Rubric* (**Appendix 3.13**).

TEACHING/LEARNING STRATEGIES

ACTIVITY	MINDS ON	ACTION	CONSOLIDATION AND DEBRIEF
1	<p>Teachers will distribute to students copies of <i>Reference Check: Is Your Boss Watching?</i> – which can be found on the IPC’s website, http://www.ipc.on.ca/images/Resources/facebook-refcheck.pdf</p> <p>In groups of four, students will read the handout, and respond to the small-group discussion questions provided (Appendix 3.1).</p>	<p>Have the class reconvene and share their answers to the discussion questions.</p> <p>Explain to students that in the case of prospective employers or university admissions, the student will 1) not necessarily ever be told that it was online information that affected a decision, and 2) not necessarily ever be given a chance to explain a negative item, or provide context for a statement.</p> <p>Explain to students that in addition to negative effects on preliminary screening (for jobs, scholarships, etc.), a number of more serious unfortunate events have occurred as a result of individuals being tracked through their profiles on social networking sites, including:</p> <ul style="list-style-type: none"> - Expulsion from colleges and universities due to the nature of some of the information contained on their profiles; - Investigations by authorities; - Dismissal from employment; - Misuse, selling or “databasing” of personal information; - Stalking and harassment; - Assault (physical). 	<p>Have students take notes on the slide/overhead of the 5 P’s (Appendix 3.2) to consider before they post information online. Teacher will briefly explain to students what the 5 P’s represent.</p> <p>As an extension of students’ learning, ask students to locate a news article that reports on a situation where information that was posted on a person’s online social networking profile has led to trouble with any of the 5 P’s. Ask them to summarize the article, and discuss how the situation could have been prevented.</p>

ACTIVITY	MINDS ON	ACTION	CONSOLIDATION AND DEBRIEF
2	<p>Students will watch a short MTV video in which Ontario Information and Privacy Commissioner Ann Cavoukian and several students are interviewed about online privacy. The video is posted on YouTube at:</p> <p>http://www.youtube.com/watch?v=vl8INvVQVNY</p>	<p>Distribute the video worksheet: <i>Online Privacy</i>. (Appendix 3.3), then replay the short video, after telling students to start answering the questions as they view the video. Take up the answers to the video.</p> <p><i>1. Possible answers include: employers or potential employers could see you as trustworthy and serious, or lazy and frivolous; photos of partying could make you seem like a heavy drinker or drug user; groups you belong to on Facebook could make you appear engaged and active, or as having poor judgement</i></p> <p><i>2. Internet archives may store data forever (e.g. Internet Archive Wayback Machine, Google and Yahoo caches, old versions of web sites), and can be searched by those who know how.</i></p> <p><i>3. You can control what you post online and set your privacy preferences to limit the initial access to people you trust, but you cannot completely control how others may subsequently copy or share the information.</i></p> <p><i>4. Online data is searchable, and can be archived, shared, and combined/matched with other data to create profiles that can be seen by anyone in the world, anytime.</i></p> <p><i>5. Possible answers include: losing out on prospective employment or education opportunities; losing the trust of a potential boyfriend/girlfriend; losing the trust of a parent.</i></p> <p><i>6. The ability to control how and when you share your personal information is an important aspect of self-determination.</i></p>	<p>For homework, those students who use a social networking site, such as Facebook, should modify their privacy settings to reflect their desired privacy.</p> <p>As an extension of students' learning, teachers can have mini-debates on the benefits and risks of social networking sites such as: Facebook, MySpace, MSN, Twitter, Tagged.com, Plaxo, Hi5 etc. (Appendix 3.4).</p> <p>Students are to complete a <i>Self-Reflection Activity</i> (Appendix 3.5).</p>

ACTIVITY	MINDS ON	ACTION	CONSOLIDATION AND DEBRIEF
3	Divide students into pairs and distribute an article (Appendices 3.7 – 3.11) to each pair for analysis.	Students will complete <i>Analysing Current Issues related to Web Privacy</i> (Appendix 3.6). Then, students will present the articles to the class for discussion.	Ask students, “ <i>What are some similarities among the issues raised in the presentations?</i> ” “ <i>Describe the impact and consequences of the Web on privacy today.</i> ”
Unit Culminating Task	Recognizing problems and identifying solutions are skills that help students develop awareness of themselves and their surroundings. Brainstorm orally with the class some <i>privacy invasion prevention tips</i> . Ask students, “ <i>What advice do you have for staying safe on the Internet?</i> ”	Students will use the Web to research potential Internet privacy breaches and devise prevention tips for others. Distribute copies of <i>Culminating Task: Staying Safe Online – Public Information Poster</i> (Appendix 3.12). Students will create a Public Information Poster to communicate safety messages to others.	Students will present their posters to the class for evaluation. Teacher may use the <i>Culminating Task Rubric</i> (Appendix 3.13) to evaluate students’ work. Students may also want to share Internet safety tips with feeder schools and display their posters in the school community.

Assessment and Evaluation of Student Learning

- assess students’ understanding of the key terms and concepts of personal information and privacy;
- assess students’ *Self-Reflection Activity*;
- evaluate students’ posters in the *Culminating Task* using the rubric provided;
- assess students’ ability to contribute to class discussion using the *Teacher Anecdotal Recording Sheet* (included in **Unit 1, Appendix 1.4**).

Professional Resources

Cavoukian, Ann, Ph.D. *Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile*. Information and Privacy Commissioner of Ontario -

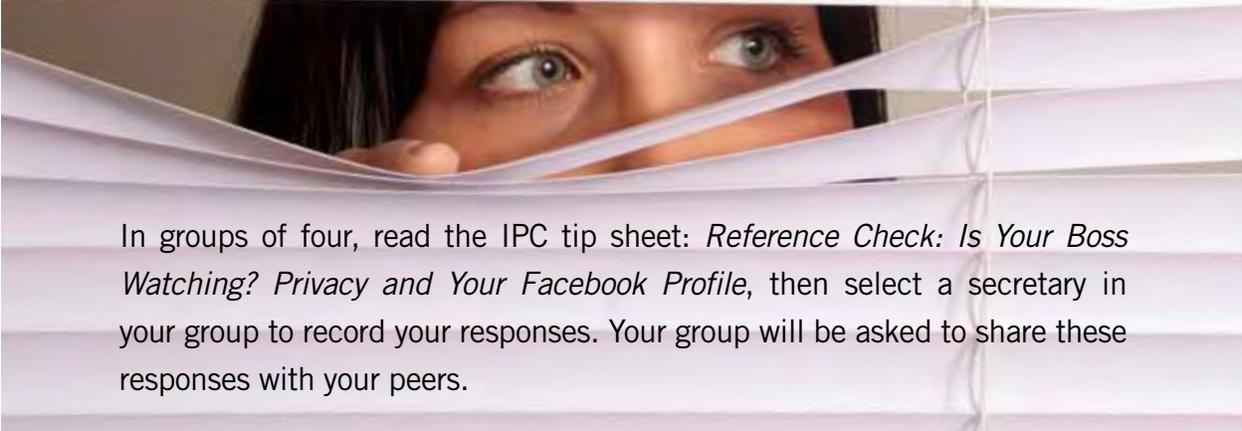
<http://www.ipc.on.ca/images/Resources/facebook-refcheck.pdf>

In Your I - <http://www.idtrail.org/InYourI/en/teacher/introduction.html>;

Media Awareness Network - <http://media-awareness.ca/english/index.cfm>.

ACTIVITY 1:

MAKE AN INFORMED CHOICE ONLINE



In groups of four, read the IPC tip sheet: *Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile*, then select a secretary in your group to record your responses. Your group will be asked to share these responses with your peers.

GROUP DISCUSSION QUESTIONS:

1. Who might be interested in the information that is contained in your online profile? How might this impact you?
2. Are you familiar with the privacy settings on your social network(s) of choice? Do you *know* who will be able to view the content you post?
3. After reading the IPC's tip sheet, would you reconsider the nature or amount of information you post on your online social networking profile, or the extent to which that information is shared? Why or why not?

ACTIVITY 1:

THE 5 P's

Before you decide to post any personal information online, remember the following 5 P's that represent the different groups or individuals who might view it.



ACTIVITY 2:

ONLINE PRIVACY



Watch the video (which is being used with the permission of MTV News Canada), then answer the following questions:

1. What are some positive and negative ways in which information about you (including pictures) posted online could affect your reputation?
2. When you post information online, how long does it stay there for?
3. Can you control access to and sharing of information online?
4. What are some of the differences between having everyone in your town know something about you and having that same information posted online?
5. Outline a scenario in which posting sensitive or controversial personal information online might have negative consequences.
6. In the video, the Information and Privacy Commissioner of Ontario says that privacy equals freedom. What do you think she means by that? Do you agree or disagree? Why or why not?

ACTIVITY 3:

MINI DEBATES: SOCIAL NETWORKING



DESCRIPTION

Debating is the forceful and logical presentation of arguments for or against an idea. You debate every day in one form or another. In the classroom, you are trying to persuade your audience and the judge (i.e. your classmates and teacher) with facts and logic, not to outshout your opponent. In a debate, the members of the “affirmative” team are for the resolution. They present arguments that support the resolution. The members of the “opposition” are against the idea or resolution. They present arguments against those offered by the affirmative team.

PURPOSE

- To develop co-operative and listening skills;
- To demonstrate an ability to present ideas and arguments effectively in a debate;
- To demonstrate critical thinking and analysis about an issue.

TASK

Debate the following resolution:

- **Be it resolved that the benefits of social networking sites outweigh the risks.**

INSTRUCTIONS

During this activity, you will work in partners to establish a position and debate with another pair with opposing viewpoints. In each group, students will debate the benefits and risks

involved with using social networking sites such as Facebook, MySpace, Twitter, Tagged, Plaxo, LinkedIn, hi5, Flickr etc. Consider issues such as privacy, security, reputation, business and social networking, fraud, exploitation, cyber-bullying, advertising, exposure, democratic participation, etc.

STEPS

- 1) In a group of four, decide on one networking site for the debate;
- 2) Divide your group into an affirmative and opposition position (for or against social networking);
- 3) The first pair to speak should make at least three points that support their argument. They have up to five minutes;
- 4) The second pair will then speak for up to five minutes, making at least three points in favour of their argument;
- 5) The first pair will then spend five minutes refuting the arguments of the second pair;
- 6) Finally, the second pair will conclude the debate by critiquing the first pair’s main arguments.

ASSESSMENT

- Self-reflection;
- Teacher feedback;
- Peer response.

ACTIVITY 3:**MINI DEBATES: SELF REFLECTION**

Answer the following questions to reflect on your understanding, opinions and values regarding the impact of social networking sites in society.



Have your knowledge and understanding of social networking sites changed as a result of this activity? How?

Have the debates influenced your opinion of the use and/or impact of social networking sites in society? Why or why not?

What do you predict will happen to social networking sites in the future?

ACTIVITY 4:**ANALYSING CURRENT ISSUES
RELATED TO WEB PRIVACY**

With a partner, read the news article provided by your teacher. Answer the following questions in the space provided.

What is the title of the article?

Summarize the main idea of the article.

What are some arguments outlined in the article that connect to or support the main idea?

Why is the issue important? Whom does it impact?

If you were to respond in an editorial, do you agree or disagree with the main message? What recommendations can you make to deal with the issue?

Facebook fakers prey on students

The Toronto Star
 Mon Jul 6 2009
 Page: A01
 Section: News
 Byline: Paola Loriggio
 Source: Special to the Star

Prospective university students are falling prey to a growing Facebook fraud as marketers set up fake academic groups to vacuum up their personal information.

After a sweep that shut down a number of fraudulent groups last month, a new batch has sprung up, targeting the classes of 2014 and 2015, and experts say more are on the way.

The stakes are high – potentially years' worth of data and thousands of contacts in a desirable demographic. So high, in fact, one company allegedly tried to bribe and blackmail a student to help a scam.

Hundreds of students in the GTA were told in June to abandon fake "Class of 2013" Facebook groups, many sporting official school logos. A sweep shut down groups targeting classes at more than a dozen major Canadian universities, including the University of Toronto, York, Ryerson and McMaster.

There is "a whole subculture" of people trying to make a quick buck by impersonating legitimate organizations and celebrities online, says Avner Levin, director of the Privacy and Cyber Crime Institute at Ryerson University.

The set-up goes beyond sending ads to those who join the fraudulent groups, Levin says. Unbeknownst

to students, marketers are building mailing lists, collecting personal information that they can store and sell for years, he says.

A spokesperson for Facebook said the company doesn't have statistics on people creating false accounts, dubbed "squatters." But she said the company removes the accounts when notified through the "report" link found on each page.

The discovery of marketer-run university groups rocked U.S. academic circles in December, after dozens of fake groups were linked to campus guidebook company College Prowler. The company apologized for misleading students.

Alerted to the U.S. scam, officials at Dalhousie University reported a fake "Class of 2013" group to Facebook administrators during the winter and had it deleted.

When that group disappeared, Tyler Thorne, an incoming Dalhousie freshman, started a new one. It wasn't long before marketers contacted him, asking to become the group's administrators.

The marketers (a "major event promotion company") tried to bribe him with money and concert tickets, said Thorne, a 17-year-old from Halifax. When that failed, he said, they threatened to blacklist him from all local bars.

Matthew Melnyk, an electronic outreach recruitment officer at Brock University, discovered a fake Brock group in February. He later

linked it to a network of more than a dozen suspicious groups targeting incoming students at major Ontario universities.

The groups were shut down in early June, but a new generation has already appeared, targeting the next two waves of freshmen.

...

Lysan Sequeira, 18, left a fake U of T group after receiving a warning message from a real university group. "It definitely changed how I behave on Facebook," she said. She tightened her profile's privacy settings, and no longer accepts friendship requests from strangers.

Ryan McNutt of Dalhousie University, who discovered the fake group linked to the school, says most universities are just starting to monitor sites like Facebook.

Levin, of the Privacy and Cyber Crime Institute, says Facebook should do more to seek out and delete squatters' accounts. He also has a warning for students who think they're safe from fraudsters because they use strict privacy controls on their Facebook accounts: Marketers can deduce demographic data from users' networks, and guess email addresses from their names and academic institutions.

Though Facebook's terms of use ban false accounts and misleading information, the groups often go unnoticed, he says.

(This is a slightly condensed version of the article.)

Spy chief's wife puts him on Facebook; Head of M16 learns millions have access to family details

The Ottawa Citizen
 Mon Jul 6 2009
 Page: A6
 Section: News
 Byline: Michael Evans
 Source: The Times, London

Diplomats and public servants are to be warned about the danger of putting details of their family and career on social networking websites. The advice comes after the wife of Sir John Sawers, the next head of MI6, put family details on Facebook – which is accessible to millions of Internet users.

Lady Sawers disclosed details such as the location of the London flat used by the couple and the whereabouts of their three children and of Sawer's parents. She put no privacy protection on her account, allowing any of Facebook's 200 million users in the open-access London network to see the entries.

Patrick Mercer, the Conservative chairman of the Commons counter-

terrorism sub-committee, said the entries were a serious error and potentially damaging.

“Sir John Sawers is in a very sensitive position and by revealing this sort of material his family have left him open to criticism and blackmail,” he told the Times. “We can't have the head of MI6 being compromised by having personal details of his life being posted on Facebook.”

David Miliband, British foreign secretary, was dismissive Sunday of the security implications of the incident. Speaking on BBC One, he said that it was “no state secret” that Sawers wore Speedo swimming trunks on family holidays. “For goodness' sake, let's grow up,” he said.

He described Sawers as an “outstanding professional” and denied the episode would compromise his career.

Identity Theft among Canada's fastest-growing crimes;

In recent years, reports have soared 500 per cent

The Globe and Mail
 Mon Jun 29 2009
 Page: A5
 Section: National News
 Byline: Omar El Akkad

If Corporal Louis Robertson of the RCMP's anti-fraud call centre needs further proof that identity theft is among the fastest-growing crimes in Canada, he need look no further than his own wallet.

Last year, Cpl. Robertson noticed a strange charge on his American Express statement originating in Ottawa at a time when he was in Washington. The man who knows more about identity theft than almost anyone in Canada has never found out who got his credit card information, or how.

"[Identity theft] is the fastest criminal market right now," Cpl. Robertson said. "There's no risk, and that's the beauty of it - if you are smart, you will disappear."

Between 1998 and 2003, identity-theft reports in Canada soared 500 per cent, according to Vanessa Giuliani, a fraud specialist with the credit information and reporting agency, Equifax Canada Inc. Ms. Giuliani was one of several

representatives of credit-related business in Ottawa in 2009 urging passage of Bill S-4, which would create several new Criminal Code offences related to identity theft. *(See note at the end of this story for more recent statistics.)*

Businesses have traditionally walked a fine line when trying to combat identity theft. If they subject people to overly intense scrutiny, they risk invading people's privacy and upsetting their best customers, while too many regulations and checks can hinder the flow of commerce. Do too little, and criminals thrive.

Cpl. Robertson estimates the financial impact of identity theft in Canada at about \$500-million a year. It's impossible to get a precise figure, given the nature of the crime and the fact that many companies are reluctant to release their fraud statistics. Identity theft has become so common that it is called traditional identity theft to differentiate it from an even more damaging variation that has grown significantly in the past couple of years: fictitious identity theft. In this scenario, a criminal

uses a real piece of identification as a basis to create a fake person who they use to apply for all the credit cards and loans a real person could. At the end of the scam, the culprit takes the money and runs, and there's nothing left to chase. Equifax estimates the average loss in an instance of successful fictitious identity theft at about \$250,000.

Such cases are often traced to organized crime, Cpl. Robertson said, adding that the RCMP has tracked identity-theft rings to everything from West African criminal groups to local biker gangs.

Identity theft can often start with one or two low-level company employees who have access to personal information databases. Given how valuable that kind of information can be to a criminal organization, employees who leave sometimes take it with them. Cpl. Robertson said companies have consulted him on what to do after discovering that anywhere from two million to 40 million identities may have been compromised.

Identity Theft Continued...

“My first answer,” he said, “is get a lawyer.”

Because identity theft is usually the work of organized rings, when uncovered, it tends to be on a large scale. Two years ago, Toronto police officers conducting a traffic stop found 15 credit reports in the back seat of a car. An investigation by Equifax and the police traced those reports to three employees at three different companies. Between them, the three had created 500 fictitious identities.

“You tend to see foot soldiers working in concert with organized groups,” Ms. Giuliani said. “They don’t always actualize identities, but when they do get it, the average loss to the industry is about \$250,000 per identity.”

Recently, firms have become aware of the risks of appearing to blow the identity-theft issue out of proportion.

Earlier this year, a senior executive at AT&T Inc. told a U.S. Senate committee that worldwide revenues from all cyber crime stand at \$1-trillion, making it

more lucrative than the drug trade.

His assertion has drawn criticism from those who call that number impossibly big.

But for Cpl. Robertson, the biggest concern isn’t the size of the identity-theft industry, but the speed with which someone’s identity can be stolen and exploited.

“Your personal identity can easily be sent to a black market in Bulgaria, and that’s it,” he said. “It’s all about speed.”

UPDATED STATISTICS from the Office of the Information and Privacy Commissioner of Ontario.

The number of cases of identity theft fraud that are reported to police are only a fraction of the actual number. The most comprehensive study (as of early 2011) measuring the impact of identity theft in Canada was a 2008 McMaster University consumer survey entitled *Measuring Identity Theft in Canada*.¹ The survey concluded that 6.5 per cent of Canadian adults, or almost 1.7 million people, were victimized by some kind of identity fraud during the previous year. Only 13 per cent of these frauds were reported to the police.

The statistics below are from an early 2011 report by the Canadian Anti-Fraud Centre (<http://www.antifraudcentre-centreantifraude.ca/english/documents/Annual%202010%20CAFC.pdf>) citing actual reported cases.

- **2010:** 18,146 victims; \$ 9,436,996.92 in reported dollar losses;
- **2009:** 14,797 victims; \$10,968,134.44 in reported dollar losses;
- **2008:** 12,309 victims; \$ 9,689,374.32 in reported dollar losses.

¹ *Measuring Identity Theft in Canada*, Susan Sproule and Norm Archer, July 2008, Mc Master eBusiness Research Centre, DeGroot School of Business.

PRIVACY RIGHTS WHEN USING EMPLOYEE-PROVIDED COMPUTERS

The Welland Tribune

Thu Apr 7 2011

Page: A7

Section: News

Column: The Law

By Alan Shanoff

Warning: Reading headlines may be hazardous to your legal health.

We should put this disclaimer on every article reporting on legal developments.

The headlines accompanying last month's Ontario Court of Appeal decision on **privacy** rights pertaining to personal material stored on computers provided by employers proves the need for such a warning.

Headlines trumpeted "Ontario court rules personal files on work computer private," "Files stored on work computer are private" and "Computer ruling seen as landmark workplace decision."

One of the articles even referred to "a **constitutional right to privacy**."

The problem is when you look at the actual decision, you'll get an entirely different perspective.

The case revolved around Sudbury high school teacher Richard Cole, who accessed a male student's e-mail account, found nude photos of a female student and copied them onto his school-issued laptop.

The nude photos were discovered by an information technologist during a routine virus scan of the school's network.

The technician reported his discovery to the principal and the photos were copied onto a disc.

The principal ordered Cole to surrender the laptop and a subsequent search of

the computer disclosed Cole's browsing history and files with large numbers of pornographic images.

This history was also saved onto a disc.

Now, if the headlines were accurate, the evidence of the nude photos of the student, the browsing history and the pornographic images discovered by school technicians would have been declared illegally obtained and inadmissible in a case against Cole where he's up on charges of possession of child pornography and fraudulently obtaining data from the male student's computer.

But that's not what the appeal court ruled. Instead the court ruled the technicians and the principal acted reasonably. The copying of the nude photos onto a disc, the seizure of the computer by the principal, the search of Cole's browsing history and saving the history onto a disc were all deemed to be reasonable and lawful.

All of this evidence is **allowable**, contrary to what the trial judge ruled.

What the Court of Appeal ruled, however, and what has led to the misleading headlines relates to what happened **after** the principal handed the computer to the police.

The police conducted further searches on the computer **without** having obtained a search warrant. They thought they were entitled to do so based solely on the permission of the principal.

The appeal court disagreed, ruling the subsequent warrantless police search of the computer was a violation of Cole's rights.

But, and it's a huge but, that didn't taint anything the school employees did, and

all of the evidence obtained and handed over to police was ruled lawful and not in violation of Cole's rights.

And now that Ontario's highest court has ruled on this point, police will now be sure to obtain a search warrant before examining any computer given to them by either a school or any employer.

Obtaining a warrant will be an easy task if police are given any evidence establishing reasonable and probable grounds for a search, as occurred in the Cole case.

The upshot is Cole will be retried on the charges and the prosecution will be entitled to use all the evidence handed over to police. Only additional evidence obtained by police after receiving the computer is inadmissible.

Whatever the ultimate outcome of the Cole prosecution, **people need to understand any computer on loan from an employer is subject to being examined by their employer.**

Depending on the reasons for the examination and the employer policies governing the use of the computers, whatever may be discovered may be admissible in any prosecution if handed over to police. Further, police can use the information provided by the employer to obtain a search warrant.

So the headlines notwithstanding, employees should understand their use of an employer-provided computer should not be considered private.

Consider yourself warned.

(Highlighting added by the Office of the Information and Privacy Commissioner of Ontario for this IPC teachers' guide.)

The Perils of Facebook; Beware of consequences of baring your soul, or other things, online

The Calgary Herald

Mon 09 Feb 2009

Page: A3

Section: News

Byline: Gwendolyn Richards

Source: Calgary Herald

Within the last few weeks, a Calgary employee in the oilfield service industry made a decision to call in sick.

He wasn't.

Instead, he went out, joining friends who shot photos of him and uploaded them to Facebook, a social networking website.

His friends "tagged" him in the pictures, which alerted those in his circle of Facebook contacts to the images that showed he wasn't at home sick after all.

Among those notified was a co-worker forced to do additional work on behalf of the supposedly sick man. That employee, no doubt displeased with having to pick up the extra work, reported the transgression to the boss.

The "sick" staff member was given an official warning that was documented in his human resources file and had to compensate for the missed day.

"There was no hiding from it," said Boyden Global Executive Search's managing director, Robert Travis, who heard about the incident directly from one of his clients.

This should serve as a cautionary tale for anyone who thinks what happens on Facebook, stays on Facebook, he said.

