

**CYBERETHICS IN ACTION: COPYRIGHT, PRIVACY, AND MEDIA
AWARENESS TEACHERS' GUIDES**

by

ARTHUR PUI-KIN LEE

A project submitted to the Faculty of Education
in conformity with the requirements for
the degree of Master of Education

Queen's University

Kingston, Ontario, Canada

September, 2010

Copyright © Arthur Lee, 2010

Abstract

New advancements in Information Communication Technology (ICT) have greatly impacted the way people interact with one another and the world. While ICT has led to many improvements, a number of problems involving ICT have also emerged, such as copyright infringement. These issues do not always experience the same level of moral adherence as their real world counterparts. For example copyright violations are not always associated with theft. The area of cyberethics examines these updated attitudes towards morally and ethically dubious acts and recommends cyberethics education for teachers to teach students ethical behaviour and values. Drawing from available literature, documents published by federal and private organizations, and credible online resources, this project develops three guides for instructors regarding the issues of: copyright, privacy, and media literacy. Each guide provides instructors with background information, lesson plan ideas, and additional resources for research and instruction. In this way, this project develops a useful tool to help instructors improve cyberethics education and address issues in ICT.

Acknowledgments

The creation and completion of this project would not have been possible without the help, time, support, and dedication of several incredible individuals. I would first like to acknowledge my supervisor Dr. John Freeman for his tireless support, guidance, and assistance. His feedback and understanding have allowed this project to succeed and his guidance throughout my academic career at Queen's has helped immeasurably.

Secondly, I would like to acknowledge Dr. Ruth Rees for her assistance as my second reader. Her feedback and hard work are greatly appreciated and have contributed greatly to the completion of the final project.

I would also like to acknowledge my wife Joscelin for her continued support and assistance throughout the project and my degree. She has always been there to support and motivate me through any difficulty or obstacle. I could not have done this program without her.

Finally, I would like to acknowledge all of my friends and family who have helped me through this time. Although they may never read this project, their friendship and support have made it possible.

Table of Contents

Abstract	ii
Acknowledgments	iii
Table of Contents.....	iv
Chapter 1: Introduction and Literature Review	1
Literature Review.....	3
History of Computer Ethics.....	4
Issues in cyberethics.....	7
Why teach cyberethics?	9
Who should be taught and why?.....	10
Computer ethics and education – What is being done?	15
How should cyberethics be taught?.....	22
Summary	26
Chapter 2: Teachers’ Guides.....	28
Teachers’ Guides Overview.....	28
Concerning Copyright: Teachers’ Guide to Copyright.....	30
Background information.....	30
Activity and lesson ideas.....	37
Additional resources.....	42
Glossary of terms.....	44
Protecting Privacy: Teachers’ Guide to Privacy	45
Background information.....	45

Activity and lesson ideas.....	50
Additional resources.....	55
Glossary of terms.....	57
Unmasking Media: Teachers' Guide to Media Awareness.....	58
Background information.....	58
Activities and lesson ideas.....	61
Additional resources.....	69
Glossary of terms.....	71
Chapter 3: Discussion.....	72
Research Connections.....	72
Directions for Further Study.....	75
My Project Experience.....	76
References.....	78
Appendix A: Copyright Scenarios.....	84

Chapter 1: Introduction and Literature Review

I remember myself as a young boy in 1992 owning my first computer, which my father had bought for me. “Learn to use this!” he said to me. “These can be very useful.” Useful indeed! I quickly learned how to install and run many computer games, which I would spend hours playing. Although not what my father had originally intended, those computer games did allow me to develop some basic computer competencies and eventually I would use more productive software, such as word processing and paint programs, almanacs, and encyclopedias, to complete school projects. Soon after, I began using the Internet through dial-up service providers like AOL (America Online) and a new world of connectivity opened up for me. My friends and I would surf the Internet reading the latest news and downloading pictures about things in which we were interested. It wasn’t until my friend received a \$200 phone bill that we realized there were dangers involved with this new technology.

Much has changed since those first days using computers and the Internet. Accessibility and speed have greatly improved, costs have lowered, and Internet use has become commonplace. The dangers involved in using computers and the Internet have also changed dramatically. Since the days of overcharged Internet access fees I have encountered stories and experienced problems regarding websites being hacked, privacy invasions, identity theft, copyright violations, computer viruses, cyberstalking, and a host of other computer-related issues.

I began to wonder who could be committing these malicious acts and for what reasons. Because of these threats, the Internet today can appear to be a dangerous place – seemingly ungoverned by any laws and morally and ethically vacant. As an educator, I started to worry how these developments might affect students and children growing up in this environment.

As part of a younger generation of individuals who have grown up with this technology, I have noticed that we are often more skilled, competent, and experienced at using computers and the Internet than older generations. Like I did myself, many young children seem to discover and explore the Internet without supervision and guidance from parents and guardians who are less adept at using new technology. While parents, guardians, and other adults are available in real-world settings to maintain and direct appropriate ethical and moral standards, the Internet lacks a similar system of supervision and instruction. In such a potentially hostile and free environment as the online world of the Internet, I began to wonder: Who is available to teach these children appropriate social conventions and good values? What values are unsupervised children learning by themselves? What are some of the important issues that need to be considered? How can the education and instruction of morally and ethically appropriate online behaviour be achieved?

As teachers who spend a great deal of time with children, a great opportunity to teach computer skills and behaviours is available. To take advantage, quality resources are needed to achieve instruction.

The purpose of this report is thus to explore some of the questions above and, based on evidence gathered through a review of the literature, develop a set of

guides for teachers to use in aiding the development of students as competent, capable, and morally and ethically good members of the online community.

Literature Review

Since the invention of the first computing machine to the creation of the Internet as a military network, the proliferation of technology use for communication, entertainment, and labour has steadily increased (International Telecommunication Union, 2009). The year 2010 marks the first time that Internet use has surpassed television use (Ipsos Reid, 2009), a feat that is not surprising when one considers how computer and Internet use have become commonplace and integrated into almost every component of people's lives in the modern world. The increased use of Internet technology, commonly referred to as ICT (information communication technology), has naturally led to examinations of its effects on individuals' lives and society across the world. While advancements in ICT have had many positive effects such as information accessibility, improved communication, and greater efficiency, these advancements have also led to a number of social issues (Dill & Anderson, 2003). Among some of the most notable problems are those concerning copyright and intellectual property violations, violations of privacy, and Internet safety. These issues all share similarities with more traditional moral problems and comparisons have been made to theft, vandalism, and threats to personal safety and security (Johnson, 2001; Tavani, 2002).

As a result of these problems, one area of intense interest concerns the ethical use of ICT in what has been called computer and cyberethics. This review

examines what computer and cyberethics are, whom it affects, and why and how they should be taught.

History of Computer Ethics.

The rise of the computer inevitably led to the field of computer ethics as scientists and researchers began to question and consider the impacts that new technology would have on society. Among the first to consider these issues was Norbert Wiener, a philosopher and scientist who began to identify the potential influence of computers during World War II (Bynum, 2008). Since computers were used in weaponry, which allowed complex decisions to be made without human intervention, Wiener realized the potential for good and evil and predicted a dramatic change to the world in the form of a technological revolution. Wiener would go on to write two books that would lay the foundation for information and computer ethics. In his work, he describes three key ethical principles by which people should live by: freedom, equality, and benevolence. By applying these principles to ICT, Wiener questioned the role of these technologies in society. As explained by Bynum (2000), Wiener explored how ICTs should be ethically integrated, potential ethical consequences and how to deal with them, and the obligations and responsibilities of people who engage with these technologies. For example, Wiener suggested the inclusion of professional guidelines to prevent unethical ICT use, and he speculated that the automation of tasks threatened to replace human workers and lead to unemployment. He also explored the concepts of ownership and intellectual property of technology and ideas, and the potential implications computer ethics would have on law and justice (Bynum, 2000).

The next major milestone came from Walter Maner in 1976 while teaching a medical ethics course. There he noticed that, when computers were involved, new ethically important considerations arose, and a need for a separate branch of applied ethics was required. He coined the term “computer ethics” to describe this field and developed and published *A Starter Kit for Teaching Computer Ethics* (1980) to educate others. A large amount of work investigating computer ethics soon followed.

Around the same time, the ACM (Association for Computing Machinery) began proposing the introduction of ethical considerations into the curriculum. Founded in 1947, the ACM established itself as the world’s first scientific and educational computing society and has become an important component of computer education, accreditation, and advancement in the computing profession. By 1991, ethical considerations were cemented in the curriculum and, since that time, the ACM Code of Ethics and Professional Conduct has become an integral part of the computer profession (Canosa & Lucas, 2008).

Moor (1985) describes computer ethics as “the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology” (p. 1). In his view, Computer Ethics (CE) problems arose because computers provide new capabilities, which lead to new choices. These new choices cause a policy vacuum, as there are no existing or adequate policies governing conduct. Additionally, these problems are different enough from traditional ones that a simple application of an existing ethical theory cannot be done, or is insufficient. What results is a “conceptual

vacuum” requiring new conceptual frameworks. Moor gives an example concerning intellectual property that makes this idea abundantly clear: The objective is to create a policy to protect a computer program as intellectual property. At a glance, this protection may seem simple but soon a number of questions are raised. What is a computer program? Can an idea or algorithm be owned? Is it the expression of the idea that is owned or is it the process? The problem is clearly not easily answered and existing ethical theory cannot be used to solve it; new frameworks must be developed to address these conceptual and policy vacuums. Computer ethics examine these vacuums and provide understanding and guidance on appropriate courses of action.

Also in 1985, Deborah Johnson published an extremely influential book, *Computer Ethics* detailing her perspective of ethical challenges involving computers, covering topics about computer software, privacy, and the social impact of technology. Unlike the position held by Moor and Maner, Johnson did not see modern ICT problems as entirely new. This difference of opinion erupted into a lengthy debate regarding the uniqueness of ICT problems, which has called into question the very legitimacy of CE as a field of study (Tavani, 2002). Despite the controversies regarding the nature of ICT problems and traditional ethics, Johnson’s book helped establish CE and bring CE issues to the forefront of technology discussions.

Today, the area of study and interest in CE has increased exponentially, opening up several branches of study including information and cyberethics. Information ethics (IE) is a component of CE that seeks to establish a foundation by

taking a macro ethical approach and examining information, information systems, and reasoning for determining ethical behaviour (Floridi, 1999). Conversely, cyberethics is a much more narrow area of study that focuses on specific behaviour and interactions that occur in the online realm. Cyberethics has been described as “a system of standards that prescribe morality and immorality in cyberspace, signifying the preservation of freedom of expression, intellectual property, and privacy” (Ki & Ahn, 2006, p. 2).

While both computer ethics and cyberethics deal with moral issues, there are subtle and important differences between the two. Unlike computer ethics, which also deal with the more physical aspects such as computer hardware and software, cyberethics deals primarily with the online world in which interaction takes place. Rather than considering ethical standards of creation, design, and implementations, cyberethics is concerned primarily with the ethical usage of the programs and systems that have been made. In other words, cyberethics is concerned with how technology is used, more than what technology can do. Some of the most frequently cited problems in cyberethics are ones concerning intellectual property rights and copyright infringement, issues of privacy, and media literacy.

Issues in cyberethics.

While there are a growing number of issues in cyberethics, this literature review focuses on three specific areas of interest. Copyright infringement, privacy concerns, and media literacy were chosen as they represent some of the most prevalent and concerning topics at this time.

Copyright infringement concerns have been present since the invention of the printing press and were a major contributing factor for the requirement of copyrighting (MacQueen, Waelde, & Laurie, 2008). However, with the transition of information storage to a digital medium, new and intensified concerns have emerged. The ease and speed with which information can be copied, and copyright violated, have resulted in new problems and considerations that include ownership of computer programs (Johnson, 2001), exceptions for social institutions (MacQueen et al., 2008), and a debate between the rights of creators and the freedoms of individual expression (*Dowling v. United States*, 1985). To compensate for these new developments, legislation continues to be enacted to protect the works created whether they are printed text or digital video.

Invasions of privacy and privacy protection are a second considerable area of interest in cyberethics and involve the balance between safeguarding one's personal information and the information needs of others (e.g., information collected by the federal government for tax purposes) (Johnson, 2001). Similar to the issues of copyright, the digitization of information has increased the fragility of privacy as information has become increasingly less secure and easier to duplicate and access (Thompson, 2001). Increased use of the computer and the Internet for social networking, online shopping, and general webpage surfing has created vulnerabilities in information security and opportunities for greater access to personal information. Additionally, novel information tracking techniques such as data mining threaten to invade privacy further (Tavani, 1999). Issues occurring from breaches in privacy security include problems such as cyberstalking, identity

theft, and computer fraud. As a result, many have recommended the diligent defence of personal information (MacQueen et al., 2008; Media Awareness Network, 2010).

