Laws and Legalities of Technology Based Cyber Crimes

Includes:
Final Report

By
Eric Fournier

Completed for: Tek Desk
Supervising Professor: Sharon Beaucage-Johnson
Trent Centre for Community-Based Education

Department: Forensic Science
Course Code: FRSC 4980Y
Course Name: Community-Based Education
Term: Fall/Winter 2010-11
Date of Project Submission: April 2011

Project ID: 4101

Call Number:

Laws and Legalities of Technology Based Cyber Crimes

By: Eric Fournier

Completed for: Tekdesk (project of Community Opportunity Innovation Network)
Course Coordinator: Sharon Beaucage-Johnson, Trent University
Trent Centre for Community-Based Education

Department: Forensic Science
Course Code: FRSC 4980Y
Course Name: Community-Based Education
Completion Date: April 2011
Project ID:4101

Dedication

This research is dedicated to allow to all individuals who experience the wonders and potential of all cyber technology and plan to use it within the legal realm.

Acknowledgement

A special thanks to both Sharon Beaucage-Johnson and Christie Nash for setting this research in motion and keeping it up in the air. Without both of you this project would not have started, progressed, and been completed in a well-polished manner. I would also like to thank Jim Hauraney who took time out of his day to help with any questions and marking.

Adrianne Schutt and Tekdesk, you made this project more enjoyable with your love and knowledge of technology, which gave me some interesting ideas and distractions when needed for a break from work. Without your determination and drive to ensure this project was continued it would have ended a long time ago.

Friends and family, without your encouragement and support this project would not have been as enjoyable and educational as it became.

Abstract

Working with Tekdesk in Peterborough, the purpose of the research was to determine all the current laws and legalities of Canadian law and where we, as Canadians, stand compared to similarly developed countries. This report contains the current research of important Canadian Laws as found in the Criminal Code, refined by relevant case law as found on canlii.org. This report also contains comparisons of Canadian laws with relevant European and American laws to determine the contrasting differences between them. The vast majority of this information was obtained and analyzed to help individuals use cyber technology safely within the accepted parameters of Canadian law. With the information gained from the cyber technology laws research it will aid in the development of programs geared to safe usage of a computer system.

Table of Contents

Key Definitions

Bulletin Board	A form of communication on the internet on which users post comments, photos and videos for others to view.
Cracking	The ability to get past the software's designed security feature in which the user is required to enter a security key.
Criminal Code	A list of offences deemed illegal with explanations to the penalties associated with each.
Cyber	Refers to the internet and technology associated with it.
Digital Forensics	A branch of forensics associated with computers, cellular phones, and other such devices.
Doctored	The modification of an original piece. Alterations, deletions or additions added to change the initial integrity of the original piece.
Downloading	The act of taking a file from the internet and copying the contents to the user's computer.
Hacking	The breaking into a computer system or network without the authorized permission of the owner. Damage must not be done to be considered hacking.
Indictable Offence	Considered a more serious offence, may be tried by judge or judge and jury.
Online	The use of the internet/web to accomplish a task such as online banking, online gaming, online dating.

Phishing	The use of a deceptive page, that looks like the normal log in page, to acquire sensitive information such as passwords or banking information.
Sexting	The sending of explicit messages or pictures via cell phone.
Social Networking	A platform for individuals to connect with others to form business or personal relationships.
Streaming	A live feed of a program done through an internet connection. These programs can include items such as sporting events, daily TV episodes, movies or music.
Summary Offence	Deemed a lesser or petty crime which would be tried by judge only.
Virus	A malicious file that, when run by the device user, can inflict damage to software or data. Viruses can be spread in a number of ways, such as shared USB drives, removable hard drives, or attachments to email messages.
Worm	A virus that does not require action from the device's user in order to spread to a new device. Worms can search out and copy themselves to new hosts without human assistance.

Introduction

Purpose of the Research

Tekdesk is based out of the Peterborough Library and offers technology help to non profit organizations and libraries. Tekdesk is willing to research computer related problems and have a computer lab to enhance their ability to teach courses and troubleshooting. The aim of Tekdesk is to provide a wide variety of services including training and boardroom sessions, helping learning with items as Microsoft Office, networking, creation of personalized web pages based on one's company specifications and customer support.

As part of a growing project based, the Trillium Foundation-funded Internet Safety Collaborative project is to roll out a technology based safety training program for social and care workers. This research is the continuation of the project, in which the first step examined the risks associated with cyber technology conducted by last year's FRSC 4890 student, Andrew MacLean. His report was a large composition of the different health risks including psychological, physical, legal, social and financial risks that are associated with the use of cyber technology. The continuation step of this project was to determine the laws and legalities of technology based cyber crimes.

The three stage step includes the relevant research to better develop current and helpful information related to cyber technology, curriculum development based on the research obtained and finally the implementation of the curriculum to the required areas and to individuals who require the teachings. From the findings of the present research, a curriculum will be developed to teach individuals in high risk areas to help keep the social/care workers safe while helping

them effectively use the cyber technology within the law. Implementation of the curriculum will occur to which teachings will be to ensure that those using the cyber technology are not only safely using the internet and related technology, but also doing so within the laws of the Canadian government. Instructions will include both the classroom settings and online delivery.

Relevant Forensic Issue

Forensics is able to be involved in a number of areas from engineering to biological to digital. This research was aimed at the digital forensic issue. With many advances in the digital technology there has been a greater increase in digital crime. An increase in digital crime requires an increase in digital forensics. In order for authorities and individuals to understand the legal implications of being connected worldwide, there must be an increase in awareness of the potential risks associated with digital technology.

Along with the growing trend of digital technology come the new ways to commit crimes. Digital technology has forever changed the way society is able to shop, communicate, bank, and store information. As a result new crimes using digital technology are being committed. With the use of cyber space, criminals are now able to steal credit card information without ever touching the card. Criminals are able to attack victims by sending malicious software which can damage an entire network of computers, causing mass terror and destruction. Criminals are able to steal an individual's identity and make fake passports and other such documents. With the ability to send and receive information over the internet, there is a growing increase in the number of explicit websites which contain child pornography, bestiality and exploitation. Due to the increase in crimes in the cyber world, there is a constant stream of cases setting new precedent. The new cases result in the development of new legislative bills that refine and or add new sections to the criminal code.

Interpreting Law

In order to decipher what the law is pertaining to each particular issue this paper will examine both the exact criminal code wording and the case law that has been developed to aid in decoding the precise meaning. The criminal code there must be vague yet precise, so that the crimes being described are not conditional. In order for this to be accomplished an understanding of the wording used must be achieved by dissecting the meaning. This is where Section 2 of the criminal code will be useful. This section is a glossary of terms that define certain of the key words throughout the code. From now on the terms such s.2 or s.3 will refer to the subsequent section of the Canadian Criminal Code, such as section 2 will be stated as s.2.

Laws written in the criminal code are open to interpretation and all encompassing in their wording and serve their purpose in this way. If the laws were extremely precise it would allow for any modification of an act to be able to get around the rules.

> *For example: if the law was to read that it is illegal to steal computer information, then any individual who stole computer hardware such as a wireless mouse could not be found guilty under this law. The law would have to be extremely lengthy in order to encompass all possible scenarios. Instead, the laws that have been stated are vague and open to interpretation in which case law has been used to determine if what an individual has done falls within the law or is deemed illegal.*

For the purpose of this paper the laws which have strong ties to technology were looked at, analyzed and case law was found to help determine what the meaning is in the criminal code in order for any individual to understand the law.

Methodology

The first step of this paper was to examine all the laws that were contained in the Canadian Criminal Code and determine the relevance to cyber technology. If the law was related to cyber technology it was held for further researched, if not, it was discarded. From the remaining laws which pertained to cyber technology it was first summarized in the associated section below. Next any helpful case law was found and summarized, from both the law and the case law around the section, a summary of the importance of this law was included and how it implications on cyber technology. Upon the completion of the Criminal Code, there was research done into the potential for any new bills that would include new legislation in the Criminal Code or included in the provincial laws.

The second aspect of this project examined how Canadian law is changing with respect to cyber technology. Canadian law is constantly redefined based on the implementation of legislative bills. To further understand that movement of cyber technology any recent change to legislation will be analyzed and included in this research paper.

The last aspect of this report analyzed how Canadian law compares to similarly developed countries based on scholarly articles. The articles chosen to be analyzed were based on either a shared similarity between Canadian law and the country, or the opposite to which offered a different view on how cyber technology and law should be handled. If the country had similar laws, it was analyzed and determined how similar the two countries' laws were, however if the law existed in another country but not in Canada it was stated what the implications of this law have on Canadian if the law were implemented.

Criminal Code

Definitions

Section 2 (1:2-20)

This section is designed to define commonly used terms throughout the Criminal Code. It is highly recommended that the reader become familiar with the terms in this section for a better understanding.

Ignorance of Law

Section 19 (1:61-62)

This section refers to the defence of not knowing that a crime is illegal a non valid excuse.

Case Law

There is no relevant case law relating to cyber technology at this time, however this section is just designed to remove the defence of not knowing laws.

Summary

The purpose of this section is to eliminate the excuse by any individual to claim that "I didn't know it was illegal."