"People need to be aware of their intended and not intended audience with respect to their online persona."

He expects there are more of these stories to come as Facebook continues to grow at an unprecedented rate. As the population of the online community expands, more people are vulnerable to getting caught when they make a misstep.

According to Facebook's statistics, there are more than 150 million people connecting on the site, and the fastest growing demographic is people 30 years and up.

The draw of Facebook has even led some employers – including the Ontario government, British Gas and Telstra, the largest telecommunications company in

Australia – to ban it from the workplace over concerns it affects productivity or disgruntled workers could harm the companies' reputations.

What one expects to be a private place to communicate with friends, to share photos and videos, may actually be the equivalent of putting your personal life up on a billboard.

Rebecca Sullivan discovered others could access her Facebook page – including personal photos – after a student brought it to her attention. It was an innocuous, albeit ironic, oversight on Sullivan's part.

After all, as a pop culture expert who teaches communications and culture at the University of Calgary, Sullivan is keenly aware social networking sites have blurred the line between public and private spheres.

"I assumed the default (on her Facebook page) would be the highest privacy settings," she said with a laugh.

Now that she has clicked the right buttons to ensure her Facebook profile is only viewed by those

Facebook Continued...

she approves, Sullivan said many don't actually realize they have to choose to protect their privacy.

"They're not often readily available and obvious to a novice," she said of the settings.

But it makes sense, considering the platform.

"The Internet does not operate on the principle of privacy, it operates on the principle of publicness," Sullivan said.

Maintaining a line between the two has been a problem since the advent of e-mail. Although a much more private form of communication than Facebook, e-mail is like a postcard: it's not just between sender and recipient.

Sullivan points out there have been cases where employees who used their work e-mail addresses to make inappropriate comments have found themselves without a job.

Social networking sites take it one step further, becoming places where private and public worlds collide – sometimes with disastrous results.

In October, 13 Virgin Atlantic employees were fired for criticizing the airline and some of its passengers on Facebook.

At the time, a spokesman for the airline said the cabin staff took part in a discussion on the social

networking site that "brought the company into disrepute and insulted some of our passengers."

Last spring, a Calgary teacher was reprimanded for posting comments about drug-using mothers on her Facebook page that prompted a complaint from a parent. The Calgary Board of Education deemed the comments offensive, had them removed and disciplined the teacher.

The Alberta Teachers' Association advises against teachers becoming Facebook friends with students, either current or recently under their guidance, while in Vancouver, the board of education has considered banning communication between teachers and students on such sites. More drastically, the teacher's union in Ohio has asked its members to remove their profiles from social networking sites.

"The Internet and social networking sites have added another dimension to an already existing problem of where public and private begin and end online," said Sullivan.

"If you really thought it was private, you're crazy."

The effects of a decision to post a racy photo or damning comment may not be immediately apparent. But once out in the ether, it is almost impossible to delete. "You are technologically incapable of

removing this stuff. Once photos are up there, anyone can download them," said Sullivan.

Steven Rothberg, founder of Internetcareersitecollegerecruiter.com, explains the danger as such: any "friend" has access to information and photos they can easily take and distribute outside Facebook.

"I could get a screen shot, post it to my blog, put your name on it," he said. At that point, there is nothing private about what was once on Facebook.

Such was the case of beauty queen Amy Polumbo, crowned Miss New Jersey last year, who was the subject of a blackmail attempt when someone sent photos – including one showing her boyfriend biting her clothed breast – from her deleted Facebook page to pageant officials.

"This was meant to be private. This was not accessible to the general public," she said during an appearance on NBC's Today show in July 2007.

Rothberg said what a lot of people don't understand is while Facebook is password protected, any information you put up on it can be shared with anyone else and the damage can be far-reaching.

Studies indicate at least 25 per cent of employers admit they use social networking sites to

Facebook Continued...

gather information about potential hires. That figure, in reality, is probably closer to 75 per cent, said Rothberg.

“It’s very hard, especially for young adults, to understand that employers have a need to have employees who have a good sense of judgment,” he said. “We are not Dr. Jekylls and Mr. Hydes; we don’t act one way in our personal lives and a completely different way in our professional lives.”

Rothberg advises job seekers – and those gainfully employed who want to stay that way – to view posting any information online the same as getting a tattoo.

“There’s nothing inherently wrong with it, but you’ve got to live with it. People will see it that you didn’t intend to see it and you didn’t want to see it,” he said.

However, he also cautions employers to take everything in context, saying young adults today are doing the same things the previous generation did.

“The only difference is we didn’t have the ability to snap a photo and upload it. Don’t punish this generation because we gave them the tools to embarrass themselves.”

Facebook is not the first place staff with Boyden Global Executive

Search look when examining candidates, said Travis.

Staff are more concerned about a criminal background or fraudulent reports of education or previous employment than photos of candidates chugging beer. But, Travis said, there are times when they do turn to the social network when looking at candidates.

“If we had any red flags around a person’s personality, ethics, behavioural issues, we would reach out to Facebook see if we could find something.”

What they find may not persuade headhunters to decide someone is a bad candidate, but it does help them learn as much as they can about a potential hire, Travis said. He added most people have locked down their Facebook profiles with privacy settings, making it difficult for search consultants to find anything.

Meanwhile, the province’s teachers’ association has written articles in its newspaper reminding members to be discreet and think twice before posting something to Facebook.

“What we basically say is, don’t put anything there that you wouldn’t want your mother to see on the front page of the Calgary Herald,” said president Frank Bruseker.

“I think it’s prudent to ask yourself, ‘Why am I posting this? Why would I share this with all these people? Do people need to know this?’”

Bruseker has an account, too, but only has about 20 contacts – mostly family. His list is meagre compared to many Facebook users who have added hundreds of “friends.” (The average user has 100 friends, according to Facebook.)

That practice is baffling to Bruseker and Sullivan alike.

It raises the question: are they friends or are they, literally, “virtual” strangers.

It’s something Sullivan said people should consider carefully, not only when someone asks to be a Facebook friend, but when reviewing the list of people already accepted.

“If we want an environment where we can just be ourselves and be private people and make inappropriate comments and tell inappropriate stories, then be careful, be protective of your environment,” she said.

“If you’re not willing to say it out loud at a neighbourhood party or put the photo on a big sign in front of your house, don’t do it online,” she said.

STAYING SAFE ONLINE

PUBLIC INFORMATION POSTER



POSTERS ARE A SIMPLE BUT EFFECTIVE WAY OF PUBLICIZING EVENTS AND COMMUNICATING IMPORTANT MESSAGES TO THE PUBLIC AT LARGE. THEY CAN BE DISPLAYED AT SPECIAL EVENTS AND AT SCHOOL OR IN THE COMMUNITY.

Purpose

- To apply knowledge and concept attainment from unit three in a culminating task;
- To raise the school community's awareness about consumer privacy on the Web.

Task

Your task is to create a **public information poster (PIP)** about an Internet consumer privacy issue. Select from one of the topics below.

Instructions

During this activity, you will work in pairs to research, plan and create a PIP that will address consumer privacy on the Web. In each group, students should consider issues that have been addressed in this unit. You will create and present your poster with a partner.

Steps

1. **Topic Selection.** Choose from one of the topics addressed in the unit:
 - surfing the Web;
 - identity theft;
 - social networking;
 - blogging;
 - your own idea – please obtain approval from teacher.
2. **Research.** Research the risks involved with your topic. You should get the information from a reliable source, such as from books, people working in the field or on reputable Internet sites, including that of the Information and Privacy Commissioner of Ontario (www.ipc.on.ca).
3. **Reference.** Be sure to reference your sources of information in your research notes and on a Reference List submitted with the poster.

4. **Information Selection.** Select the information you will include on the poster. Choose information and/or tips that are effective.
5. **Editing.** Have your information checked by your peer or teacher. Make sure you use correct spelling, punctuation and grammar.
6. **Production.** Decide how you will make your poster. You may draw, use computer graphics, clipart, Photoshop, etc.
7. **Design.** Design an effective and appealing PIP. It is important to make your poster attractive and easy to read.
 - Choose a background colour that will not overwhelm the message;
 - Use appropriate pictures or graphics; and
 - Choose fonts that are easy to read – consider colour and size and be careful not to mix too many different fonts together.
8. **Publication.** Think carefully about where you will put up your posters. Try to find a location where many people will see them, but where they will not get lost in the crowd. The goal is to increase the school community's awareness about the privacy risks involved on the Web.

Assessment

- Teacher observation and feedback;
- Peer editing.

Evaluation

- See the attached Culminating Task Rubric: *Staying Safe Online Public Information Poster (Appendix 3.13)*.

CULMINATING TASK RUBRIC:

STAYING SAFE ONLINE

PUBLIC INFORMATION POSTER

Student(s):

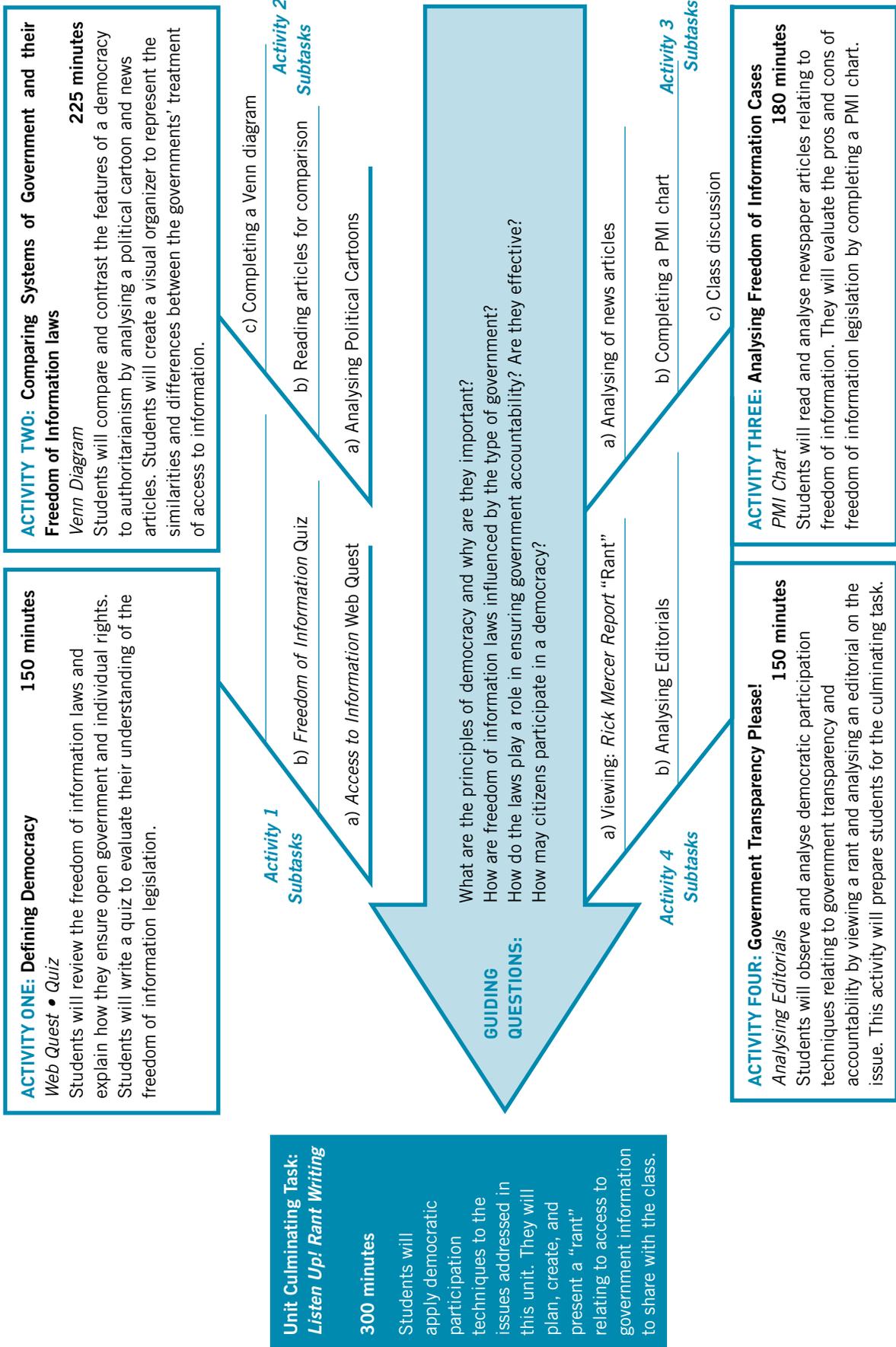
Mark:

/40

Criteria	Level R (0-49%)	Level 1 (50-59%)	Level 2 (60-69%)	Level 3 (70-79%)	Level 4 (80-100%)
KNOWLEDGE AND UNDERSTANDING					
• knowledge of topic	- poster demonstrates inaccurate or insufficient understanding of the topic	- poster demonstrates limited understanding of the topic	- poster demonstrates some understanding of the topic	- poster demonstrates considerable understanding of the topic	- poster demonstrates thorough and accurate understanding of the topic
THINKING AND INQUIRY					
• research	- little or no research present	- research lacks sufficient depth	- research shows limited depth	- research shows adequate depth	- research shows great depth
• supporting details and tips	- inadequate supporting details	- poor supporting details	- limited supporting details	- adequate selection of supporting details	- excellent selection of supporting details
COMMUNICATION					
• language conventions	- uses language conventions with very limited accuracy	- uses language conventions with limited accuracy	- uses language conventions with some accuracy	- uses language conventions with considerable accuracy	- uses language conventions skilfully and correctly
• organization of presentation	- presentation was disorganized, confusing	- presentation was organized in an ineffective manner	- presentation organized in a somewhat effective manner	- presentation organized in an effective manner	- presentation organized in a highly effective manner
APPLICATION					
• design elements	- ineffective use of colour, text, and visuals	- inappropriate or ineffective use of colour, text, and visuals	- colour, text, and visuals were utilized somewhat effectively	- colour, text, and visuals were utilized effectively	- colour, text, and visuals were utilized highly effectively
• reference list	- no sources listed	- uses limited citations with accuracy	- uses some citations with accuracy	- uses citations with considerable accuracy	- uses citations with thorough accuracy

Unit Four - Overview of Unit Activities

“Open Government and Freedom of Information Matters”



UNIT 4

Open Government and Freedom of Information Matters

Time | 1005 minutes

Description and Purpose

The purpose of this unit is two-fold: to deepen students' understanding of freedom of information legislation and its connection to the principles of a democracy, and to allow students to apply some of the features inherent in a democracy – active citizenship and participation. In this unit, students will review the features of a democracy and compare them to other types of government with respect to accessing personal and government information. They will read and analyse a variety of articles and opinion pieces, with a focus on the effectiveness of the legislation in ensuring government accountability and the development and/or support of authors' arguments. They will also demonstrate active citizenship by developing, supporting and presenting their opinions through written and oral communication.

Guiding Questions

What are the principles of democracy and why are they important?

How are freedom of information laws influenced by the type of government?

How do the laws play a role in ensuring government accountability? Are they effective?

How may citizens participate in a democracy?

Prior Knowledge and Skills

- Key Concepts – types of government; rights, freedoms and responsibilities (Grade 10 Civics);
- Think, pair, share instructional strategy;
- Note-taking;
- Computer and Internet research and literacy;
- Discussing and sharing ideas in a class;
- Critical thinking and analysis: comparing and contrasting, logical development of arguments;
- Working with others;
- Stylistic devices such as metaphor, similes, imagery, etc.

Planning Notes/Preparation

- Access to a projector;
- Reserve a computer lab for students (or have students access the website at home);
- Reserve an LCD projector and computer to view *Rick Mercer Report*;
- Access to the Internet for *Rick Mercer Report Rant*
(http://www.youtube.com/watch?v=YlwVo9O6zto&feature=channel_video_title)
- Photocopy appropriate Appendices for students, depending on activities chosen;
- Access to a DVD/video camera to film student “Rant.”

Materials List

- Copies of *Your Right to Access Information* Web Quest (**Appendix 4.1**);
- Copy of Teacher Key: *Your Right to Access Information* Web Quest (**Appendix 4.2**);
- Copies of the *Freedom of Information Quiz* (**Appendix 4.3**);
- Overhead: Answer Key: *Freedom of Information Quiz* (**Appendix 4.4**);
- Copies of *Analysing Political Cartoons: Democracy vs. Dictatorship* (**Appendix 4.5**);
- Copies of *Comparing Access to Information* (**Appendix 4.6**);
- Copies of the *Venn Diagram Activity* (**Appendix 4.7**);
- Copies of *Analysing Access to Information Cases* (**Appendix 4.8**);
- Copies of *Freedom of Information request uncovers diagnostic errors* (**Appendix 4.9**);
- Copies of *Public kept from 20 per cent of Elton John concert tickets* (**Appendix 4.10**);
- Copies of *DineSafe cuts rate of sickness Food-related illness cases have plunged 30% since Star exposed violations in city's eateries* (**Appendix 4.11**);
- Copies of *Daycare parents triumph* (**Appendix 4.12**);
- Copies of *Government Transparency Please!* (**Appendix 4.13**);
- Copies of Culminating Task: *Listen Up! Rant Writing* (**Appendix 4.14**);
- Copies of “*Rant*” *Evaluation Rubric* (**Appendix 4.15**);
- Copies of the *Teacher Anecdotal Recording Sheet* (**See Unit 1, Appendix 1.4**).

TEACHING/LEARNING STRATEGIES

ACTIVITY	MINDS ON	ACTION	CONSOLIDATION AND DEBRIEF
1	<p>Ask students, “What do you know about the term democracy?”</p> <p>“What are the key features of a democracy?”</p> <p>Sample answers might include: political equality; majority rule; minority representation; responsible government; representation by population; decision-making for the common good; the rule of law; and universal human rights, freedoms, and responsibilities.</p>	<p>Next, distribute copies of <i>Your Right to Access Information</i> Web Quest (Appendix 4.1) and explain that in Ontario, the IPC oversees provincial access to information laws. Take students to a computer lab and have them complete the Web Quest to learn about the access to information laws in Ontario.</p>	<p>Take up the answers using Teacher Key: <i>Your Right to Access Information</i> Web Quest (Appendix 4.2).</p> <p>Students take the <i>Freedom of Information</i> Quiz (Appendix 4.3) to evaluate their understanding of the Web Quest. Teachers may use the <i>Answer Key: Freedom of Information</i> Quiz (Appendix 4.4) to take up the answers with students and clarify any questions they may have.</p>
2	<p>Ask students, “What are some ways you can show dissatisfaction with the government of the day?” (E.g. protesting, petitioning, sit-ins, political/editorial cartoons, writing letters to members of government, letters to the editor among others, joining Facebook groups.)</p> <p>“How are editorial or political cartoons a method of democratic participation?”</p> <p>“How are they different from other forms of democratic participation?”</p>	<p>Distribute the handout <i>Analysing Political Cartoons: Democracy vs. Dictatorship</i> (Appendix 4.5) for students to work with a partner to complete.</p>	<p>Take up the answers with students.</p> <p>Review the main features of a democracy (see Activity 1) and review the features of a dictatorship, namely that power is in the hands of one individual, usually with the power of the military. Nazi Germany would be a good example of this as it was characterized by strong militarism, secret police, power in the hands of one man (or here the eye can represent the Nazi Secret police).</p>
	<p>Ask students, “How might access to information differ in a communist or a fascist regime?”</p> <p>“What might be the impact of a lack of access to information?”</p>	<p>Distribute to students <i>Comparing Access to Information</i> (Appendix 4.6) and the <i>Venn Diagram</i> (Appendix 4.7). After reading the two articles, <i>Ottawa Bans Chemical Used in Soft Vinyl Toys; Voluntary Plan Failed and Chernobyl: Once and Future Shock</i>, students complete the Venn diagram. Teacher may assess the Venn diagram for critical thinking.</p>	<p>Ask students, “What correlation exists between an individual’s right-to-know and the type of government based on the articles?”</p> <p>“What impact can access of information laws have on society?”</p>

ACTIVITY	MINDS ON	ACTION	CONSOLIDATION AND DEBRIEF
3	Ask students, “ <i>What problems can they foresee with the power of access to information laws?</i> ” “ <i>Why might there be a problem?</i> ”	Divide students into groups of four. Distribute <i>Analysing Access to Information Cases (Appendix 4.8)</i> to each group. Provide each group member with a different access to information article (Appendices 4.9 – 4.12). Students will read their article and complete the questions individually. Then, groups will share the issue raised in the article and complete the <i>PMI</i> chart as a group (Appendix 4.8).	Ask students: “ <i>What are some conclusions that can be made about the access to information legislation in Canada?</i> ” “ <i>How effective are the laws?</i> ” “ <i>What concerns with the freedom of information legislation have been raised in the articles?</i> ” “ <i>How might the legislation change in the future to promote the common good?</i> ”
4	Access the Internet to show students Rick’s Rant on Government Transparency from Season Six, January 27, 2009 (http://www.youtube.com/watch?v=YlwVo9O6zto&feature=channel_video_title) Ask students to consider, “ <i>What is the opinion that Rick presents in the last few moments of his rant?</i> ” “ <i>What arguments does he use to support that opinion and are they effective?</i> ” And, “ <i>What techniques does he use to convey his opinion?</i> ” “ <i>What protects Canadians from government secrecy?</i> ”	Students will read an editorial piece about government transparency and answer questions to analyse the issue and the stylistic techniques of the editorial. (Appendix 4.13)	Take up the answers to the questions. Ask students “ <i>Compare how the rant and the editorial present and develop an opinion.</i> ” “ <i>Which of the two pieces was more effective and why?</i> ”
Unit Culminating Task	Refer to the “Rant” from Appendix 4.13 to analyse the elements of a “rant.” Distribute to and read with students the <i>Culminating Task: “Listen Up!” Rant Writing (Appendix 4.14)</i> .	Students will plan, develop, and create a Rick Mercer-style “Rant” on access to government information. Students will present their rants to their classmates.	Evaluate student rants using the “ <i>Rant</i> ” <i>Evaluation Rubric (Appendix 4.15)</i> .

Assessment and Evaluation of Student Learning

- assess students' note-taking and understanding of the website;
- evaluate students' knowledge and understanding of freedom of information laws with the *Freedom of Information Quiz*;
- assess students' critical thinking and analysis skills with the Venn Diagram;
- using the *Teacher Anecdotal Recording Sheet*, assess students' ability to work in a group and contribute to class discussion (**Unit 1, Appendix 1.4**).

Professional Resources

"Government Transparency Please." Rick Mercer Report. Season Six. Episode: 27 Jan. 2009.

http://www.youtube.com/watch?v=YlwVo9O6zto&feature=channel_video_title

Information and Privacy Commissioner/Ontario Website:

<http://www.ipc.on.ca/english/Home-Page/>

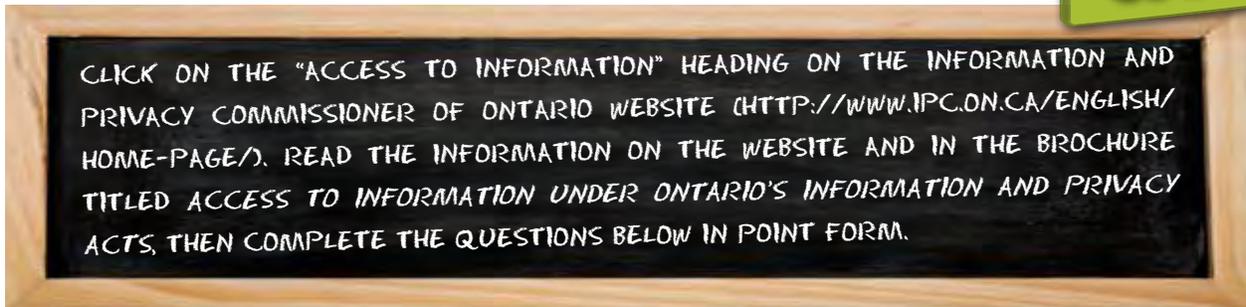
Access to Information under Ontario's Information and Privacy Acts brochure

ACTIVITY 1:

YOUR RIGHT TO ACCESS INFORMATION



Student: _____



1. Which two *Acts* give you the right to request access to government-held information in Ontario?

a

b

2. To which government organizations does the provincial *Act* apply? The municipal *Act*?

PROVINCIAL ACT	MUNICIPAL ACT
•	•
	•
•	•
	•
•	•
	•
•	•
	•
	•

3. What is the *Directory of Institutions* and where can it be accessed?

4. What kind of information may I request? What kind of information can I not obtain through these *Acts*?



Source: Turner, Morrie. "Wee Pals: Freedom of Information Act." 7 Jan. 2009 <gocomics.com>

5. How do I find out what records provincial and local government organizations have?
6. How do I request the information I want?
7. If that does not work, what do I do then?
8. To whom must the request form or written letter be forwarded?
9. What are the costs involved in submitting a request form or letter?
10. How long must I wait for a response to my request?
11. When might an exemption apply to the request for information?
12. What if the government organization denies me access to information requested under the provincial or municipal *Acts*? What then?