The final issue considered is that of media awareness or media literacy. A response to the marked increase in media messages, forms, and techniques, media awareness and literacy aims to protect people from being unknowingly swayed, coerced, and manipulated by media. Defined as “the ability to access, analyze, evaluate and communicate messages in a wide variety of forms” (Aufderheide & Firestone, 1993, p. 7), media literacy’s goal is to create critical citizens who create positive social change through democratic action and creation of media (Kellner & Share, 2007; Thoman & Jolls, 2004).

Why teach cyberethics?

The question of whether moral education should be in schools has had a long history of debate. But as schools are social institutions, the teaching of ethics is commonplace whether acknowledged through character and virtue education programs or implicit in teacher and student attitudes and imbedded in the hidden curriculum (Robertson, 2005). The core reasons for teaching cyberethics are essentially the same as teaching any other ethics – to uphold and impart societal values, to promote respect for one another, and to encourage ethical decision-making.

However, knowing that ethics are involved in ICT does not necessarily mean that cyberethics must be taught. Some may question whether or not cyberethics are any different than traditional ethics and, if not, whether they need to be taught in school at all. This very concern has been raised in the “uniqueness debate” between

“philosophers” such as Maner and Moor, who assert that ICT causes new ethical problems that cannot be understood with existing frameworks, and “traditionalists” like Johnson who insist that nothing new or special exists in ethical issues involving computers (Tavani, 2002).

In either case, the fact that so much debate and discussion have occurred legitimizes computer ethics and cyberethics teaching and provides strength to arguments for its inclusion in the curriculum. If in fact there is no difference between cyberethics and traditional ethics, there should be no reason to prevent its inclusion, as ethics involving ICT can serve as more modern and relevant examples. On the other hand, if there is a difference between cyberethics and traditional ethics, new frameworks, discussions, and education should be taught to benefit students. As teachers are increasingly incorporating and relying on technology to improve education, the inclusion of cyberethics seems to be the next logical step.

Who should be taught and why?

Beyond traditional ethics of right and wrong, several reasons exist as to why the specific need for cyberethics exists; these reasons become exposed when looking at who needs cyberethics education the most. For example, in an age where 100% of eighth grade students surveyed believe that online social networking is “an important life skill” (Nguyen, 2009, p. 1663), ICT has become a dominant force. For most adults, this change is apparent, with old skills being adapted and applied to new environments. The group that computer and information ethics may have the most impact is on the younger generation of individuals who have grown up not knowing a time without the modern ICTs of today. Dubbed “digital natives”

(Prensky, 2001), these individuals have been immersed in a media and technology rich environment since birth, and are adept and capable of using these new technologies.

Prensky (2005) argues that simple immersion prepares these young people to effectively navigate their ICT-rich environments. Others, however, are not convinced it is that simple and have argued that, although technology may be embedded in students' lives, the skills to effectively use them may not be (Bennet, Maton, & Kervin, 2008). Contrary to what Prensky suggests, Bennet et al. found that, while a large proportion of young people are highly adept with technology, a significant proportion of young people do not even have access to it. The researchers argue that sweeping generalizations cannot be made, as "there is as much variation within the digital native generation as between the generations" (p. 5). Moreover, Bennet et al. found no clear evidence that young people learned differently or better. They concluded that, while some "digital natives" may be adept at using technology for everyday tasks, these skills do not necessarily translate to academic tasks, do not indicate improved critical thinking, and cannot be applied to all students. As incidents involving cyber crimes and violations of privacy and intellectual properties continually appear in the news (ETPRO, 2009), one cannot simply assume young people are fully capable of navigating cyberspace safely and ethically.

Even teachers make false assumptions about the abilities of young people. Kafai, Nixon, and Burnam (2007) found that preservice teachers had difficulty explaining student behaviour regarding computer and Internet use. This finding is

especially important considering teachers are at least partially responsible for the ethical education of young people (Choulat, 2010). While the study found that preservice teachers at times could predict students' judgments of appropriate behaviour (e.g., it is inappropriate to copy text from the Internet to finish an assignment), they could not explain or predict the students' justifications. The majority of teachers predicted that students' reasoning for the unacceptable behaviour would be due to social conventions. For example, copying from the Internet violates copyright laws against plagiarism, or using the computer for non-work related tasks violates classroom rules. However, students tended to justify their behaviours based on more personal reasons. For example, copying text from the Internet was wrong, unless it helped them improve their grades or do better in school.

The differences in teacher prediction versus student justification are important for several reasons. First, it shows that, even if students are displaying appropriate behaviour, the reasons may vary and assumptions cannot be made. Second, it highlights the fact that students' beliefs may differ from the ethical standards and social conventions that preservice teachers follow and a better understanding of the beliefs is needed. Finally, it indicates that ethical issues are complex, and teachers cannot simply rely on a list of rules for students' understanding.

In addition to the failed assumptions that teachers may make regarding student abilities, ICTs have revealed issues that increase the complexities of moral reasoning in cyberspace. One such challenge is the online disinhibition effect

suggested by John Suler (2004). He argues that, as a result of changes in the way people interact on the Internet versus face-to-face, a shift in behaviour has been noticed where people are less restrained and express themselves more openly. People share secrets and personal information that they would customarily not, and it can even result in unusual acts of kindness and generosity, or what Suler calls benign disinhibition.

However, this disinhibition phenomenon can also result in negative manifestations, also called toxic disinhibition, such as rude language, threats, crime, and violence. The distinction between these two is not always clearly defined and what begins as benign may end up being toxic. As examples, a harsh criticism may be therapeutic; an initially open remark may end up being embarrassing later.

Suler (2004) argues that this complex effect is the result of at least six factors brought about through ICT, which include: dissociative anonymity, invisibility, asynchronicity, solipsistic introjection, dissociative imagination, minimization of status and authority, and individual differences and predispositions. Together, the factors combine to give users a feeling of anonymity and a freedom from responsibility and authority. As a result, an almost alternate identity is created in which individuals possess a false sense of security free from consequences. While the freedom to express oneself without consequence may have positive aspects, it can also lead to harmful effects for individuals and for those with whom they interact. To combat these toxic disinhibition effects, it is important that teachers educate students on acceptable behaviours and help them understand the consequences of their online actions (Ki & Ahn, 2006).

In addition to the disinhibition effect, feelings of disengagement have also been suggested as a factor in ethical problems involving ICT (Milson & Chu, 2002). While disinhibition reduces one's sense of self-consciousness, disengagement leads one to disregard, minimize, or ignore the consequences of one's behaviour. Together, disinhibition and disengagement have the effect of not only losing concern over what one does on the Internet, but also what happens because of it. The disengagement is doubly potent since it not only severs users' feelings of responsibility, it also distances and dehumanizes the connection of others. Milson and Chu (2002) argue that disinhibition and disengagement make cyberspace a "morally treacherous terrain" that requires cyberethics education, net-based citizenship, or what they call netizenship.

Whether or not the disinhibition and disengagement effects are to blame for unethical behaviours, dysfunctional or ethically dubious activities continue to exist and consistently occupy space in the media. Without a way of addressing problems such as copyright infringement, invasions of privacy, and lack of media awareness, these issues show no signs of disappearing. Young people are tasked with maintaining and improving the world as they become the new leaders and replace the older generation. Without the proper guidance, it can be difficult growing up in an environment saturated with ICT, and learning to navigate one's way through a dangerous environment while developing ethical decision-making skills. The factors that threaten these youths' safety and security, combined with inaccurate assumptions of their abilities, arguably make them the group that needs computer and cyberethics education the most.

Computer ethics and education – What is being done?

The first changes that come to mind in updating school curricula are those involving updating ICT hardware and software, and technology knowledge and skills. These changes can be readily seen as school boards and governments have adopted numerous technology and computer studies into their curricula and program of studies. However, as Ki and Ahn (2006) note, understanding of computers cannot be effective with emphasis put only on the functional sphere.

While it is important to ensure students are capable of using new technologies, it is equally important to integrate technology *attitudes* into the curriculum. Simply giving students the means and abilities to manipulate new technology without also teaching them the rules of its use can be troublesome. Like giving children a set of markers without explaining that they must keep their drawings within the page, the exploration of their new marking tool can end up with messy and unwanted results.

By incorporating CE, students can not only become familiar with how to use technology, but how to use technology *ethically*. This education comes in the form of media literacy and computer and information ethics programs that not only give students the skills necessary to navigate their media- and technology-rich environments, but do so with the ability to critically evaluate and ethically make decisions.

While the desired area of study is intended for the elementary and secondary school levels, a review of literature at the post-secondary level is also necessary. The introduction of CE began at the post-secondary level, influencing the adoption of CE

at lower levels (McQuade, 2007). Research at the university level may hint at future directions of CE education at the secondary and elementary levels. Additionally, analysis of post-secondary CE provides information on what the knowledge, skills, and attitudes of the next generation of people may be. More specifically, this examination may demonstrate the abilities of future teachers who have a direct impact on young children.

The role of CE education first appeared at the post-secondary level through Maner's (1980) workshops on teaching computer ethics and with resources like Deborah Johnson's (1985) seminal book, *Computer Ethics*. Developments from the ACM such as the introduction of a professional code of ethics and requirements for accreditation have also pushed the adoption of computer ethics courses.

Today, many post-secondary institutions include some form of CE programming. A survey of universities in California and internationally showed that a majority (82.4%) of professors in the Information Science and Engineering departments teach some form of computer ethics (Barroso & Melara, 2004). Other important findings show that CE is primarily taught as a separate course by experienced professors, and that the importance of CE is growing as more universities are including CE as a mandatory course. While the survey presents some intriguing findings, one must also keep in mind that these results were based on a survey of only 68 respondents located primarily in one region of the United States.

A more recent survey by Spradling, Soh, and Ansorge (2008) examined the programs of 251 universities across the United States. Their study not only

investigated which institutions were providing CE education, but also why other institutions did not. Confirming results from the previous study done by Barroso and Melara (2004), a majority of schools surveyed (88%) included ethics in their programs, with it being taught mostly by the computer science faculty. This information reflects a promising attitude towards CE education as CE appears to be an acknowledged and important component of computer science programs.

Even with the positive direction of CE education, there have been a number of obstacles and challenges to integrating professional ethics in the computing curriculum. Although the results found by Spradling et al. (2008) are hopeful, the results were based on 251 of 700 administered surveys, a response rate of only 36%. This low response rate may lead some to speculate that those who did not respond (the majority) could have little or no CE programming. Additionally, while there does seem to be an increase in the inclusion of CE courses, far less positive results were found when respondents were asked about faculty training. Spradling et al. (2008) found that 168 (77%) of the 218 surveyed institutions responded that no training is provided with only 50 (23%) respondents reporting that CE training is provided. While there was a correlation between training provisions and ethics course requirements, a large group of faculty surveyed responded that they were responsible for their own training or had to seek training from outside the university or college.

Training was also a major factor of programs that did not teach CE. Of the programs surveyed that did not offer CE, the most common answer as to why they did not, was a lack of faculty training, followed closely by a lack of room in the

curriculum. The results of Spradling et al. (2008) are overall very positive as they show that CE is being taken seriously and is beginning to be a mandatory component of computer science programs. The primary concern now seems to be adequately preparing faculty by providing the proper training and development.

Research by Greening, Kay, and Kummerfeld (2006) has provided further evidence of training issues in CE education and, in addition, identified and discussed four other primary challenges. The first challenge concerns the integration of ethical content into technical units. There has been some debate whether to teach ethical content as a separate unit as it would allow more time to cover material such as ethical case studies in more depth. However, Greening et al. and other educators such as Martin (1999) fear that separating the ethical issues will result in a lack of connection and poorly reflect the integration of ethical issues and computing in the field. Finally, Greening et al. note that, even in courses that claim to take an integrative approach, ethics are often simply appended to existing content. The challenge then is not only to include ethics content within the courses but to adequately integrate the material.