Parties to Offence

Section 21 (1:63-68)

This section makes it illegal to commit or encourage and individual to commit and act as well as state that it is illegal to omit an action in order to help commit an offence.

Case Law

R. v. Bishop, 2007 ONCJ 441 (2)

This case law discusses the differences between being or not being a party in a committed offence. If an electronic document was recorded and stored on another's computer with the intent to help the individual, then in this instance they could be charged as a party to the crime. However, if they are unaware of the implications or the purpose of this document and it is stored in a regular manner as not to conceal it, then the individual should not be charged with being a party to the offence.

Summary

Based on this section it makes it illegal to help commit an illegal act by an active mean. In other words, if the individual is only present at the scene that does not make them a party to the offence. They must actively participate in the crime, such as by supplying an instrument with knowledge of the intent of the other individual. In order to omit an act, it would be in the use of actively not performing a duty, such as not activating a password on a file type to allow another individual access. The final aspect of this section is that it is illegal to encourage other individual to commit a crime. With the ease of communications based on cyber technologies via email, text, phone, instant messaging, etc. this may be very easily, done and has the potential of serious backlash and scanning of logs, chats and other such mediums in order to find evidence which may link the individual.

Defence of Personal Property

Section 38 (1:100-101)

This section makes it allowed that one can prevent access to or take back personal property providing they do not cause bodily harm to the individual. This section also makes it an

assault should an individual try to take personal property from the individual who it belongs to if it is currently in their possession.

Case Law

At this time there is case law in the area of cyber technology.

Summary

The reason this section is interesting and should prove to be a task in the future is the use of malicious software (malware, viruses, Trojans, spyware, etc) to ensure that the individual's data is protected. Should dangerous software be used to protect personal or sensitive information there would be an argument to be made that the user should have every right if attacked to use as much force as necessary (see appendix figure 1) to protect the data contained on the computer. With the use of force, it would only be what is absolutely required to prevent and stop an individual from taking the data. As stated in the criminal code, there can be no bodily harm caused in the protection of the personal property. At this point the repercussions of infecting one's computer must be considered by the courts with regards to whether this fact is considered causing bodily harm to the user or owner of the infected computer.

.

Sabotage

Section 52 (1:113-114)

This section is designed to prohibit the act of sabotage against the safety, security or defence of Canada or any military presence in Canada.

Case Law

Hydro One v. Society of Energy Professionals, 2006 CanLII 42249 (3)

This case does not deal specifically with the idea of sabotage for the purpose of threatening Canada, but brings into the idea that the use of a potential cyber attack/crime that would result in this charge. The case law discusses the threat of sabotage to a hydro company to shut down the network removing control of the power grids.

Summary

At this point there have been no implications of the potential use for sabotage to occur with the use of cyber technology. However there is potential for this to occur and should be regarded accordingly. With the ability to sabotage a number of systems as many are connected it is only a matter of time before an individual(s) goes to extreme measures to be heard or make a demonstration.

Forged Passports

Section 57 (1:116-118)

Under this section it makes it illegal to make changes to, use, or distribute a forged passport. Along with this section there is a subsection that defines what constitutes a passport, penalties associated with being charged with a forged passport and the onus of proving the forged passport was believed to be real is on the charged individual.

Case Law

Canada (Minister of Citizenship and Immigration) v. Chen, 2003 FCT 330 (4)

This case discusses the findings of a potentially forged passport. It was believed that the passport was for forged but the forensic report could not confirm. The board believed that the photograph of the individual was doctored up (changed) and then reattached to the supporting documents. This case law brings about many potential ways in which cyber technology could be used to not only create but also doctor, plan, exchange, sell and ultimately use the passport.

R. v. Taft, 2003 BCCA 104 (5)

This case law discusses the attempted appeal on a number of fake identities and forgery accounts. The accused was charged with several counts of making fake identities, bank accounts, and forging names and signatures. When he learned that he was under investigation, he left Vancouver to create a website in Montreal which advertised the creation of more fake identifications, for a fee. Upon his arrest further eluded police by providing the officers with fake documents. It wasn't until the accused prints were identified that his actual identity was known. With the ease of travel and access to the internet, the accused was able to set up a website, create multiple forgery locations and delay court processes based on information obtained by simple want ads in the newspaper.

Summary

With the ease of access to internet, it is extremely easy to change/manipulate government documentation, which can lead to serious charges. The ability to create a webpage is relatively simple. As a result, individuals need to keep in mind that they should use care when wording personal information presented on this webpage as it could lead to fraud. This section also brings to light that the onus is on the individual to prove that the passport in their possession was not known to be fraudulent. With the internet so prevalent today it makes it extremely difficult to prevent access to forged documents. Growing concerns for terrorist threats suggest that police will not take this offence lightly.

Disobeying statute

Section 126 (1:251-252)

This section is the all-encompassing section for any act made by parliament that isn't in the criminal code. Some acts that fall under this section of the criminal code would be the Broadcasting act, Copyright act and the Income tax act. It further states the penalty should anyone not follow the act, or omits to follow a rule whereby required.

Case Law

At this time there is no relevant case law, but as mentioned earlier this is to encompass anything that could happen in the near future that dealing with two significant acts in the area of cyber technology (Broadcasting/Copyright).

Summary

This section is the precursor to any potential changes to an act that have yet to set out a punishment for breaking that statute. This section will become important in future cases that deal specifically with areas as mentioned above to which there is not a clear cut penalty associated with the offence.

Sexual Offences/definitions

Section 150/150.1 (1:283-292)

This is a very long section as it includes relevant definitions of ages, consent, etc. and then the appropriate subsections including the different offences and defences to each subsection. Section 150.1 discusses reasonable defences based on the age of the accused and complaintant. This section also discusses the problems associated with the credibility of children and the ability to allow hearsay evidence under given circumstances. The credibility of a child testifying must

be taken as such, meaning that facts may be skewed or incorrect, but it should not be compared to evidence given by an adult. The hearsay rule is allowed in this case, as the competence of a child or having a child testify may be more harm to the child so therefore hearsay may be permitted. The information in this section will be used for later sections which refer to definitions included in section 150 or section 150.1 directly.

Case Law

This section is purely for the ability to define key terms and concepts that are later used.

Summary

With all sections, the appropriate wording is required and for that purpose section 150 is used in any sexual offences when it comes to deal with words such as guardian or public place as well as when consent may not be used as a defence.

Sexual Interference

Section 151 (1:292-293)

This section discusses the potential for direct or indirect touching of an individual for a purpose that is sexual in nature. It also discusses the minimum and maximum punishments for the section. With this section comes the ability to limit the accused's type of work and the locations they can work when they are released as per section 161 (Order of Prohibition). The type of work can be limited to not be in a public area that would bring the individual into contact with an individual under 16 years old. Further restrictions can be added to prohibit the use of a computer system for the purpose of communicating with persons under the age of 16.

Case Law

R. v. Innerebner, 2010 ABQB 188 (6)

This case law discusses the potential restriction of the use of a computer system with the ability to converse with individuals under the age of 16. With this potential restriction comes two interesting aspects; the first being how long the restriction can be imposed and the second being when can a system be used for communications with persons under 16. In the case of the first aspect it was stated that the individual could be restricted for as long as life or any lesser duration deemed by the courts. When it comes to communications with persons under 16, the ability to communicate using a computer system is extremely easy from a multitude of angles such as email, discussion boards, social networking sites or instant messaging.

Summary

With this section, the potential for future consequences makes sexual interference a large concern. Penalties can cause not only a short period of damage to one's lifestyle, but also impact the rest of their life with the inability to ever own, use or be close to a computer network ever again. Based on a number of judgements made by various levels of judges, the use of computers has made children much more susceptible to luring and the subsequent sexual interference or other sexual charges. Due to this fact many judges have yet to make a statement of the potential for certain charges, however many seem to be increasingly adding the prohibition terms to limit an individual's use of a computer.

Invitation to Sexual Touching

Section 152 (1:293-294)

This section states the law for the invitation of an individual to touch the body of any individual for a sexual purpose. Touching does not have to be accomplished merely the stating of an invitation is sufficient. This section applies to those who invite an individual under the age

of 16 to directly or indirectly be involved in sexual touching. This section has now been consistently grouped with section 172.1 which was added to the criminal code in 2007 (7).

Case Law

With the addition of section 172.1 there are many cases that have included both of these, such as *R. v. A.G., 2007 CanLII 21975 (ON S.C.)* (8) which deals with emails sent to an individual. The emails were deemed nasty and disgusting by the judge, based on the sexual language used however there was no indication that the emails had the potential to be sexual in nature. The second case law that examined invitation to sexual touching was *R. v. Smith, 2007 BCSC 1955* (9), in which the individual encouraged the female to undress and touch herself. Based on the evidence presented in R. v. Smith it was found that since the Smith was involved in section 152, section 172.1 also applied.

Summary

This section of the criminal code makes it illegal to encourage an child to touch themselves. With the ease of communication today the added subsection of 172 to include 172.1 was necessary. By creating this addition it allowed for the incorporation of cyber technologies to be included with the offence of sexual invitation so that rather than just by word of mouth, gesture, or written material. All forms of computer systems are now included. Based on statistics obtained by Environics Research Group in 2004(10) as mentioned in the case of *R. v. Jarvis, 2006 CanLII 27300* (11), 79% of youth surveyed have internet at home. This figure has likely increased drastically in the past 6 years. This shows the increasing need to not only be aware of what the potential dangers are on the internet, but also what to do if one becomes in endangered.