ACTIVITY 1 - TEACHER KEY: YOUR RIGHT TO ACCESS INFORMATION WEB QUEST

1. Which two *Acts* give you the right to request access to government-held information?
 - a. Ontario's *Freedom of Information and Protection of Privacy Act* (the provincial *Act*)
 - b. *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act*)
2. To which government organizations does the provincial *Act* apply? The municipal *Act*?

PROVINCIAL <i>ACT</i> – PROVINCIAL GOVERNMENT ORGANIZATIONS	MUNICIPAL <i>ACT</i> – LOCAL GOVERNMENT ORGANIZATIONS
• all provincial ministries and most provincial agencies;	• municipalities;
• many boards and commissions;	• police services boards;
• colleges of applied arts and technology;	• public library boards;
• universities;	• school boards;
• (and hospitals, as of Jan. 1, 2012).	• conservation authorities;
	• boards of health;
	• transit commissions;
	• certain municipal electricity corporations;
	• certain local housing corporations.

3. What is the *Directory of Institutions* and where can it be accessed?
 - It lists all of the government organizations covered by the Acts and can be accessed directly from www.mgs.gov.on.ca/en/infoaccessandprivacy.
4. What kind of information may I request? What kind of information may I not obtain through these *Acts*?
 - The *Acts* give everyone a general right of access to general records held by government organizations. The information may be recorded in printed form, on film, by electronic means or otherwise, and it includes such things as photographs and maps. You also have the right to request access to, and correction of, your personal information held by government organizations.
 - You cannot use FOI to request information held by **private** companies such as Royal Bank, Sears, Imperial Oil, etc.
5. How do I find out what records provincial and local government organizations have?
 - First, determine whether the information is held by a provincial or local government organization by referring to the online *Directory of Records*.
6. How do I request the information I want?
 - Call the appropriate government organization to see if the information is available over the counter.
7. If that does not work, what do I do then?
 - You can make a written freedom of information request by completing a request form (a generic form is available on the IPC's website). Alternatively you may write a letter stating that you are requesting information under (list which of the two *Acts* you are using).

8. To whom must the request form or written letter be forwarded?
 - Forward the request to the Freedom of Information and Privacy Co-ordinator at the government organization most likely to have the information you are looking for.
9. What are the costs involved in submitting a request form or letter?
 - You **must** submit a \$5 cheque with your request, and you may be charged for photocopying, shipping costs, the costs of searching for the records you have requested and/or preparing them for disclosure, or any other costs incurred in responding to the request. (The **average** fee for general requests to provincial organizations in 2010 was \$39.97; at the municipal level, \$25.68).
10. How long must I wait for a response to my request?
 - Usually a response will be received within 30 days of the government organization receiving the request.
11. When might an exemption apply to my request for information?
 - For example, you **cannot** obtain another person's personal information through an FOI request. (Business information is not personal information.) Nor can you obtain cabinet records.
12. What if the government organization denies me access to information I requested under the provincial or municipal *Acts*? What then?
 - It must give you written notice of its decision – including citing the specific exemption or exemptions it is basing its decision on – and inform you of your right to appeal the decision to the Information and Privacy Commissioner.

ACTIVITY 1:

FREEDOM OF INFORMATION QUIZ

Circle the correct answer.

- (1) Which of the following local government organizations does Ontario's *Municipal Freedom of Information and Protection of Privacy Act* apply to?
- Municipalities;
 - Police services;
 - School boards;
 - All of the above.
- (2) In practical terms, that *Act* provides Ontarians with the right to access to:
- Most of the information held by local government organizations, with specific and limited exemptions;
 - About 50 per cent of the information held by local government organizations;
 - About 25 per cent of such information;
 - About 25 per cent of paper records held by local government.
- (3) A discretionary exemption that could be claimed to exclude some records from being accessed (depending on the circumstances) is:
- Solicitor-client privilege;
 - Law enforcement;
 - Information about inter-government relations, if the information was received in confidence;
 - All of the above.
- (4) A freedom of information request sent to a municipality should be addressed to:
- The mayor;
 - The treasurer;
 - The freedom of information co-ordinator;
 - None of the above.
- (5) Which of the following provincial organizations does Ontario's *Freedom of Information and Protection of Privacy Act* apply to?
- Ministries;
 - Most provincial agencies;
 - Children's Aid Societies;
 - Both (a) and (b).
- (6) Can either *Act* be used to request information held by private sector organizations?
- Yes;
 - No;
 - Only in very specific cases.
 - None of the above.
- (7) What is the initial fee that must accompany a freedom of information request?
- \$5;
 - \$25;
 - \$50;
 - \$100.
- (8) Under both *Acts*, a government organization is required (with limited exceptions) to respond to an FOI request within how many days after receiving the request and the fee?
- 15 days;
 - 30 days;
 - 60 days;
 - 100 days.
- (9) If a provincial or local government organization denies a requester access to the information he or she is seeking, which of the following can the requester file an appeal to:
- The Ministry of Municipal Affairs and Housing;
 - The Ombudsman;
 - The Information and Privacy Commissioner of Ontario;
 - The Premier.
- (10) Does the organization that a requester can appeal a government office's access decision to have the authority to order the government organization to release the records sought by the requester?
- Yes.
 - No.
 - All of the above.
 - None of the above.

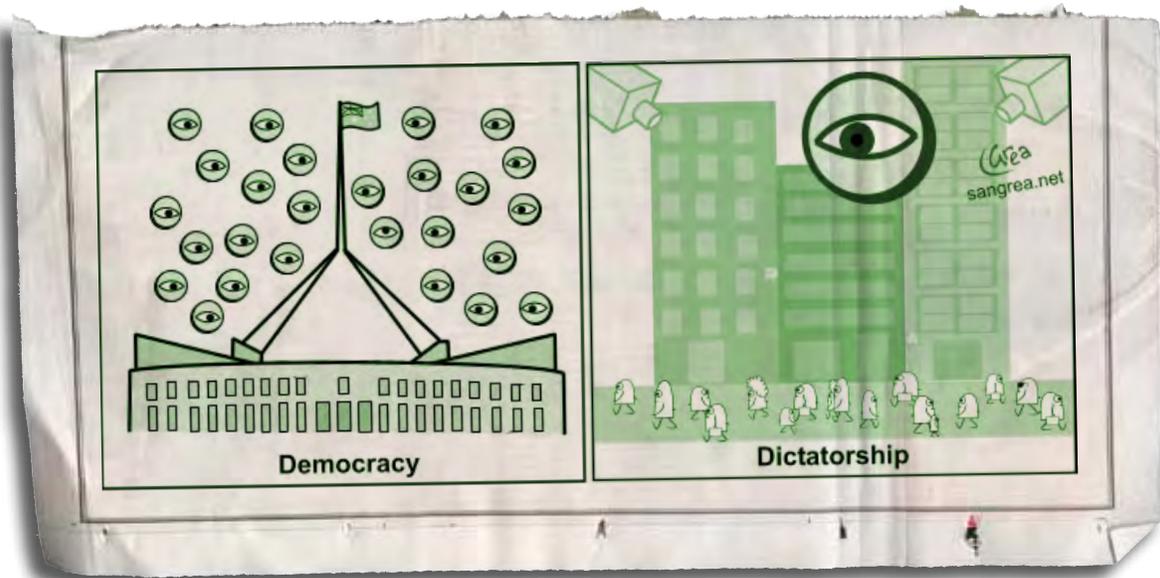
Source: Information and Privacy Commissioner/Ontario – www.ipc.on.ca

ACTIVITY 1: ANSWER KEY: FREEDOM OF INFORMATION QUIZ

- (1) (d) All of the above;
- (2) (a) Most of the information held by local government organizations, with limited exceptions;
- (3) (d) All of the above; (Such a decision, however, could be appealed to the Information and Privacy Commissioner.)
- (4) (c) Freedom of information co-ordinator;
- (5) (d) Both (a) and (b);
- (6) (b) No;
- (7) (a) \$5 fee;
- (8) (b) 30 days;
- (9) (c) Information and Privacy Commissioner of Ontario;
- (10) (a) Yes. If the Commissioner upholds the appeal, she has the authority under the Acts to order a government organization to release records requested under FOI.

ACTIVITY 2:

ANALYSING POLITICAL CARTOONS: Democracy vs. Dictatorship



Complete the following questions for the political cartoon above.

Step 1: Interpreting the Cartoon

1. What is the title and/or caption of the cartoon? Is it an ironic or sarcastic title? Explain.

2. Describe the objects, symbols, people, or characters in the cartoon. What is their mood?

3. To what issue, event or theme is the cartoon related?

Step 2: Evaluating the Cartoon

4. What is the cartoonist's view of the issue, event or theme? Is it biased for or against issue? Is it a positive or negative view? Explain.

5. What message is the cartoonist trying to convey about the role of the people and/or government?

6. Determine if the cartoonist's message is effective? Explain your answer.

7. According the cartoon, what is the key difference between a democracy and a dictatorship with respect to open government and individual rights?

ACTIVITY 2:

COMPARING ACCESS TO INFORMATION

Read the **two** articles, *Ottawa Bans Chemical Used in Soft Vinyl Toys; Voluntary Plan Failed*, and *Chernobyl: Once and Future Shock*. As you are reading, pay attention to the freedom of information laws in each society.

OTTAWA BANS CHEMICAL USED IN SOFT VINYL TOYS; VOLUNTARY PLAN FAILED

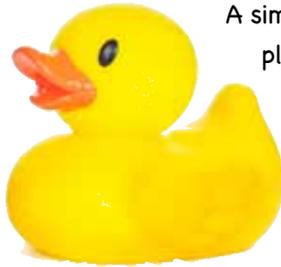
Sarah Schmidt
CanWest News Service
June 20, 2009

OTTAWA - Conceding that a decade-old voluntary ban on hormone-disrupting chemicals in children's toys has not worked, Health Canada yesterday announced new regulations requiring companies to get phthalates out of soft vinyl toys.

The proposed ban will prevent the use of six phthalates in bath toys, teething rings, rattles and other children's products, such as vinyl bibs. The chemical additive, used to soften toys, can cause reproductive problems.

Health Canada is taking the step after its own market survey last year found the widespread presence of phthalates in soft plastic toys and other items for young children that are likely to be mouthed, such as rubber ducks.

The results, released to CanWest News Service under **access to information laws**, found elevated levels of phthalates ranging from 0.2 to 39.9% by weight of the plastic known as polyvinyl chloride in three-quarters of the items - 54 of 72 of the children's products tested.



A similar phthalates ban has been in place in the European Union since 1999, where concentration levels cannot exceed 0.1% in children's products. A ban in the United States came into effect last year.

The new regulations will also effectively ban lead in children's products by proposing a maximum of 90 milligrams of lead per kilogram of product, or 90 mg/kg. The current lead limit for toys intended for children under three years old is 600 mg/kg total lead.

The government won praise from nearly all corners yesterday.

"This is great news for parents," said Aaron Freeman, policy director for Environmental Defence, which has been lobbying for a ban for years.

Judy Wasylycia-Leis, health critic for the New Democrats, first raised the issue back in 1997 when she was first elected.

"It's good news. Finally, the government has acted. It's been a long, hard struggle. I think the science has been in for a long time."

- Published in the National Post, June 20, 2009

CHERNOBYL: ONCE AND FUTURE SHOCK

ON APRIL 26, 1986, THERE WAS A MAJOR ACCIDENT AT THE CHERNOBYL NUCLEAR POWER STATION, LOCATED IN UKRAINE ... SOUTH OF THE BORDER OF BELARUS. AT THAT TIME, BELARUS AND THE UKRAINE WERE PART OF THE SOVIET UNION (THE UNITED SOVIET STATES OF RUSSIA - U.S.S.R.). THE ACCIDENT RESULTED IN THE RELEASE OF LARGE QUANTITIES OF RADIOACTIVE SUBSTANCES INTO THE ATMOSPHERE AND HAD DEVASTATING EFFECTS ON THE POPULATION, LIVESTOCK AND THE ENVIRONMENT.

A liquidator's story

This article was first published in Index 1/9 by Index on Censorship (www.indexoncensorship.org), which granted permission for it to be reprinted.

For the first time in print, a Belarusian scientist gives his personal recollections of the secrecy that, in the crucial period immediately following the Chernobyl accident, left the unsuspecting public exposed to fallout.

On the Monday morning, 28 April, at the Nuclear Energy Institute of the Belarusian Academy of Sciences, I switched on the apparatus – the gamma-spectrometer and the dosimeters: everything was (in physicists' slang) 'hot,' which meant that there had been a big nuclear accident on the Institute's premises: our dosimetrist ran out of the laboratory, and reported that the level in the yard was about 300 microroentgens an hour. Then he was summoned by telephone to monitor the radiation contamination round the nuclear reactor of the Institute of Radioactive Technology; so that was the main source of the accident! But they had their own dosimetrists there, and the dose level was almost the same; the same was true in the vicinity of a third nuclear device... Moreover, it was clear that the radiation levels fell the further one went inside the building... When the head of the dosimetry service, A Lineva, telephoned the Central Public Health Station of Minsk, they said, 'This is not your accident.'

We looked at the tall smoke-stack, and then at the map of Europe, and we saw that the wind was blowing radiation towards Sweden. In fact, we learned later, on 1 May the level of



radioactive contamination in Stockholm was 17 Curies per square kilometre from Caesium-137, and 87 Curies per square kilometre from Iodine-131.

But in our place, they brought me in a twig from the yard, and I observed that it was emitting radiation...the gamma-spectrometer showed Iodine-11 and other 'young' radionuclides... Later we tested soil and trees from many regions of Belarus, and the Institute started to measure the specific activity of foodstuffs arriving for the Institute canteen and the crèche.

Meanwhile, the dosimetry service headed by M V Bulyha was monitoring the radiation cloud hanging above Minsk.

We started to ring our relatives and friends in Minsk, advising them about safety measures. But this did not last long: at around midday, our telephones were cut off. And a couple of days later, we specialists were called into the Secrecy Department, and made to sign a

29-point document forbidding us to divulge secrets connected with the accident at the Chernobyl-plant. These included the structure of the RDMK-1000 reactor, the amount of uranium, etc, 'secrets' that had already been published in scientific literature.

And meanwhile out in the street, radioactive rain was falling...

We went home from work without looking from side to side; it was painful to see how the children were playing in the radioactive sand, and eating ices.

In our street, I went up to a street vendor and told her to stop selling her sausages, as radioactive rain was falling. But she just said: 'be off, you drunkard! If there'd been an accident, they'd have announced it on radio and TV.' A naive soul, she believed in the righteousness of the Soviet authorities.

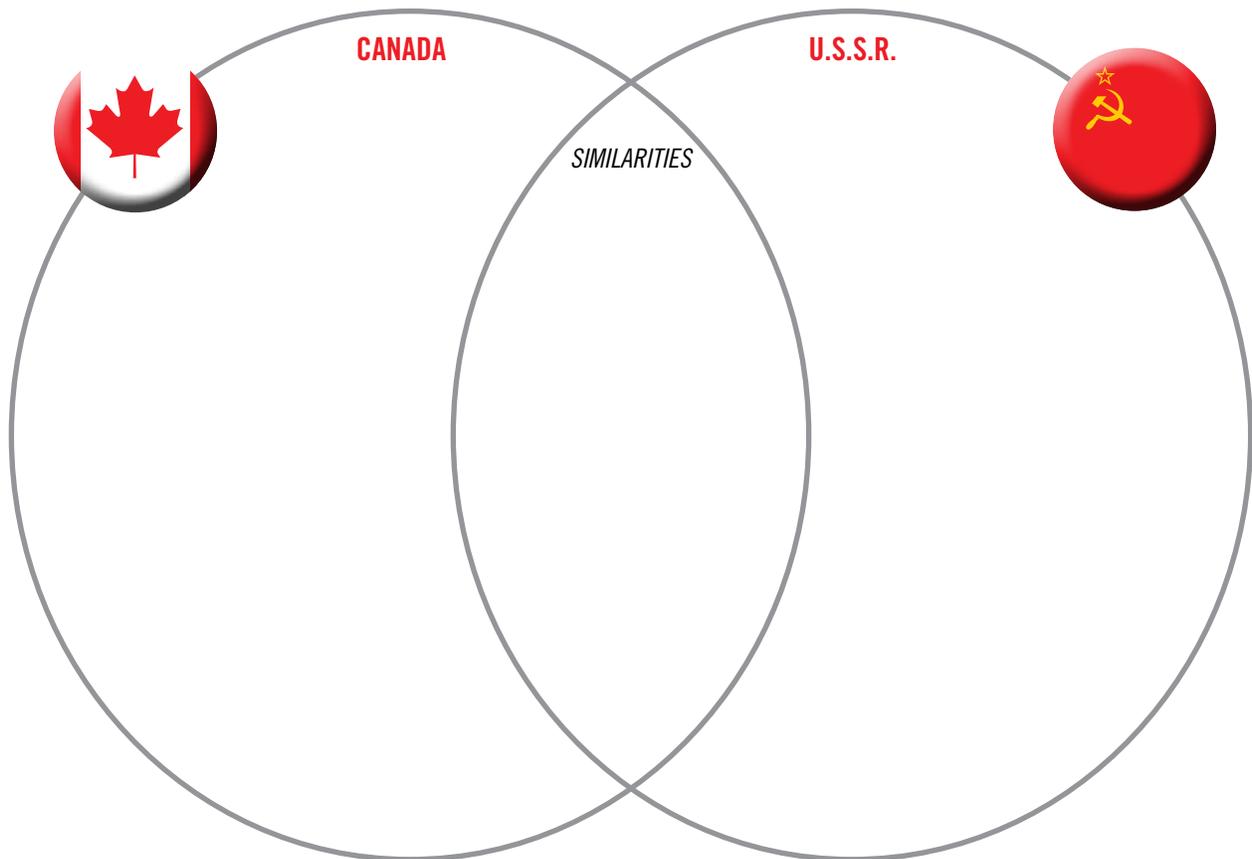
In the evening, on Central TV, Moscow showed us how tractors with great swirls of dust behind them were tilling the soil down in Naroula country, part of which lies in the 30-kilometre zone around the Chernobyl station. Then, on 1 May, as always, children and adults marched in columns through the streets without even guessing at the consequences. So now, today, in Belarus we have some 400 children with thyroid cancer...who at that time knew nothing about Iodine-131...

Mikhail Byckau is a nuclear physicist, who from mid-May 1986 until his retirement from the International Sakharov Institute of Radioecology in April 1995, played an active role in the 'liquidation' (clean-up) and monitoring programmes in the contaminated area.

ACTIVITY 2:

VENN DIAGRAM

Based on the information provided in the two articles, complete the Venn Diagram below to compare the access to information in Canada and the former U.S.S.R. Consider the following points of comparison: type of information known, commitment to open government, consequences of government action.



ACTIVITY 3:

ANALYSING ACCESS TO INFORMATION CASES

A. Individually, answer the questions below using the article provided by your teacher.

Summarize the main idea of the article. Provide some examples from the article.

If a freedom of information law didn't exist, which facts and/or evidence would not be known? What would/might have been the impact?

In your opinion, how effectively was the freedom of information law applied to the issue? Explain.

- B. In your group, complete the PMI chart provided by your teacher to outline the Plusses, Minuses, and Implications of the access to information laws in each of the articles.

PMI

Plusses, Minuses, and Implications

Student(s): _____

+	-	I

Freedom of Information request uncovers diagnostic errors

Sun 30 Nov 2008
BY JEN SKERRITT
The Canadian Press

WINNIPEG – Documents obtained by the Winnipeg Free Press show one Manitobawoman's mastectomy may have been unnecessary and several other patients received incomplete diagnoses after their biopsies went missing.

The incidents occurred months before pathology officials said diagnostic errors were "extremely unlikely."

Documents obtained through a Freedom of Information request reveal that health officials launched seven critical incident investigations into diagnostic errors between July 2007 and March 2008, including the probe into errors made by a veteran St. Boniface Hospital pathologist.

Critical incidents are defined as serious, unintended events suffered by a patient in a health care facility, and are investigated by an internal review committee.

In March, Diagnostic Services Manitoba CEO Jim Dalton denied there were any problems with the province's pathology program and told the Free Press that diagnostic errors or botched tests were "extremely unlikely."

Documents refute that and show that multiple investigations into pathology errors were under way at the time.

In two separate incidents in July and November 2007, groups of samples and specimens were lost which prompted exhaustive searches of a pathology lab and various other health facilities.

As a result, several patients did not receive a complete diagnosis and others had to be retested.

Several other patients had to have a second biopsy after a piece of lab equipment malfunctioned in September 2007. Some patients did not receive a complete evaluation as a result.

A mistake interpreting a breast tumour sample in July 2007 led to one woman being misdiagnosed with aggressive breast cancer.

Subsequent reviews of the woman's case by an Ontario laboratory and second pathologist found there was "no evidence of invasive cancer" and that the woman's mastectomy may have been unneeded.

The woman isn't identified in the documents because of privacy concerns, but documents say the case will be reviewed by her physician.

Another patient did not receive appropriate antibiotics after a follow-up pathology report wasn't sent to that patient's physician last February. The mistake led to an extended hospital stay.

"If we found through one of these investigations that we thought there was an unusual event or unusual risk, we would make it public," Dalton said last week. "But certainly the rate of these incidents is well within the norm I'd put that up against any laboratory in North America."

Dalton said the pathology program is in excellent shape and that these incidents involve a small number of specimens out of the millions that are processed each year.

Dalton couldn't say how many patients may have received an incomplete diagnosis due to lost specimens, but said human error was responsible in the case of the woman who had a mastectomy.

"No errors are good, and we're not trying to gloss these over and say they're OK," he said. "Most reports are timely, accurate, and I think the system works very well and people should have confidence in it."

PUBLIC KEPT FROM 20 PER CENT OF ELTON JOHN CONCERT TICKETS

The Sault Star

Sat Jun 27 2009

Page: A4

Section: News

Byline: DENIS ST. PIERRE, SUN MEDIA;

Nearly 20 per cent of tickets to the now-infamous Elton John concert in Sudbury last year were not available for sale to the public. The information, which the City of Greater Sudbury unsuccessfully tried to suppress, was released Thursday – more than 15 months after the concert was held.

The city spent tens of thousands of dollars in its efforts to withhold the ticket information, which had been requested by The Sudbury Star. After a lengthy process launched by The Star, Ontario's freedom of information commissioner ordered the city to publicly release the information this month.

Despite the ruling that it had wrongly withheld public information--and the huge expense of taxpayers' money in its failed attempt--the city issued a news release Thursday claiming to have achieved victory.

According to the law, a municipality has to pass a three-pronged legal test in order to keep such information private. If the municipality does not pass all three parts of the legal test, it must release the information.

In this case, the province's freedom of information commissioner ruled the city's refusal to release the ticket information did not pass the legal test.

The city's position met two of the required criteria, but failed categorically to meet the third condition. As a result, the city was wrong to withhold the information from the public.

The city's version of the ruling comes across differently. "The city won two of three arguments," the municipality stated in its news release, without specifying it ultimately "lost" the legal test.

The information the city was forced to release shows 1,227 tickets out of a total of 6,386 – just under 20 per cent – were withheld from public sale prior to the Elton John concert of March 2008.

DineSafe cuts rate of sickness; Food-related illness cases have plunged 30% since Star exposed violations in city's eateries

The Toronto Star
 Fri 17 Apr 2009
 Page: GT01
 Byline: Robert Cribb
 Source: Toronto Star

Cases of food-borne illness began to fall almost immediately after Toronto began making restaurant inspection results public in 2001.

Now, eight years after the city launched the DineSafe program that publishes inspection results online and in restaurant windows, cases of individual food-borne illnesses in Toronto have dropped 30 per cent, says a Toronto Public Health report.