The need to educate students on computer ethics is clear and the most direct way of passing on this knowledge is through the teaching staff. However, Greening et al. (2006) found that there are a number of obstacles, which form the second challenge: empowering staff. In 1991, the ACM mandated inclusion of ethical and social issues in computing. This mandate caused strong criticism, however, as there was a lack of specificity in what exactly to include and how to include it. Even with additions to the curricula in 2001, Greening et al. found that the lack of

specifications has remained. One suggested option is to employ experts or specialists in the teaching of ethics, allowing the staff to focus on their expertise. This solution is undesirable as it takes away from the intended integration of ethics. Moreover, bringing in a specialist may send a message that the present staff is incompetent or unable to embrace the very ethics they are promoting. The challenge must therefore be met with an improvement in the training and resources available to the teachers as well as clear boundaries and expectations. As teachers are the most direct link to the education of students, the challenge of empowering teachers is a clear goal.

The third challenge identified by Greening et al. (2006) turns from the teachers to the students. A primary reason for integrating ethics into curriculum is to help students connect ethics and ethical decision-making with events in their real lives. Without proper attention, students are unlikely to adopt the endorsed standards. The challenge of achieving student engagement is therefore a vital component to internalizing a commitment to ethical standards. To achieve internalization, three recommendations are presented: high levels of integration, early introduction, and staff adoption and empowerment. In addition, a degree of relevancy is needed.

The facilitation of valued learning is the fourth challenge described by Greening et al. (2006). Valued learning involves using authentic learning tasks and takes a “deep” approach to learning that goes beyond surface content and simple attributions. Greening and colleagues warn, for example, that simply approaching ethics from a legal perspective does not necessarily move students to deeper

understanding of complex ethical principles and dilemmas. Just as technical content requires “deep” learning and instruction, the teaching and learning of ethics requires the same attention and passion.

The fifth and final challenge put forth by Greening et al. involves doing justice to the content. Part of the challenge in empowering the teaching staff lies in giving them the knowledge and skills necessary to feel competent in their teaching; this competency involves the ability to adequately cover the material. Adequately covering CE content poses a challenge for several reasons including the matter of space and a lack of experience by educators. Technical curricula are already crowded with information, and the addition of ethical content risks diluting the content, inadequately covering the material, or presenting the content too quickly leading to confusion and error. A major challenge remains the teachers’ ability to competently teach the ethics material. Since the requirement for the inclusion of ethics is fairly recent, most educators are unfamiliar or inexperienced with teaching ethics. Coupled with the lack of clear requirements and boundaries and a lack of support and training, doing justice to the content becomes increasingly difficult.

The five challenges presented by Greening et al. (2006), and supported by others (e.g., Spradling et al., 2008), show that, even though CE education has made great progress, there are a number of obstacles still to overcome.

Since the development of CE, much of computer ethics education has been focused on the post-secondary level to students majoring in the computer sciences, information sciences, and engineering. However, as computer use has become ubiquitous, a trend towards CE education for all students has developed. This push

towards CE education for people developing and engineering ICT, as well as people who simply use the technology, has led to a call for education at lower levels of schooling from elementary to secondary schools (McQuade, 2006). The need for CE education at lower levels makes sense as young people arguably require greater training as they are developing moral values and ICT skills concurrently. Moreover, a growing body of research has found that the previously more sophisticated and mature problems experienced by college students like cyberstalking, academic dishonesty, and intellectual property violations are increasingly affecting adolescents and young adults as well (McQuade, 2006).

Enabled by advancements and increasing exposure, students in elementary and secondary schools are becoming more involved as both victims and perpetrators of crime and abuse. A growing number of children are experiencing cyberbullying, unwanted sexual solicitations, harassments, and engaging in illegal activities (McQuade, 2006). McQuade suggests that following years of largely unsupervised online activities, students may be “technologically savvy but naïve to the dangers that same technology poses” (p. 1). As most students have experience using computers years before they enter post-secondary institutions, there is no reason to wait before CE is taught.

The instruction and education of ethics and morals plays a prominent part in the socialization role adopted by schools. Character and virtues education components are a part of many schools and, with the increasing pervasiveness of computers in education, it is not difficult to imagine the inclusion of a computer or cyberethics component.

In 2008, a national baseline study was performed by Educational Technology, Policy, Research, and Outreach (ETPRO), which explored Cyberethics, Cybersafety, and Cybersecurity (C3) in public and private K-12 educational settings. The survey of C3 educational awareness policies, initiatives, curriculum, and practices assessed the current status of programs and provided information for future program design. This survey resulted in several key findings on the current status of K-12 cyberethics education. Across all areas, the survey found inadequate levels of education stemming from poor training and preparation of teachers, inadequate commitment to C3, and narrow coverage of information. With barriers similar to those facing CE education at the post-secondary level, the K-12 educational setting shares problems of adequate teacher training and confidence.

How should cyberethics be taught?

To combat some of the issues mentioned above and address some of the reasons for teaching cyberethics, several suggestions on how to effectively teach cyberethics have been made.

The first step has generally been to outline a set of goals or basic principles. For Ki and Ahn (2006), this outline is expressed as a set of four core goals: respect for others, not infringing upon other people's intellectual property rights, using information productively, and using ICT for acceptable time periods so that it does not harm life. For many others, these goals often take the shape of an acceptable use policy (AUP) (Baum, 2005; Crystal, Geide, & Salpeter, 2000). The Ten Commandments of Computer Use is a widely quoted document from The Computer Ethics Institute (2005); lists of rules and regulations regarding Internet use, Internet

etiquette, and appropriate ICT language have also been recommended (Bell 2002; Crystal et al.; Ki & Ahn, 2006).

These rules and regulations must not be the only way of educating students in cyberethics (Carpenter, 1996). The reasoning behind appropriate versus inappropriate behaviour is often due to personal reasons, rather than social conventions like classroom rules (Kafai, Nixon, & Burnam, 2007). To genuinely and thoroughly educate students on ethical rights and wrongs, a deeper change must occur beyond simply obeying the rules. Before enforcing rules, children must discuss and understand the reasons behind each issue.

For students to engage in appropriate online behaviours and decision-making, a solid moral and ethical foundation is essential (Yamano, 2006). There is a clear and important difference that distinguishes moral rules from moral reasoning. For example, if a child steals, a common response is to tell the child that there are rules against stealing. However, as Covalleskie (1992) points out,

They should not be taught not to steal because there is a rule against stealing. The rule is not the reason we teach children not to steal. What they need to understand is that the rule against stealing exists only because stealing is wrong, and why this is so. (p. 176)

It is this moral decision-making or reasoning that is the ultimate goal. The inclusion of these social conventions is not without its merits, as rules and regulations establish boundaries, provide structure, and model appropriate behaviour. However, care must be taken not to rely solely on these conventions for adequate CE education.

Beyond the establishment of a set of goals and policies, perhaps the most important recommendation to cyberethics education is improved teacher training

and support from school districts. Teacher training has been the primary contributing factor to cyberethics education (Educational Technology Policy, Research, & Outreach, 2009; Greening et al., 2006; Kafai et al., 2007). Lack of training is frequently cited as the reason for inadequate cyberethics education, or complete lack thereof. Part of the responsibility rests with educational institutions, as cyberethics education must be included with improvements in ICT instruction. Teaching students how to use a computer must also entail how to ethically use it as well. If teachers are expected to teach these values, adequate support in the form of teacher training and professional development are a must. As shown in the survey by Kafai et al. (2007), teachers are not immediately aware of the ethical reasoning abilities of young students, nor are they prepared to teach them. Improved training may help not only with teacher preparation, but also in teacher confidence resulting in more eager adoption of cyberethics education.

Turning towards cyberethics education itself, recommendations for improvement include taking a more in-depth and integrative approach that spans the course of the semester or course term. As indicated by ETPRO's (2009) baseline survey, when cyberethics is covered, it is usually with a very limited scope touching on only a few topics and over the course of one class, or one-time assemblies. Offering such limited exposure can have negative results, as a lack of adequate coverage separates the content from situations and little is gained from such brief encounters (Greening et al., 2006). A fully integrated cyberethics program gives students the opportunity to engage in moral dilemmas that occur on a daily basis and provides more time for discussion and deeper comprehension. Additionally,

with more frequent interaction, a more updated understanding of the ethical issues can be achieved. As technology advances quickly, technology standards, policies, procedures, content, and ethical analysis must keep pace.

In addition to overcoming some of the obstacles in cyberethics education, a number of useful teaching strategies have been recommended. Finding good strategies for teaching cyberethics can be achieved to some extent by looking at strategies used for teaching traditional ethics. Some of the most notable approaches attempt to encourage moral development through active participation and discussion. One method that has shown success is the use of role-playing and case studies.

Using mock trials and role-play, Canosa and Lucas (2008) were able to successfully engage undergraduate students and examine a variety of ethical problems involving ICT. Trials were set up similar to a debate, with students being required to research, prepare, and present arguments to the class. This formal step was followed by a more informal discussion of the topics. With a near 100% participation rate, students were stimulated to think more deeply about the issues and examine both sides.

The participation aspect of mock trials added a real-world element, which is something that has been recommended by many others as it focuses on the students in a learner-centred approach (Applin, 2006; Ki & Ahn, 2006). Discussing real-world issues also helps students better connect to what is being taught and allows them to apply their learning directly to their everyday lives.

Summary

As technology continues to advance and ICTs become an even greater part of people's everyday lives, the need for education and training to address the arising social and ethical problems is more present than ever. In such an ungoverned and free arena as the Internet, the dependence on the moral and ethical behaviour of its users is what will prevent its misuse (Maner, 1976; Moor, 1985). In particular, the moral development of children growing up in an online environment is most important as their awareness of ethical issues is not fully formed, and a number of dangers may threaten their safety and their views of right and wrong. To prevent young people from becoming inconsiderate, disengaged, dysfunctional, or carelessly disinhibited citizens of cyberspace, a well-developed cyberethics education is recommended. A review of available and enacted cyberethics education shows promise as a large number of post-secondary schools surveyed offer courses in ICT-related ethics and the adoption, interest, and status of cyberethics is growing.

The teaching of cyberethics is no easy task, however, as there are a number of obstacles that hinder its progress. Deficits in training and teacher confidence are barriers that require more support from school districts and policy makers. Improved programming to include more integrated and comprehensive coverage of ICT ethics issues is also needed. Despite these challenges, positive teaching strategies have been adopted as the use of case studies, mock trials, engaging discussions, and a learner-centred approach to teaching suggest progress is being made.

In the chapter to follow, a collection of teachers' guides that address the above challenges are presented on three main issues. The first guide will cover the area of copyright; outlining background information, highlighting several current issues and providing links to additional resources. The second guide will cover privacy, and the final guide will address media awareness. These guides will provide a means of improving cyberethics education by addressing the challenges and incorporating suggestions from the information reviewed above.

Chapter 2: Teachers' Guides

Teachers' Guides Overview

I provide three guides below: one dealing with the issue of copyright infringement; the second about privacy; and the third about media literacy.

Although not a comprehensive list, these three issues presented are among the most common related to cyberethics (Johnson, 2001; Media Awareness Network, 2010). The purpose of the following guides is to provide an overview of some of the moral and ethical concerns surrounding each issue. Also included in the guides are lessons intended to promote discussion, engage students, and open communication to other important topics.

The structure of each guide is similar: background information highlighting some of the significant events and positions, then some suggested activities to encourage analysis and discussion, and finally additional resources for extension. A glossary of terms is included at the end of each topic. The sections are not intended to be a comprehensive presentation of all the cyberethics issues that are involved, nor is the guide a step-by-step formula to achieving moral and ethical excellence. Rather, the guides serve as an overview of some of the more prominent concerns associated with each issue in each topic and is intended to inform students of current possible moral and ethical quandaries and appropriate behaviour. Additionally, the discussions resulting from the activities may help develop moral and ethical decision-making and behaviour involving ICT.

The background information provided aims to give instructors a good working knowledge of the topic and to give confidence in leading students in discussions around each topic. Being adequately informed should facilitate teachers doing justice to the issues and be prepared for discussion.

It is expected, when new cases and issues relating to each topic arise, that the information provided in the guides can assist understanding, and that the additional resources provided may generate other quality sources of information. The activities section of each topic outlines lesson ideas that can be used to spur discussion and challenge the students to question and consider multiple aspects of cyberethics issues. Teachers are encouraged to modify and adapt the included lessons, as well as to develop and incorporate new lessons wherever possible.

© concerning © opyright: Teachers' Guide to Copyright

Background information.