Sexual Exploitation

Section 153 (1:295-297)

This section is designed to cover individuals between the ages of 16 and less than 18 in which the complainant and the defendant have a pre-existing non-sexual relationship, where the defendant is in, or could be viewed to be in, a position of authority. This section does not deal directly with the use of cyber technology, but gives an option to which sexual exploitation can be accomplished with the use of a computer and cyber technology.

Case Law

R. v. Lithgow, 2007 ONCJ 534 (12)

This case discusses the starting of a relationship between a teacher and a student in which emails were exchanged, eventually leading to sexual experiences. Again this event allowed for section 172.1 to play a role. The sexual nature of the emails, based on the individual's age and the position of authority led to the charges.

The final section of 153 discusses the potential for a young person to be exploitive of another young person. Unfortunately, determining case law for this aspect is extremely difficult based on the numerous possible publication bans that can be implemented to protect the identities of the victim. Publication bans can also subsequently protect the identity of the defendant, as a result of their association with the victim.

Summary

The use of the internet poses as a great threat with the ability to discretely converse in a sexual nature with an individual through chat or email. This section again looks at the newly added section of 172.1 and allows for multiple charges to be made based on the individuals' ages. Based on this section, one could potentially be charged should they be in a teenage

relationship and at some point be exploitive against their partner. For example if a male individual of 17 years old is dating a female of also 17 and has nude photos of her, which she allowed, then showed them to his best friend, he could potentially be charged under this section.

Order of Prohibition

Section 161.(1) (1:303-304)

This section is designed to limit privileges of an individual convicted of several sections in the criminal code. Limitations may include the ability to attend certain locations, employment types, and the use of a computer with the potential to converse with persons under the age of 16. These conditions can be changed over the individual's life, and reduced as the individual progresses. A breach in these conditions could result in further sentencing, with an indictable offence resulting in up to two years. A summary offence carries a max penalty of 6 months in prison and/or a fine up to $5000.

Case Law

R. v. Tootoosis, 2010 ABQB 574(13)

In this case, D. Tootoosis was convicted of several charges, including possession of child pornography. Based on the number and severity of charges, the judge imposed a lifetime ban on several items including; attending public parks, being in a position of trust for someone under 16 in a workplace setting, and the use of a computer for communications with individuals under 16 . These items included attending public areas where persons under 16 could be expected to be present, obtaining employment where he could be viewed as a person of trust to an individual under the age of 16, and using a computer system with the purpose of communicating with persons under 16 years old.*R. v. Safaee, 2009 BCSC 1350* (14)

This is a second case that makes use of section 161. The court determined that for a period of 10 years, the convicted may not have access to a computer with the purpose of communicating with individuals under the age of 16. The accused in this case was charged with sexual assault and was only limited to a 10 year prohibition from a computer as opposed to the child pornography case earlier which resulted in a lifetime ban. The sentencing length is entirely up to the judge which is often decided by taking into account the seriousness of the charge, the likelihood to reoffend and past criminal convictions.

Summary

With this section being able to limit the convicted individual's ability to work, move and use a computer, it poses serious consequences for being charged with any one of a number of charges, from possession of child pornography to any one of a number of sexual charges. The impacts of this section could be extremely detrimental to trying to obtain employment or even enjoy one's daily lifestyle. There appears to be no standard as to the length of time one can be prohibited from activities, but it appears that more serious or past offences will increase the time the prohibition will last. With jobs increasingly relying on the use of computers, a judgement limiting computer use would make securing employment extremely difficult. Avoiding positions of trust to figures under 16 may create additional job search difficulties.

Voyeurism

Section 162 (1:304-305)

This section makes it illegal for an individual to observe or record an individual who has reasonable expectation of privacy. The observee who is being recorded must usually be either in a position to be potentially nude or be nude for this section to apply. If the tape or viewing is for a sexual nature, the observee does not need to be nude or likely to be nude.

Case Law

At this time there is no case law that relates the potential for voyeurism to be a concern associated with cyber technology.

Summary

Though there is currently no case law outlining the potential for this section of the criminal code, one must first consider the potential for cyber relations via Skype or webcam. Many computers and laptops now have a built in webcam, and many computers and laptops can be found in private areas such as the bedroom or den. With that being said, there is the potential for remote activation of the webcams (via malicious software). This would allow for these cameras being turned on surreptitiously, and photos or video footage recorded, distributed etc. The reasons outlined above made the inclusion of this section relevant.

Corrupting Morals

Section 163 (Punishment in Section 169) (1:305-311 and 323)

This section makes it illegal to distribute, copy, publish, circulate, etc. any material that is deemed to be obscene material to the general public, as well as the publication of a "crime comic" which may depict a real crime. Any other material depicting exploitation of sex, crime, horror, cruelty and violence should be considered obscene under this section.

Case Law

R. v. Butler, 1990 CanLII 2614 (MB C.A.) (15)

This case examines two aspects associated with this section of the code: whether the individual is being infringed upon based on The Charter of Rights and Freedoms, and whether there is potential for sanction based on the benefit it produces for society. The judge felt that the Charter was not infringed upon, and that the Criminal Code clearly defines what is classified as

obscene material. The second issue was also dismissed, as there was no reason to for the judge to believe the material benefitted society by being published and distributed.

Summary

This section plays an important role in cyber technology because of the ease of both access and availability. It is vitally important to recognize the ability to both circulate and create obscene material, and to have it available for distribution. With regard to this section, distribution could be anything from posting a photograph, seeding a file, or adding an attachment. These are common occurrences online, and could result in an individual being charged.

Child Pornography

Section 163.1 (1:311-315)

The child pornography section of the Criminal Code is a very lengthy section, making it illegal under a number of circumstances to have or create any form of child pornography, and describing the different ways one can be charged under this section. The key parts of this section include section is definitions to what child pornography is, what child pornography can include, that accessing, viewing and transmitting child pornography is illegal.

Case Law

With this section serving as a definition section to many of the sexual charges that can be laid, and the punishments that can ensue based on the means to which the child pornography was used, there is no case law possible.

Summary

The child pornography section was added to this report on the basis of the definition of child pornography and terms associated with it. Due to the wording of the Criminal Code, the

image or representation does not have to be a real individual. A cartoon drawing or illustration of an individual under 18 could be classified as child pornography. The second issue with this section is the potential for "sexting" charges to be considered based on section 163.1(1)(b)- being any written material sexual in nature. Private recordings of lawful sexual activities (between individuals of the ages outlined in the criminal code) cannot be prosecuted when kept private. Charges may be laid if the recordings are shown to someone else (deeming them no longer private).

Luring a Child

Section 172.1 (1:326-328)

One of the few sections that directly requires the use of a computer system to facilitate the commission of several sexual offences is luring a child. This section requires other sections to be applied to it including section 153(1), 155, 163.1. This section requires the communication with an individual under the age of 18, 16, or 14, depending on the section in question. In section 172.1 it is also stated that the excuse of believing the individual was old enough is not valid, unless the accused took reasonable steps to ascertain this.

Case Law

R. v. Smith, 2007 BCSC 1955 (CanLII) (9)

As mentioned earlier in this report, this case examines the idea of more than the mere luring of a child, but the idea of grooming a child for sexual exploitation. The case involves an individual who encouraged the child to engage in sexual touching via an instant messaging program. It was deemed by a judge that even though the individual did not specifically say the exact specific words (as the spelling was incorrect) it was implied by what the accused was saying and to the manner in which he was saying it.

Summary

With the addition of this section to the Criminal Code, it allows the prosecution to directly charge an individual with the use of a computer system to lure or groom a child (under the age of 18) in a number of situations.

Spreading False News

Section 181 (1:339)

Section 181 is designed to eliminate the publication of information that one knows is false and may cause or will cause injury or mischief.

Case Law

There was no documented case law pertaining to “Spreading of False News”.

Summary

The reason this section was included in this report was because of the ease and ability to post anything anywhere on the web with little to no filters. An individual could easily post something to be misleading for the purpose of mischief. There is also the ability to cause harm by leading an individual to a malicious website which can infect the host computer, causing damage to the computer or the information stored on it. This may result in physical, emotional or mental harm.

Interception of Communications

Section 184 (1:345-348)

This section makes it illegal to purposely intercept a private conversation. This can be done in a number of ways, such rerouting texts or emails or recording phone messages.

Case Law

R. v. Giles, 2007 BCSC 1147 (16)

This case discusses complaints and violations of an individual's rights and freedoms based on the police examining the contents of a Blackberry memory card in order to read and examine emails that were stored on the memory chip. It was ruled that since the messages were properly delivered to its intended destination before being examined by the police that it was not considered an interception of communication.

Smyth v. Pillsbury Co. 914 F.Supp.97 (E.D. Pa. 1996) as cited in *Briar v. Canada (Treasury Board), 2003 PSSRB 3 (CanLII)* (17)

Based on this case it is currently not against the law for a company to monitor, intercept, or read emails. Companies may fire employees based on the content of emails sent. This illustrates a situation in which an individual accesses the private conversation, and is taken to court over the matter of a private electronic conversation being intercepted.