It is the clearest evidence yet of the public health benefits of transparency, says John Filion, chair of the city's board of health.

"This is the first time I've seen that food-borne illness took a dramatic plunge after we introduced DineSafe. That shows the public not only has a right to know the results of inspection, but that the public benefits from it. It's just good public policy because it provokes a much higher standard



among the establishments that you're inspecting."

DineSafe was the result of the Star's "Dirty Dining" investigation in 2000 (based on freedom of information requests), which found hundreds of city restaurants had serious food safety violations, from repeated cockroach and mice infestations to food temperature violations that produce bacteria and filthy food preparation surfaces. Yet none of the suspect eateries had been shut down and only a handful had been fined a few hundred dollars.

Worse still, details of those

violations were hidden from the public.

Prompted by the stories and public outrage, then-mayor Mel Lastman ordered an inspection blitz of downtown eateries. Within days, city inspectors had logged hundreds of violations and failed the majority of restaurants they visited.

After a heated political debate that lasted a year, the city adopted a far-reaching disclosure system that posts green, yellow or red signs at the entrance to every restaurant in the city noting the results of its last two inspections.

DineSafe Continued...

More detailed information on every eatery is available on the city's website.

The Toronto Public Health report, to be released today, says DineSafe "resulted in a dramatic increase in compliance with food safety regulations among Toronto's food establishments."

"I do feel it's reasonable to suggest that the DineSafe program in Toronto, which occurred at the same time as we saw a decrease in food-borne illness and an

improvement in food safety compliance, played a role," said Dr. David McKeown, Toronto's medical officer of health.

Prior to DineSafe, compliance with food safety regulations in Toronto restaurants sat at 42 per cent, Filion said.

Today, compliance is more than 90 per cent.

"Clearly, the public benefits of rigorous inspection standards and full disclosure of inspection results were proven in Toronto."

Other cities across Ontario and Canada have adopted similar disclosure models following Toronto's lead. But there remain no mandatory province-wide disclosure rules for local public health units.

"I really can't understand why there hasn't been," Filion said.

"There should be similar standards and the standards should be the ones that best protect the public."

MANY CASES BUT FEW OFFICIALLY RECORDED

1 in 6: people suffer food-borne illness, but fewer than one per cent of cases are officially recorded.

437,093: estimated cases of food-related illness occur annually in Toronto.

102,717: people with symptoms of gastrointestinal illness seek medical care.

26,706: physicians request stool samples from patients.

21,365: patients submit stool samples for testing.

20,297: stool samples are tested by laboratories.

2,395: laboratory-confirmed cases of a provincially reportable disease.

1,928: cases of illness attributable to food reported to Toronto Public Health annually.

Source: Toronto Public Health



Less than 24 hours after “disturbing” Star probe, minister promises new website with reports on individual daycares

Daycare parents triumph

By Dale Brazao, Robert Cribb
and Kerry Gillespie

Toronto Star

May 29, 2007

The wall of secrecy surrounding abuses in daycares has tumbled less than 24 hours after a Star investigation documented troubling problems in centres across Ontario.

Parents concerned about the quality of care their children are receiving in licensed centres will soon be able to visit a ministry website listing serious incidents and inspection findings.

Mary Anne Chambers, Minister of Children and Youth Services, said yesterday her ministry will

launch the website by the fall. Chambers is also considering a stronger colour-coding system in which a red licence posted at a daycare would indicate a serious problem.

Findings of the Star probe included incidents of children being physically assaulted, left to wander away in public places, fed allergy-triggering foods that nearly killed them and being forced to play in filthy surroundings. The Star found numerous cases where daycares with these problems were allowed to remain open, sometimes for years.

The cases were drawn from provincial and municipal records

of inspections, enforcement, complaints and serious incidents, obtained through a series of requests under the *Freedom of Information Act* that took two years.

Chambers called the revelations “disturbing.”

“What I read in the Toronto Star (yesterday) is unacceptable,” she said. “I think parents deserve to be able to access information that relates to their child’s care.”

The proposed website will contain a “more robust form of reporting,” including details on why a centre has a provisional licence – a tool used by the ministry to allow daycares with

Daycare Continued...

substandard conditions to remain open.

There are 57 daycares in the province operating under a provisional licence. White licences mean there are no problems, yellow licences are provisional. Chambers said she favours a stronger colour-coding system, similar to the well-known restaurant rating system. "When you walk up to a restaurant door you see a red label on that door and you know there's a problem. We can do that," Chambers said.

In the wake of the Star investigation, parents across the GTA flooded the newspaper with phone calls and emails with a clear message for the Ontario government: When it comes to children's safety and well-being, there should be no secrecy.

If daycares are dangerous, dirty or allow children to wander off unattended, parents should know about it, they said.

"It's a no-brainer," said Andrew Stalony, who recently entrusted care of his 15-month-old son, Ryan, to a daycare in Mississauga. "There is no question we should have the right to know what's going on. You're letting someone else take care of your child."

During Question Period at the provincial legislature yesterday, Chambers was attacked by both opposition parties for hiding

the problems at daycares. "The minister and her government made efforts to keep this information under wraps for two years," Progressive Conservative Leader John Tory said, referring to the length of time it took the Star to get the information.

Chambers denied this, noting that daycares with provisional licences are required to hand out a government pamphlet titled *Attention Parents. This centre does not meet all the requirements of the Day Nurseries Act.*

She also said the province has hired more inspectors and now conducts unannounced reviews of daycares as well as the annual inspections. The changes protect children better, she said.

The minister said she also favours posting the data collected by the ministry on serious occurrences at daycares – ranging from children who were temporarily missing to abuse allegations, which daycares must report to the ministry.

"I agree the serious occurrences should be there. I really do want to take a look at our ability to report any kind of serious occurrence. One of the things we have to be cognizant (of) is volume of data and ability to manage 4,000 pieces of data online."

The Toronto Star investigation, based on thousands of daycare

incidents, inspection reports and complaints, uncovered serious problems including children wandering off unattended, being forcibly confined in closets and storage rooms, and being served meals prepared in mice-infested kitchens. There were 5,814 serious occurrences reported by licensed daycares across Ontario in 2005-2006, including nearly 3,000 injuries, 674 missing children reports and 675 allegations of abuse or mistreatment, according to data analysed by the Star.

One parent who contacted the Star had tried on her own to obtain similar information. Karen Krawec said she eventually gave up in frustration after trying to get information on daycare centres in York Region to help her decide whom to entrust with the care of her young son.

"I was first told that I would not be able to access the information," Krawec said. "Later on when I quoted the *Freedom of Information Act*, I was advised that it would be a lot of work to dig up all of the records so I would have to pay the hourly wage.

"They said it would cost hundred of dollars and (take) several months," Krawec said. "After consulting my MP, who did nothing for me, I finally gave up."

Daycare Continued...

Lisa MacLeod, Tory MPP for Nepean-Carleton and her party's critic on children and youth, said there has to be absolute transparency for government-run daycares. "If we're going to be doing this for restaurants, we should be doing it for daycares," she says. "We are dealing with the physical safety and emotional well-being of our children."

Under the province's Day Nurseries Act, daycares are required to post their licence inside the daycare, where parents can see it. Provisional licences must also be posted, allowing parents to see issues in which the daycare is failing to meet minimum provincial standards.

But posting licences isn't nearly enough, say parents.

Carrie Makins has been shopping for a daycare for her two children without much information to work with, she says. "The only way of sourcing daycare is by my gut feel and word of mouth.

Really, there is no information and no transparency for parents and that's unfair, because they're taking care of our kids for 40 hours a week and that's a huge influence on their life.

"You're paying these people to take care of the most precious people in your life; you need to make sure they're in good hands."

"The state of daycare in this country is appalling both in terms of the space available and the unhealthy conditions presented," said Deborah Wilson, whose daughter is in a downtown daycare.

"To think that a daycare facility can continue to operate on a provisional licence is devastating to me. I truly hope that this article will reinforce to our government that decisive action needs to be taken to improve daycare in this country."

Julie Wallis, whose two grandsons are cared for in a Toronto daycare,

says Canadians are "burying their heads in the sand" on the daycare issue. "A website put forward by the provincial government is needed."

Transparency would force daycares to be more vigilant about maintaining standards, says Teresa Wong, who has a 4-year-old in daycare. "It would also make them clean up their act if they knew somebody was watching," she said.

"People forget this is a service industry and the client is the child," said Anne Eisenberg. "That's the problem, the focus isn't on the child. We lost that a long time ago.

"It's a money issue."

Daniela Fiacco, who operates the Columbus Children's Centre, says she supports parents' requests for information. "Our records are there. If parents want to see them, we let parents look at them. We have nothing to hide."

ACTIVITY 4:

GOVERNMENT TRANSPARENCY PLEASE!



A. ANALYSING EDITORIALS

What is an editorial?

- The editorial serves as the official view of the newspaper, after editors consider many sides of an issue. It is usually the opinion of the newspaper's editorial board.

Content

- deals with a current issue that is affecting people;
- may attempt to influence, by giving readers all of the facts and concerns;
- offers suggestions and indications as to outcomes;
- at major newspapers, the opinion, if offered, will not be an extreme view, it will usually be well prepared and informed, taking into consideration many aspects from both sides of the debate.

Construction

- official view of the paper, so it is wisely thought out;
- clear and concise wording; usually free of emotive terms;
- usually balanced, presenting all aspects of the situation/event/issue;
- written on an important topic, often a deep-seated problem, one that is likely to be of interest or concern to many readers;
- does not normally include reported speech.

Source: Revised by IPC from original posted at <http://www.ohassta.org/resources/politics.htm>

B. SHINING A LIGHT ON THE PMO

The issue of government accountability and transparency is a hot political issue. Examine a recent editorial below and answer the questions that follow to analyse the author's message and style.

The Hamilton Spectator

By: Lee Prokaska

Robert Marleau should indeed release his dogs into the Privy Council Office.

The federal information commissioner, who is about to retire, is threatening to seize documents from the Privy Council Office, which supports the Prime Minister's Office and cabinet. Marleau is unable to proceed with 150 access-to-information complaints because he can't get the information he needs to do so.

He could seize the files he needs as early as this week. And what a show that would be.

As Canadians, we pride ourselves on our system of parliamentary democracy. We believe in openness, in defaulting to disclosure, in distinguishing ourselves from other nations where secrecy is both the common practice and the accepted norm. The spectacle of an information commissioner raiding the highest bureaucratic office in the federal government in no way fits with our self-image.

And Marleau should not be forced by lack of co-operation or otherwise – to exercise the considerable legal powers of his office. The Privy Council Office should not be closed to Canadians seeking information, as we have the freedom to do under the federal **Access to Information Act**. It is a bad situation, both in fact and in appearance.

Prime ministerial secrecy is not new; the late Pierre Trudeau kept information on a reasonably

tight leash. That leash grew even tighter under both Brian Mulroney and Jean Chrétien, but it is safe to say that Stephen Harper's office seems the most secretive when it comes to controlling the flow of information. Given that Harper's government has, so far, a pretty solid track record, the pathological need to control is worrisome. The level of resistance to releasing information works against Harper and his cabinet, suggesting there must be something worth hiding. It suggests smoke, leaving Canadians to wondering how bad the fire is.

The apparent need to control and to set itself up as being above the federal watchdog seems to mirror a growing desire from within to see the Prime Minister's Office, the Privy Council and cabinet as an executive branch of government in the image of the U.S. presidency. That executive branch approach, while entrenched in the United States, is not part of Canada's founding history. But it may be part of the reason behind the growing adversarial, dysfunctional nature of our Parliament, which has seen its governing functions increasingly stripped away.

It is interesting to note, though, that Marleau pointed out earlier this year that Canadians know less than ever about what its government is doing, in sharp contrast to U.S. President Barack Obama's push for openness in the United States.

Certainly releasing information can be uncomfortable, and messy questions may follow. But those who govern -- federally and provincially -- must remember that they work for us. When we want to know what's going on, we should not be hearing "No" over and over again. Marleau is right to keep pushing on our behalf.

Source: Prokaska, Lee. *The Hamilton Spectator*. 29 Jun 2009: A12.

COMPLETE THE QUESTIONS BELOW.

What opinion does the author have about government transparency?

What arguments and/or evidence does he provide to support his opinion?

In your opinion, how effective is his argument? Explain.

Identify the stylistic devices that the author uses to support his opinion. Consider devices such as facts, allusions, comparisons, metaphor, loaded language, repetition, etc. Are they effective?

CULMINATING TASK:**DESCRIPTION**

Popularized by Canadian comedian, Rick Mercer, a “rant” is the sister to the soliloquy (monologue) and distant cousin of debate; it is an individual self-expression, or more simply put, an opinion. It is something that the “ranter” thinks should be known, and they’re not afraid to tell you about it. A rant is usually done with wit and humour, at the same time expressing a position, a stance, or an issue that you think is important. The viewers should be entertained, but at the same time are left with a lasting impression about the topic. A good rant usually includes the following:

- **A topic that is current** – the topic should not be threatening, not include profanity or malign an individual or organization’s reputation;
- **Clear and concise message;**
- **Effectively convinces the audience of your opinion;**
- **Clear structure:**
 - **Intro** – Establish the topic of the “rant”
 - **Middle** – Provides a challenging statement which makes the listener/viewer think....The “AHA!” moment;
 - **End** – Wrap up with a statement that leaves the listener/viewer with an understanding of the topic.

Source: Memorial University - <http://www.mun.ca/rant/>

PURPOSE

- To apply knowledge and concept attainment from unit four in a culminating task;
- To demonstrate democratic participation.

TASK

Your task is to plan, develop and create a one to two minute “Rant” about one of the issues raised in the unit.

INSTRUCTIONS

During this activity, you will work in groups of three or four to plan, write, create and present a one to two minute “Rant” that will address access to information laws. In your group, consider issues that have been addressed in this unit.

STEPS

1. **Topic Selection.** Choose from one of the access to information topics addressed in the readings:

- government spending;
- Office of the Prime Minister;
- health;
- education;
- environment;
- labour;
- freedom of information laws;
- your own idea – please see teacher for approval.

2. **Planning.** Use the *Planning Your “Rant”* handout to outline your “Rant.”

3. **Create.** Create your “rant” and present it to the class for teacher evaluation. If you have access to a DVD camera and are comfortable with its use, you may want to videotape your “Rant.”

ASSESSMENT

- *Planning Your “Rant”* Outline

EVALUATION

- “Rant” Rubric (**Appendix 4.15**)

CULMINATING TASK: PLANNING YOUR “RANT”

Use the following guidelines and questions to help you plan and develop your “Rant.”

1. My topic is: _____
2. My purpose is: _____
3. My audience is: _____
4. My research collection (facts that I have learned to give my Rant credibility):

	Source
	Source
	Source
	Source

5. For each point, you may provide encouragement, hints and/or cautions. For example, use the following starter statements at various times in your rant.

- Don't worry if...
- Make sure you...
- If you feel...

6. Check off the stylistic devices you plan to use:

- | | |
|--|--|
| <input type="checkbox"/> allusion | <input type="checkbox"/> personification |
| <input type="checkbox"/> alliteration | <input type="checkbox"/> quotation |
| <input type="checkbox"/> anecdote | <input type="checkbox"/> rhetorical question |
| <input type="checkbox"/> effective repetition | <input type="checkbox"/> satire |
| <input type="checkbox"/> facts | <input type="checkbox"/> simile |
| <input type="checkbox"/> humour | <input type="checkbox"/> statistics |
| <input type="checkbox"/> hypothetical scenario | <input type="checkbox"/> word invention |
| <input type="checkbox"/> illustrative example | <input type="checkbox"/> other |
| <input type="checkbox"/> metaphor | |

7. What visuals/props will you use?

8. Decide on the following:

- Tone;
- Volume;
- Emphasis;
- Variation in speed;
- Repetition.

9. Decide on the mannerisms and/or actions that might accompany your “Rant.” Use facial expressions and body language to convey your message effectively.

10. Practice, practice, practice!

11. Present your “Rant” to the class for evaluation. If you have access to a DVD camera and are comfortable with its use, you may want to videotape your “Rant.”

CULMINATING TASK RUBRIC:

"RANT" EVALUATION

Students:

Mark: /40

Criteria	Level R (0-49%)	Level 1 (50-59%)	Level 2 (60-69%)	Level 3 (70-79%)	Level 4 (80-100%)
KNOWLEDGE AND UNDERSTANDING					
• knowledge of the subject	- rant demonstrates little or no understanding of topic	- rant demonstrates limited understanding of topic	- rant demonstrates some understanding of topic	- rant demonstrates considerable understanding of topic	- rant demonstrates thorough and accurate knowledge of topic
THINKING AND INQUIRY					
• opinion	- rant does not state an opinion	- opinion is weak	- opinion is adequate	- opinion is good	- opinion is excellent
• supporting details (research, visuals, props)	- inadequate supporting details to support opinion	- weak supporting details to support opinion	- limited supporting details to support opinion	- adequate selection of supporting details to support opinion	- excellent selection of supporting details to support opinion
COMMUNICATION					
Delivery: • eye contact • volume • tone • pace • facial expressions • body language • use of stylistic devices	- communicates opinion orally with no effectiveness	- communicates opinion orally with limited effectiveness	- communicates opinion orally with some effectiveness	- communicates opinion orally with considerable effectiveness	- communicates opinion orally with a great degree of effectiveness
• organization	- rant is disorganized, confusing	- rant is not well organized	- rant is organized somewhat effectively	- rant is considerably organized	- rant is highly organized and effective
APPLICATION					
• process	- no outline provided	- incomplete rant outline	- somewhat complete rant outline	- adequately completed rant outline	- thoroughly completed rant outline
• presentation	- did not include rant elements	- limited use of rant elements	- some use of rant elements	- considerable use of rant elements	- thorough and effective use of rant elements
• references	- no sources provided	- reference list incomplete or not properly formatted	- reference list completed but with several errors	- reference list completed with minor errors	- reference list completed and properly formatted

11*12

RESOURCES

What Students Need to Know

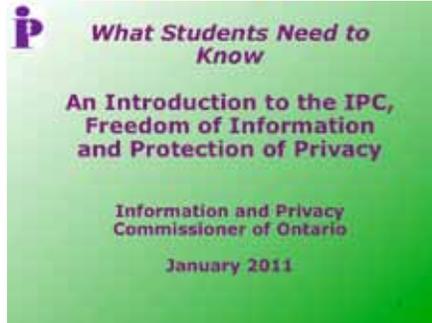


ACTIVITY 1:

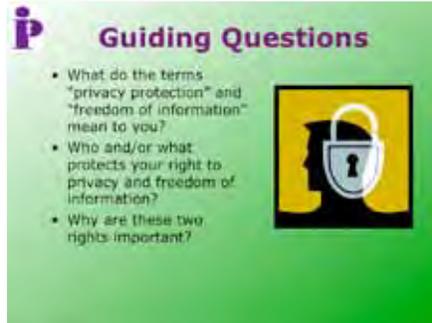
WHAT STUDENTS NEED TO KNOW

INTRODUCTORY POWERPOINT

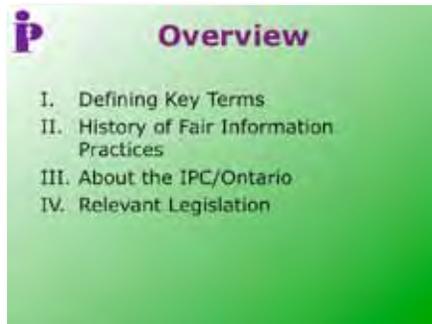
SLIDE 1



SLIDE 2



SLIDE 3



SLIDE 4



SLIDE 5

iP **Defining Privacy**

Privacy is a fundamental human right.
What does this mean?

SLIDE 6

iP **Key Terms**

- "Privacy" involves control over the collection, use and disclosure of personal information.
- "Personal information" is any information that is about you or can identify you.
- Can you think of any examples of "personal information?"

SLIDE 7

iP **Key Terms (Cont'd)**

Freedom of information (FOI), or "access to information" refers to:

- public access to general records relating to the activities of government – ranging from administration and operations to legislation and policy to ensure accountability and transparency of government activities;
- access to records of your own *personal* information that government offices may hold.

SLIDE 8

iP **II. History of Fair Information Practices**

Illustrations from the Ages

PREHISTORIC TIMES 19th century
 20th century 21st century

SLIDE 9


Internationally Recognized Privacy Principles

- In 1980, the Organization for Economic Co-operation and Development (OECD) developed voluntary Guidelines on the Protection of privacy and Transborder Flows of Personal Data.
- They have served as the blueprint for the development of national privacy laws.

SLIDE 10


OECD Principles

- Only necessary information should be collected;
- Where possible, it should be collected directly from the individual to whom it pertains (the data subject);
- The data subject should be told why the information is needed;

SLIDE 11


OECD Principles (Cont'd)

- The information should be used only for the intended purpose;
- The information should not be used for other (secondary) purposes without the data subject's consent; and
- The data subject should be given the opportunity to see and correct his/her personal information if it's incorrect.

SLIDE 12


Global Privacy Standard

- Created in 2006
- Goal: create a single instrument for businesses and technology companies to evaluate their privacy enhancing practices.

SLIDE 13

iP Global Privacy Standard Principles:

1. Consent
2. Accountability
3. Purposes
4. Collection Limitation – Data Minimization
5. Use, Retention, Disclosure Limitation

SLIDE 14

iP Global Privacy Standard Principles (Cont'd)

6. Accuracy
7. Security
8. Openness
9. Access
10. Compliance

SLIDE 15

iP

**III. About the IPC/
Ontario**

SLIDE 16

iP Mandate and Role

- The Information and Privacy Commissioner is appointed by the Ontario Legislative Assembly and is independent of the government of the day.
- The Commissioner's mandate includes overseeing the access and privacy provisions of these Acts:
 - Freedom of Information and Protection of Privacy Act (FIPPA);
 - Municipal Freedom of Information and Protection of Privacy Act (MFIPPA); and
 - Personal Health Information Protection Act (PHIPA).

SLIDE 17

iP **Mandate and Role (Cont'd)**

The Commissioner is responsible for:

- Investigating privacy complaints;
- Resolving appeals, including those involving refusals to provide access to information;
- Ensuring that government organizations and health information custodians comply with the access and privacy provisions of the Acts;
- Educating the public about access and privacy issues;
- Conducting research to promote understanding of privacy and access issues.

SLIDE 18

iP **The Acts**

The role of the Information and Privacy Commissioner/Ontario (IPC) is set out in **three** statutes (The Acts):

1. the *Freedom of Information and Protection of Privacy Act (1988) - FIPPA*;
2. the *Municipal Freedom of Information and Protection of Privacy Act (1991)- MFIPPA*; and
3. the *Personal Health Information Protection Act (2004) - PHIPA*.

SLIDE 19

iP **What do the Acts cover?**

The two public sector Acts (*FIPPA* and *MFIPPA*) provide the public with a right of access to information held by the government in accordance with the following principles :

- Information should be available to the public;
- Exemptions to the right to access should be **limited and specific**; and
- Decisions on the disclosure of government information should be reviewed independently of government.

SLIDE 20

iP **What do the Acts cover? (Cont'd)**

- The other key purposes of these two public sector Acts are:
 - to protect the personal information held by *government* organizations and;
 - to provide individuals with a right of access to their **own** personal information.

SLIDE 21

What organizations are covered by the public-sector Acts?

- **FIPPA (the provincial Act)**
 - Provincial ministries;
 - Most provincial agencies, boards and commissions;
 - Community colleges;
 - Universities;
 - Hospitals - as of January 1, 2012;
- **MFIPPA (the municipal Act)**
 - Municipalities;
 - Police boards;
 - School boards;
 - Boards of health, transit commissions and most other local boards.