Simply put, copyright is “the right to copy” exclusively given to the owner, usually the creator of the work. This copyright covers all original dramatic, musical, artistic, and literary works (including computer programs) and allows the ability to produce, reproduce, or permit anyone else to do so (CIPO, 2010). Though copyright does not cover ideas, it exists as soon as the work is created and generally lasts until approximately 50 years after the author dies.

Several exceptions allow the use of copyrighted materials. In the United States, materials used for commentary, criticism, reporting, research, teaching, or scholarship are allowed limited use without permission from rights holders under what is called *fair use*. In Canada, a similar, though more restrictive, set of provisions allows the use of copyrighted material under what is called *fair dealing*. (For more information on the differences between fair use and fair dealing, see additional resources). In addition, libraries, museums, and archives are allowed limited use of copyrighted materials for private study, research, or review; certain exceptions are also in place for persons with perceptual disabilities.

Copyright History

The roots of copyrighting can be traced back to the invention and use of the printing press in the 15th century in Europe. Up until that time copying largely involved reproducing works by hand, which required considerable time and labour. With the invention of the printing press, works could be quickly and easily reproduced. While this increased efficiency allowed the proliferation of information

that was deemed appropriate by those in power, it also permitted the distribution of unacceptable materials such as criticisms towards the church or government. To control the type and distribution of information, governments issued licenses to printers, which granted them exclusive printing rights for a limited amount of time.

While the rights of the publishers were protected, the rights of the authors still needed improvement. In 1709, the first copyright statute came into place in the form of the Copyright Act of 1709, generally known as the Statute of Anne. This act granted full legal printing rights to the authors in 14-year terms throughout England and Scotland. It was the first formal legal recognition of property rights and ownership by the creator. Printing, reprinting, or importing without consent was punishable with the destruction of the property in question and a substantial fine.

The next significant event involved the Berne Convention for the Protection of Literary and Artistic Works. First held in the Switzerland capital in 1886, it is an international agreement that protects and governs copyright for members who sign the treaty. Before this agreement, copyright regulation was only governed under the respective countries and only concerned works in the country where originally created. With the international agreement, copyright laws could be applied to works regardless of the origin with authors being protected in countries across the world. Several updates to the Berne Convention were made following its initial inception to adapt to the changing form of works. The Copyright Act 1911 came into play and, in addition to adjusting some of the copyright laws, included the protection of sound recordings. Later, the Copyright Act 1956 replaced the 1911 Act and responded to technological advancement to include film and broadcasts. In 1967, the Berne

Convention became known as the World Intellectual Property Organization; in 1974, it became part of the United Nations as a specialized agency. Today almost all countries (over 180) are members of the convention.

Further adaptations to changing technology have come in the form of the Copyright, Designs and Patents Act 1988 (CDPA 1988) and the TRIPS Agreement 1994. Similar to previous updates, which expanded to include sound and video recordings, the CDPA 1988 extended copyright protection to new technologies such as computer programs, or software, and cable and satellite broadcasting. More importantly, updates were made to adapt to the changes in copying that were occurring. Photocopying, re-recording video and audiocassettes, and broadcasting had become popular and readily available to individuals. The CDPA 1988 was added to regulate this activity, deter piracy, and protect copyright owners. While certain provisions were granted for educational, library, and archival uses, the copying of items for commercial resale was prohibited. The CDPA 1988 also for the first time recognized the moral rights of authors, including a claim to authorship and the right to object to derogatory treatment of their work. Essentially this provision means that authors have a moral right to be identified and recognized for the work that they have done and the right to protect the work's integrity against those who would attempt to violate it.

In 1994, yet another update in the international protection of copyright was made in the form of the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS Agreement 1994). Primarily driven by international trade,

this agreement put in place a set of provisions for members and candidates of the World Trade Organization (WTO).

In the United States, 1998 saw the implementation of the Digital Millennium Copyright Act (DMCA). This copyright law enacted two treaties of the World Intellectual Property Organization (WIPO), which criminalizes production and dissemination of technology, devices, or services intended to violate copyrighted works.

Canadian Copyright

Copyright legislation in Canada has not been as extensive or involved as in the United States and the United Kingdom, but Canada does comply with the Berne Convention agreement and has signed numerous WIPO (World Intellectual Property Organization) treaties.

Being a former British colony, Canada's copyright legislation corresponded heavily to that in the UK following British law until 1924 before passing its own heavily British influenced Copyright Act. Since that time, few significant changes have been made. The most drastic change came in 1988 with the modification to adapt to new technology and include protection of computer programs, clarify the rights of artists, make restrictions on private copying, and allow fair use for certain public institutions such as schools, libraries, museums, and broadcasters.

A further review of the Act in 1997 led to proposed amendments in Bill C-60. The bill would give stronger rights to copyright holders, especially in cases involving computers and online copying of materials from file-sharing networks. The bill

failed to pass, however, as a defeat of the Liberal government in 2006 resulted in the Parliament being dissolved.

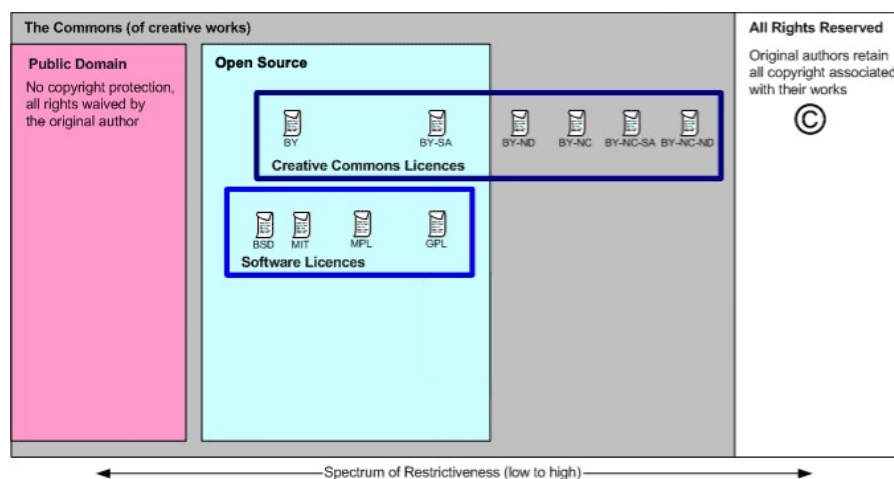
In 2008, Bill C-61, the successor to Bill C-60, was introduced as another attempt to update the Copyright Act. Again this bill failed to pass as an election was called.

The most recent effort at modernizing copyright legislation is the recently tabled Bill C-32 in 2010. It attempts to balance the rights of consumers and creators and clarify regulations around backing-up materials, responsibilities of Internet service providers (ISPs), fair-dealing, time-shifting of television shows, and protection around Digital Rights Management (DRM). As of this writing, Bill C-32 has not passed into law.

Copyright and Licensing

The extensive use of copyright has at times been accused of being too restrictive and impinging on freedoms to create and innovate. However, the restrictions and allowances of copyrighted work are separated by more than whether it is copyrighted or not, and are divided into a number of levels of licensing that provide balance of freedom and protection. At one end is the public domain, where a work is essentially not copyrighted and free to use or copy without permission or penalty. On the other end is copyrighted work, where the exclusive rights to use, perform, and copy are given to the copyright holder(s). In between are a number of licensing categories, each having its own range of licensing options, including: open-source, creative commons, and general public licensing (GPL). A

simple illustration of the spectrum of software licenses taken from creativecommons.ca is seen below.



retrieved Aug. 20, 2010.

GPL is a popular license that protects creative works while retaining the freedom to share, distribute, and perform modifications without cost *or* for a fee. Falling under what is called a *copyleft* license, all derivatives must also carry the same licensing agreement. By doing so, using a GPL allows the work to be freely available but remains protected under the parent license.

Open-Source licensing essentially pertains to software and works that possess a license that does not restrict the free (unconstrained and without cost) distribution and redistribution of the source code, the software, and all modifications and derived works. In addition, the Open Source Initiative (2010) has outlined several criteria, which include: integrity of the author's source code, no discrimination against persons or groups, no discrimination against fields of endeavour, distribution of license, license must not be specific to a product, license must not restrict other software, and license must be technology-neutral. By ascribing to these criteria, open-source creates a community that promotes the

sharing of knowledge and innovation. Several notable open-source programs include: Linux, Firefox, and OpenOffice.

The Creative Commons (CC) license is yet another option for protecting creators' work while maintaining freedom. Whereas copyrighted works have "all rights reserved," a CC license is more akin to having "some rights reserved." Using a system of criteria, creators can protect their work while encouraging pre-defined uses by others. These uses can vary from giving open access to source code, allowing others to copy, distribute, display, and perform freely, only for noncommercial purposes, without derivatives, or only with proper credit given. The flexibility and range of options allow a more customizable level of copyright protection.

Activity and lesson ideas.

The lessons below explore copyright through a review of copyright history, a set of case studies revealing current issues, a lesson on proper citation of sources, and a set of scenarios for students to apply their learning. Through these lessons students will gain an understanding of copyright and acquire skills to prevent copyright violations.

Copyright Timeline

The objective of this activity is for students to construct a meaningful timeline of events regarding copyright. By creating a timeline students can see a progression of media types, problems that have arisen, and the changes that have been made to adapt to and resolve these problems. Seeing this process from the beginning would allow students to form a clearer idea of how modern copyright acts have been introduced and what they do.

Steps for this activity consist of:

- Select a number of events that you would like students to research (somewhere between 10 – 15 should be adequate).
- Ask students individually or in small groups to find 10 – 15 events regarding copyright that they think are important and why.
- Have students construct a timeline (with or without pictures) to be shared with the rest of the class.
- Display the timelines in class and have a “gallery walk” so that students can look at and compare each other’s timelines.

- As a class, construct a timeline of 15 – 20 significant events involving copyright having students suggest events and justifying their choices. Be prepared for negotiation and mediating compromise.

Additional timeline resources can be found at:

<http://www.arl.org/pp/ppcopyright/copyresources/copytimeline.shtml>

Case Studies

Case studies provide an excellent opportunity to connect copyright issues with real-world events and current trends. Analysis of these events can lead to engaging discussions where students can critically examine the moral and ethical issues involved as well as the laws and regulations that govern the behaviours and determine the outcomes. Because copyright legislation continues to change, I recommend that that teachers use the most current or significant cases and events be used. Three additional examples and discussion questions have been provided below.

Case Study #1 – School plagiarism

<http://www.nytimes.com/2002/02/14/us/school-cheating-scandal-tests-a-town-s-values.html?ref=plagiarism>

Case Study #2 – Google vs. Viacom Copyright Lawsuit

<http://www.nytimes.com/2010/06/24/technology/24google.html?ref=copyrights>

Case Study #3 – Yoga Wars

<http://www.washingtonpost.com/wp-dyn/content/article/2010/08/22/AR2010082203071.html>

The following are some questions that teachers can use in a discussion:

Who is involved and what is at issue?

Do you agree with the outcome? Why or why not?

Is there another solution to the problem?

Could the issue have been prevented? How?

Can you think of similar situations you have heard of or encountered? Please describe them.

Do you get the reference? Referencing Lesson

The importance of properly referencing ideas, quotes, and the work of others is something that cannot be overstated. As technology has made it easier than ever to copy and paste images and text without bothering to properly cite sources, bad habits can easily form. The repercussions and penalties that may result in the future make it important to ensure students acquire this skill. Properly referencing is important for a number of reasons including:

- to prevent instances of plagiarism
- to give credit to others' work
- to help others find your sources, and
- to give credibility to your own work.

For this lesson:

- Ask the students to write a short story based on something of interest to them.

This interest can be a book, comic, song, television show, or movie. If they are doing this story on a computer, tell them to include a picture in the story as well.

- When the students have completed their stories, explain the importance of referencing (see links below for more information and activity reference).

- Explain that referencing is basically who, what, when, and where.

<http://www.library.usyd.edu.au/elearning/learn/referencing/index.php>

[http://www.library.usyd.edu.au/elearning/learn/referencing/activities/index.p
hp](http://www.library.usyd.edu.au/elearning/learn/referencing/activities/index.php)

- Ask students to find and reference some/all/several of the following items:

- Book
- Book chapter
- Website
- Picture from a website
- Journal article

For more information on citing works, and a useful tool for referencing visit:

<http://www.apastyle.org/learn/faqs/index.aspx>

Citation Machine - <http://citationmachine.net/>

Scenarios

Copyright is a complex and extremely intricate set of rules, regulations, and exemptions that are often difficult to understand. The use of scenarios that one may encounter in the real world can be beneficial to students understanding copyright, connecting what is learned with their personal experience, and applying ethical behaviour to their lives.