Summary

At this time there are very few citations on the subject of emails/texts being read/deleted/copied or intercepted by those other than the police. This will likely change, should these methods continue to be a convenient and a quick means of keeping in touch and sending sensitive information from one location to another.

Betting/Lottery/Gambling Laws

Section 202-207 (1:398-411)

The six sections in the betting and lottery section make it illegal under a number of circumstances to be involved in betting and gambling. This section makes it illegal to be involved in almost any process from which betting can occur. This includes placing a bet, having

someone place a bet, taking a bet, organizing a location to take a bet, or importing items to place a bet. This section is of importance because of online gambling and betting.

Case Law

Due to the nature of this section and because the Canadian government has yet to make a ruling as to the legality of online gambling it has been left to the provincial governments to determine the laws. Based on the Ontario government in 2010 it was announced that online gambling will occur with the help of the OLG (Ontario Lottery and Gaming Corporation) in 2012 (18).

Summary

Except the OLG or the government setting up a betting website, it is deemed illegal to place or be involved in placing of any bets online. However it appears that there is some room in the interpretation to the laws; this is due to the fact that in the Criminal Code it is deemed illegal to make any device or apparatus for the purpose of recording or registering bets (section 202.(1)(b)). There are several Canadian companies that pride themselves on creating internet gambling games such as "Cryptologic." Until more cases come forward and the changes are made to the current internet gaming laws, it should be noted that internet gambling in Ontario is illegal and the advertisement of gambling websites is also illegal (19).

Suicide – Counselling

Section 241 (1:464-465)

It has been deemed illegal by the Criminal Code to counsel or aid anyone to commit suicide. Section 241 also states the penalty for being charged and convicted under this section.

Case Law

Currently there is no definitive case law that helps determine the potential for a cyber crime to be committed.

Summary

This section was included because of the issue of William Melchert-Dinkel, who used internet chat rooms to encourage individuals to commit suicide while being recorded by a webcam. Further information can be found in the reference sections (20). Unfortunately, since the trial is still ongoing, there is no final result to include in this document.

Traps to Cause Bodily Harm

Section 247 (1:470-471)

This section makes note that an individual who sets or has possession of an object with the idea of a trap being set can be found guilty. The trap must cause bodily harm or death to be included.

Case Law

At this time there is no documented relevant case law.

Summary

With the previous study done by Andrew MacLean (21), this section was chosen to be included for its potential to be used in a future application of cyber technology. There have been serious threats such as financial problems, stress, health problems as outline in the research conducted by Andrew MacLean, associated with cyber technology, and it is highly possible to cause bodily harm.

Criminal Harassment

Section 264.(1) (1:550-557)

According to section 264, one can be charged with criminal harassment based on a persistent conduct which causes one to fear for their safety, or the safety of people they know. Based on this and similar sections (264.1 - Uttering Threats and 265- Assault) it requires the accused to be without lawful excuse.

Case Law

R. v. Labrentz, 2010 ABPC 11 (CanLII) (22)

This case brings to light the issue of a number of harassing emails sent to an individual. Based on these numbers of emails, it was deemed by the judge that there was beyond a reasonable doubt persistence which caused the receiver of the emails to fear for their life or the lives of individuals they know.

R. v. Fenton, 2008 ABQB 251 (CanLII) (23)

This trial was ordered to be redone based on a number of errors of the trial judge. One of the key issues in this case was that the accused posted on a blog what was considered to be a death threat and claimed that he had the right to freedom of press. The judge overturned this reasoning and required a new trial to be done.

Summary

Based on the case law developed in terms of cyber technology, it makes individuals who are in Canada accountable for the words that they use on the internet. This means that careful choice of words must be exercised when writing in cyberspace.

Fraudulent Concealment

Section 341 (1:657)

Section 341 makes it illegal to take, obtain, remove or conceal anything for fraudulent purposes.

Case Law

Currently there is no documented relevant case law.

Summary

This section is of interest in the idea of online anonymity and the potential challenges that may occur by creating a fake name or location in the cyber world.

Theft, Forgery, Use, Possession of Credit Cards

Section 342, 342.01, 342.1, 342.2 (1:657:662)

These multiple sections mentioned above make it illegal under a number of circumstances to steal, forge, and possess credit cards or instrumentation for the purpose of any of the above. The final two sections (342.1 and 342.2) address the unauthorized use of a computer, including the means to obtain passwords or devices to obtain computer services.

Section 342 is specifically designed to make illegal the theft, creation and use of credit cards that should not be used because of the nature in which they were obtained. This section also states the penalties for the associated charges.

Section 342.01 addresses the making, selling, importing or exporting of forged credit cards. This section makes it illegal to possess or try to possess any instrumentation for the purpose of forging credit cards.

Section 342.1 sets out instances in which an individual can be charged for unauthorized use of a computer, including fraudulently obtaining computer service, interception of computer communications, the use of a computer for the purpose of mischief (section 430) and giving an individual a password or other access for the purposes above.

Finally, section 342.2 sets out that by having possession of a device that is capable of obtaining unauthorized computer service, the individual can be charged. This includes the making, possessing, selling, using or distribution of any instrument possible of doing this.

Case Law

Currently there is no relevant case law that helps to decipher where the line to be crossed is and what is deemed to be legal or not.

Summary

This section was required to be included in this report for two main reasons; the first is that many of these sections require the use of a computer to be charged under them, and second the potential for future changes made by case law. There is a large change in online fraud, much of which involves the stealing of credit card information from an illegitimate site (phishing). Along with the theft of credit card information, these malicious sites may also add keylogger software. This would allow for the perpetrator to record any passwords and user names used by the individual who was attacked.

Forgery

Section 366 (1:699-700)

The forgery section sets out that it is illegal to make or edit a document for the purpose to be acted on as an authentic document. One can be charged with this section only if the document is complete and if it is a document binding by law.

Case Law

Currently there is no documented case law that can be used to help understand forgery and its potential uses with cyber technology.

Summary

With several programs such as Photoshop now available, it is extremely easy to manipulate a document and make it look authentic. Along with doctoring a document, sending a forged signature across the web can be done simultaneously. Based on the potential for individuals to encounter this, it was included in this project.

Using Mails to Defraud

Section 381 (1:715)

Fraud is a very broad section which makes it illegal to use of deceit, falsehood or other fraudulent means to defraud the public of any property, money or valuable security or service. This section further goes on to discuss the penalties associated with this charge. Section 381 is the use of mails to defraud the public by means of a scheme to obtain money.

Case Law

Unfortunately there is no informative case law under the fraud section for the purpose of cyber technology.

Summary

With the ability to be deceitful on the internet, and with the use of technology, this section is potentially inclusive of the ability to be fraudulent. The difficulty occurs when the individuals may be in different jurisdictions (see virtual crime and jurisdiction below). This section may prove worthy in future cases when examining issues such as phishing. The creator of a phishing site is deceitful to anyone entering the webpage or viewing the scam emails. Unfortunately, this section only has information pertaining to material mail, but as mentioned earlier, the use of email is becoming so prevalent that it would be recommended that this section be given future consideration.

Mischief

Section 430 (1:755-759)

The final criminal code section examines the section of mischief. This section makes it illegal to damage, destroy, or obstruct personal or lawful use of both property and data. Section 430 also makes it illegal to render property dangerous.

Case Law

Currently there is no existing case law on this section.

Summary

Based on the above description of mischief, it shows a significant correlation between cyber technology/cyber crimes and the data transferred throughout. With the ability to use a computer system to damage or destroy data, it makes this section a backbone in prosecution of cyber crimes. With the introduction of a malicious software, it not only provides a defence for a number of crimes such as child pornography, but it also encompasses the ability to create malicious software that would make the data useless or no longer able to perform the originally intended function. The creation of malicious software that disrupts how data should function is covered under this law.

Broadcasting Act

Broadcasting Without or Contrary to Licence

Section 32.(1) (24:23)

Section 32.(1) of the Broadcasting Act makes it illegal to broadcast a program without a licence (unless exempt from requiring a licence). This section also defines the penalties against individuals or corporations.

Case Law

Canadian Radio-television and Telecommunications Commission (Re), 2010 FCA 178 (CanLII)(25)

This case is between the CRTC and the subsequent internet service providers as to whether or not they should be held accountable in the broadcasting sense for what is viewed or able to be viewed on the internet. It was felt that because the internet providers did not transmit programs, they cannot be held accountable.

Summary

This section brings light to the idea of live streaming programs over the internet. With many sites offering this ability, the difficulty of jurisdiction comes into play. With this act it has the potential for anyone not only stating that the material being showing may have copyright protection but also that if the site does not have the proper licence that more fines/jail time could ensue.

Contravention of Regulation or Order

Section 32.(2) (24:24)

Section 32.(2) makes it illegal for individual(s) to contravene any regulation stated in the Broadcasting Act, and states that by doing so they can be charged as an individual or corporation.

Contravention of Conditions of Licence

Section 33 (24:24)

The mentioned section in the Broadcasting Act makes it illegal to not comply with the licensing agreement, and states that in doing so, either the individual or corporation could be charged.