SLIDE 22

Personal Health Information Protection Act, 2004

- This is Ontario's health privacy legislation;
- It governs the manner in which personal health information may be collected, used and disclosed within the health care system

SLIDE 23

For more information,
Visit:
www.ipc.on.ca

ACTIVITY 2:

PRIVACY is your **RIGHT**

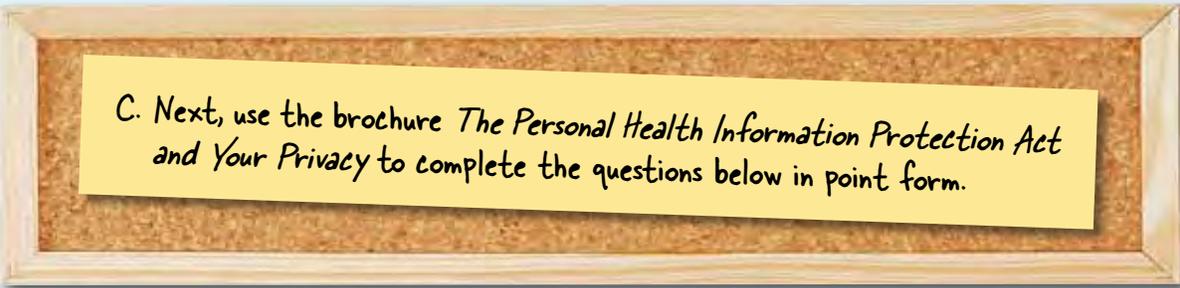
Student: _____



A. Visit the Information and Privacy Commissioner of Ontario website at www.ipe.on.ca.

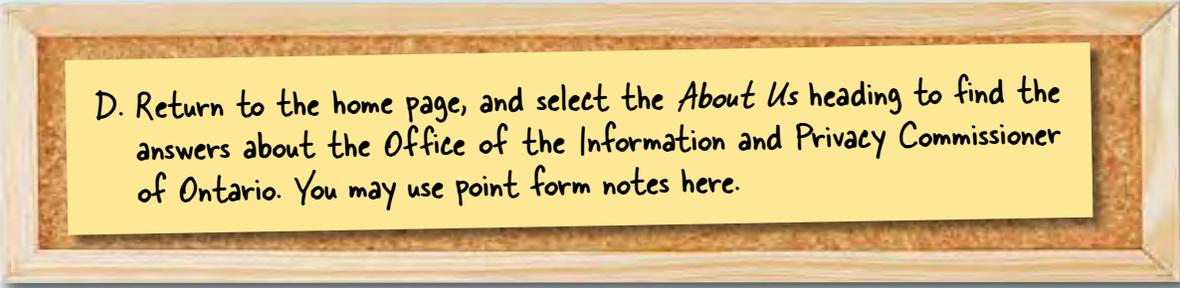
B. Click on the "Privacy" heading and select the "For the Public" subsections. Read the information in the subsections focusing on the brochure *Your Privacy and Ontario's Information and Privacy Commissioner* to answer the following questions. You may use point form here.

1. Which two *Acts* help to protect your personal information held by provincial and local government organizations?
 - a.
 - b.
2. To which organizations does the provincial *Act* apply? The municipal *Act*?
3. What is meant by "personal information?" Provide examples.
4. How do government organizations obtain information about me?
5. How do the *Acts* protect my personal information?
6. Who has access to my personal information?
7. How do I request correction of my personal information?



C. Next, use the brochure *The Personal Health Information Protection Act and Your Privacy* to complete the questions below in point form.

8. What is the *Personal Health Information Protection Act*?
9. What is considered personal health information?
10. As a patient, do I have the right to see my personal health information?
11. What do I do if I have a complaint?



D. Return to the home page, and select the *About Us* heading to find the answers about the *Office of the Information and Privacy Commissioner of Ontario*. You may use point form notes here.

12. Who is the present Information and Privacy Commissioner of Ontario? When was he/she first appointed?
13. List two of the awards or recognition received by the Information and Privacy Commissioner.
 -
 -
14. Under its statutory mandate, what are the key roles of the IPC?

TEACHER ANECDOTAL RECORDING SHEET

Student: _____

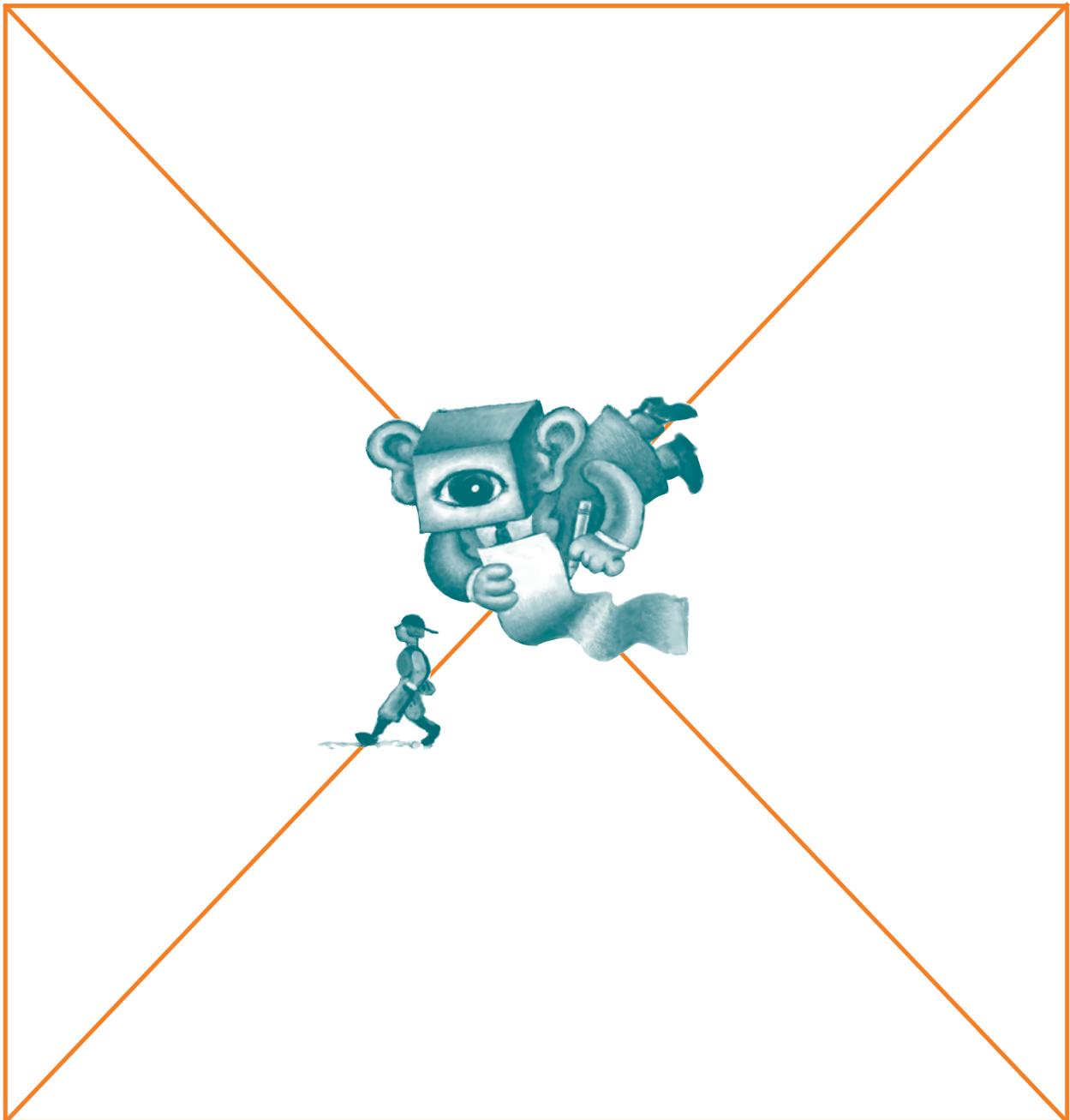
Scale: 1=seldom 2=occasionally 3=frequently 4=regularly**Performance Task****Scale**

<input type="checkbox"/> communicates ideas clearly and effectively	1	2	3	4
<input type="checkbox"/> demonstrates orally an understanding of the content	1	2	3	4
<input type="checkbox"/> shows respect for the ideas of others	1	2	3	4
<input type="checkbox"/> listens without interrupting	1	2	3	4
<input type="checkbox"/> contributes to discussions	1	2	3	4
<input type="checkbox"/> asks appropriate questions	1	2	3	4
<input type="checkbox"/> carries out assignments independently; completes them on time	1	2	3	4
<input type="checkbox"/> works effectively in a small group	1	2	3	4

ACTIVITY 1:

WHO IS WATCHING?

In a group of four, individually record examples of what you think is “personal or private information” on the placemat below. Then, as a group, decide what these examples have in common.



ACTIVITY 2:

PRIVACY QUIZ



Circle T for True or F for False,
based on your knowledge of privacy.

- | | | |
|---|---|--|
| T | F | 1. When a company asks you for personal information, it is safe to assume that it has a good reason for doing so. |
| T | F | 2. The first thing you should do if you receive an abusive message online is delete it. |
| T | F | 3. There are multiple ways that your activities online can be tracked. |
| T | F | 4. Any organization can refuse to provide a service unless you give it the personal information it seeks from you. |
| T | F | 5. A teacher is allowed to search you for drugs or weapons. |
| T | F | 6. You don't have to worry about information that appears about you, or is posted by you, online; eventually, it will disappear. |
| T | F | 7. Anyone who works in a hospital, pharmacy or doctor's office can access your health information for any reason. |
| T | F | 8. If you've never had a credit card or bank loan, there's no reason to check your credit report. |
| T | F | 9. It's okay to create a Facebook account for your pre-teen brother or sister, reporting their age as 14. |
| T | F | 10. You can be suspended from school for something you post online, even if you do it at home on your own computer. |
| T | F | 11. Once a company has your personal information, it can do whatever it wants to with that information. |
| T | F | 12. As long as you don't tell anyone your password for an account, no one can discover what it is. |
| T | F | 13. Privacy policies are too long and too difficult to read – it's not worth the effort of looking these up. |

TEACHER ANSWER KEY: PRIVACY QUIZ

- (1) **False.** You should not give information to anyone unless you know **why** they want it and **what** they plan to do with it, unless you are required, by law, to do so.
- (2) **False.** WiredSafety and the IPC teach a three-step response to online abuse or cyberbullying: *Stop, Block, and Tell Someone*. First, you need to “Stop” – don’t respond right away, take a moment to calm down. Next, you should “Block” the cyberbully, or limit your communications to those you trust. Finally, “Tell Someone” – let a trusted person know what is happening. This is why it is important not to delete the messages; it is better to be able to prove exactly what was said.
- (3) **True.** Currently, the best known means of tracking are advertising cookies. However, there are other ways of tracking you across websites, including your IP address, cookies placed to keep you logged in to Facebook or other sites, and something called “browser fingerprinting,” which can occur if your browser configuration is rare or unique.
- (4) **False.** The federal *Personal Information Protection and Electronic Documents Act* requires organizations to supply individuals with a service even if they refuse consent to collect, use or disclose their personal information, **unless** that information is required to fulfil the explicitly specified and legitimate purpose.
- (5) **True.** A teacher or principal has the authority under Ontario’s Education Act to conduct a search where there are reasonable grounds to believe that a school rule has been violated and the evidence of the breach will be found on the student.
- (6) **False.** While some content may disappear, you should not depend on this happening. If information online is indexed by one or more search engines or is stored by the Internet Archive’s Wayback Machine, it can be found later by those who know how. Material might also be copied, saved or redistributed by other people, or even appear in an online news site.

However, if there is material online you’d like to have taken down (particularly if it is offensive or harmful material about you posted by another person), there are steps you can take. First, ask the person who posted the information to take it down. Alternatively, politely ask the webmaster of the site to remove the information, explaining why. Once you have done this, you can also ask Google or other search engines to remove it from their results (though, given time, this will happen automatically). Some companies, such as Reputation Defender, will also provide this service for a fee. Finally, if you can’t get the material down, try to control your online reputation by posting positive information, or explaining why the “negative” material is wrong – let people see you the way you want to be seen.

- (7) **False.** The *Personal Health Information Protection Act* strictly defines the circumstances under which your health information can be used or disclosed. Here is a link to that Act: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm.

(8) **False.** Identity theft can happen to anyone – even teenagers. Similar to your online reputation, you should periodically check your financial reputation, and take steps to correct any inaccuracies. Checking your credit report is not difficult – you can get a free copy by writing to one of the credit bureaus. (Contact information for the bureaus is provided in the IPC paper, *If you wanted to know... What if you're a victim of identity theft or your credit/bank card is lost or stolen*, which is the focus of another lesson in this unit.)

(9) **False.** This would violate a number of Facebook's terms of service. Specifically, you are not permitted to create an account for anyone else (without permission), and you are not allowed to provide false personal information. Facebook does not permit anyone under the age of 13 to open an account.

In general, the consequence for creating a false account is that the account will be deleted if discovered. However, if you create a false account and use it for malicious purposes (to harm the person whose name you are using, or someone else), there may be further repercussions involving either your school or the police.

(10) **True.** Your actions online, particularly when they are harmful to others, are not consequence-free. Again, threats, malicious comments and other forms of cyberbullying do not need to take place on school property to warrant the involvement of teachers, principals, or even police.

(11) **False.** The federal *Personal Information Protection and Electronic Documents Act (PIPEDA)* generally requires private sector organizations to obtain consent when they collect, use or disclose personal information and to collect, use and disclose it only for purposes that are stated and reasonable. (There are exemptions from these requirements for some purposes, such as journalistic and literary purposes.)

(12) **False.** If you use common passwords (such as "1234" or "LetMeIn"), or a password associated with you (such as your pet's name), your password might be discovered through simple guesswork. Dictionary words are harder to guess, but can be discovered by a "brute force" search by a computer in a matter of hours. That is why it is important that you use strong passwords – combinations of letters and symbols that are at least eight characters long. For instance, you could use the phrase, "My birthday is October 21 and I'm 17," as "MbiO21&I17."

(13) **False.** Some privacy policies are indeed very long, and written in "legal-ese" – which can make them difficult to comprehend. However, there is a broad range of important information that can be included in these policies, raising red flags or reassuring you. A company might note, for example, that it owns any information uploaded to the site, and will reuse it as it chooses – or that it will never use the information for any other purpose than what it was collected for, without your permission.. As well, many companies have started to make their privacy policies much more understandable, in order to attract or keep customers. If you are not comfortable with the way a company presents this important information to you (or with the policies themselves), say so, or consider other companies. Staying informed is the best way of staying in control of your personal information.

ACTIVITY 4:

DEFINING INVASION OF PRIVACY



A) IDENTITY THEFT

Theft of personal information can be the starting point to a range of crimes – from financial fraud and forgery to abuse of government programs.

Examples of identity fraud include:

- the use of stolen credit cards or credit card numbers;
- fraudulently obtaining money, loans, finance and credit;
- fraudulently obtaining benefits, pensions, or entitlements;
- evading the payment of taxes, levies or other debts.



B) DEBIT AND CREDIT CARD FRAUD

Fraud committed using a credit card or debit card as a fraudulent source. Credit card fraud can happen several ways:

- Your card could be lost or stolen and used to purchase goods and services;
- A criminal could obtain your card number and expiry date and use this information to manufacture a counterfeit card;
- You could inadvertently provide your card number and expiry date to a criminal over the phone or Internet.



C) STALKERS AND HARASSMENT

“Stalker” is used to describe someone that follows or observes (a person) persistently, especially out of obsession or derangement. “Harassment” is to trouble persistently or incessantly with repeated annoyances, threats, or demands.



D) SHARING OR SELLING PERSONAL INFORMATION TO DIRECT MARKETERS

The term used to describe when private companies sell or share a customer’s personal information (such as name, address, phone number, age, interests, etc.) to a third party without the customer’s consent.

Sources:

<http://www.business.mcmaster.ca/IDTDefinition/defining/idfraudTCF.htm>
[http:// www.cba.ca](http://www.cba.ca)
<http://legal-dictionary.thefreedictionary.com/>

ACTIVITY 4:

CASE STUDIES: PRIVACY AT RISK?

Privacy is about control over your own information. If control is in the hands of someone other than you, your privacy can be lost. Once your privacy is lost, it is very difficult to get it back or repair any resulting damage.

Identify the *type of abuse* of personal information in the space below each scenario, and explain your choice. Choose from the following: identity theft, debit and credit card fraud, stalkers and harassment, and sharing or selling personal information to direct marketers.



1. A man, using someone's stolen birth certificate and SIN card, obtained a driver's licence from the provincial government. He then used these three pieces of ID to open fraudulent bank accounts and proceeded to steal more than \$170,000 from several banks.

2. A reporter got a call from Canadian Tire because his application for a Canadian Tire credit card seemed suspicious. It turned out someone else had filled out the application. If the application had been approved, the criminal could have racked up purchases on the card, in the reporter's name. The person had also tried to apply for a MasterCard. These actions could have damaged the reporter's personal credit rating.

3. In an Interac scam, the cashier at a store "double-swiped" the shopper's debit card, once on the store's machine and then again to enter the data from the magnetic stripe on her own computer under the counter. Then, by watching the shopper closely, the cashier learned his PIN number. This made it possible to duplicate the debit card and access the shopper's bank account.

4. An actress in the United States was killed by an obsessive stalker, who had obtained her home address by hiring a private investigator. The investigator used a Department of Motor Vehicles licence database to find her address.
-
-

5. A woman received a 12-page letter from a stranger. He knew her birthday, the fact that she was divorced, the kind of soap she used in the shower, her favourite magazines, and many other details about her life. It turned out he was a convicted rapist, and one of his jobs at the prison was entering data from consumer surveys. The woman had sent in a completed questionnaire in order to get the free samples and coupons promised by the company. She had assumed her information would be kept confidential by company employees.
-
-

6. A woman returned home from a stay in hospital, where she had been diagnosed with cancer. The next day she received a phone solicitation from a local funeral home; the funeral home asked for her by name, even though she had an unlisted number. After much pressing, the salesperson admitted that he had been given her number by someone from the hospital.
-
-

7. Do you have an example? Add it here.
-
-

Source: Adapted from and used with the permission of the Office of the Information and Privacy Commissioner for Alberta

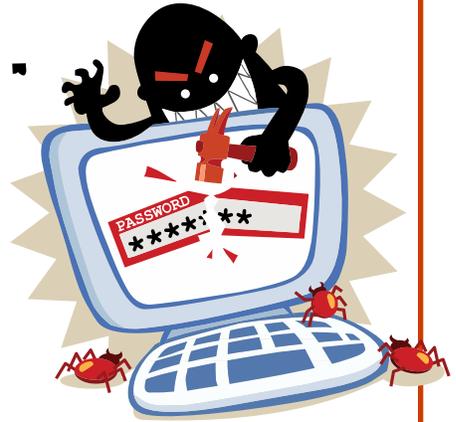
ACTIVITY 4: TEACHER KEY FOR CASE STUDIES: *PRIVACY AT RISK?*

1. Identity theft;
2. Debit and credit card fraud;
3. Debit and credit card fraud;
4. Sharing or selling personal information to marketers without consent;
5. Sharing or selling personal information to marketers without consent;
6. Stalkers and harassment.

Source: Adapted from and used with the permission of the Office of the Information & Privacy Commissioner for Alberta

FINAL TASK:

**“If you wanted to know...
What if you’re a victim of
identity theft or your
credit/bank cards are lost
or stolen?”**



Visit the website below to view the IPC article, *“If you wanted to know ...What if you are a victim of identity theft or your debit/bank cards are lost or stolen?”* Read the article and answer the following questions in your notes. Be prepared to submit your responses to your teacher for evaluation.

<http://www.ipc.on.ca/images/Resources/identitytheft.pdf>

1. How does one verify if impersonation has occurred?
2. What is a credit bureau?
3. What is a credit report?
4. How long does information remain on your credit report?
5. What is a credit score?
6. How many credit bureaus are there in Ontario?
7. What is the process to request a credit report?
8. What should you do if you discover you are a victim of identity theft?
9. What should you do if your credit or bank cards are lost or stolen?
10. How do I avoid becoming a victim of identity theft?

MARK: /10

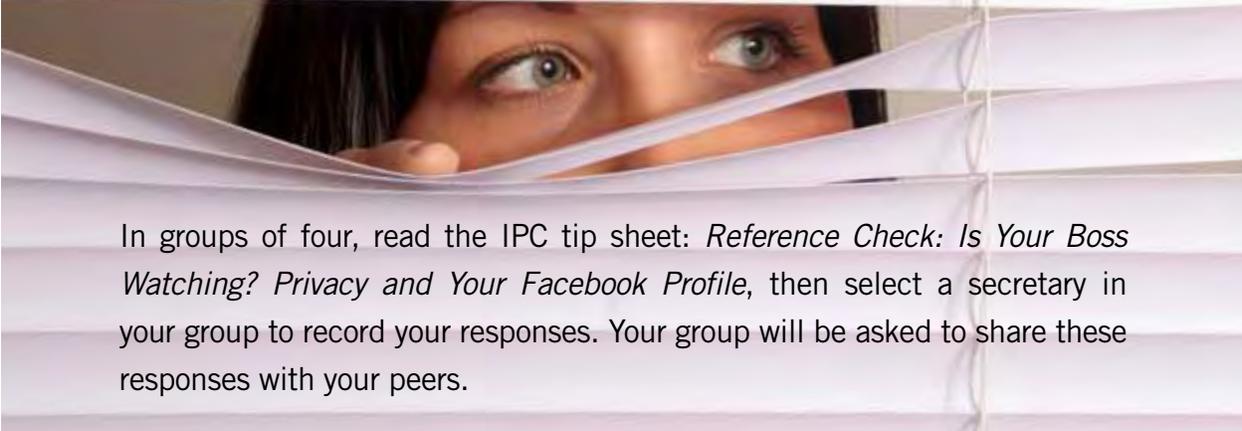
**FINAL TASK:
TEACHER ANSWER KEY:**

“If you wanted to know.... What if you’re a victim of identity theft or your credit/bank cards are lost or stolen?”

- 1. How does one verify if impersonation has occurred?**
 - Contact a credit bureau to check your credit report for fraudulent activity.
- 2. What is a credit bureau?**
 - A credit-reporting agency is a private institution which serves retailers and other credit grantors by providing them with information about your credit record.
- 3. What is a credit report?**
 - A credit report is a profile of how you pay your financial obligations. It is created when you first borrow money or apply for credit. If you make your payments on time, or miss a payment, or if you have gone over your credit limit, this information will be on your record.
- 4. How long does information remain on your credit report?**
 - Six years.
- 5. What is a credit score?**
 - A credit score, not part of your report, is a mathematical formula that translates the information in your credit report into a three digit number that lenders use to make decisions. The higher your credit score, the more likely you are to be approved for loans or credit and receive favourable rates.
- 6. How many credit bureaus are in Ontario?**
 - There are three credit bureaus: Equifax Canada, TransUnion Canada, and Experian Canada.
- 7. What is the process to request a credit report?**
 - You can request your reports free of charge, via mail or phone, or for a fee via the Internet.
- 8. What should you do if you discover you are a victim of identity theft?**
 - Immediately report this to the police. Cancel all existing credit cards, accounts, passwords and personal identification numbers (PINs) and explain why. Close accounts that you know, or believe have been tampered with or opened fraudulently.
- 9. What should you do if your credit or bank cards are lost or stolen?**
 - Call your credit grantors immediately upon discovering that your cards are missing. Most will have round-the-clock service phone numbers for emergencies. Write down the name of each person you speak with.
- 10. How do I avoid becoming a victim of identity theft?**
 - Pay attention to your billing cycles;
 - Review bills and statements on a regular basis;
 - Monitor account balances and activity;
 - Shred all personal records and financial statements;
 - Obtain a separate credit card (with the lowest credit limit available) that will be dedicated to online purchases only.

ACTIVITY 1:

MAKE AN INFORMED CHOICE ONLINE



In groups of four, read the IPC tip sheet: *Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile*, then select a secretary in your group to record your responses. Your group will be asked to share these responses with your peers.

GROUP DISCUSSION QUESTIONS:

1. Who might be interested in the information that is contained in your online profile? How might this impact you?
2. Are you familiar with the privacy settings on your social network(s) of choice? Do you *know* who will be able to view the content you post?
3. After reading the IPC's tip sheet, would you reconsider the nature or amount of information you post on your online social networking profile, or the extent to which that information is shared? Why or why not?

ACTIVITY 1:

THE 5 P's

Before you decide to post any personal information online, remember the following 5 P's that represent the different groups or individuals who might view it.



ACTIVITY 2:

ONLINE PRIVACY



Watch the video (which is being used with the permission of MTV News Canada), then answer the following questions:

1. What are some positive and negative ways in which information about you (including pictures) posted online could affect your reputation?
2. When you post information online, how long does it stay there for?
3. Can you control access to and sharing of information online?
4. What are some of the differences between having everyone in your town know something about you and having that same information posted online?
5. Outline a scenario in which posting sensitive or controversial personal information online might have negative consequences.
6. In the video, the Information and Privacy Commissioner of Ontario says that privacy equals freedom. What do you think she means by that? Do you agree or disagree? Why or why not?