Steps in a lesson plan could involve:

- Divide students into small groups to discuss a selection of scenarios from the included “Scenarios Handout” (see Appendix A).
- Instruct students to answer the following questions for each scenario:
 - Who is involved?
 - What is/are the issue(s)?
 - Has there been a violation of copyright? How?
 - Do you think that this outcome is fair? Why? Why not?
- As a class, discuss each scenario before referring to the solution.
- Follow up with any questions students may have.

Additional resources.

Canadian Copyright Act and Bills

Bill C-32: Dissecting Canada's New Copyright Bill - <http://blip.tv/file/3716994>

Bill C-32 - http://podcast.cbc.ca/spark/plus-spark_20100606_spark116b.mp3

Bill C-60: Death and details of Bill C-60 -

http://www.cbc.ca/news/background/internet/downloading_music.html

Canadian Copyright Act - <http://www.media->

[awareness.ca/english/resources/legislation/canadian_law/federal/copyright_act/cdn_copyright_ov.cfm](http://www.media-awareness.ca/english/resources/legislation/canadian_law/federal/copyright_act/cdn_copyright_ov.cfm)

Canadian Copyright Act - <http://www.mapleleafweb.com/features/copyright-law-canada-introduction-canadian-copyright-act>

Canadian Teachers' Federation. - <http://www.ctf-fce.ca/>

Additional Information

A Very Short History of Computer Ethics -

http://www.southernct.edu/organizations/rccs/resources/research/introduction/bynum_shrt_hist.html

Copyright Laws & Fair Use - <http://www.stfrancis.edu/content/cid/copyrightbay/>

Excellent resource for teaching copyright to students -

<http://www.teachingcopyright.org/>

Technology and Learning's Copyright Primer: Fair Use Copyright Quiz -

<http://www.halldavidson.net/Quiz%20.pdf>

Copyright Scenarios - <http://blog.lib.umn.edu/copyinfo/scenarios/>

Downloading Television is Legal in Canada - http://news.cnet.com/2100-1025_3-5121479.html

Council of Ministers of Education Canada -

<http://www.cmec.ca/Programs/Copyright/Pages/default.aspx>

Canadian Intellectual Property Office -

<http://www.cipo.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/home>

Fair Dealing (Canada) vs. Fair Use (USA) -

http://llc.georgebrown.ca/llc/pagecontent/faculty_links/copyright_comparison_us_can_e.pdf

Copyright Guide - <http://library.concordia.ca/help/copyright/>

Movies in the public domain - <http://www.openflix.com/>

Open Source Initiative - <http://www.opensource.org/osd.html>

Interactive Links

Citation Machine - <http://citationmachine.net/>

Teachertube.com – numerous videos. Search “copyright.”

Creative Commons Video - <http://mirrors.creativecommons.org/getcreative/>

Fair-Use Four-Factor Analysis - <http://www.lib.umn.edu/copyright/checklist.phtml>

Video explaining copyright “A Fair(y) Use Tale” -

http://www.youtube.com/watch?v=CJn_jC4FNDo

Glossary of terms.

BitTorrent: a popular P2P file sharing protocol.

Creative Commons: a license that allows other creators open access to the work's source code under publicized terms and conditions.

Digital Rights Management (DRM): DRMs are a form of digital lock that protect digital content and prevent the material from being copied.

Fair Dealing (similar to Fair Use in the United States): a clause in the Copyright Act that allows the use of copyrighted materials for activities including education, research, private study, criticism, review, and news reporting.

Internet Service Providers (ISPs): ISPs are private companies that provide consumers with access to the Internet. Some of the major companies in Canada include Bell Canada, Rogers, Shaw, and Telus.

Open Source: a license that allows unrestricted and gratis access to source code, use, distribution, and redistribution of the original work and all modifications and derivatives.

Peer-to-peer (P2P) technology: a network of computers used to share files through uploading and/or downloading.

Public Domain: works that are no longer under copyright, or have failed to qualify for copyright. These items may be used and copied freely without permission from the original copyright holder.

Time-Shifting (of Television): backing-up of television shows for later viewing using a digital recording device such as a personal video recorder (PVR) (e.g., Tivo).

Protecting Privacy: Teachers' Guide to Privacy

Background information.

Privacy is something that we all come to expect as a fundamental human right but the protection of that privacy is something that cannot be taken for granted. With the development of ICT (Information Communication Technology), people's personal information is increasingly being kept in digital form. Unlike traditional paper-based forms, digital information is much easier to copy, collect, and distribute, often undetected. The consequences on privacy are enormous as the information obtained can be exposed, leading to humiliation, economic and physical harm, and discrimination. The protection and valuation of privacy must therefore become a primary concern for all members of society in the digital age.

In addition to being a basic human right, privacy is also a key element to a democratic society. Only with confidentiality and without the fear of surveillance can people act freely and think critically. A right to privacy allows people to question authority and express opinions, both of which are vital to preserving democracy. At the same time, however, the collection of private information is needed to ensure safety and security, and provide essential services. Personal information identifies individuals, grants access to services, and allows planning to take place. The issues that exist regard the balance between these two sides.

Although the Canadian Charter of Rights and Freedoms does not reference privacy explicitly, rights to liberty, security of the person, and the right to be free from unreasonable search or seizure apply directly to elements of privacy. In

Canada, several federal and provincial laws exist that protect personal information and regulate the types of personal information that can be collected and how it can be used.

The Privacy Act of Canada, introduced in 1983, is federal legislation that regulates how federal government institutions collect, store, and use personal information. These laws also restrict what kind of information can be collected and how. For example, under the Privacy Act, with limited exceptions:

- No personal information can be collected unless it relates directly to an operating program or activity of the institution.
- A government institution shall inform the individual of the purpose for collecting the information.
- Personal information will only be retained for a reasonable amount of time as is necessary.
- Personal information will not be disclosed without consent of the individual.
- Personal information will be used only for the purposes under which it was collected.
- Every individual, on request, will be given access to his or her collected information, especially to correct inaccuracies or omissions.

In addition to the Privacy Act, a second piece of privacy legislation, PIPEDA (Personal Information Protection and Electronic Documents Act), protects individuals in the private sector. Similar to the Privacy Act, PIPEDA regulates how personal information is collected, used, or disclosed, but to federally regulated agencies such as telecommunications companies, airlines, banks, broadcasters, and

online businesses. The law also applies to some private organizations such as insurance companies.

Beyond the two federal privacy laws, provincial laws are in place to help regulate businesses and organizations in the private sector. Banking and health-related laws are sector-specific, while more general consumer protection laws also exist to protect privacy. Many businesses and websites have detailed privacy policies in place to secure information.

Privacy Intrusions

The practice of collecting personal information is not new, as government, schools, and business institutions have long gathered data for taxation, informing policy, and record keeping. Still privacy is not just about if or how information is collected, but is also in establishing a balance between the collection of information needed while preserving as many rights and freedoms of the individual as possible.

Invasions of privacy go beyond what is simply needed and can occur in a variety of ways, some direct and others more covert. The Internet provides many people with a feeling of anonymity, as it seems difficult to be recognized among the millions of other users and abundance of information. However, this lack of identifiability is not entirely true, and several ways can thwart this anonymity. For example, all access to the Internet goes through Internet Service Providers (ISPs) who allow customers to transfer data through their networks. As a result of data passing through these ISPs, one's online activities can be monitored. While ISPs tend to have strict ethical and legal reasons for not doing so, the ability to track people is there. Another way of tracing computer use is through a computer's IP (Internet

Protocol) address. An IP address is similar to a name and address given to a device that identifies the source of the data being transferred. By monitoring an IP address, ISPs and others can see what services have been accessed. As safe and secure as a computer may appear to be, ways exist to circumvent security and violate privacy.

The success of the Internet is largely based on the massive amounts of connections across different information sources. However, the connections and networks that allow people to use the Internet are also a source of vulnerability. Unsecured networks and inadequate computer security can allow hackers to infiltrate a computer and copy stored credit card numbers, addresses, phone numbers, and other personal information. The viruses spread through the Internet and email are also capable of compromising computers and extracting information. An awareness of these threats can help prevent these attacks from occurring.

The reasons for invading privacy are plentiful and vary depending on how the private information will be used. Marketing and advertising are some of the primary uses of obtaining personal information. Products can be targeted directly to individuals based on their preferences and viewing habits. This information is gathered in a number of ways. Often, this information is given voluntarily through online surveys, memberships and registration forms, contests, and quizzes. However, this information is also collected discreetly through Internet cookies, web bugs, or spyware that has been unknowingly installed.

The process of data mining takes information collection a step further by employing numerous algorithms to analyze the data. By doing so, seemingly random online browsing can expose patterns and relationships that provide more distinctive

and implicit aspects of personal information. The danger here is that the information collected is being used for purposes not explicitly authorized and is done without the awareness of the user. Furthermore, while certain details are knowingly obtained from explicit information, the data in this case are being manipulated to discover implicit aspects of individuals that may be more private.

In addition to the quizzes, registration forms, and online surveys, social networking sites have become a serious threat to personal privacy. Increasingly popular, social networking sites encourage communicating and sharing information with others. Personal profiles can display almost anything from address and date of birth to current employment, political views, and personal photos. Even with filters limiting initial access, data can be copied and transferred by those who have been given access. Once posted, there is no controlling where the information will end up or who will eventually gain access. Unlike information that is unknowingly obtained by hackers or through data mining, control over whether this information is displayed is possible. Care should be taken in considering what information is provided to best protect privacy.

Privacy Protection

Despite the many threats to privacy, steps can be taken to limit the vulnerabilities and improve protection. Some of these steps are listed below:

- Be aware of your personal information and question why people want your information.
- Find out to whom you are giving your information and for what purpose.
- Make sure online forms are secure.

- Read and review the privacy policies of the websites you visit.
- Use up-to-date virus scanning software.
- Delete cookies and clear your Internet browser's memory cache after using.
- Give only the minimum amount of information necessary to complete transactions.
- Use passwords to protect networks, profiles, and private documents.
- Use privacy protection tools such as encryption and filtering software.

Activity and lesson ideas.

The following lessons examine privacy through an analysis of websites, a review of current privacy issues, and an evaluation of privacy settings in the popular social networking site Facebook. Through these lessons students will gain understanding of techniques used that invade privacy, develop knowledge of current events involving privacy, and learn ways to better secure their information using privacy settings.

Website Analysis

As children are spending more and more time online, threats towards their personal privacy increase as well. To prevent an unwanted loss of their privacy and augment their awareness of tactics used to invade privacy, having students analyze popular websites is a useful exercise. By examining how information is collected, students can develop critical evaluation skills and begin to question the motives behind information collection and discuss the moral and ethical issues involved.

One lesson plan consists of the following steps:

- As a class, develop a definition of what privacy is and what it involves.
- Discuss and create a list of what information is considered private information (e.g., date of birth, address, social insurance number, etc.).
- List ways in which websites attempt to obtain this information.
- Give students a list of websites (see links for more information) to visit and ask them to list the methods these sites use to obtain information and the type of information they request.
- Rank the websites in terms of privacy protection.
- Follow up with a discussion on privacy:
 - Did you discover anything that surprised you about private information?
 - What are some of the potential benefits and consequences of giving your private information to these websites?
 - Do you think that these websites are justified in asking for this information? Why or why not?
 - What can you do to protect your privacy?

Links to most popular websites based on traffic:

http://www.readwriteweb.com/archives/most_popular_websites_for_kids.php

<http://www.media->

[awareness.ca/english/resources/educational/teaching_backgrounders/internet/popular_childrens_web.cfm](http://www.media-awareness.ca/english/resources/educational/teaching_backgrounders/internet/popular_childrens_web.cfm)

<http://www.alexa.com/topsites>

Debate/Case Study

Case studies provide an excellent opportunity to connect privacy issues with real-world events and current trends. Analysis of these events can lead to engaging discussions where students can critically examine the moral and ethical issues involved. These activities may include a discussion and examination of each side of the issues including: rights to gather information and information privacy, surveillance and intrusion, democratic obligation, and personal rights and freedoms.

Because these issues are so contentious, they also lend themselves well to debate. It is suggested that the most current or significant cases and events be used to engage student interest. The following are suggested examples of issues current at the time of writing.