Limitation

Section 34 (24:24)

Section 34 of the Broadcasting Act sets a statute of limitations on both Section 32.(2) and section 33 of no more than 2 years. This means that charges must be laid within 2 years of the date that the incident occurred.

Copyright Act

Offences

Section 42.(1) (26:64)

Section 42 is a large section of the copyright act, making it illegal to import, make for the purpose of sale, sell, trade, or otherwise distribute material that infringes on copyright protection. The section goes on to state the penalties, based on both summary and indictable offences.

Case Law

Disney Enterprises Inc. v. Click Enterprises Inc., 2006 CanLII 10213 (ON S.C.)(27)

This case was deemed to be copyright infringement, where Click Enterprises was selling downloadable copies of Disney movies over the net at a flat rate. This allowed users to pay a fee for a monthly membership and download an unlimited number of movies. This case law demonstrates the dangers in being involved in offering a file for download.

R. v. J.P.M., 1996 CanLII 10198 (NS C.A.)(28)

The case above discusses the infringement of the Copyright Act based on a user uploading software and the appropriate files to then download and use the software. The defence that the software was coded and scrambled was denied, based on the idea of ease of transmission.

Summary

This section makes use of copyright protection and the potential for an individual to be charged with copyright infringements. This section has been constantly referred to in the battle of source coding, torrents and other such material. Currently the potential for charges exists in this battle, and further rulings will result in a more defined understanding of the Copyright Act as it pertains to cyber technology.

Highway Traffic Act (Ontario)

Display Screen

Section 78 (29)

Section 78 prohibits drivers of a motorized vehicle from having a display screen within view, such as a computer or television. This section also makes exceptions for emergency services workers, and allows GPS devices to be in view of drivers.

Summary

With the increase in reduction of size and functionality of computers and cyber technology, what is to prevent a driver from using an application on a tablet or similar device for the use of directive instructions and/or map, which is fine until the tablet is used for use of entertainment purposes for example of watching a movie while driving. Or the alternative is that

if one is driving across the road to cut the neighbour's grass while using an "iPod Touch" it would also be deemed illegal.

Wireless Communication Devices

Section 78.1 (29)

The Wireless Communication Devices section sets out that it is illegal for drivers of a motor vehicle to operate a hand held wireless device capable of sending and receiving text, mail, data or voice communications.

Summary

With the potential to be charged for operating a motor vehicle while using a wireless device, it brings into question the ability to be caught and the difficulties enforcing this law. This act also poses problems such as using an iPod while cutting the grass on a riding lawn mower (as mentioned above) to which both the lawnmower is deemed a motorized vehicle and the iPod is deemed a wireless communication device.

Outcomes

Summary-Legal

With the use of cyber technology so prevalent in today's modern society, it is apparent that the use of it in our daily lives may have consequences. This project was designed to determine the legal risks associated with using technology. Based on the legal writings found in the Canadian Criminal Code, Broadcasting Act, Copyright Act and the Traffic Act, it was determined what was found to be illegal when using cyber technology and the associated potential penalties. A chart has been created in the appendix stating the maximum and minimum penalty (if applicable) for each of the laws covered above (see chart 1 in appendix).

New and Upcoming

Canadian Changes

Recently there has been little published media discussing changes to any laws in the criminal code. However there have been changes made to a few sections of the criminal code, with the most noted being section 172.1 which added the use of luring a child with a computer as an offence in 2002(30). It was then later revised to change many ages in the criminal code for sexual offences to be changed from the age of 14 (which was current until 2007) and later changed to age 16 in August of 2007. Along with this change coming from Bill C-22 were updates and changes to the requirements of the duty of all ISP (internet service providers) to include new requirements to report any child pornography on their network (31) and failure to do so would result in increased fines. The most recent Bill to make a significant change in the criminal code in relation to cyber technology came from Bill C-54, also known as the "Protecting Children from Sexual Predators Act" (32). This new Bill added new mandatory sentences for certain penalties such as internet luring and a new law which prohibits the providing of sexual explicit material to a child. Bill C-54 set new laws which have developed since this project initially took form in mid April 2010 to the final submission of this report in March 2011.

Other recent changes that have become a trend in both Canadian and provincial cyber technologies would include the monitoring of internet usage. This was made apparent when a document was received which discussed the removal of service to a client for breaching the terms of copyright material by the use of uploading a game so that other members could use the game without having to pay for it. A copy of the report is included in the appendix (figure 2). In the report, the ESA (Entertainment Software Association) requested that McMaster

University disable the account of the student whom infringed the copyright laws. Another recent trend that has been observed is ISP's sending their clients messages when there has been a breach in the terms of service between the individual and the ISP (including copyrighted material infringements), and that if changes are not made the service will be cut.

Currently there is a movement across Canada to reduce the effects of cyber technology and driving. There is a large push to eliminate drivers from using hand held devices while driving (cell phones), at this point the following provinces have some legislation concerning this: British Columbia, Prince Edward Island, Saskatchewan, Newfoundland and Labrador, Nova Scotia, Quebec and Ontario(33). Though other provinces have not added specifc penalties for using a hand held device while driving, this does not limit the province from laying charges. Charges for using a cell phone while driving can be a fine, demerit points or suspension of licence depending on the severity of the charge and the actions of the driver while using the cell phone. It seems that there is no standard countries are following when determining what charges are appropriate when with a driver who used a hand held device. The chart found in the appendix (chart 2) shows the variations in penalties from all the countries as of June 2009 (34) with fines ranging from $100 and the potential to have jail time. Canada was not the first to impose a cell phone ban, nor will they be the last. The ban on cell phone use while driving shows that we, as Canadians, are open to change and trying to ensure that the roads are safer from drivers that would normally be distracted by cell phones.

Global Changes

It appears that on a global scale many companies are changing locations, being shut down or changing the style of services they provide in order to ensure that they cannot be prosecuted by the law. The first example of this comes from the use of live streaming websites (atdhe.net)

which was removed and "seized" by the USA Homeland Security. This website previously broadcasted live streaming tv, movies, and sports over the internet, allowing an individual who did not have access to the channel or did not wish to pay the pay-per-view price access to viewing the event. This site was very popular, and was removed around January of 2011. Within a month, a new site with an almost identical URL has been posted and showcasing the same events (TV, movies and sports) under the new URL of "atdhenet.tv/index.html". Even the seizure of a previous webpage it does not prevent the creators from making another one, under a similar name, to which the police need to start the proper investigations over again.

Downloading and uploading have been a hot topic in number of conversations both for their financial possibilities (iTunes/Netflix) as well as unauthorized access to copyrighted materials with programs such as Bit Torrent, Vuze and Lime Wire. These programs operate similar to Napster, that allowed users to both download and upload media for other people to use without having to purchase the items. Lime Wire was recently shut down in October of 2010 for copyright infringements and forced to stop allowing users to upload and download software.

Lastly, another major global change is the amount of funding being placed into internet security. It was announced by Prime Minister Harper on Feb. 17th that $90 million over 5 years would be allocated to internet security. This seems like a large amount of money but many have raised the flag that the U.K. last year alone invested about $1.03 billion into national cyber security (35). It appears that many similarly developed countries including Canada are trying to strike back against cyber attacks (such as internet breaches and hacking) by placing funding into security and various preventative measures. Overall, it appears that many nations recognize the dangers of cyber technology but have yet to figure out how to protect their citizens.

Canadian Comparison

Identity

The significance and protection of identity in the online world-Dan Svantesson (36)

Identity in terms of cyber space is difficult to determine and many entities have different views on what identity exactly means. Without the use of an artificial identity online, there is no way to protect one's self without releasing personal details. When considering the concept of personal details, there must be further examination as to what is considered personal and in which situation is it personal and in which situation is it not.

> *For example in the case of medical history, there is no reason that Ebay should require or benefit from having this information, however if one is looking online for quick medical help then past medical history may be beneficial to the "online" doctor to make a more informed diagnosis.*

It appears that in every situation there is a requirement for some form of privacy but in another instance that piece of information is required and creates a more informed result. How can one have the idea of privacy on the internet by avoiding the use of a universal identity was discussed in Computer Law & Security Review, which discussed the changing use of identity in a cyber world. An individual may have multiple identities on the web depending on the situation. In the article, it was proposed that individuals use a different identity in each situation in order to conceal some amounts of privacy; this was accomplished by using different identities in online gaming, dating and banking (36). In using multiple identities the individual is keeping certain information hidden from others who do not require access to that information.

The above Australian view has the hint of a common teaching in Canadian society for individuals starting to use cyberspace. The current instructions for youth in Canada using cyber technology include the standard practice of "don't use your real name or location". This is a great practice in trying to keep an individual safe from predators, but if the individual is trying to buy something online, how can they get the item delivered if both the name and location are not accurate. This raises the question of how much information can be private on the internet and still allow the user to experience what cyberspace has to offer.

Ownership

From music tracks to Google maps: Who owns computer-generated works? Mark Perry, Thomas Margoni (37).