ACTIVITY 3:

MINI DEBATES: SOCIAL NETWORKING



DESCRIPTION

Debating is the forceful and logical presentation of arguments for or against an idea. You debate every day in one form or another. In the classroom, you are trying to persuade your audience and the judge (i.e. your classmates and teacher) with facts and logic, not to outshout your opponent. In a debate, the members of the “affirmative” team are for the resolution. They present arguments that support the resolution. The members of the “opposition” are against the idea or resolution. They present arguments against those offered by the affirmative team.

PURPOSE

- To develop co-operative and listening skills;
- To demonstrate an ability to present ideas and arguments effectively in a debate;
- To demonstrate critical thinking and analysis about an issue.

TASK

Debate the following resolution:

- **Be it resolved that the benefits of social networking sites outweigh the risks.**

INSTRUCTIONS

During this activity, you will work in partners to establish a position and debate with another pair with opposing viewpoints. In each group, students will debate the benefits and risks

involved with using social networking sites such as Facebook, MySpace, Twitter, Tagged, Plaxo, LinkedIn, hi5, Flickr etc. Consider issues such as privacy, security, reputation, business and social networking, fraud, exploitation, cyber-bullying, advertising, exposure, democratic participation, etc.

STEPS

- 1) In a group of four, decide on one networking site for the debate;
- 2) Divide your group into an affirmative and opposition position (for or against social networking);
- 3) The first pair to speak should make at least three points that support their argument. They have up to five minutes;
- 4) The second pair will then speak for up to five minutes, making at least three points in favour of their argument;
- 5) The first pair will then spend five minutes refuting the arguments of the second pair;
- 6) Finally, the second pair will conclude the debate by critiquing the first pair’s main arguments.

ASSESSMENT

- Self-reflection;
- Teacher feedback;
- Peer response.

ACTIVITY 3:**MINI DEBATES: SELF REFLECTION**

Answer the following questions to reflect on your understanding, opinions and values regarding the impact of social networking sites in society.



Have your knowledge and understanding of social networking sites changed as a result of this activity? How?

Have the debates influenced your opinion of the use and/or impact of social networking sites in society? Why or why not?

What do you predict will happen to social networking sites in the future?

ACTIVITY 4:**ANALYSING CURRENT ISSUES
RELATED TO WEB PRIVACY**

With a partner, read the news article provided by your teacher. Answer the following questions in the space provided.

What is the title of the article?

Summarize the main idea of the article.

What are some arguments outlined in the article that connect to or support the main idea?

Why is the issue important? Whom does it impact?

If you were to respond in an editorial, do you agree or disagree with the main message? What recommendations can you make to deal with the issue?

Facebook fakers prey on students

The Toronto Star
 Mon Jul 6 2009
 Page: A01
 Section: News
 Byline: Paola Loriggio
 Source: Special to the Star

Prospective university students are falling prey to a growing Facebook fraud as marketers set up fake academic groups to vacuum up their personal information.

After a sweep that shut down a number of fraudulent groups last month, a new batch has sprung up, targeting the classes of 2014 and 2015, and experts say more are on the way.

The stakes are high – potentially years' worth of data and thousands of contacts in a desirable demographic. So high, in fact, one company allegedly tried to bribe and blackmail a student to help a scam.

Hundreds of students in the GTA were told in June to abandon fake "Class of 2013" Facebook groups, many sporting official school logos. A sweep shut down groups targeting classes at more than a dozen major Canadian universities, including the University of Toronto, York, Ryerson and McMaster.

There is "a whole subculture" of people trying to make a quick buck by impersonating legitimate organizations and celebrities online, says Avner Levin, director of the Privacy and Cyber Crime Institute at Ryerson University.

The set-up goes beyond sending ads to those who join the fraudulent groups, Levin says. Unbeknownst

to students, marketers are building mailing lists, collecting personal information that they can store and sell for years, he says.

A spokesperson for Facebook said the company doesn't have statistics on people creating false accounts, dubbed "squatters." But she said the company removes the accounts when notified through the "report" link found on each page.

The discovery of marketer-run university groups rocked U.S. academic circles in December, after dozens of fake groups were linked to campus guidebook company College Prowler. The company apologized for misleading students.

Alerted to the U.S. scam, officials at Dalhousie University reported a fake "Class of 2013" group to Facebook administrators during the winter and had it deleted.

When that group disappeared, Tyler Thorne, an incoming Dalhousie freshman, started a new one. It wasn't long before marketers contacted him, asking to become the group's administrators.

The marketers (a "major event promotion company") tried to bribe him with money and concert tickets, said Thorne, a 17-year-old from Halifax. When that failed, he said, they threatened to blacklist him from all local bars.

Matthew Melnyk, an electronic outreach recruitment officer at Brock University, discovered a fake Brock group in February. He later

linked it to a network of more than a dozen suspicious groups targeting incoming students at major Ontario universities.

The groups were shut down in early June, but a new generation has already appeared, targeting the next two waves of freshmen.

...

Lysan Sequeira, 18, left a fake U of T group after receiving a warning message from a real university group. "It definitely changed how I behave on Facebook," she said. She tightened her profile's privacy settings, and no longer accepts friendship requests from strangers.

Ryan McNutt of Dalhousie University, who discovered the fake group linked to the school, says most universities are just starting to monitor sites like Facebook.

Levin, of the Privacy and Cyber Crime Institute, says Facebook should do more to seek out and delete squatters' accounts. He also has a warning for students who think they're safe from fraudsters because they use strict privacy controls on their Facebook accounts: Marketers can deduce demographic data from users' networks, and guess email addresses from their names and academic institutions.

Though Facebook's terms of use ban false accounts and misleading information, the groups often go unnoticed, he says.

(This is a slightly condensed version of the article.)

Spy chief's wife puts him on Facebook; Head of M16 learns millions have access to family details

The Ottawa Citizen
 Mon Jul 6 2009
 Page: A6
 Section: News
 Byline: Michael Evans
 Source: The Times, London

Diplomats and public servants are to be warned about the danger of putting details of their family and career on social networking websites. The advice comes after the wife of Sir John Sawers, the next head of MI6, put family details on Facebook – which is accessible to millions of Internet users.

Lady Sawers disclosed details such as the location of the London flat used by the couple and the whereabouts of their three children and of Sawer's parents. She put no privacy protection on her account, allowing any of Facebook's 200 million users in the open-access London network to see the entries.

Patrick Mercer, the Conservative chairman of the Commons counter-

terrorism sub-committee, said the entries were a serious error and potentially damaging.

“Sir John Sawers is in a very sensitive position and by revealing this sort of material his family have left him open to criticism and blackmail,” he told the Times. “We can't have the head of MI6 being compromised by having personal details of his life being posted on Facebook.”

David Miliband, British foreign secretary, was dismissive Sunday of the security implications of the incident. Speaking on BBC One, he said that it was “no state secret” that Sawers wore Speedo swimming trunks on family holidays. “For goodness' sake, let's grow up,” he said.

He described Sawers as an “outstanding professional” and denied the episode would compromise his career.

Identity Theft among Canada's fastest-growing crimes;

In recent years, reports have soared 500 per cent

The Globe and Mail
 Mon Jun 29 2009
 Page: A5
 Section: National News
 Byline: Omar El Akkad

If Corporal Louis Robertson of the RCMP's anti-fraud call centre needs further proof that identity theft is among the fastest-growing crimes in Canada, he need look no further than his own wallet.

Last year, Cpl. Robertson noticed a strange charge on his American Express statement originating in Ottawa at a time when he was in Washington. The man who knows more about identity theft than almost anyone in Canada has never found out who got his credit card information, or how.

"[Identity theft] is the fastest criminal market right now," Cpl. Robertson said. "There's no risk, and that's the beauty of it – if you are smart, you will disappear."

Between 1998 and 2003, identity-theft reports in Canada soared 500 per cent, according to Vanessa Giuliani, a fraud specialist with the credit information and reporting agency, Equifax Canada Inc. Ms. Giuliani was one of several

representatives of credit-related business in Ottawa in 2009 urging passage of Bill S-4, which would create several new Criminal Code offences related to identity theft. *(See note at the end of this story for more recent statistics.)*

Businesses have traditionally walked a fine line when trying to combat identity theft. If they subject people to overly intense scrutiny, they risk invading people's privacy and upsetting their best customers, while too many regulations and checks can hinder the flow of commerce. Do too little, and criminals thrive.

Cpl. Robertson estimates the financial impact of identity theft in Canada at about \$500-million a year. It's impossible to get a precise figure, given the nature of the crime and the fact that many companies are reluctant to release their fraud statistics. Identity theft has become so common that it is called traditional identity theft to differentiate it from an even more damaging variation that has grown significantly in the past couple of years: fictitious identity theft. In this scenario, a criminal

uses a real piece of identification as a basis to create a fake person who they use to apply for all the credit cards and loans a real person could. At the end of the scam, the culprit takes the money and runs, and there's nothing left to chase. Equifax estimates the average loss in an instance of successful fictitious identity theft at about \$250,000.

Such cases are often traced to organized crime, Cpl. Robertson said, adding that the RCMP has tracked identity-theft rings to everything from West African criminal groups to local biker gangs.

Identity theft can often start with one or two low-level company employees who have access to personal information databases. Given how valuable that kind of information can be to a criminal organization, employees who leave sometimes take it with them. Cpl. Robertson said companies have consulted him on what to do after discovering that anywhere from two million to 40 million identities may have been compromised.

Identity Theft Continued...

“My first answer,” he said, “is get a lawyer.”

Because identity theft is usually the work of organized rings, when uncovered, it tends to be on a large scale. Two years ago, Toronto police officers conducting a traffic stop found 15 credit reports in the back seat of a car. An investigation by Equifax and the police traced those reports to three employees at three different companies. Between them, the three had created 500 fictitious identities.

“You tend to see foot soldiers working in concert with organized groups,” Ms. Giuliani said. “They don’t always actualize identities, but when they do get it, the average loss to the industry is about \$250,000 per identity.”

Recently, firms have become aware of the risks of appearing to blow the identity-theft issue out of proportion.

Earlier this year, a senior executive at AT&T Inc. told a U.S. Senate committee that worldwide revenues from all cyber crime stand at \$1-trillion, making it

more lucrative than the drug trade.

His assertion has drawn criticism from those who call that number impossibly big.

But for Cpl. Robertson, the biggest concern isn’t the size of the identity-theft industry, but the speed with which someone’s identity can be stolen and exploited.

“Your personal identity can easily be sent to a black market in Bulgaria, and that’s it,” he said. “It’s all about speed.”

UPDATED STATISTICS from the Office of the Information and Privacy Commissioner of Ontario.

The number of cases of identity theft fraud that are reported to police are only a fraction of the actual number. The most comprehensive study (as of early 2011) measuring the impact of identity theft in Canada was a 2008 McMaster University consumer survey entitled *Measuring Identity Theft in Canada*.¹ The survey concluded that 6.5 per cent of Canadian adults, or almost 1.7 million people, were victimized by some kind of identity fraud during the previous year. Only 13 per cent of these frauds were reported to the police.

The statistics below are from an early 2011 report by the Canadian Anti-Fraud Centre (<http://www.antifraudcentre-centreantifraude.ca/english/documents/Annual%202010%20CAFC.pdf>) citing actual reported cases.

- **2010:** 18,146 victims; \$ 9,436,996.92 in reported dollar losses;
- **2009:** 14,797 victims; \$10,968,134.44 in reported dollar losses;
- **2008:** 12,309 victims; \$ 9,689,374.32 in reported dollar losses.

¹ Measuring Identity Theft in Canada, Susan Sproule and Norm Archer, July 2008, Mc Master eBusiness Research Centre, DeGroote School of Business.

PRIVACY RIGHTS WHEN USING EMPLOYEE-PROVIDED COMPUTERS

The Welland Tribune

Thu Apr 7 2011

Page: A7

Section: News

Column: The Law

By Alan Shanoff

Warning: Reading headlines may be hazardous to your legal health.

We should put this disclaimer on every article reporting on legal developments.

The headlines accompanying last month's Ontario Court of Appeal decision on **privacy** rights pertaining to personal material stored on computers provided by employers proves the need for such a warning.

Headlines trumpeted "Ontario court rules personal files on work computer private," "Files stored on work computer are private" and "Computer ruling seen as landmark workplace decision."

One of the articles even referred to "a **constitutional right to privacy.**"

The problem is when you look at the actual decision, you'll get an entirely different perspective.

The case revolved around Sudbury high school teacher Richard Cole, who accessed a male student's e-mail account, found nude photos of a female student and copied them onto his school-issued laptop.

The nude photos were discovered by an information technologist during a routine virus scan of the school's network.

The technician reported his discovery to the principal and the photos were copied onto a disc.

The principal ordered Cole to surrender the laptop and a subsequent search of

the computer disclosed Cole's browsing history and files with large numbers of pornographic images.

This history was also saved onto a disc.

Now, if the headlines were accurate, the evidence of the nude photos of the student, the browsing history and the pornographic images discovered by school technicians would have been declared illegally obtained and inadmissible in a case against Cole where he's up on charges of possession of child pornography and fraudulently obtaining data from the male student's computer.

But that's not what the appeal court ruled. Instead the court ruled the technicians and the principal acted reasonably. The copying of the nude photos onto a disc, the seizure of the computer by the principal, the search of Cole's browsing history and saving the history onto a disc were all deemed to be reasonable and lawful.

All of this evidence is **allowable**, contrary to what the trial judge ruled.

What the Court of Appeal ruled, however, and what has led to the misleading headlines relates to what happened **after** the principal handed the computer to the police.

The police conducted further searches on the computer **without** having obtained a search warrant. They thought they were entitled to do so based solely on the permission of the principal.

The appeal court disagreed, ruling the subsequent warrantless police search of the computer was a violation of Cole's rights.

But, and it's a huge but, that didn't taint anything the school employees did, and

all of the evidence obtained and handed over to police was ruled lawful and not in violation of Cole's rights.

And now that Ontario's highest court has ruled on this point, police will now be sure to obtain a search warrant before examining any computer given to them by either a school or any employer.

Obtaining a warrant will be an easy task if police are given any evidence establishing reasonable and probable grounds for a search, as occurred in the Cole case.

The upshot is Cole will be retried on the charges and the prosecution will be entitled to use all the evidence handed over to police. Only additional evidence obtained by police after receiving the computer is inadmissible.

Whatever the ultimate outcome of the Cole prosecution, **people need to understand any computer on loan from an employer is subject to being examined by their employer.**

Depending on the reasons for the examination and the employer policies governing the use of the computers, whatever may be discovered may be admissible in any prosecution if handed over to police. Further, police can use the information provided by the employer to obtain a search warrant.

So the headlines notwithstanding, employees should understand their use of an employer-provided computer should not be considered private.

Consider yourself warned.

(Highlighting added by the Office of the Information and Privacy Commissioner of Ontario for this IPC teachers' guide.)

The Perils of Facebook; Beware of consequences of baring your soul, or other things, online

The Calgary Herald

Mon 09 Feb 2009

Page: A3

Section: News

Byline: Gwendolyn Richards

Source: Calgary Herald

Within the last few weeks, a Calgary employee in the oilfield service industry made a decision to call in sick.

He wasn't.

Instead, he went out, joining friends who shot photos of him and uploaded them to Facebook, a social networking website.

His friends "tagged" him in the pictures, which alerted those in his circle of Facebook contacts to the images that showed he wasn't at home sick after all.

Among those notified was a co-worker forced to do additional work on behalf of the supposedly sick man. That employee, no doubt displeased with having to pick up the extra work, reported the transgression to the boss.

The "sick" staff member was given an official warning that was documented in his human resources file and had to compensate for the missed day.

"There was no hiding from it," said Boyden Global Executive Search's managing director, Robert Travis, who heard about the incident directly from one of his clients.

This should serve as a cautionary tale for anyone who thinks what happens on Facebook, stays on Facebook, he said.

"People need to be aware of their intended and not intended audience with respect to their online persona."

He expects there are more of these stories to come as Facebook continues to grow at an unprecedented rate. As the population of the online community expands, more people are vulnerable to getting caught when they make a misstep.

According to Facebook's statistics, there are more than 150 million people connecting on the site, and the fastest growing demographic is people 30 years and up.

The draw of Facebook has even led some employers – including the Ontario government, British Gas and Telstra, the largest telecommunications company in

Australia – to ban it from the workplace over concerns it affects productivity or disgruntled workers could harm the companies' reputations.

What one expects to be a private place to communicate with friends, to share photos and videos, may actually be the equivalent of putting your personal life up on a billboard.

Rebecca Sullivan discovered others could access her Facebook page – including personal photos – after a student brought it to her attention. It was an innocuous, albeit ironic, oversight on Sullivan's part.

After all, as a pop culture expert who teaches communications and culture at the University of Calgary, Sullivan is keenly aware social networking sites have blurred the line between public and private spheres.

"I assumed the default (on her Facebook page) would be the highest privacy settings," she said with a laugh.

Now that she has clicked the right buttons to ensure her Facebook profile is only viewed by those

Facebook Continued...

she approves, Sullivan said many don't actually realize they have to choose to protect their privacy.

"They're not often readily available and obvious to a novice," she said of the settings.

But it makes sense, considering the platform.

"The Internet does not operate on the principle of privacy, it operates on the principle of publicness," Sullivan said.

Maintaining a line between the two has been a problem since the advent of e-mail. Although a much more private form of communication than Facebook, e-mail is like a postcard: it's not just between sender and recipient.

Sullivan points out there have been cases where employees who used their work e-mail addresses to make inappropriate comments have found themselves without a job.

Social networking sites take it one step further, becoming places where private and public worlds collide – sometimes with disastrous results.

In October, 13 Virgin Atlantic employees were fired for criticizing the airline and some of its passengers on Facebook.

At the time, a spokesman for the airline said the cabin staff took part in a discussion on the social

networking site that "brought the company into disrepute and insulted some of our passengers."

Last spring, a Calgary teacher was reprimanded for posting comments about drug-using mothers on her Facebook page that prompted a complaint from a parent. The Calgary Board of Education deemed the comments offensive, had them removed and disciplined the teacher.

The Alberta Teachers' Association advises against teachers becoming Facebook friends with students, either current or recently under their guidance, while in Vancouver, the board of education has considered banning communication between teachers and students on such sites. More drastically, the teacher's union in Ohio has asked its members to remove their profiles from social networking sites.

"The Internet and social networking sites have added another dimension to an already existing problem of where public and private begin and end online," said Sullivan.

"If you really thought it was private, you're crazy."

The effects of a decision to post a racy photo or damning comment may not be immediately apparent. But once out in the ether, it is almost impossible to delete. "You are technologically incapable of

removing this stuff. Once photos are up there, anyone can download them," said Sullivan.

Steven Rothberg, founder of Internetcareersitecollegerecruiter.com, explains the danger as such: any "friend" has access to information and photos they can easily take and distribute outside Facebook.

"I could get a screen shot, post it to my blog, put your name on it," he said. At that point, there is nothing private about what was once on Facebook.

Such was the case of beauty queen Amy Polumbo, crowned Miss New Jersey last year, who was the subject of a blackmail attempt when someone sent photos – including one showing her boyfriend biting her clothed breast – from her deleted Facebook page to pageant officials.

"This was meant to be private. This was not accessible to the general public," she said during an appearance on NBC's Today show in July 2007.

Rothberg said what a lot of people don't understand is while Facebook is password protected, any information you put up on it can be shared with anyone else and the damage can be far-reaching.

Studies indicate at least 25 per cent of employers admit they use social networking sites to

Facebook Continued...

gather information about potential hires. That figure, in reality, is probably closer to 75 per cent, said Rothberg.

“It’s very hard, especially for young adults, to understand that employers have a need to have employees who have a good sense of judgment,” he said. “We are not Dr. Jekylls and Mr. Hydes; we don’t act one way in our personal lives and a completely different way in our professional lives.”

Rothberg advises job seekers – and those gainfully employed who want to stay that way – to view posting any information online the same as getting a tattoo.

“There’s nothing inherently wrong with it, but you’ve got to live with it. People will see it that you didn’t intend to see it and you didn’t want to see it,” he said.

However, he also cautions employers to take everything in context, saying young adults today are doing the same things the previous generation did.

“The only difference is we didn’t have the ability to snap a photo and upload it. Don’t punish this generation because we gave them the tools to embarrass themselves.”

Facebook is not the first place staff with Boyden Global Executive

Search look when examining candidates, said Travis.

Staff are more concerned about a criminal background or fraudulent reports of education or previous employment than photos of candidates chugging beer. But, Travis said, there are times when they do turn to the social network when looking at candidates.

“If we had any red flags around a person’s personality, ethics, behavioural issues, we would reach out to Facebook see if we could find something.”

What they find may not persuade headhunters to decide someone is a bad candidate, but it does help them learn as much as they can about a potential hire, Travis said. He added most people have locked down their Facebook profiles with privacy settings, making it difficult for search consultants to find anything.

Meanwhile, the province’s teachers’ association has written articles in its newspaper reminding members to be discreet and think twice before posting something to Facebook.

“What we basically say is, don’t put anything there that you wouldn’t want your mother to see on the front page of the Calgary Herald,” said president Frank Bruseker.

“I think it’s prudent to ask yourself, ‘Why am I posting this? Why would I share this with all these people? Do people need to know this?’”

Bruseker has an account, too, but only has about 20 contacts – mostly family. His list is meagre compared to many Facebook users who have added hundreds of “friends.” (The average user has 100 friends, according to Facebook.)

That practice is baffling to Bruseker and Sullivan alike.

It raises the question: are they friends or are they, literally, “virtual” strangers.

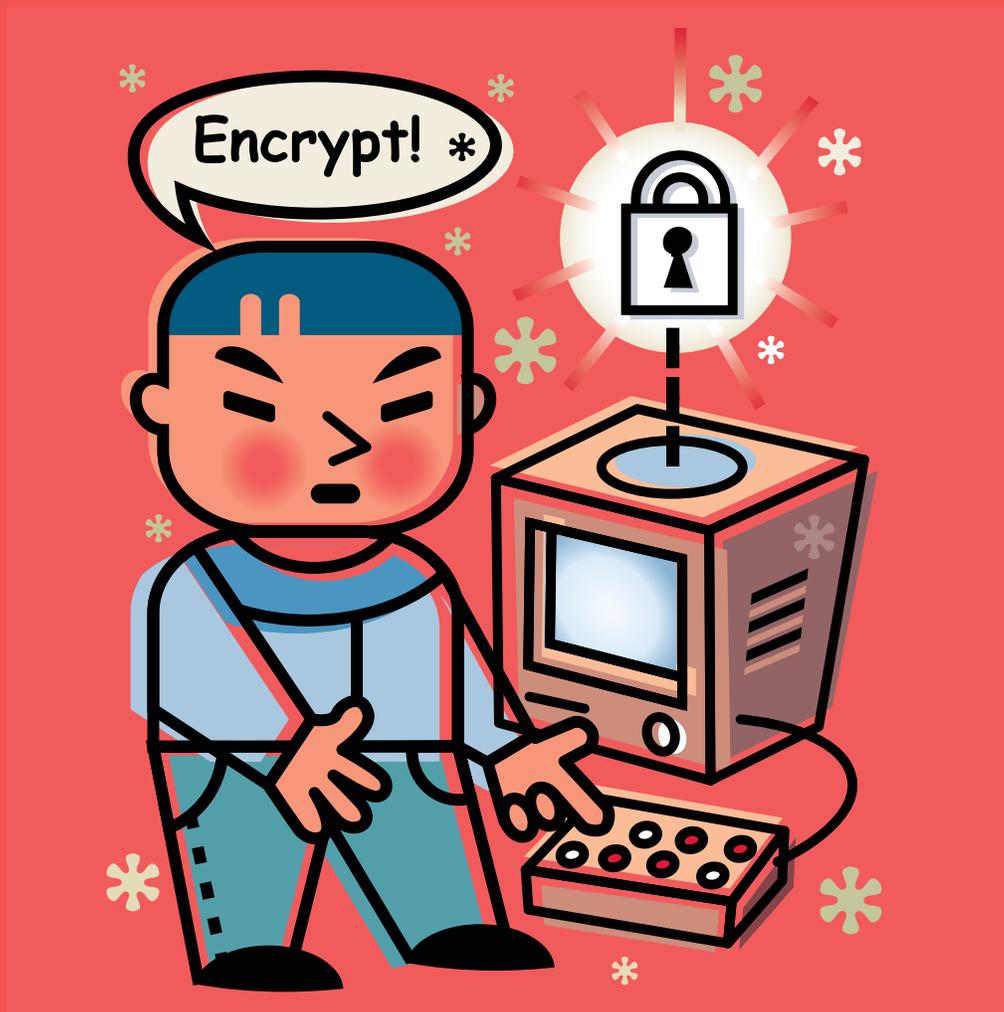
It’s something Sullivan said people should consider carefully, not only when someone asks to be a Facebook friend, but when reviewing the list of people already accepted.