Case #1 - Identification Cards

http://debatepedia.idebate.org/en/index.php/Debate:_Identity_Cards

<http://canadaonline.about.com/library/issues/blinationalid.htm>

<http://www.cippic.ca/national-id-cards/>

Case #2 - Canadian Long Census Form Debate

<http://www.vancouversun.com/technology/Census+least+Canadians+privacy+concerns+Civil+liberties+group/3450360/story.html>

<http://www.nytimes.com/2010/07/24/world/americas/24canada.html>

<http://www.theglobeandmail.com/report-on-business/your-business/grow/expanding-the-business/business-concerned-over-census-changes/article1653800/?cid=art-rail-leadership>

Case #3 - Full Body Scanners at Airports

http://debatepedia.idebate.org/en/index.php/Debate:_Full-

[body_scanners_at_airports](http://debatepedia.idebate.org/en/index.php/Debate:_Full-body_scanners_at_airports)

[http://www.nytimes.com/2010/08/07/nyregion/07scan.html?_r=1&scp=1&sq=ful](http://www.nytimes.com/2010/08/07/nyregion/07scan.html?_r=1&scp=1&sq=full%20body%20scanners&st=cse)
[l%20body%20scanners&st=cse](http://www.nytimes.com/2010/08/07/nyregion/07scan.html?_r=1&scp=1&sq=full%20body%20scanners&st=cse)

<http://www.cbc.ca/canada/story/2010/01/05/security-canada-us-airport.html>

http://news.cnet.com/8301-31921_3-20012583-281.html

Facebook Frenzy!

Social networking sites have become increasingly popular with many young adults visiting these sites daily, often several times a day. The aim of these sites is to encourage communication among their users, which results in a large exchange of information. Due to the tremendous amount of information that can be shared, protecting one's privacy can be challenging. Additionally, as the sites are updated, settings can change unless they are monitored frequently and carefully.

The objective of this lesson is to highlight the types of information that can be gained from social networking sites like Facebook and what can be done to protect one's privacy. These activities include:

- Create a false Facebook profile filled with the personal information of a fictitious individual. Feel free to be creative here.
- After the dummy account has been created, invite students to look at the profile.

- As a class, list the various types of personal information that can be found and discuss what can be done with this information.
- Alternatively, you can challenge students to find certain information embedded in the account from a premade list. For example, date of birth, current location, city of birth, favourite movie, information on relatives, etc.
- Now task the students with finding ways to make this account more private. Students can create a set of instructions, uncover settings for each piece of information, or modify settings for certain scenarios (e.g., pictures can be viewed by everyone except your grandparents, or only your closest three friends have access to your email address, etc.).
- After completing the task, discuss the privacy of social networking sites. Were students surprised by anything they found? Did they discover anything useful? Will they change anything in their own profiles after this lesson?

Additional information on Facebook privacy can be found here:

<http://www.media->

[awareness.ca/english/resources/educational/teaching_backgrounders/privacy/facebook_privacy.cfm](http://www.media-awareness.ca/english/resources/educational/teaching_backgrounders/privacy/facebook_privacy.cfm)

<http://www.cbc.ca/technology/story/2010/05/26/facebook-privacy.html>

Additional resources.

Additional Information:

Canadian Privacy Act - <http://www.statcan.gc.ca/about-apercu/law-acte-eng.htm>

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

Office of the Privacy Commissioner of Canada - <http://www.priv.gc.ca/>

Online Ethics Center -

<http://www.onlineethics.org/Topics/EmergingTech/TechCases/netprivacy.aspx>

Privacy News, Information, and Action - <http://privacy.org/>

Privacytown - <http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca01304.html>

Youth Privacy - <http://www.youthprivacy.ca/>

Articles:

NY Times – How Privacy Vanishes Online -

http://www.nytimes.com/2010/03/17/technology/17privacy.html?_r=1&scp=1&sq=how%20privacy%20can%20vanish%20steve%20lohr&st=cse

PC World - Privacy is Not Dead -

http://www.pcworld.com/businesscenter/article/191506/privacy_is_not_dead_just_evolution.html

Interactive Links:

Jo Cool or Jo Fool - http://www.media-awareness.ca/english/games/jocool_jofool/index.cfm

Reclaim Privacy Facebook Privacy Scanner - <http://www.reclaimprivacy.org/>

Teaching Privacy in a 2.0 World Video - <http://vodpod.com/watch/2823011-teaching-privacy-in-a-2-0-world-by-mike-hominick>

Videos generated by the Office of the Privacy Commissioner of Canada -

<http://www.youtube.com/user/PrivacyComm>

Glossary of terms.

Cookie: An electronic text file stored by the user's web browser that saves a record of a website visit for purposes of tracking, authentication, and personalization.

Data Mining: A set of automated techniques used to extract patterns of buried information from data. Data mining is used for a variety of purposes including: profiling, marketing, surveillance, and scientific research.

Encryption: The transformation of information into code for protection and security.

Hacker: One who intrudes on another person's computer by circumventing computer security.

Malware: Any *malicious software*, including spyware, which is harmful to the user's computer by gathering information without permission.

Personal information: Information about an identifiable individual that is recorded in any form. This information includes: race/colour, national or ethnic origin, religion, age, marital status, address, blood type, etc.

Social Networking: Interaction and information sharing between people with common interests through online groups and communities such as Facebook and Twitter.

Spyware: Embedded software used to gather personal information.

Web Bugs: Transparent graphics generally used to measure the number of hits on a website, detailed information regarding online purchases, and user-submitted information.

Unmasking Media: Teachers' Guide to Media Awareness

Background information.

In today's technology and information heavy world, efforts at understanding media and developing skills to navigate the media-saturated environment have become extremely important. Access and exposure to different types of media occur constantly through television, radio, and the computer so that new ways of managing this bombardment are necessary. Help has come in the form of media awareness programs. Originally conceived as a method to inoculate people from the dangers of mass media, media awareness now aims to protect people by developing their knowledge, skills, and attitudes regarding the media.

This type of media awareness has been referred to as the media literacy approach, with media literacy being defined by many organizations such as the CML (Center for Media Literacy) and NAMLE (National Association for Media Literacy Education) as "the ability to access, analyze, evaluate and communicate messages in a wide variety of forms." (Aufderheide & Firestone, 1993, p. 7). The goals of media literacy are to encourage a critical analysis and creation of media that promotes civic and democratic action. While conventional notions of literacy involve print, media literacy is concerned with the understanding of a variety of texts. Audio, video, print, and combinations of all three, form what is considered media with all being texts that communicate a message. Media literacy goes beyond simple comprehension of these texts by encouraging a development of critical thinking skills to analyze and evaluate these messages.

In the United States, the Center for Media Literacy (CML) has established a group of five core concepts to guide media literacy initiatives. They are:

1. All media messages are constructed.
2. Media messages are constructed using a creative language with its own rules.
3. Different people experience the same media message differently.
4. Media have embedded values and points of view.
5. Most media messages are organized to gain profit and/or power.

In Canada, media literacy programs differ across provinces, but media education has achieved official status across the country. Canada has been recognized as a leader in the field of media education with collaborative development from organizations such as the Western and Northern Canadian Protocol for Collaboration in Education (WNCP) and the Atlantic Provinces Education Foundation (APEF). Similar to the five core concepts developed by the CML, the Ontario Ministry of Education has developed a list of eight key concepts of Media Literacy:

1. The media construct reality.
2. Media construct versions of reality.
3. Audiences negotiate meaning.
4. Media messages contain commercial implications.
5. Media messages contain ideology and values.
6. Media messages contain political and social messages.
7. Form and content are closely related in each medium.
8. Each medium has a unique aesthetic form.

Using these concepts as a guide, a framework for media literacy education can be developed, and a set of organized goals for media literacy exists.

Accessibility and knowledge regarding how to utilize media are often the first steps towards media literacy and are necessary to understand the digital world.

As technology improves, it is important to stay updated with current media applications and be able to learn how to operate them.

Gaining access to media is only the beginning, however, as being able to operate media is far different than being able to understand and use it. The skills of analysis and evaluation of media allow students to move from passive operation to critical manipulation of the media. The final skill towards media literacy is in the communication of media messages. While access, analysis, and evaluation provide ways of receiving information, it is equally important to be able to distribute and create media. A large component and benefit of new technology is the ability to create and submit content. Websites like Youtube.com, Flickr.com, and Tumblr.com, depend on user-generated content to exist. The ability to contribute to such sites is extremely valuable.

Critical media literacy contains moral and ethical components. As students are developing critical media literacy skills, they will acquire the knowledge that media are embedded with values. It is not only a recognition of these values that is important, but also a push towards good values and decision-making. The inclusion of computer ethics into media literacy fits well as students can not only learn to operate, analyze, evaluate, and create media, but also they can do so ethically.

Activities and lesson ideas.

The lessons below will enhance students' media awareness using an evaluation of media techniques, an exercise in website construction, an evaluation of different points of view in the media, and finally an analysis of students' digital identities.

"Reality" TV

While Internet use has begun overtaking television in popularity, television is still a major medium of message transmission for students and is a good example of how media manipulates information.

The objective of this activity is to highlight some of the techniques used by media to portray reality and arouse discussion about these techniques and their consequences. Through this exercise, students will be able to evaluate and respond to media. Steps include:

- Create a set of cue cards, each with the name of a television show on it. The selected shows should cover a wide range of genres and interests. It is recommended that the instructor be familiar with the shows selected and choose popular or current shows will help engage the students. See the included list for some suggested shows.
- Distribute the cards to the students, individually or in small groups.
- Draw a line on the board and label one end 'realistic,' and the opposite end 'unrealistic.'

- Ask the students to place their card along the continuum and justify their reasoning by explaining aspects of the show that make it realistic or unrealistic.
- After all the students have placed their shows along the continuum, ask if there are any disagreements and why.
- Encourage discussion about techniques that make a show more realistic (e.g., based on true events, using real people vs. actors, complex storylines, etc.) and ask how they feel about the use of these techniques. Do they feel manipulated? Is this manipulation appropriate for television shows to do? When is a manipulation of reality appropriate? When isn't it appropriate?

Television Show List Suggestions:

- | | |
|---------------------------------|---------------------------|
| - Naruto | - Canada's Next Top Model |
| - Survivor | - American Idol |
| - Big Brother | |
| - Saturday Night Live | |
| - Amazing Race | |
| - King of the Hill | |
| - The Simpsons | |
| - Buffy the Vampire Slayer | |
| - Dawson's Creek | |
| - Friends | |
| - Fox News | |
| - CNN | |
| - The Daily Show | |
| - The Office | |
| - Blue Planet/ Planet Earth | |
| - Candid Camera | |
| - CSI | |
| - Degrassi: The Next Generation | |
| - Seinfeld | |
| - Gossip Girl | |

Webpage Construction

A component of developing media awareness is encouraging the production of new media. As use of the Internet continues to increase, students are likely to encounter and interact with numerous websites daily. As part of media awareness education, it is important that students can competently and critically analyze not only the surface aspects of a website, but also the underlying components. Having students create their own websites while under the supervision and direction of a teacher can encourage them to consider aspects of websites, including: design, presentation, content, and the numerous decisions necessary in construction.

Several suggestions are listed below:

- As a class, visit several reputable and appropriate websites (e.g., www.louvre.fr/louvrea.htm, www.nasa.gov, www.nationalgeographic.com)
- Discuss and create a list of elements of a good website
- Have students choose a topic of interest, plan and create a website (see website construction links for more information).
- If students have completed lessons on copyright, ensure they supply proper references and follow regulations.
- Encourage students to use a variety of texts (e.g., pictures, videos, music, etc.).
- After students have created their websites, discuss their projects.
 - o What was the most challenging part of building your website?

- What did you like best about the project? What did you enjoy the least? Why?
- How would this website be different if not completed for school? What changes would you make and why?

Furthermore, a discussion of the differences between website construction in school compared to construction at home may give insight into the ethical and moral use and creation of the Internet. Why should these behaviours be different and why? What makes the use of some websites at home inappropriate at school? Should there be a difference?

Website Construction Links:

<http://www.kidsturncentral.com/topics/computers/htmakewp.htm>

http://personalweb.about.com/od/basicwebdesigntips/Basic_Web_Design_Tips_to_Get_Your_Started_in_the_Right_Direction.htm

<http://www.wikihow.com/Make-a-Website>

<http://sites.google.com>

<http://www.webs.com/>

Also consult school administrators and computer technicians for school-approved and/or endorsed website construction programs and licenses.