The idea of who owns an idea is nearly impossible to determine based on the realm that ideas are infinite and cannot be defined, and it cannot proven that someone thought of the idea prior to another without having some material record. When it comes to artistic work created with computers, it seems that there is debate about who owns the work… is the owner the one who created the software or the one who created it using the software. Based on a recent ruling in Australian courts, it was determined that based on the current understanding of the Turing test (proposed by Alan Turing), a computer system is not able to be creative, and thus the individual using the software is deemed the owner of the product and software produced(37).

The article (Google maps) it makes a mention that currently Canadian law has not made a ruling as to who is the rightful owner of anything created by software or a computer system. This will become an interesting should a case be brought before the courts as it will be a ground breaking change in both computer systems and Canadian law. It appears from the information in this article that the United Kingdom, South Africa and New Zealand have changed the wording

in their respective Copyright Acts to include a statement that the individual to which created such work is deemed to be the author rather than the software and its associated members.

Virtual Crime

Beyond griefing: Virtual crime Angela Adrian(38)

This article discusses the current challenges in the laws when it comes to crime committed over the internet. The increase in number of individuals playing cyber games causes an increase of cyber crimes committed in these games. The author talks about the different types of cyber crimes committed in games or related to a game, such as the attempt to steal information such as the user name and password with the use of a phishing website or the attempt to steal in-game items with misleading or fictional trades that deceives a user into giving up an in-game item with no gain.. The issue is that many of the games are offered in a number of countries all with differing laws, and confusion about whether one can be charged based on a crime that may have been committed in a number of countries, and which country's set of laws applies in a given context. Another issue with the potential for virtual crime is that many law enforcement agencies are not willing to intervene and rather the software creators enforce the rules and sort out the problems on their own. Unlike the U.K., Canada does not have a "Computer Misuse Act"(38) to which new legislation has been developed and enforced in a way that activity is deemed to be illegal if the following conditions are met:

1. He causes a computer to perform any function with an intent to secure access to any program or data held in any computer or to enable any such access to be secured;
2. The access he intends to secure or to enable to be secured, is unauthorised
3. He knows at the time when he causes the computer to perform the function that this is the case

Based on this article it seems that some countries are more concerned with ensuring that all aspects of life are covered and all its citizens should be protected.

It appears that the U.K. has started to take extra steps to ensure that there are legal implications for breaking the law, be it relating to a virtual item or a material item. U.K. jurisdiction also encourages the designers of these virtual worlds should find ways to police them within the games to ensure that fair play is used throughout. Both law enforcers and game developers have attempted to create a universal set of standards, but it appears that, like many great ideas there is the absence of funding to ensure that there is enough support be effective.

Jurisdiction

State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction Georgios I. Zekos(39)

One of the largest problems in cyber technology law is cyberspace jurisdiction. Based on the idea that cyberspace does not fall into a geographical location; it becomes extremely difficult to pinpoint who has jurisdiction. In traditional jurisdiction, an individual is governed by the laws of the jurisdiction based on where their body physically is, as opposed to cyber jurisdiction, where one is not necessarily committing an act in one given geographical location. Past the computer there is no material way to determine cyberspace jurisdiction other than where the individual is at the time of logging into cyberspace. There are different laws in just about every area from every aspect of life such as hunting, traffic and mandatory sentencing laws. The difficulty arises when the individual is physically located in a different area than the crime he or she is committing:

> *If a crime was committed in the Toronto region of Canada but the individual flees the area they would still be prosecuted based on the laws that were current in that geographical location. However, if an individual sitting in a cafe in Toronto is using the*

internet to commit a crime in cyberspace to simply reduce the performance of a computer in South America is it possible to state that because South America doesn't have the same law that the individual cannot be prosecuted? Can it be deemed that the individual be prosecuted as to where the physical being was when the crime was committed?

Because of these challenges there needs to be an international cyberspace law. This law would propose that governments would be required to not only comply but also enforce the rules set out. Once again the problem arises that every country would have to agree to the terms set out, otherwise any non-conforming country could be used remotely as base of operations for illicit activity. Should the cyber jurisdiction play out, how would the areas be divided up? How would trials occur? Who would cover costs? These are among some of the more pressing questions which serve to identify the difficulty countries face when trying to figure out cyber law. Until there is significant funding in place there will not be a working system.

Without the help, funding and determination of everyone the idea of a global cyberspace jurisdiction is a flop. The combined efforts of all countries would ensure the safest, most effective and accepted terms for all countries. It goes without saying that the idea of controlling a "virtual" area would be extremely difficult and lead to differences in opinion making the entire idea of jurisdiction of cyberspace an interesting process to watch unfold.

Conclusion

Technology offers users a world of convenience, from online banking and shopping, and dating, to gaming, communication (social networks and chat sites), to news and business opportunities. However, all these opportunities present chances for an individual to run into trouble, whether posting inappropriate words on a blog or sending an email. It appears that with every opportunity to use cyber technology lawfully there is just as many opportunities to use it unlawfully. Cyber technology has the potential to entangle the user in a world of legal issues. Cyber technology may be used to move information from one location to another with a click of a button, though the information being sent may incur the serious offence of "using the mail to defraud", or the content of the message may lead to the user being charged with "criminal harassment". A criminal could use a computer to obtain credit card information or a passport, either of which could be considered offences under the Criminal Code. The use of a computer to upload photos or publish them to the web may result in child pornography or corrupting morals charges, which have serious associated jail times. Broadcasting TV and movies on the internet for everyone to enjoy, for instance if they missed it earlier in the day or didn't have access to that channel, can result in a serious fine of millions of dollars. Other examples of potentially unlawfully activities that technology facilitates include the potential to win a few dollars on an online gambling site (as of the date of this document is written), or using a cell phone to send a message while driving, which may result in a fine. Cyber technology can be the machine on which the crime was done, such as the computer used to store child pornography, or it can be the means by which the crime was committed, such as using cyber technology to create malicious software in order to attack computer systems and obtain sensitive information. Whether the

computer is being accessed for personal use, or for business, or with the intent to commit a crime, no user is safe from being charged unless they abide by the Criminal Code, Acts and the constantly developing case law.

When looking at Canada and the rest of the world, there are apparent similarities; each country recognizes the problems associated with cyberspace but have yet to find a proper solution. There seems to be a lack of funding (as with most crime prevention methods) to create and enforce cyber laws, as well as a lack of a consensus of the types of information that should be free and the association with identity. How can one be held accountable for actions in cyber space if both jurisdiction and identity cannot be solved. Until similarly developed countries can sit down and create an international law that is accepted globally it will be difficult to enforce cyberspace. With that being said, it appears that Canada and the United States are co-operating with each other when it comes to cases of cyber crime being committed in one location when the effects are felt in the other, as seen in the case of facebook spam messages(42).

Canada is keeping pace with the UK, Australia, and the US in many of its cyber technology laws, such as driving while using a wireless device, and adding sections like the "misuse of computers act". This is strong evidence to support that the more cyber crime continues, the more changes will occur to not only try and reduce the occurrence of cyber crime, but also to eliminate exploitations of existing laws that enable illicit activity within the cyber community. Over the years, many additions have been made to the Criminal code (as mentioned earlier), and this process will continue as required.

Learning Experience

Barriers

Canlii

The most prevalent barrier to the research for this paper is the wide variety of writing styles in which Canlii has been done in. There seems to be no generalized structure or format that states the relevant charges against the accused, a clear and concise conclusion or the linking to a change in the previously accepted terms. The lack of a polished document in the different Canlii cases lead to the extended period of time that was spent sorting through cases that contained the potential to be relevant information. Secondly, the results found when using the advanced search feature on Canlii were extremely limited. When searching it would pull up a large number of cases that contained any of the keywords used – for instance, the word "computer" – , which resulted in displaying any case that had the mention of a computer, regardless of how relevant that computer was to the investigation. If a police officer took notes on a computer, or the individual had a computer, or there was a mention of an email taken from the computer, all would return results… none of which would be relevant when looking for an individual trying to create a computer virus. The ability to filter results based on the important sections of the criminal code, or by date, would have enabled a much faster result in obtaining the information. A final problem when looking at the Canlii pages was that when analyzing the different cases it was impossible to determine the relevance of the issue without reading through the entire case. There was a lack of a summary of the case facts, and each case required multiple pages to discuss the findings. In the end, the case could have been summed up much more precisely and just highlighted the key issues in the case.

Literature

With cyber technology being so prevalent in today's society it was surprising to find a lack of literature discussing the potential problems with current laws. There are very few scholarly articles which analyzed both the lack of cyber laws and where Canada stood in respect to the world. Based on this lack of literature it appears that many articles are either in the process of being published or there is a lack of research in this area, both of which could be the case. As mentioned, cyber technology is an extremely difficult concept to grasp when discussing theft as there is rarely a physical that is taken - how can one be in trouble for taking of something that doesn't exist? The concept is similar to copywriting a thought which has no tangible representation, or stealing an idea that has not been made flesh which too many seems unfathomable.

Access

Many scholarly articles are published in a journal or book, in which case the only way to obtain the article is by owning the journal/book or by spending up to $35 per article. Though Trent University does subscribe to several journals there were several instances where the articles were unobtainable and thus limiting the amount of information that can be examined. With access to more articles, additional resources could have been analyzed and further expanded upon.