“If we want an environment where we can just be ourselves and be private people and make inappropriate comments and tell inappropriate stories, then be careful, be protective of your environment,” she said.

“If you’re not willing to say it out loud at a neighbourhood party or put the photo on a big sign in front of your house, don’t do it online,” she said.

STAYING SAFE ONLINE

PUBLIC INFORMATION POSTER



POSTERS ARE A SIMPLE BUT EFFECTIVE WAY OF PUBLICIZING EVENTS AND COMMUNICATING IMPORTANT MESSAGES TO THE PUBLIC AT LARGE. THEY CAN BE DISPLAYED AT SPECIAL EVENTS AND AT SCHOOL OR IN THE COMMUNITY.

Purpose

- To apply knowledge and concept attainment from unit three in a culminating task;
- To raise the school community's awareness about consumer privacy on the Web.

Task

Your task is to create a **public information poster (PIP)** about an Internet consumer privacy issue. Select from one of the topics below.

Instructions

During this activity, you will work in pairs to research, plan and create a PIP that will address consumer privacy on the Web. In each group, students should consider issues that have been addressed in this unit. You will create and present your poster with a partner.

Steps

1. **Topic Selection.** Choose from one of the topics addressed in the unit:
 - surfing the Web;
 - identity theft;
 - social networking;
 - blogging;
 - your own idea – please obtain approval from teacher.
2. **Research.** Research the risks involved with your topic. You should get the information from a reliable source, such as from books, people working in the field or on reputable Internet sites, including that of the Information and Privacy Commissioner of Ontario (www.ipc.on.ca).
3. **Reference.** Be sure to reference your sources of information in your research notes and on a Reference List submitted with the poster.

4. **Information Selection.** Select the information you will include on the poster. Choose information and/or tips that are effective.
5. **Editing.** Have your information checked by your peer or teacher. Make sure you use correct spelling, punctuation and grammar.
6. **Production.** Decide how you will make your poster. You may draw, use computer graphics, clipart, Photoshop, etc.
7. **Design.** Design an effective and appealing PIP. It is important to make your poster attractive and easy to read.
 - Choose a background colour that will not overwhelm the message;
 - Use appropriate pictures or graphics; and
 - Choose fonts that are easy to read – consider colour and size and be careful not to mix too many different fonts together.
8. **Publication.** Think carefully about where you will put up your posters. Try to find a location where many people will see them, but where they will not get lost in the crowd. The goal is to increase the school community's awareness about the privacy risks involved on the Web.

Assessment

- Teacher observation and feedback;
- Peer editing.

Evaluation

- See the attached Culminating Task Rubric: *Staying Safe Online Public Information Poster (Appendix 3.13)*

CULMINATING TASK RUBRIC:

STAYING SAFE ONLINE**PUBLIC INFORMATION POSTER**

Student(s):

Mark:

/40

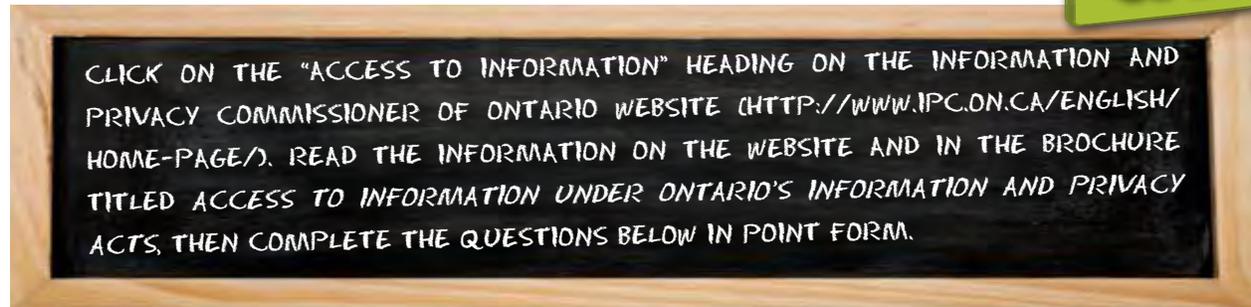
Criteria	Level R (0-49%)	Level 1 (50-59%)	Level 2 (60-69%)	Level 3 (70-79%)	Level 4 (80-100%)
KNOWLEDGE AND UNDERSTANDING					
• knowledge of topic	- poster demonstrates inaccurate or insufficient understanding of the topic	- poster demonstrates limited understanding of the topic	- poster demonstrates some understanding of the topic	- poster demonstrates considerable understanding of the topic	- poster demonstrates thorough and accurate understanding of the topic
THINKING AND INQUIRY					
• research	- little or no research present	- research lacks sufficient depth	- research shows limited depth	- research shows adequate depth	- research shows great depth
• supporting details and tips	- inadequate supporting details	- poor supporting details	- limited supporting details	- adequate selection of supporting details	- excellent selection of supporting details
COMMUNICATION					
• language conventions	- uses language conventions with very limited accuracy	- uses language conventions with limited accuracy	- uses language conventions with some accuracy	- uses language conventions with considerable accuracy	- uses language conventions skilfully and correctly
• organization of presentation	- presentation was disorganized, confusing	- presentation was organized in an ineffective manner	- presentation organized in a somewhat effective manner	- presentation organized in an effective manner	- presentation organized in a highly effective manner
APPLICATION					
• design elements	- ineffective use of colour, text, and visuals	- inappropriate or ineffective use of colour, text, and visuals	- colour, text, and visuals were utilized somewhat effectively	- colour, text, and visuals were utilized effectively	- colour, text, and visuals were utilized highly effectively
• reference list	- no sources listed	- uses limited citations with accuracy	- uses some citations with accuracy	- uses citations with considerable accuracy	- uses citations with thorough accuracy

ACTIVITY 1:

YOUR RIGHT TO ACCESS INFORMATION



Student: _____



1. Which two *Acts* give you the right to request access to government-held information in Ontario?

a

b

2. To which government organizations does the provincial *Act* apply? The municipal *Act*?

PROVINCIAL ACT	MUNICIPAL ACT
•	•
	•
•	•
	•
•	•
	•
•	•
	•
	•

3. What is the *Directory of Institutions* and where can it be accessed?

4. What kind of information may I request? What kind of information can I not obtain through these *Acts*?



Source: Turner, Morrie. "Wee Pals: Freedom of Information Act." 7 Jan. 2009 <gocomics.com>

5. How do I find out what records provincial and local government organizations have?
6. How do I request the information I want?
7. If that does not work, what do I do then?
8. To whom must the request form or written letter be forwarded?
9. What are the costs involved in submitting a request form or letter?
10. How long must I wait for a response to my request?
11. When might an exemption apply to the request for information?
12. What if the government organization denies me access to information requested under the provincial or municipal *Acts*? What then?

ACTIVITY 1 - TEACHER KEY: YOUR RIGHT TO ACCESS INFORMATION WEB QUEST

1. Which two *Acts* give you the right to request access to government-held information?
 - a. Ontario's *Freedom of Information and Protection of Privacy Act* (the provincial *Act*)
 - b. *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act*)
2. To which government organizations does the provincial *Act* apply? The municipal *Act*?

PROVINCIAL <i>ACT</i> – PROVINCIAL GOVERNMENT ORGANIZATIONS	MUNICIPAL <i>ACT</i> – LOCAL GOVERNMENT ORGANIZATIONS
• all provincial ministries and most provincial agencies;	• municipalities;
• many boards and commissions;	• police services boards;
• colleges of applied arts and technology;	• public library boards;
• universities;	• school boards;
• (and hospitals, as of Jan. 1, 2012).	• conservation authorities;
	• boards of health;
	• transit commissions;
	• certain municipal electricity corporations;
	• certain local housing corporations.

3. What is the *Directory of Institutions* and where can it be accessed?
 - It lists all of the government organizations covered by the *Acts* and can be accessed directly from www.mgs.gov.on.ca/en/infoaccessandprivacy.
4. What kind of information may I request? What kind of information may I not obtain through these *Acts*?
 - The *Acts* give everyone a general right of access to general records held by government organizations. The information may be recorded in printed form, on film, by electronic means or otherwise, and it includes such things as photographs and maps. You also have the right to request access to, and correction of, your personal information held by government organizations.
 - You cannot use FOI to request information held by **private** companies such as Royal Bank, Sears, Imperial Oil, etc.
5. How do I find out what records provincial and local government organizations have?
 - First, determine whether the information is held by a provincial or local government organization by referring to the online *Directory of Records*.
6. How do I request the information I want?
 - Call the appropriate government organization to see if the information is available over the counter.
7. If that does not work, what do I do then?
 - You can make a written freedom of information request by completing a request form (a generic form is available on the IPC's website). Alternatively, you may write a letter stating that you are requesting information under (list which of the two *Acts* you are using).

8. To whom must the request form or written letter be forwarded?
 - Forward the request to the Freedom of Information and Privacy Co-ordinator at the government organization most likely to have the information you are looking for.
9. What are the costs involved in submitting a request form or letter?
 - You **must** submit a \$5 cheque with your request, and you may be charged for photocopying, shipping costs, the costs of searching for the records you have requested and/or preparing them for disclosure, or any other costs incurred in responding to the request. (The **average** fee for general requests to provincial organizations in 2010 was \$39.97; at the municipal level, \$25.68).
10. How long must I wait for a response to my request?
 - Usually a response will be received within 30 days of the government organization receiving the request.
11. When might an exemption apply to my request for information?
 - For example, you **cannot** obtain another person's personal information through an FOI request. (Business information is not personal information.) Nor can you obtain cabinet records.
12. What if the government organization denies me access to information I requested under the provincial or municipal *Acts*? What then?
 - It must give you written notice of its decision – including citing the specific exemption or exemptions it is basing its decision on – and inform you of your right to appeal the decision to the Information and Privacy Commissioner.

ACTIVITY 1:

FREEDOM OF INFORMATION QUIZ

Circle the correct answer.

- (1) Which of the following local government organizations does Ontario's *Municipal Freedom of Information and Protection of Privacy Act* apply to?
- Municipalities;
 - Police services;
 - School boards;
 - All of the above.
- (2) In practical terms, that *Act* provides Ontarians with the right to access to:
- Most of the information held by local government organizations, with specific and limited exemptions;
 - About 50 per cent of the information held by local government organizations;
 - About 25 per cent of such information;
 - About 25 per cent of paper records held by local government.
- (3) A discretionary exemption that could be claimed to exclude some records from being accessed (depending on the circumstances) is:
- Solicitor-client privilege;
 - Law enforcement;
 - Information about inter-government relations, if the information was received in confidence;
 - All of the above.
- (4) A freedom of information request sent to a municipality should be addressed to:
- The mayor;
 - The treasurer;
 - The freedom of information co-ordinator;
 - None of the above.
- (5) Which of the following provincial organizations does Ontario's *Freedom of Information and Protection of Privacy Act* apply to?
- Ministries;
 - Most provincial agencies;
 - Children's Aid Societies;
 - Both (a) and (b).
- (6) Can either *Act* be used to request information held by private sector organizations?
- Yes;
 - No;
 - Only in very specific cases.
 - None of the above.
- (7) What is the initial fee that must accompany a freedom of information request?
- \$5;
 - \$25;
 - \$50;
 - \$100.
- (8) Under both *Acts*, a government organization is required (with limited exceptions) to respond to an FOI request within how many days after receiving the request and the fee?
- 15 days;
 - 30 days;
 - 60 days;
 - 100 days.
- (9) If a provincial or local government organization denies a requester access to the information he or she is seeking, which of the following can the requester file an appeal to:
- The Ministry of Municipal Affairs and Housing;
 - The Ombudsman;
 - The Information and Privacy Commissioner of Ontario;
 - The Premier.
- (10) Does the organization that a requester can appeal a government office's access decision to have the authority to order the government organization to release the records sought by the requester?
- Yes.
 - No.
 - All of the above.
 - None of the above.

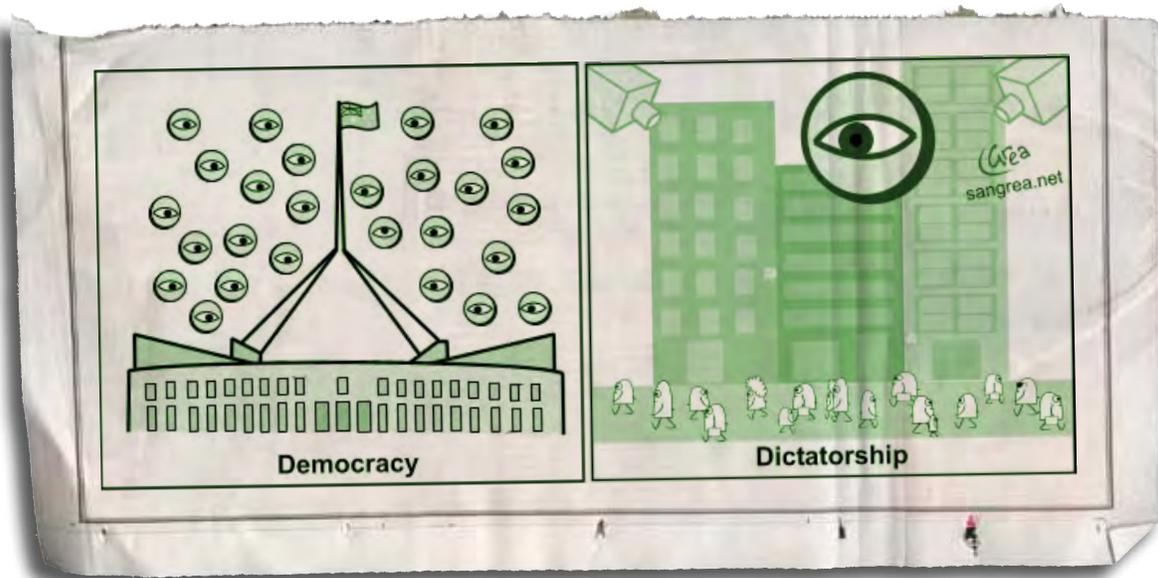
Source: Information and Privacy Commissioner/Ontario – www.ipc.on.ca

ACTIVITY 1: ANSWER KEY: FREEDOM OF INFORMATION QUIZ

- (1) (d) All of the above;
- (2) (a) Most of the information held by local government organizations, with limited exceptions;
- (3) (d) All of the above; (Such a decision, however, could be appealed to the Information and Privacy Commissioner.)
- (4) (c) Freedom of information co-ordinator;
- (5) (d) Both (a) and (b);
- (6) (b) No;
- (7) (a) \$5 fee;
- (8) (b) 30 days;
- (9) (c) Information and Privacy Commissioner of Ontario;
- (10) (a) Yes. If the Commissioner upholds the appeal, she has the authority under the Acts to order a government organization to release records requested under FOI.

ACTIVITY 2:

ANALYSING POLITICAL CARTOONS: Democracy vs. Dictatorship



Complete the following questions for the political cartoon above.

Step 1: Interpreting the Cartoon

1. What is the title and/or caption of the cartoon? Is it an ironic or sarcastic title? Explain.

2. Describe the objects, symbols, people, or characters in the cartoon. What is their mood?

3. To what issue, event or theme is the cartoon related?

Step 2: Evaluating the Cartoon

4. What is the cartoonist's view of the issue, event or theme? Is it biased for or against issue? Is it a positive or negative view? Explain.

5. What message is the cartoonist trying to convey about the role of the people and/or government?

6. Determine if the cartoonist's message is effective? Explain your answer.

7. According the cartoon, what is the key difference between a democracy and a dictatorship with respect to open government and individual rights?

ACTIVITY 2:

COMPARING ACCESS TO INFORMATION

Read the **two** articles, *Ottawa Bans Chemical Used in Soft Vinyl Toys; Voluntary Plan Failed*, and *Chernobyl: Once and Future Shock*. As you are reading, pay attention to the freedom of information laws in each society.

OTTAWA BANS CHEMICAL USED IN SOFT VINYL TOYS; VOLUNTARY PLAN FAILED

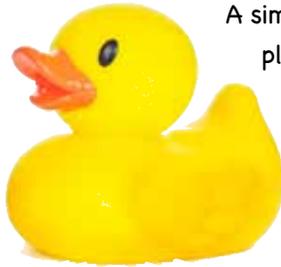
Sarah Schmidt
CanWest News Service
June 20, 2009

OTTAWA - Conceding that a decade-old voluntary ban on hormone-disrupting chemicals in children's toys has not worked, Health Canada yesterday announced new regulations requiring companies to get phthalates out of soft vinyl toys.

The proposed ban will prevent the use of six phthalates in bath toys, teething rings, rattles and other children's products, such as vinyl bibs. The chemical additive, used to soften toys, can cause reproductive problems.

Health Canada is taking the step after its own market survey last year found the widespread presence of phthalates in soft plastic toys and other items for young children that are likely to be mouthed, such as rubber ducks.

The results, released to CanWest News Service under **access to information laws**, found elevated levels of phthalates ranging from 0.2 to 39.9% by weight of the plastic known as polyvinyl chloride in three-quarters of the items - 54 of 72 of the children's products tested.



A similar phthalates ban has been in place in the European Union since 1999, where concentration levels cannot exceed 0.1% in children's products. A ban in the United States came into effect last year.

The new regulations will also effectively ban lead in children's products by proposing a maximum of 90 milligrams of lead per kilogram of product, or 90 mg/kg. The current lead limit for toys intended for children under three years old is 600 mg/kg total lead.

The government won praise from nearly all corners yesterday.

"This is great news for parents," said Aaron Freeman, policy director for Environmental Defence, which has been lobbying for a ban for years.

Judy Wasylycia-Leis, health critic for the New Democrats, first raised the issue back in 1997 when she was first elected.

"It's good news. Finally, the government has acted. It's been a long, hard struggle. I think the science has been in for a long time."

- Published in the National Post, June 20, 2009

CHERNOBYL: ONCE AND FUTURE SHOCK

ON APRIL 26, 1986, THERE WAS A MAJOR ACCIDENT AT THE CHERNOBYL NUCLEAR POWER STATION, LOCATED IN UKRAINE ... SOUTH OF THE BORDER OF BELARUS. AT THAT TIME, BELARUS AND THE UKRAINE WERE PART OF THE SOVIET UNION (THE UNITED SOVIET STATES OF RUSSIA - U.S.S.R.). THE ACCIDENT RESULTED IN THE RELEASE OF LARGE QUANTITIES OF RADIOACTIVE SUBSTANCES INTO THE ATMOSPHERE AND HAD DEVASTATING EFFECTS ON THE POPULATION, LIVESTOCK AND THE ENVIRONMENT.

A liquidator's story

This article was first published in Index 1/9 by Index on Censorship (www.indexoncensorship.org), which granted permission for it to be reprinted.

For the first time in print, a Belarusian scientist gives his personal recollections of the secrecy that, in the crucial period immediately following the Chernobyl accident, left the unsuspecting public exposed to fallout.

On the Monday morning, 28 April, at the Nuclear Energy Institute of the Belarusian Academy of Sciences, I switched on the apparatus – the gamma-spectrometer and the dosimeters: everything was (in physicists' slang) 'hot,' which meant that there had been a big nuclear accident on the Institute's premises: our dosimetrist ran out of the laboratory, and reported that the level in the yard was about 300 microroentgens an hour. Then he was summoned by telephone to monitor the radiation contamination round the nuclear reactor of the Institute of Radioactive Technology; so that was the main source of the accident! But they had their own dosimetrists there, and the dose level was almost the same; the same was true in the vicinity of a third nuclear device... Moreover, it was clear that the radiation levels fell the further one went inside the building... When the head of the dosimetry service, A Lineva, telephoned the Central Public Health Station of Minsk, they said, 'This is not your accident.'

We looked at the tall smoke-stack, and then at the map of Europe, and we saw that the wind was blowing radiation towards Sweden. In fact, we learned later, on 1 May the level of



radioactive contamination in Stockholm was 17 Curies per square kilometre from Caesium-137, and 87 Curies per square kilometre from Iodine-131.

But in our place, they brought me in a twig from the yard, and I observed that it was emitting radiation...the gamma-spectrometer showed Iodine-11 and other 'young' radionuclides... Later we tested soil and trees from many regions of Belarus, and the Institute started to measure the specific activity of foodstuffs arriving for the Institute canteen and the crèche.

Meanwhile, the dosimetry service headed by M V Bulyha was monitoring the radiation cloud hanging above Minsk.

We started to ring our relatives and friends in Minsk, advising them about safety measures. But this did not last long: at around midday, our telephones were cut off. And a couple of days later, we specialists were called into the Secrecy Department, and made to sign a

29-point document forbidding us to divulge secrets connected with the accident at the Chernobyl-plant. These included the structure of the RDMK-1000 reactor, the amount of uranium, etc, 'secrets' that had already been published in scientific literature.

And meanwhile out in the street, radioactive rain was falling...

We went home from work without looking from side to side; it was painful to see how the children were playing in the radioactive sand, and eating ices.

In our street, I went up to a street vendor and told her to stop selling her sausages, as radioactive rain was falling. But she just said: 'be off, you drunkard! If there'd been an accident, they'd have announced it on radio and TV.' A naive soul, she believed in the righteousness of the Soviet authorities.

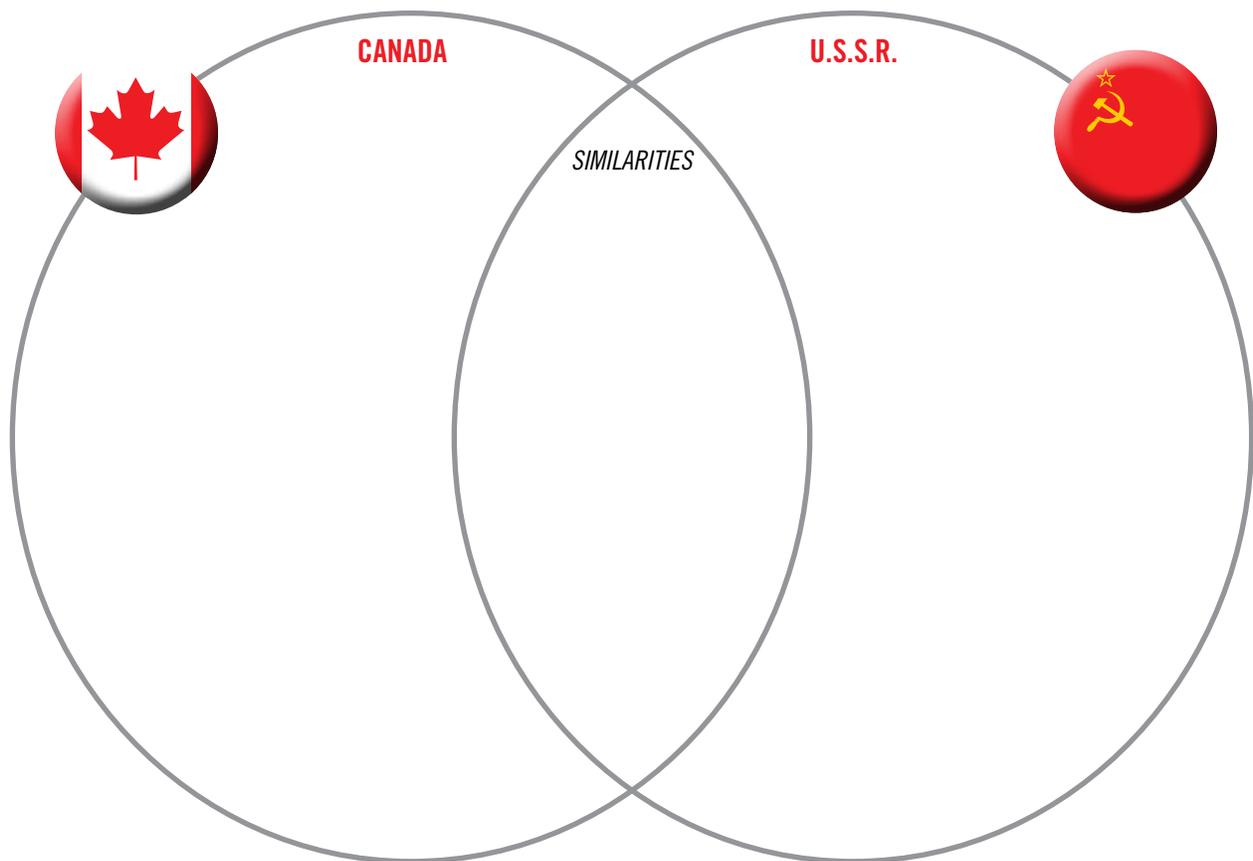
In the evening, on Central TV, Moscow showed us how tractors with great swirls of dust behind them were tilling the soil down in Naroula country, part of which lies in the 30-kilometre zone around the Chernobyl station. Then, on 1 May, as always, children and adults marched in columns through the streets without even guessing at the consequences. So now, today, in Belarus we have some 400 children with thyroid cancer...who at that time knew nothing about Iodine-131...