****As a separate activity or additional component, have students create an advertisement for a given product. Some recommended products may include: shoes and other clothing, perfume, make-up, automobiles, cereal, board games, soft drinks and other food, movies, and music. Creating an advertisement will allow students to explore and analyze components of advertising and encourage**

awareness of advertisement techniques and strategies. Some areas to consider may include: audience, advertising techniques, attention-getting strategies, text (i.e., audio, video, print, and combinations), and presentation of the advertisement.

What's New(s)?

A primary consideration for the quality of information depends on the source of the information. For many people, a primary source of daily information comes from the news, either through video or radio broadcasts, or through print such as the newspaper. However, these sources of information are not all the same as they differ in their presentation, delivery, and occasionally even content. For this reason, it is important to highlight these differences and improve student awareness and critical evaluation skills. Several suggestions are given below:

- Have students compare and contrast coverage of the same news story in multiple newspapers.
- Remind students to look for differing points of view, opinions, presentation layout, etc., in print and in pictures.
- Use some discussion questions to guide students if necessary, such as:
 - What is the purpose of the media texts?
 - Who is their audience?
 - What similarities and differences do you notice?
 - Why are these differences present?
 - Who is producing these media and what are the reasons for production?

- Use a similar method to examine multiple news websites (e.g., cbc.ca, bbc.co.uk, cnn.com, foxnews.com).
- Finally, examine differences between different media types (newspapers vs. websites).
- Discuss these differences and their consequences.
 - o Which medium is more engaging? Why?
 - o Which medium is more accurate?
 - o Why is it important to use multiple sources when doing research?
 - o What are the consequences of inaccurate information? How can this inaccuracy be prevented?

My Digital Identity

As information becomes increasingly digitized and people spend more of their lives online, their identities begin to take on digital and virtual qualities as well. People develop online profiles and avatars to represent themselves as they interact with the virtual world and with other people. It is important to understand that these interactions experienced online still have a connection to the physical world and that virtual interactions can have real consequences. To make this connection, it is important to create an awareness of one's identity online and examine how it fits in the real world. Several suggestions for activities are given below:

- As a class, create a list of some non-digital activities done by students in the class. These can be sports activities, clubs that they are members of, hobbies, interests, etc.
- Ask students to describe themselves by creating a list of things that make up their identity. Give an example (e.g., My name is Tom Smith, I am a boy, I play basketball, I love collecting old cameras, I am very tall and have brown eyes, etc.).
- Discuss the idea of digital or online identities and tell the students that they will be attempting to map their digital/online identities onto each other.
- Ask the students to first draw a box representing their physical identity on a large piece of paper.
- Next have students add some of their online activities. These can be websites they frequent, message boards and forums of which they are members, social networking sites, email accounts, online subscriptions, hobbies and creative activities that have digital components, online sites they use for school, work, shopping, etc.
- Also ask the students to indicate the activities that have an avatar or profile.
- Next, have students individually, in pairs, or in small groups work to connect each of their online or digital activities with something in the physical world (e.g., flickr.com account ←photo sharing with friends and family→My Physical Identity).

- Finally, as a class or in small groups, discuss the activity.
 - Was there anything about your online identity that surprised you?
 - What were the connections that were the most difficult to make?
Why?
 - Were there any connections you could not make?
 - Did you find digital representations of all the activities listed in your physical identity and vice versa? What activities were missing?
 - How closely do your physical and digital/online identities match?

Additional resources.

Additional Information:

Adbusters - <https://www.adbusters.org/>

Center for Media Literacy - <http://www.medialit.org/>

Canadian Teachers' Federation - <http://www.ctf-fce.ca/>

Media Awareness Network - <http://www.media-awareness.ca/>

Media Literacy Kit - http://www.medialit.org/bp_mlk.html

National Association for Media Literacy Education - <http://name.net/>

Media Literacy: United States Teaching Standards -

http://www.frankwbaker.com/state_lit.htm

Articles:

NY Times – Lessons on Watching Television -

<http://www.nytimes.com/1990/12/10/us/for-students-in-an-electronic-age-lessons-on-watching-television.html?scp=5&sq=media%20literacy&st=Search>

NY Times - Teaching the Young to Read Ads -

<http://www.nytimes.com/2010/04/27/business/media/27adco.html?scp=3&sq=media%20literacy&st=Search>

Activity Ideas:

Media Lesson Plans –

<http://www.shambles.net/pages/learning/resources/medialess/>

PBS Media Education Activity Ideas -

http://www.pbs.org/teachers/media_lit/getting_started.html

Passport to the Internet - <http://www.media->

[awareness.ca/english/catalogue/products/descriptions/passport.cfm](http://www.media-awareness.ca/english/catalogue/products/descriptions/passport.cfm)

Glossary of terms.

Advertisement: A form of communication or public notice used to persuade an audience to acquire or experience some product or service.

Analog: Media software that has a physical quality and presence.

Avatar: A computer user's online or digital representation of himself/herself. Usually depicted in two-dimensional or three-dimensional form, it can include factual and non-factual information regarding the user's name, appearance, background, and all other elements of description.

Digital: Storage and transmission of information through the reduction and reassembly of discrete values (digits).

Digital/Online Identity: A social identity that one develops through online communities, interactions, and expression using the Internet and other digital media.

Mass Media: Channels of communication involving the flow of messages produced by a few for the consumption of many people.

Media: Sound, images, print, or a combination of all three.

Media Literacy: The ability to access, analyze, evaluate, and communicate messages in a wide variety of forms.

Text: A coherent set of symbols used to transmit and communicate a message through print, video, audio, or a combination of the three.

Chapter 3: Discussion

This project involved the use of a literature review to develop a set of three teachers' guides designed to help better understand and promote discussion around the areas of copyright, privacy, and media literacy. In this final chapter, I explain the connections to research that directed the creation of the guides as well as further directions of study. I then reflect on my experience in writing this project including some of the challenges and realizations that occurred, and changes I would make in hindsight.

Research Connections

The motivation behind writing these three teachers' guides was to create a useful tool for introducing and instructing topics involved in the ethical and moral use of ICT (Information Communication Technology). The first step in this process involved a review of cyberethics, exploring its history and development. This exploration was followed by an examination of the need for cyberethics education, as well as its current status in the primary, secondary, and post-secondary school systems.

As all cyberethical issues have an online basis, all share some fundamental cyber-related problems. Because of this commonality, it was important to conduct research regarding the development of cyberethics itself and examine its inherent challenges before moving onto specific issues regarding copyright, privacy, and media literacy. One of the major debates in the field has been whether or not

cyberethics is a unique area of ethics that deserves study (Johnson, 1985; Moor, 1985; Tavani, 2002). With recommendations of Tavani (2002) and Floridi (2002), this report sides with the idea that cyberethics is separate from traditional ethics; furthermore, new measures of education are needed to develop the proper knowledge, skills, and attitudes in students.

My review of the literature also revealed several challenges and recommendations for improving cyberethics education, which ultimately led me to the development of the guides. One of the primary concerns of cyberethics was the noted lack of easily accessible information and training (ETPRO, 2008; Greening et al., 2006; Kafai et al., 2007). The main intention of these guides, therefore, is to provide a way for teachers to quickly and easily find this information and equip themselves with the knowledge to steer their students confidently through the material. From a training perspective, creating a useful tool also meant developing guides simple enough to use so that any teacher, no matter how experienced, could easily pick up, comprehend, and apply the guides to classroom instruction without assistance. This ease of use was achieved through the background information and additional information sections in each of the guides. My providing a brief history of the topic and the issues should help teachers acquire a quick overview explaining the problem's development, some of the key stakeholders involved, and current and future directions. Additionally, a glossary is included with each guide to explain key terms. Numerous links to online resources are given to help teachers find additional information and keep their knowledge current. Finally, lesson suggestions are independent of one another and not given in any particular order or with

prescriptive detail so that teachers may pick and choose whichever lessons they want, or adapt them as necessary.

A second major obstacle in the education of cyberethics is the limited scope and lack of depth of coverage of the topic (Greening et al., 2006). While these three teachers' guides do not cover the numerous cyberethical issues and information, they extend the available resources to improve both breadth and depth.

The three topics of copyright, privacy, and media awareness were chosen as they represent some of the most salient cyberethical issues at present. Within each guide and in addition to the background information, the lessons and lesson ideas provided are intended to both introduce issues relating to each of the topics and motivate a desire for further learning. Following the suggestions of Canosa and Lucas (2008), several lessons focus on role-play through debate, or examining real-life scenarios in case studies. Most of the lessons also encourage active participation by the students, to help engage the students and allows students to have a voice so they begin developing their own moral reasoning, as recommended by Covalleskie (1992) and Yamano (2006). In particular, the lessons involving debates, dilemmas, and case studies challenge students to take a critical approach in analyzing the scenarios and to engage in meaningful discussions with each other.

Suggestions to further expand the coverage of these topics are the inclusion of acquiring important skills and an evaluation of student attitudes regarding some of the issues (comparing the pre and post their activities). Lesson suggestions such as learning how to properly cite and reference different materials, how to evaluate and improve Facebook privacy settings, and how to construct a website give

students important skills in managing their lives online. Evaluating students' online identities, and debating the rights and wrongs of copyright behaviours and privacy violations can challenge students to examine their attitudes regarding each topic.

Directions for Further Study

As this project only seeks to develop a useful document for teachers to use, the next logical step is to implement the guides and study their effectiveness. Only by using the guides will their potential effectiveness be known and problems addressed. A major limitation of the project concerns the connection between the ICT issues presented and the moral and ethical behaviours of students. Without studying the effects of these guides, it is unknown whether or not education regarding these issues would have any impact on students' ethical and moral behaviour at all. Even if students are able to gain skills and knowledge regarding these issues, the effect on their behaviour is unknown and cannot be attributed to the guides without proper study.

A second area for further study regards the numerous other cyberethical issues not discussed in the three guides. Issues such as cyberbullying, online vandalism, hacking, cybertheft, Internet addictions, and problems surrounding pornography and explicit material are all areas that should be explored in addition to the three presented in this project. Also, as technology continues to improve and innovations appear, new challenges and problems will inevitably arise. Currently, new online legislations concerning copyright are being discussed and the

implications of such legislation on copyright and other issues, such as privacy and personal freedoms, provide many areas for study.

My Project Experience

Carrying out this project allowed me to explore areas and interests in my own life, while developing a guide for teaching areas that I believe to be important for students to learn.

Having a passion for technology and education, I grabbed this opportunity to analyze current ICT issues and develop lesson plans. However, as the project progressed, I experienced several challenges. It was extremely difficult at first to find a method of separating the issues as they are all very well connected with each other; moreover, it was difficult to cover one issue without also addressing another. Only by first going back and researching the history and development of cyberethics and each issue on its own was I able to competently and clearly define the issues on which to focus.

A second challenge concerned the overall scope of the project. Originally planned to cover five specific topics, the amount of information soon became overwhelming as each issue is capable of being its own project containing its own history, development, problems, and direction. As I researched each issue, I invariably found more information. I eventually made the decision to focus on only three issues instead of the original five. In hindsight, I should have started with three issues or perhaps even have focused on creating a comprehensive guide for one issue alone. In this way I may have avoided confusion of subject areas while also

freeing myself to overlap into other issues and go into greater depth. Despite this obstacle, I was able to learn a great deal in the various issues, and the project allowed me to cover a wider range of cyberethical issues.

What began as a project intended for others allowed me to look into questions I had often wondered myself. Forcing myself to choose only three of the many possible issues, I took one what I believed to be the most important and interesting topics. Researching information on copyright, I was able to uncover the legalities of infringement behaviour, which also led me to discover how Canadian copyright legislation differs from that of the United States. Similarly, research on privacy legislation informed me on exactly what personal information was protected, the limits of privacy, and consequently on what can be done to protect privacy. Finally, the information gathered on media awareness made me question and consider my own online interactions with media and technology and evaluate my motivations for using ICT. Upon completing this project, I hope that some of this interest is evident in the guides. My intention is also to spark the curiosity of those who may use these guides, as they did for me.