Timeline

When this project was designed and started in late April of 2010 there was the expectation to answer a number of significant questions. Unfortunately, the court system takes time to start an investigation, and significant time to determine the severity of the case and its eventual outcome. Until the results of the case are published on Canlii, no analysis could be

made. Cyber technology is growing in popularity, and as a result cyber crime has also increased. This increase results in ground breaking changes happening all the time, from injunctions to stop websites from broadcasting to an individual being charged in one country and upheld in another. With new cases constantly coming through the courts it only makes sense that based on the technology driven society that new additions will be added to the criminal code and subsequently more case laws will result from future cases.

Recommendations

Ethical

There needs to be a continuation of this project that analyzes the ethical issues associated with the use of cyber technology. This would include changing cyber technology to manipulate coding to achieve a new result, and the use of internet theft at which no physical material item has been taken. Is it unethical to take an non tangible object and if not when is it considered immoral or unethical. Ethics is a very difficult topic to breeze over and serious consideration must be given to a number of situations when using cyber technology.

Continuation

A continuation step of this research should be completed that examines the hazards of using cyber technology. Examples of potential hazards include legal implications, health risks and technological dangers such as viruses, scams or loss of information. It is also recommended that it be determined which hazards are more prominent in order to eventually create public education curriculums. The popularity of cyber technology in most modern industries reinforces that it is important to recognize both the positive aspects (speed to which information can be obtained), as well as the negative aspects (malware, child pornography) of cyber technology to

insure that serious damages are not done to an individual/company/community if the appropriate steps are not taken to prevent them.

Re-examination

The topics explored in this document should be re-examined in the next few years to see if there is new precedent that has redefined a section of the criminal code. Has there been any attempt to police the cyber world? Has there been a global shift in the views of cyber technology? Is there a cyber law which governs all countries? With many of topics currently lacking information or precedent, and the growing crime rates and regular discovery of crimes based on cyber technology, it would only be logical to see changes in these areas in the future.

Processing of Evidence

Processing and seizing of digital and subsequently cyber data is becoming increasingly difficult in the scientific manner, for that reason alternative methods to the current practices should be examined. It would serve the community a benefit to discuss the hardships associated with the idea of jurisdiction, processing and storing of digital information and cyber technology, in addition to possible changes to the way we view cyber technology on a global, country and provincial scale.

References

1. Greenspan EL. Martin's Annual Criminal Code 2009 student edition, Aurora 2009.
2. R. v. Bishop, 2007 ONCJ 441 (CanLII) http://www.canlii.org/en/on/oncj/doc/2007/2007oncj441/2007oncj441.html
3. Hydro One v. Society of Energy Professionals, 2006 CanLII 42249 (ON L.A.) http://www.canlii.org/en/on/onla/doc/2006/2006canlii42249/2006canlii42249.html
4. Canada (Minister of Citizenship and Immigration) v. Chen, 2003 FCT 330 (CanLII) http://www.canlii.org/en/ca/fct/doc/2003/2003fct330/2003fct330.html
5. R. v. Taft, 2003 BCCA 104 http://www.canlii.org/en/bc/bcca/doc/2003/2003bcca104/2003bcca104.html
6. R. v. Innerebner, 2010 ABQB 188 http://www.canlii.org/en/ab/abqb/doc/2010/2010abqb188/2010abqb188.html
7. Bill C-22: An Act to amend the Criminal Code (age of protection) and to make consequential amendments to the Criminal Records Act http://www2.parl.gc.ca/Sites/LOP/LegislativeSummaries/Bills_ls.asp?lang=E&ls=c22&source=library_prb&Parl=39&Ses=1
8. R. v. A.G., 2007 CanLII 21975 (ON S.C.) http://www.canlii.org/en/on/onsc/doc/2007/2007canlii21975/2007canlii21975.html
9. R. v. Smith, 2007 BCSC 1955 http://www.canlii.org/en/bc/bcsc/doc/2007/2007bcsc1955/2007bcsc1955.html
10. Messerlian C, Byrne AM, Derevensky JL. Gambling, Youth and the Internet: Should We Be Concerned? The Canadian Child and Adolescent Psychiatry Review. Feb 2004:13(1);3-6.
11. R. v. Jarvis, 2006 CanLII 27300 http://www.canlii.org/en/on/onca/doc/2006/2006canlii27300/2006canlii27300.html
12. R. v. Lithgow, 2007 ONCJ 534 http://www.canlii.org/en/on/oncj/doc/2007/2007oncj534/2007oncj534.html
13. R. v. Tootoosis, 2010 ABQB 574 http://www.canlii.org/en/ab/abqb/doc/2010/2010abqb574/2010abqb574.html
14. R. v. Safaee, 2009 BCSC 1350 (CanLII) http://www.canlii.org/en/bc/bcsc/doc/2009/2009bcsc1350/2009bcsc1350.html
15. R. v. Butler, 1990 CanLII 2614 (MB C.A.) http://www.canlii.org/en/mb/mbca/doc/1990/1990canlii2614/1990canlii2614.html
16. R. v. Giles, 2007 BCSC 1147 http://www.canlii.org/en/bc/bcsc/doc/2007/2007bcsc1147/2007bcsc1147.html
17. Briar v. Canada (Treasury Board), 2003 PSSRB 3 (CanLII) http://www.canlii.org/en/ca/pssrb/doc/2003/2003pssrb3/2003pssrb3.html
18. http://www.cbc.ca/news/canada/toronto/story/2010/08/10/ontario-gambling-olg546.html
19. Tuzyk J, Hoffner J. Ontario Prohibits Advertising of Illegal Internet Gambling. Blake, Cassels & Graydon LLP. 2008.
20. http://www.ottawacitizen.com/news/topic.html?t=Person&q=William+Melchert-Dinkel
21. MacLean A. Cyber Safety – The Risks of Network Technology. April 2010.

22. R. v. Labrentz, 2010 ABPC 11 (CanLII) http://www.canlii.org/en/ab/abpc/doc/2010/2010abpc11/2010abpc11.html
23. R. v. Fenton, 2008 ABQB 251 (CanLII) http://www.canlii.org/en/ab/abqb/doc/2008/2008abqb251/2008abqb251.html
24. Justice Minister. Consolidation Broadcasting Act. S.C. 1991, c.11. February 9th 2011. http://laws.justice.gc.ca/PDF/Statute/B/B-9.01.pdf
25. Canadian Radio-television and Telecommunications Commission (Re), 2010 FCA 178 (CanLII) http://www.canlii.org/en/ca/fca/doc/2010/2010fca178/2010fca178.html
26. Justice Minister. Consolidation Copyright Act. Chapter C-42. February 9th 2011. http://laws.justice.gc.ca/PDF/Statute/C/C-42.pdf
27. Disney Enterprises Inc. v. Click Enterprises Inc., 2006 CanLII 10213 (ON S.C.) http://www.canlii.org/en/on/onsc/doc/2006/2006canlii10213/2006canlii10213.html
28. R. v. J.P.M., 1996 CanLII 10198 (NS C.A.) http://www.canlii.org/en/ns/nsca/doc/1996/1996canlii10198/1996canlii10198.html
29. Consolidated Highway Traffic Act. January 1st 2011. http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90h08_e.htm
30. http://www.media-awareness.ca/english/resources/ legislation/canadian_law /federal/criminal_code/criminal_code_child.cfm
31. http://www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=4847402&file=4
32. http://www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=4762347&file=4
33. http://www.ccohs.ca/oshanswers/safety_haz/cellphone_driving.html#_1_6
34. http://www.cellular-news.com/car_bans/
35. http://www.cbc.ca/news/canada/story/2011/02/17/cyber-attacks-harper142.html
36. Svantesson D. The significance and protection of identity in the online world. Computer Law & Security Review. 2011:27;1-3.
37. Perry M, Margoni T. From music tracks to Google maps: Who owns computer-generated works? Computer Law & Security Review. 2010:26;621-629.
38. Adrian A. Beyond griefing: Virtual crime. Computer Law & Security Review. 2010:26;640-648.
39. Zekos G. State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction. International Journal of Law and Information Technology. 2007:15(1);1-37.
40. http://www.mto.gov.on.ca/english/safety/distracted-driving/index.shtml
41. http://3.bp.blogspot.com/_DPX1jvBtmXQ/SzxPIbxHz5I/AAAAAAAAABM/iF8X89Uga3Q/s400/Use+of+Force+Wheel.JPG
42. http://www2.macleans.ca/2010/10/05/montreal-man-ordered-to-pay-1-billion-to-facebook/