Mikhail Byckau is a nuclear physicist, who from mid-May 1986 until his retirement from the International Sakharov Institute of Radioecology in April 1995, played an active role in the 'liquidation' (clean-up) and monitoring programmes in the contaminated area.

ACTIVITY 2:

VENN DIAGRAM

Based on the information provided in the two articles, complete the Venn Diagram below to compare the access to information in Canada and the former U.S.S.R. Consider the following points of comparison: type of information known, commitment to open government, consequences of government action.



ACTIVITY 3:

ANALYSING ACCESS TO INFORMATION CASES

A. Individually, answer the questions below using the article provided by your teacher.

Summarize the main idea of the article. Provide some examples from the article.

If a freedom of information law didn't exist, which facts and/or evidence would not be known? What would/might have been the impact?

In your opinion, how effectively was the freedom of information law applied to the issue? Explain.

- B. In your group, complete the PMI chart provided by your teacher to outline the Plusses, Minuses, and Implications of the access to information laws in each of the articles.

PMI

Plusses, Minuses, and Implications

Student(s): _____

+	-	I

Freedom of Information request uncovers diagnostic errors

Sun 30 Nov 2008
BY JEN SKERRITT
The Canadian Press

WINNIPEG – Documents obtained by the Winnipeg Free Press show one Manitoba woman's mastectomy may have been unnecessary and several other patients received incomplete diagnoses after their biopsies went missing.

The incidents occurred months before pathology officials said diagnostic errors were "extremely unlikely."

Documents obtained through a Freedom of Information request reveal that health officials launched seven critical incident investigations into diagnostic errors between July 2007 and March 2008, including the probe into errors made by a veteran St. Boniface Hospital pathologist.

Critical incidents are defined as serious, unintended events suffered by a patient in a health care facility, and are investigated by an internal review committee.

In March, Diagnostic Services Manitoba CEO Jim Dalton denied there were any problems with the province's pathology program and told the Free Press that diagnostic errors or botched tests were "extremely unlikely."

Documents refute that and show that multiple investigations into pathology errors were under way at the time.

In two separate incidents in July and November 2007, groups of samples and specimens were lost which prompted exhaustive searches of a pathology lab and various other health facilities.

As a result, several patients did not receive a complete diagnosis and others had to be retested.

Several other patients had to have a second biopsy after a piece of lab equipment malfunctioned in September 2007. Some patients did not receive a complete evaluation as a result.

A mistake interpreting a breast tumour sample in July 2007 led to one woman being misdiagnosed with aggressive breast cancer.

Subsequent reviews of the woman's case by an Ontario laboratory and second pathologist found there was "no evidence of invasive cancer" and that the woman's mastectomy may have been unneeded.

The woman isn't identified in the documents because of privacy concerns, but documents say the case will be reviewed by her physician.

Another patient did not receive appropriate antibiotics after a follow-up pathology report wasn't sent to that patient's physician last February. The mistake led to an extended hospital stay.

"If we found through one of these investigations that we thought there was an unusual event or unusual risk, we would make it public," Dalton said last week. "But certainly the rate of these incidents is well within the norm I'd put that up against any laboratory in North America."

Dalton said the pathology program is in excellent shape and that these incidents involve a small number of specimens out of the millions that are processed each year.

Dalton couldn't say how many patients may have received an incomplete diagnosis due to lost specimens, but said human error was responsible in the case of the woman who had a mastectomy.

"No errors are good, and we're not trying to gloss these over and say they're OK," he said. "Most reports are timely, accurate, and I think the system works very well and people should have confidence in it."

PUBLIC KEPT FROM 20 PER CENT OF ELTON JOHN CONCERT TICKETS

The Sault Star

Sat Jun 27 2009

Page: A4

Section: News

Byline: DENIS ST. PIERRE, SUN MEDIA;

Nearly 20 per cent of tickets to the now-infamous Elton John concert in Sudbury last year were not available for sale to the public. The information, which the City of Greater Sudbury unsuccessfully tried to suppress, was released Thursday – more than 15 months after the concert was held.

The city spent tens of thousands of dollars in its efforts to withhold the ticket information, which had been requested by The Sudbury Star. After a lengthy process launched by The Star, Ontario's freedom of information commissioner ordered the city to publicly release the information this month.

Despite the ruling that it had wrongly withheld public information--and the huge expense of taxpayers' money in its failed attempt--the city issued a news release Thursday claiming to have achieved victory.

According to the law, a municipality has to pass a three-pronged legal test in order to keep such information private. If the municipality does not pass all three parts of the legal test, it must release the information.

In this case, the province's freedom of information commissioner ruled the city's refusal to release the ticket information did not pass the legal test.

The city's position met two of the required criteria, but failed categorically to meet the third condition. As a result, the city was wrong to withhold the information from the public.

The city's version of the ruling comes across differently. "The city won two of three arguments," the municipality stated in its news release, without specifying it ultimately "lost" the legal test.

The information the city was forced to release shows 1,227 tickets out of a total of 6,386 – just under 20 per cent – were withheld from public sale prior to the Elton John concert of March 2008.

DineSafe cuts rate of sickness; Food-related illness cases have plunged 30% since Star exposed violations in city's eateries

The Toronto Star
 Fri 17 Apr 2009
 Page: GT01
 Byline: Robert Cribb
 Source: Toronto Star

Cases of food-borne illness began to fall almost immediately after Toronto began making restaurant inspection results public in 2001.

Now, eight years after the city launched the DineSafe program that publishes inspection results online and in restaurant windows, cases of individual food-borne illnesses in Toronto have dropped 30 per cent, says a Toronto Public Health report.

It is the clearest evidence yet of the public health benefits of transparency, says John Filion, chair of the city's board of health.

"This is the first time I've seen that food-borne illness took a dramatic plunge after we introduced DineSafe. That shows the public not only has a right to know the results of inspection, but that the public benefits from it. It's just good public policy because it provokes a much higher standard



among the establishments that you're inspecting."

DineSafe was the result of the Star's "Dirty Dining" investigation in 2000 (based on freedom of information requests), which found hundreds of city restaurants had serious food safety violations, from repeated cockroach and mice infestations to food temperature violations that produce bacteria and filthy food preparation surfaces. Yet none of the suspect eateries had been shut down and only a handful had been fined a few hundred dollars.

Worse still, details of those

violations were hidden from the public.

Prompted by the stories and public outrage, then-mayor Mel Lastman ordered an inspection blitz of downtown eateries. Within days, city inspectors had logged hundreds of violations and failed the majority of restaurants they visited.

After a heated political debate that lasted a year, the city adopted a far-reaching disclosure system that posts green, yellow or red signs at the entrance to every restaurant in the city noting the results of its last two inspections.

DineSafe Continued...

More detailed information on every eatery is available on the city's website.

The Toronto Public Health report, to be released today, says DineSafe "resulted in a dramatic increase in compliance with food safety regulations among Toronto's food establishments."

"I do feel it's reasonable to suggest that the DineSafe program in Toronto, which occurred at the same time as we saw a decrease in food-borne illness and an

improvement in food safety compliance, played a role," said Dr. David McKeown, Toronto's medical officer of health.

Prior to DineSafe, compliance with food safety regulations in Toronto restaurants sat at 42 per cent, Filion said.

Today, compliance is more than 90 per cent.

"Clearly, the public benefits of rigorous inspection standards and full disclosure of inspection results were proven in Toronto."

Other cities across Ontario and Canada have adopted similar disclosure models following Toronto's lead. But there remain no mandatory province-wide disclosure rules for local public health units.

"I really can't understand why there hasn't been," Filion said.

"There should be similar standards and the standards should be the ones that best protect the public."

MANY CASES BUT FEW OFFICIALLY RECORDED

1 in 6: people suffer food-borne illness, but fewer than one per cent of cases are officially recorded.

437,093: estimated cases of food-related illness occur annually in Toronto.

102,717: people with symptoms of gastrointestinal illness seek medical care.

26,706: physicians request stool samples from patients.

21,365: patients submit stool samples for testing.

20,297: stool samples are tested by laboratories.

2,395: laboratory-confirmed cases of a provincially reportable disease.

1,928: cases of illness attributable to food reported to Toronto Public Health annually.

Source: Toronto Public Health



Less than 24 hours after “disturbing” Star probe, minister promises new website with reports on individual daycares

Daycare parents triumph

By Dale Brazao, Robert Cribb
and Kerry Gillespie

Toronto Star

May 29, 2007

The wall of secrecy surrounding abuses in daycares has tumbled less than 24 hours after a Star investigation documented troubling problems in centres across Ontario.

Parents concerned about the quality of care their children are receiving in licensed centres will soon be able to visit a ministry website listing serious incidents and inspection findings.

Mary Anne Chambers, Minister of Children and Youth Services, said yesterday her ministry will

launch the website by the fall. Chambers is also considering a stronger colour-coding system in which a red licence posted at a daycare would indicate a serious problem.

Findings of the Star probe included incidents of children being physically assaulted, left to wander away in public places, fed allergy-triggering foods that nearly killed them and being forced to play in filthy surroundings. The Star found numerous cases where daycares with these problems were allowed to remain open, sometimes for years.

The cases were drawn from provincial and municipal records

of inspections, enforcement, complaints and serious incidents, obtained through a series of requests under the *Freedom of Information Act* that took two years.

Chambers called the revelations “disturbing.”

“What I read in the Toronto Star (yesterday) is unacceptable,” she said. “I think parents deserve to be able to access information that relates to their child’s care.”

The proposed website will contain a “more robust form of reporting,” including details on why a centre has a provisional licence – a tool used by the ministry to allow daycares with

Daycare Continued...

substandard conditions to remain open.

There are 57 daycares in the province operating under a provisional licence. White licences mean there are no problems, yellow licences are provisional. Chambers said she favours a stronger colour-coding system, similar to the well-known restaurant rating system. "When you walk up to a restaurant door you see a red label on that door and you know there's a problem. We can do that," Chambers said.

In the wake of the Star investigation, parents across the GTA flooded the newspaper with phone calls and emails with a clear message for the Ontario government: When it comes to children's safety and well-being, there should be no secrecy.

If daycares are dangerous, dirty or allow children to wander off unattended, parents should know about it, they said.

"It's a no-brainer," said Andrew Stalony, who recently entrusted care of his 15-month-old son, Ryan, to a daycare in Mississauga. "There is no question we should have the right to know what's going on. You're letting someone else take care of your child."

During Question Period at the provincial legislature yesterday, Chambers was attacked by both opposition parties for hiding

the problems at daycares. "The minister and her government made efforts to keep this information under wraps for two years," Progressive Conservative Leader John Tory said, referring to the length of time it took the Star to get the information.

Chambers denied this, noting that daycares with provisional licences are required to hand out a government pamphlet titled *Attention Parents. This centre does not meet all the requirements of the Day Nurseries Act.*

She also said the province has hired more inspectors and now conducts unannounced reviews of daycares as well as the annual inspections. The changes protect children better, she said.

The minister said she also favours posting the data collected by the ministry on serious occurrences at daycares – ranging from children who were temporarily missing to abuse allegations, which daycares must report to the ministry.

"I agree the serious occurrences should be there. I really do want to take a look at our ability to report any kind of serious occurrence. One of the things we have to be cognizant (of) is volume of data and ability to manage 4,000 pieces of data online."

The Toronto Star investigation, based on thousands of daycare

incidents, inspection reports and complaints, uncovered serious problems including children wandering off unattended, being forcibly confined in closets and storage rooms, and being served meals prepared in mice-infested kitchens. There were 5,814 serious occurrences reported by licensed daycares across Ontario in 2005-2006, including nearly 3,000 injuries, 674 missing children reports and 675 allegations of abuse or mistreatment, according to data analysed by the Star.

One parent who contacted the Star had tried on her own to obtain similar information. Karen Krawec said she eventually gave up in frustration after trying to get information on daycare centres in York Region to help her decide whom to entrust with the care of her young son.

"I was first told that I would not be able to access the information," Krawec said. "Later on when I quoted the *Freedom of Information Act*, I was advised that it would be a lot of work to dig up all of the records so I would have to pay the hourly wage.

"They said it would cost hundred of dollars and (take) several months," Krawec said. "After consulting my MP, who did nothing for me, I finally gave up."

Daycare Continued...

Lisa MacLeod, Tory MPP for Nepean-Carleton and her party's critic on children and youth, said there has to be absolute transparency for government-run daycares. "If we're going to be doing this for restaurants, we should be doing it for daycares," she says. "We are dealing with the physical safety and emotional well-being of our children."

Under the province's Day Nurseries Act, daycares are required to post their licence inside the daycare, where parents can see it. Provisional licences must also be posted, allowing parents to see issues in which the daycare is failing to meet minimum provincial standards.

But posting licences isn't nearly enough, say parents.

Carrie Makins has been shopping for a daycare for her two children without much information to work with, she says. "The only way of sourcing daycare is by my gut feel and word of mouth.

Really, there is no information and no transparency for parents and that's unfair, because they're taking care of our kids for 40 hours a week and that's a huge influence on their life.

"You're paying these people to take care of the most precious people in your life; you need to make sure they're in good hands."

"The state of daycare in this country is appalling both in terms of the space available and the unhealthy conditions presented," said Deborah Wilson, whose daughter is in a downtown daycare.

"To think that a daycare facility can continue to operate on a provisional licence is devastating to me. I truly hope that this article will reinforce to our government that decisive action needs to be taken to improve daycare in this country."

Julie Wallis, whose two grandsons are cared for in a Toronto daycare,

says Canadians are "burying their heads in the sand" on the daycare issue. "A website put forward by the provincial government is needed."

Transparency would force daycares to be more vigilant about maintaining standards, says Teresa Wong, who has a 4-year-old in daycare. "It would also make them clean up their act if they knew somebody was watching," she said.

"People forget this is a service industry and the client is the child," said Anne Eisenberg. "That's the problem, the focus isn't on the child. We lost that a long time ago.

"It's a money issue."

Daniela Fiacco, who operates the Columbus Children's Centre, says she supports parents' requests for information. "Our records are there. If parents want to see them, we let parents look at them. We have nothing to hide."

ACTIVITY 4:

GOVERNMENT TRANSPARENCY PLEASE!



A. ANALYSING EDITORIALS

What is an editorial?

- The editorial serves as the official view of the newspaper, after editors consider many sides of an issue. It is usually the opinion of the newspaper's editorial board.

Content

- deals with a current issue that is affecting people;
- may attempt to influence, by giving readers all of the facts and concerns;
- offers suggestions and indications as to outcomes;
- at major newspapers, the opinion, if offered, will not be an extreme view, it will usually be well prepared and informed, taking into consideration many aspects from both sides of the debate.

Construction

- official view of the paper, so it is wisely thought out;
- clear and concise wording; usually free of emotive terms;
- usually balanced, presenting all aspects of the situation/event/issue;
- written on an important topic, often a deep-seated problem, one that is likely to be of interest or concern to many readers;
- does not normally include reported speech.

Source: Revised by IPC from original posted at <http://www.ohassta.org/resources/politics.htm>

B. SHINING A LIGHT ON THE PMO

The issue of government accountability and transparency is a hot political issue. Examine a recent editorial below and answer the questions that follow to analyse the author's message and style.

The Hamilton Spectator

By: Lee Prokaska

Robert Marleau should indeed release his dogs into the Privy Council Office.

The federal information commissioner, who is about to retire, is threatening to seize documents from the Privy Council Office, which supports the Prime Minister's Office and cabinet. Marleau is unable to proceed with 150 access-to-information complaints because he can't get the information he needs to do so.

He could seize the files he needs as early as this week. And what a show that would be.

As Canadians, we pride ourselves on our system of parliamentary democracy. We believe in openness, in defaulting to disclosure, in distinguishing ourselves from other nations where secrecy is both the common practice and the accepted norm. The spectacle of an information commissioner raiding the highest bureaucratic office in the federal government in no way fits with our self-image.

And Marleau should not be forced by lack of co-operation or otherwise – to exercise the considerable legal powers of his office. The Privy Council Office should not be closed to Canadians seeking information, as we have the freedom to do under the federal **Access to Information Act**. It is a bad situation, both in fact and in appearance.

Prime ministerial secrecy is not new; the late Pierre Trudeau kept information on a reasonably

tight leash. That leash grew even tighter under both Brian Mulroney and Jean Chrétien, but it is safe to say that Stephen Harper's office seems the most secretive when it comes to controlling the flow of information. Given that Harper's government has, so far, a pretty solid track record, the pathological need to control is worrisome. The level of resistance to releasing information works against Harper and his cabinet, suggesting there must be something worth hiding. It suggests smoke, leaving Canadians to wondering how bad the fire is.

The apparent need to control and to set itself up as being above the federal watchdog seems to mirror a growing desire from within to see the Prime Minister's Office, the Privy Council and cabinet as an executive branch of government in the image of the U.S. presidency. That executive branch approach, while entrenched in the United States, is not part of Canada's founding history. But it may be part of the reason behind the growing adversarial, dysfunctional nature of our Parliament, which has seen its governing functions increasingly stripped away.

It is interesting to note, though, that Marleau pointed out earlier this year that Canadians know less than ever about what its government is doing, in sharp contrast to U.S. President Barack Obama's push for openness in the United States.

Certainly releasing information can be uncomfortable, and messy questions may follow. But those who govern -- federally and provincially -- must remember that they work for us. When we want to know what's going on, we should not be hearing "No" over and over again. Marleau is right to keep pushing on our behalf.

Source: Prokaska, Lee. *The Hamilton Spectator*. 29 Jun 2009: A12.

COMPLETE THE QUESTIONS BELOW.

What opinion does the author have about government transparency?

What arguments and/or evidence does he provide to support his opinion?

In your opinion, how effective is his argument? Explain.

Identify the stylistic devices that the author uses to support his opinion. Consider devices such as facts, allusions, comparisons, metaphor, loaded language, repetition, etc. Are they effective?

CULMINATING TASK:**DESCRIPTION**

Popularized by Canadian comedian, Rick Mercer, a “rant” is the sister to the soliloquy (monologue) and distant cousin of debate; it is an individual self-expression, or more simply put, an opinion. It is something that the “ranter” thinks should be known, and they’re not afraid to tell you about it. A rant is usually done with wit and humour, at the same time expressing a position, a stance, or an issue that you think is important. The viewers should be entertained, but at the same time are left with a lasting impression about the topic. A good rant usually includes the following:

- **A topic that is current** – the topic should not be threatening, not include profanity or malign an individual or organization’s reputation;
- **Clear and concise message;**
- **Effectively convinces the audience of your opinion;**
- **Clear structure:**
 - **Intro** – Establish the topic of the “rant”
 - **Middle** – Provides a challenging statement which makes the listener/viewer think....The “AHA!” moment;
 - **End** – Wrap up with a statement that leaves the listener/viewer with an understanding of the topic.

Source: Memorial University - <http://www.mun.ca/rant/>

PURPOSE

- To apply knowledge and concept attainment from unit four in a culminating task;
- To demonstrate democratic participation.

TASK

Your task is to plan, develop and create a one to two minute “Rant” about one of the issues raised in the unit.

INSTRUCTIONS

During this activity, you will work in groups of three or four to plan, write, create and present a one to two minute “Rant” that will address access to information laws. In your group, consider issues that have been addressed in this unit.

STEPS

1. **Topic Selection.** Choose from one of the access to information topics addressed in the readings:
 - government spending;
 - Office of the Prime Minister;
 - health;
 - education;
 - environment;
 - labour;
 - freedom of information laws;
 - your own idea – please see teacher for approval.
2. **Planning.** Use the *Planning Your “Rant”* handout to outline your “Rant.”
3. **Create.** Create your “rant” and present it to the class for teacher evaluation. If you have access to a DVD camera and are comfortable with its use, you may want to videotape your “Rant.”

ASSESSMENT

- *Planning Your “Rant”* Outline

EVALUATION

- “Rant” Rubric (**Appendix 4.15**)

CULMINATING TASK: PLANNING YOUR “RANT”

Use the following guidelines and questions to help you plan and develop your “Rant.”

1. My topic is: _____
2. My purpose is: _____
3. My audience is: _____
4. My research collection (facts that I have learned to give my Rant credibility):

	Source
	Source
	Source
	Source

5. For each point, you may provide encouragement, hints and/or cautions. For example, use the following starter statements at various times in your rant.

- Don't worry if...
- Make sure you...
- If you feel...

6. Check off the stylistic devices you plan to use:

- | | |
|--|--|
| <input type="checkbox"/> allusion | <input type="checkbox"/> personification |
| <input type="checkbox"/> alliteration | <input type="checkbox"/> quotation |
| <input type="checkbox"/> anecdote | <input type="checkbox"/> rhetorical question |
| <input type="checkbox"/> effective repetition | <input type="checkbox"/> satire |
| <input type="checkbox"/> facts | <input type="checkbox"/> simile |
| <input type="checkbox"/> humour | <input type="checkbox"/> statistics |
| <input type="checkbox"/> hypothetical scenario | <input type="checkbox"/> word invention |
| <input type="checkbox"/> illustrative example | <input type="checkbox"/> other |
| <input type="checkbox"/> metaphor | |

7. What visuals/props will you use?

8. Decide on the following:

- Tone;
- Volume;
- Emphasis;
- Variation in speed;
- Repetition.

9. Decide on the mannerisms and/or actions that might accompany your “Rant.” Use facial expressions and body language to convey your message effectively.

10. Practice, practice, practice!

11. Present your “Rant” to the class for evaluation. If you have access to a DVD camera and are comfortable with its use, you may want to videotape your “Rant.”

CULMINATING TASK RUBRIC:

"RANT" EVALUATION

Students:

Mark: /40

Criteria	Level R (0-49%)	Level 1 (50-59%)	Level 2 (60-69%)	Level 3 (70-79%)	Level 4 (80-100%)
KNOWLEDGE AND UNDERSTANDING					
• knowledge of the subject	- rant demonstrates little or no understanding of topic	- rant demonstrates limited understanding of topic	- rant demonstrates some understanding of topic	- rant demonstrates considerable understanding of topic	- rant demonstrates thorough and accurate knowledge of topic
THINKING AND INQUIRY					
• opinion	- rant does not state an opinion	- opinion is weak	- opinion is adequate	- opinion is good	- opinion is excellent
• supporting details (research, visuals, props)	- inadequate supporting details to support opinion	- weak supporting details to support opinion	- limited supporting details to support opinion	- adequate selection of supporting details to support opinion	- excellent selection of supporting details to support opinion
COMMUNICATION					
Delivery: • eye contact • volume • tone • pace • facial expressions • body language • use of stylistic devices	- communicates opinion orally with no effectiveness	- communicates opinion orally with limited effectiveness	- communicates opinion orally with some effectiveness	- communicates opinion orally with considerable effectiveness	- communicates opinion orally with a great degree of effectiveness
• organization	- rant is disorganized, confusing	- rant is not well organized	- rant is organized somewhat effectively	- rant is considerably organized	- rant is highly organized and effective
APPLICATION					
• process	- no outline provided	- incomplete rant outline	- somewhat complete rant outline	- adequately completed rant outline	- thoroughly completed rant outline
• presentation	- did not include rant elements	- limited use of rant elements	- some use of rant elements	- considerable use of rant elements	- thorough and effective use of rant elements
• references	- no sources provided	- reference list incomplete or not properly formatted	- reference list completed but with several errors	- reference list completed with minor errors	- reference list completed and properly formatted