References

- Aufderheide, P., & Firestone, C. (1993). *Media literacy: A report of the national leadership conference on media literacy*. Queenstown, MD: Aspen Institute.
- Applin, A. (2006). A learner-centered approach to teaching ethics in computing. *Proceedings of the Special Interest Group in Computer Science Engineering 2006*, 1-5.
- Barroso, P., & Melara, G. (2004). Teaching of computer ethics at the state of California's universities and other countries. *ETHICOMP E-Journal*, 1(3). Retrieved August, 17, 2010 from http://www.ccsr.cse.dmu.ac.uk/journal/articles/barroso_p_teaching.html
- Baum, J. J. (2005). Cyberethics: The new frontier. *Techtrends*, 49(6), 54-55.
- Bell, M. A. (2002). Kids can care about cyberethics! In P. Barker & S. Rebelsky (Eds.), *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2002*, 127-132.
- Bynum, T. W. (2000). The foundation of computer ethics. *ACM SIGCAS Computers and Society*, 30(2), 6-13.
- Bynum, T. W. (2008). Chapter 2: Milestones in the history of information and computer ethics. In K. E. Himma & H. T. Tavani (Eds.), *The handbook of information and computer ethics*. Hoboken, NJ: Wiley. Retrieved August 19, 2010 from <http://library.books24x7.com.proxy.queensu.ca/toc.asp?site=QLUOC&bookid=26058>

- Canosa, R. L., & Lucas, J. M. (2008). Mock trials and role-playing in computer ethics courses. *Proceedings of the 39th Special Interest Group in Computer Science Engineering technical symposium on Computer science education 2008*, 148-152.
- Carpenter, C. (1996). Online ethics: What's a teacher to do? *Learning and Leading with Technology*, 40, 58-60.
- Choulat, T. (2010). Teacher education and Internet safety. In D. Gibson & B. Dodge (Eds.), *Proceedings of Society for Information Technology & Teacher Education International Conference 2010*, 2583-2589.
- CIPPO – Canadian Intellectual Property Office. Retrieved Aug. 12, 2010 from http://www.cipo.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/h_wr00003.html?OpenDocument
- Covaleskie, J. F. (1992). Discipline and morality: Beyond rules and consequences. *The Educational Forum*, 56, 173-183.
- Crystal, J., Geide, C., & Salpeter, J. (2000). The concerned educator's guide to safety and cyber-ethics. *Technology & Learning*, 21(4), 24-31.
- Dill, B. J., & Anderson, R. E. (2003). Ethics-related technology policies in schools. *Social Science Computer Review*, 21(3), 326-339.
- Dowling v. United States, 473 U.S. 201 (1985).
- Educational Technology, Policy, Research, and Outreach [CTPRO]. (2009). National cyberethics, cybersafety, cybersecurity baseline study. *The Education Digest*, 74(7), 35-44.

- Floridi, L. (1999). Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology*, 1, 37-56.
- Greening, T., Kay, J., & Kummerfeld, B. (2004). Integrating ethical content into computing curricula. *Proceedings of the 6th conference on Australasian computing education*, 91-99.
- International Telecommunication Union. (2009). *The world in 2009: ICT facts and figures*. Retrieved Sept. 1, 2010 from: http://www.itu.int/ITU-D/ict/material/Telecom09_flyer.pdf
- Ipsos Reid (2009). *Weekly Internet usage overtakes television watching*. Retrieved July 10, 2010 from <http://www.ipsos-na.com/news-polls/pressrelease.aspx?id=4720>
- Johnson, D. (1985). Should computer programs be owned? *Metaphilosophy*, 16, 276-288.
- Johnson, D. (2001). *Computer Ethics* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.
- Kafai, Y., Nixon, A., & Burnam, B. (2007). Digital dilemmas: How elementary preservice teachers reason about appropriate computer and Internet use and their predictions of students' judgments and justifications. *Journal of Technology and Teacher Education*, 15, 409-424.
- Kellner, D., & Share, J. (2007). Critical media literacy: Crucial policy choices for a twenty-first-century democracy. *Policy Futures in Education*, 5(1), 59-69.

- Ki, H., & Ahn, S. (2006). A study on the methodology of information ethics education in youth. *International Journal of Computer Science and Network Security*, 6(6), 91-100.
- MacQueen, H., Waelde, C., & Laurie, G. (2008). *Contemporary intellectual property: Law and policy*. New York: Oxford University Press.
- Maner, W. (1980). *A starter kit for teaching computer ethics*. Hyde Park, NY: Helvetia Press (published in cooperation with the National Information and Resource Center for Teaching Philosophy). [Originally self-published by Maner in 1978.]
- Martin, C. D. (1999). From awareness to responsible action (part 2): Developing a curriculum with progressive integration of ethics and social impact. *ACM SIGCSE Bulletin*, 31(4), 10-12.
- Media Awareness Network. (2010). *Practical tips for protecting online privacy*. Retrieved August 13, 2010 from http://www.media-awareness.ca/english/resources/issues_resources/issues_tipsheets/protecting_online_privacy.cfm
- McQuade, S. C. (2007). We must educate young people about cybercrime before they start college. *The Chronicle of Higher Education* 53(18). Retrieved August 12, 2010 from <http://find.galegroup.com.proxy.queensu.ca/gtx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T002&prodId=CPI&docId=A156585439&source=gale&srcprod=CPI&userGroupName=queensulaw&version=1.0>

- Milson, A. J., & Chu, B. (2002). Character education for cyberspace: Developing good netizens. *The Social Studies*, 93(3), 117-119.
- Moor, J. H. (1985). What is computer ethics? *Metaphilosophy*, 16, 266-275.
- Nguyen, T. T. (2009). Internet safety - responsibilities and readiness. In I. Gibson et al. (Eds.), *Proceedings of Society for Information Technology & Teacher Education International Conference 2009*, 1660-1665.
- Prensky, M. (2001). Digital natives, digital immigrants part 1. *On The Horizon*, 9(5), 1-6.
- Prensky, M. (2005). Listen to the natives. *Educational Leadership*, 63(4), 8-13.
- Robertson, H. (2005). Can schools be value-free zones? *Education Forum Toronto*, 31(2), 8.
- Spradling, C.L., Soh, L., & Ansorge, C.J. (2008). Ethics training and decision-making: Do computer science programs need help? *Proceedings of the Special Interest Group in Software Engineering 2008*, 153-157.
- Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior*, 7, 321-326.
- Tavani, H. T. (1999). Informational privacy, data mining, and the Internet. *Ethics and Information Technology*, 1, 137-145.
- Tavani, H. T. (2002). The uniqueness debate in computer ethics: What exactly is at issue, and why does it matter? *Ethics and Information Technology*, 4, 37-54.
- Thoman, E., & Jolls, T. (2004). Media literacy – A national priority for a changing world. *American Behavioral Scientist*, 48(1), 18-29.

Thompson, P. B. (2001). Privacy, secrecy and security. *Ethics and Information Technology*, 3, 13-19.

Yamano, P. (2006). Cyberethics in the elementary classroom: Teaching responsible use of technology. In C. Crawford et al. (Eds.), *Proceedings of Society for Information Technology & Teacher Education International Conference 2006*, 3667-3670.

Appendix A: Copyright Scenarios

***Note:** While the scenarios here are presented with information regarding the legalities of copyright, this focus should not prevent a discussion surrounding the fairness or morality of each situation. As can be seen in the history of copyright, laws can be changed as new situations and considerations emerge.

Scenario #1

James has just missed the last showing for a movie that he has been meaning to see for a long time. His friends have been saying it is the best movie they have ever seen. Eager to join in on conversations about the movie John decides to download the movie from an Internet website.

Unless the movie studio has given permission, or the copyright holders have been reimbursed, downloading the movie is a direct violation of copyright law. Downloading the movie for free prevents the studio from gaining revenue to which it is entitled.

Scenario #2

While at work Mary has missed an episode of her favourite television show. Unfortunately the episode will not be airing again anytime soon and is unavailable from the network website. Mary decides that, since it is important to keep up with the storyline for next week's episode, she is going to try and download it through a free website specializing in television file rips.

Just because a website is free does not mean that it is legal. In the United States, unless the network has given permission or the copyright holders have been reimbursed, this is an infringement of copyright as it prevents networks from generating revenue through advertisements or subscriptions. In Canada, however, the downloading of files from peer-to-peer networks has been deemed *legal*, although uploading is not. Therefore, as long as Mary is not uploading the TV show she has downloaded, she is not violating copyright.

Scenario #3

Jane is an avid music lover and is constantly seen listening to music on her ipod at concerts and in music shops. She regularly spends all of her money on the latest records, concerts, and tracks from itunes. Unfortunately, there is always more music that she wants to listen to and that she does not have enough money for. She decides to download a few albums and tracks every now and then to support her music habit.

Unfortunately for Jane, copyright violations do not depend on how many times you have obeyed the laws, only when you break them. Downloading music without purchasing or permission is still an infringement of copyright.

Scenario #4

A professor is teaching a film studies course. She records a television show using her PVR and copies it onto a DVD. She then places it in the school library for her students to study after class.

In Canada, a copy of any broadcast may be made and kept for 30 days to be evaluated for educational use. After 30 days, the broadcast must be destroyed or royalties paid. This evaluation copy may not be shown in class without payment of royalties to the copyright holder

In the United States, because the professor is using the television show for academic purposes, it falls under fair use and is not in violation of copyright law. However, this use may not qualify if the show does not directly apply to what is being studied (e.g., a television show illustrating lighting techniques for film studies is acceptable, whereas a show shown for its amusement may not be).

Scenario #5

A band writes and records an album's worth of songs, signs to a label, re-records the material, and puts one song out as a single. That single gets played on radio and today, we hear the song in a restaurant.

There are three copyrights in music: the sound recording, performance rights of the artist, and composition rights (the song and lyrics).

As the creators, the band holds the rights to their composition. After signing with the label and re-recording, the label will own the rights of the recording. The label owns the single, and for the radio to play the recording it must have authorization to comply with copyright. Finally, the restaurant playing the song from the radio to the public is an infringement of copyright unless the restaurant has received permission or is compensating the band.

Scenario #6

Mr. Thompson, the English teacher, downloaded the black-and-white horror classic *Night of the Living Dead* from the Internet Archive and has decided to show the movie to his class for Halloween.

In Canada, videos/DVDs cannot be shown in public places, including classrooms, without public performance rights from the copyright owner. Even if the video is for educational purposes, and no admission is being charged, the title's rights must be purchased or given. However, if the works are in the public domain, which in this case they are, they can be used and copied freely. Mr. Thompson has therefore not violated any copyright laws.

Scenario #7

Carmen makes a CD of her favourite playlist so that she can enjoy it in her car. One day her best friend Jenny listens to it and asks to borrow the CD.

If Carmen owns each of the original tracks, either downloaded, from a CD, etc., she may make a copy for personal use under the Canadian Copyright Act. The act has established a system of levy fees on blank media to provide royalty payments to the authors and creators. This copy, however, cannot be made for someone else or for any other purpose including selling/renting out, distributing, communicating to others, or performing the recording in public. By lending it to her friend, Carmen would be violating the Copyright Act.

Scenario#8

Saneal's favourite band is Radiohead. Being a budding musician he decides to cover their song "Paranoid Android" and frequently plays it live when performing. He gets such a positive response to the cover that he records it to a CD for release.

The copyrights that exist in this case are the recording, the performance, and the composition. Since this is a cover, there is no violation of copyright on the original recording. The performance rights also don't apply since they have to do with Radiohead's performance. As long as the live performance isn't recorded, it also does not infringe on copyright. The only problem in this scenario is when Saneal records the cover to a CD. For this action to comply with copyright laws, he would have to get what is called a *mechanical licence* from the persons(s) who hold the copyrighted music.

Scenario #9

An instructor copies the papers submitted by the students in her class and brings them to the library to place on reserve.

Since the act of creating a work automatically entitles the author copyright status, each of the students will own the copyright to his or her paper. The instructor will need permission from each student to copy the papers and should get the permissions before bringing the papers to the library.

If an instructor gets permission to copy a student-authored work for use in library reserves, she would need new permission to use the work again during any subsequent academic term.

Scenario #10

Andrew is an art lover and regularly frequents the museums and galleries in his hometown. Often he brings his camera and takes photographs of his favourite pieces to share with his friends. One of these pictures is very striking, and captures a group of people looking intently at some of the artwork in the background. One of Andrew's friends copies this picture with a computer scanner and submits it to be published in a photography magazine as his own.

As the photographs Andrew is taking are likely of lower quality, they would not compete in the same market as the original and would not take away any revenue by this reproduction. This photography would, therefore, not likely violate any of the copyrights of the artwork.

Andrew would be automatically given copyright over the work he created through his picture. His friend copying Andrew's artwork for publication would therefore violate copyright unless Andrew had given the friend permission.

Another thing to keep in mind is the privacy of the people in the photograph. Especially if the photograph will be published or displayed in public, permission from the people in the photo may be needed, or they may request that the photograph be deleted or destroyed.