Appendix

Chart 1: Summary of sentence length based on conviction

Section Number Criminal Code	Section Name	Minimum Sentence	Maximum Sentence
21	Parties to Offence	N/A	N/A
38	Defence to Personal Property	N/A	N/A
52	Sabotage	N/A	I/O not exceeding 10 years
57	Forged Passport	N/A	I/O not exceeding 14 years S/O
126	Disobeying Statute	N/A	I/O not exceeding 2 years
151	Sexual Interference	I/O 45 days S/O 14 days	I/O not exceeding 10 years S/O not exceeding 18 months
152	Invitation to Sexual Touching	I/O 45 days S/O 14 days	I/O not exceeding 10 years S/O not exceeding 18 months
153	Sexual Exploitation	I/O 45 days S/O 14 days	I/O not exceeding 10 years S/O not exceeding 18 months
161	Order of Prohibition	N/A	Life of certain amenities
162	Voyeurism	N/A	I/O not exceeding 5 years S/O
163	Corrupting Morals	N/A	I/O not exceeding 2 years S/O
163.1	Child Pornography	I/O 45days or 1 year S/O 14days or 90 days	I/O not exceeding 10 years S/O not exceeding 18 months
172.1	Luring a Child	N/A	I/O not exceeding 10 years S/O not exceeding 18 months
181	Spreading False News	N/A	I/O not exceeding 2 years
184	Interception of Communications	N/A	I/O not exceeding 5 years
202-207	Betting/Lottery/ Gambling Laws	N/A – 3months	I/O not exceeding 2 years

Section Number Criminal Code	Section Name	Minimum Sentence	Maximum Sentence
241	Suicide Counselling	N/A	I/O not exceeding 14 years
247	Traps to Cause Bodily Harm	N/A	I/O-intent-not exceeding 5yrs I/O-causes-not exceeding 10yrs I/O-death-life
264	Criminal Harassment	N/A	I/O not exceeding 10 years S/O
341	Fraudulent Concealment	N/A	I/O not exceeding 2 years
342	Theft, Forgery of Credit Card	N/A	I/O not exceeding 10 years S/O
366	Forgery	N/A	I/O not exceeding 10 years S/O
381	Using Mails to Defraud	N/A	I/O not exceeding 2 years
430	Mischief	N/A	I/O up to life S/O
Broadcasting	**Section Name**	**Minimum Sentence**	**Maximum Sentence**
32.(1)	Broadcasting Without Licence	N/A	Individual-$20,000 per day Corporation-$200,000 per day
32.(2)	Contravention of Regulation	N/A	Individual-$25,000 first offence Corporation-$250,000 first offence
33	Contravention of Licence	N/A	S/O
Copyright	**Section Name**	**Minimum Sentence**	**Maximum Sentence**
42.(1)	Offences	N/A	I/O $1million/5years S/O $25thousand/6months
Highway Traffic	**Section Name**	**Minimum Sentence**	**Maximum Sentence**
78	Display Screen	N/A	$155 (40)
78.1	Wireless Communication Devices	N/A	$155 (40)

*I/O = Indictable Offence
*S/O = Summary Offence

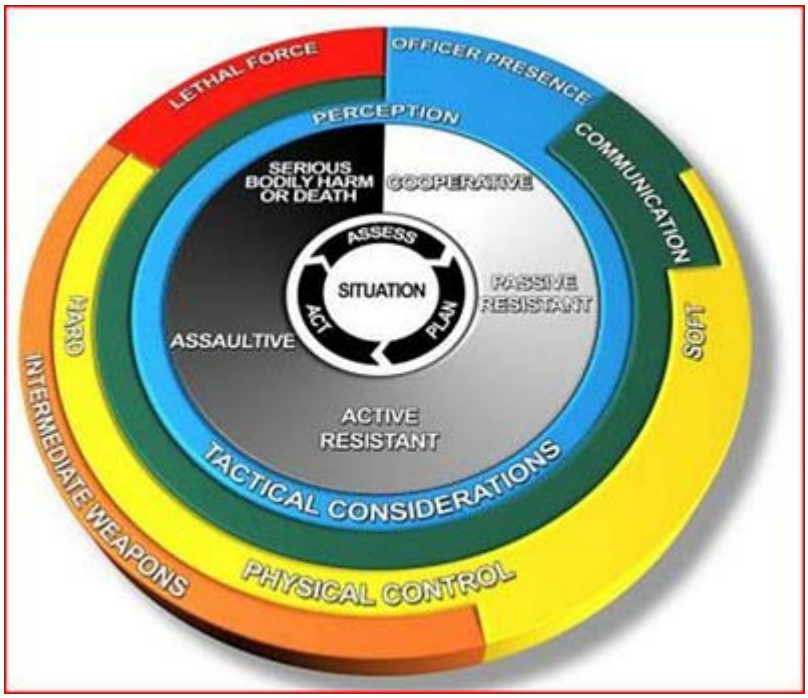

Figure 1: Force wheel indicating the required force allowed in any given situation by a Peace Officer (41).

> Hash: SHA1
>
> Entertainment Software Association
> 575 7th Street, NW, Suite 300
> Washington, DC 20004 USA
>
> Attention: Intellectual Property Enforcement
> Telephone: 2 0
> E-mail:copyright@theesa.com
>
> 12-14-2010
>
> Name:
> ISP: McMaster University
> ESA Reference Number: 2 6
> IP Address:
> Date of Infringement: 2010-12-13T09:13:29.78Z
>
> Dear McMaster University:
>
> The Entertainment Software Association ("ESA") is a trade association that represents the intellectual property interests of numerous companies that publish interactive games for video game consoles, personal computers, handheld devices and the Internet in the United States of America, in Canada, and in other countries (collectively referred to as "ESA members"). ESA is authorized to act on behalf of ESA members whose copyright and other intellectual property rights it believes to be infringed as described herein.
>
> ESA is providing this letter of notification to make McMaster University aware of material on its network or system that infringes the exclusive copyright rights of and is unlawful towards one or more ESA members.
>
> ESA members are entitled to the full protection of Canadian intellectual property laws, including the Copyright Act, R.S.C. 1985, c. C-42, as amended, in such entertainment software products.
>
> Based on the information at its disposal on 2010-12-13T09:13:29.78Z, ESA has a good faith belief that the IP address infringes the rights of one or more ESA members by offering for sale or download unauthorized copies of game products protected by copyright, or offering for sale or download material that is the subject of infringing activities. The copyrighted works that have been infringed include but are not limited to:
>
> CRYSIS
>
> The unauthorized copies of such game product(s) or the material that is the subject of

Figure 2: Breach of copyright terms resulting in blocking the offenders IP from the McMaster internet connection.

Chart 2: Countries that have banned the use of hand held cell phones while driving (34)

Country	Banned	Notes
Australia	Yes	Banned in all states - fines vary though.
Austria	Yes	Fines vary - up to US$22 per incident
Bahrain	Yes	Offenders face fines - possibly prison
Belgium	Yes	Phones can be used without a hands-free unit when the car is stationary - but not while in traffic (such as at traffic lights)
Brazil	Yes	Ban imposed Jan. 2001
Botswana	Being debated	The attorney general is drafting the legislation
Canada	Variable	Banned in Newfoundland (Dec2002) fines up to C$180 - Banned in Québec (Apr 2008) fines up to C$100.
Chile	Yes	
China	Yes	Reported to be covered by general "good driving practice" legislation.
Czech Republic	Yes	
Denmark	Yes	Ban imposed July 1998 - US$60 fine for infringements
Egypt	Yes	Fines of about US$100 per offence.
Finland	Yes	Ban imposed January 2003 - US$55 fine for infringements
France	Yes	Banned 2003, EUR40 fine per infraction
Germany	Yes	Ban imposed Feb. 2001 - usage allowed without a hands-free unit only when the engine is switched off. Fine of €40 per infraction
Greece	Yes	
Hong Kong	Yes	
Hungary	Yes	Not often implemented by the police
India - New Delhi	Yes	New Delhi - Ban extended to ban all use of cell phones when driving, including use with a hands-free unit - July 2001 **Andhra Pradesh - Ban now enforced with prison sentences**
Ireland	Yes	Banned, with a US$380 and/or up to 3 months imprisonment on a third offence. Handsfree kits allowed, although that is subject to review.
Isle of Man	Yes	Banned since July 2000
Israel	Yes	
Italy	Yes	Fines of up to US$124 per infraction
Japan	Yes	Ban imposed Nov. 1999
Jersey	Yes	Ban imposed Feb. 1998
Jordan	Yes	Ban imposed Oct. 2001
Kenya	Yes	Ban imposed late 2001
Malaysia	Yes	
Mexico	Partial	Ban in Mexico City
Netherlands	Yes	Fines up to €2,000 or two weeks in jail
New Zealand	Being debated	Under debate - consultation being sought from interested parties
Norway	Yes	Fines of over $600 per infraction
Pakistan	Partial	Banned in Islamabad
Philippines	Yes	
Poland	Yes	Fine of PLN200 ($100) - can be higher if contested.
Portugal	Yes	
Romania	Yes	
Russia	Yes	Ban imposed by Prime Minister - March 2001
Singapore	Yes	
Slovak Republic	Yes	
Slovenia	Yes	
South Africa	Yes	
South Korea	Yes	Ban imposed July 2001 - US$47 fine + 15 points on the license.
Spain	Yes	
Sweden	No	
Switzerland	Yes	
Taiwan	Yes	If the driver is using a reflective screen on the car, local privacy laws forbid stopping the car for violating the ban.
Thailand	Yes	Bill proposed in May 2000
Turkey	Yes	
Turkmenistan	Yes	Signed into law with effect from May 1st 2003, by President Saparmyrat Turkmenbasy
UK	Yes	Banned from December 2003
Zimbabwe	Yes	Ban imposed in Sept 2001, announced via official news agency only though, so not confirmed