Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Laws of Canada as they Pertain to Computer Crime

This paper examines the existing laws in the Criminal Code of Canada as they pertain to computer crime. For the purpose of this paper, the definition of computer crime will be that of the Investigation Bureau of the Ontario Provincial Police: any criminal activity involving the copy of, use of, removal of, interference with, access to, manipulation of computer systems, and/or their related functions, data or programs (Stinnissen, p.3). The objective is to assess the laws as they stand and examine whether Canada is fall...

Copyright SANS Institute
Author Retains Full Rights

AD

Laws of Canada as they Pertain to Computer Crime

Submitted by Donna Simmons
May 2002

Introduction

This paper examines the existing laws in the *Criminal Code of Canada* as they pertain to computer crime. For the purpose of this paper, the definition of computer crime will be that of the Investigation Bureau of the Ontario Provincial Police:

> any criminal activity involving the copy of, use of, removal of, interference with, access to, manipulation of computer systems, and/or their related functions, data or programs (Stinnissen, p.3).

The objective is to assess the laws as they stand and examine whether Canada is falling behind the times or a leader in the international fight against computer crime. The paper begins with an overview of the applicable sections of the *Criminal Code of Canada*, followed by cases of computer criminals that have been arrested in Canada. Opinions on both sides of the debate are presented. The paper concludes that there are other remedies that could be implemented that would help win the war on computer crime to a much greater degree than making changes to the *Criminal Code.*

The Laws

In 1985 Canada passed the *Criminal Law Amendment Act*. This amendment added Section 342.1 to the *Criminal Code of Canada* (hereafter referred to as the *Code*) as well as adding Subsection (1.1) to Section 430 of the *Code*. The *Criminal Law Improvement Act 1997* added Subsection (d) to Section 342.1(1).

The most relevant sections of the Code as they pertain to this paper read as follows:

> **342.1** (1) Every one who, fraudulently and without colour of right,
>
> *(a)* obtains, directly or indirectly, any computer service,
>
> *(b)* by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (*a*) or (*b*) or an offence under section 430 in relation to data or a computer system, or

(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (*a*), (*b*) or (*c*)

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

(2) In this section,
"computer password" means any data by which a computer service or computer system is capable of being obtained or used;

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(a) contains computer programs or other data, and

(b) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other function;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.

"traffic" means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way (Criminal Code of Canada, part IX).

430. (1) Every one commits mischief who wilfully

(a) destroys or damages property;

(b) renders property dangerous, useless, inoperative or ineffective;

(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or

(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

(1.1) Every one commits mischief who wilfully

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the lawful use of data; or

(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto. (Criminal Code of Canada, part XI).

Other laws in the *Code* that relate to computer crime include, but are not restricted to:

Section 184 – unlawful interception of private communications
Section 326 – theft of telecommunication services
Section 327 – possession of device to unlawfully obtain the use of a telecommunication facility or services.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The Cases

In April 1993 “Coaxial Karma” was arrested for breaking into a Laval University computer**.** He had information that the system had many accounts that were never used and they all had a four-letter password. Using a brute force attack he was eventually (after 72,000 attempts) able to gain access to saphir.ulaval.ca, a cluster VAX/VMS. An operator discovered the 72,000 failed login attempts for one account and called the Royal Canadian Mounted Police (RCMP). The exact charges brought against him and his sentence are not clear, but being a juvenile he pretty much got by with a slap on the wrist, not even losing his computer.

In September of the same year, “SubHuman Punisher” was arrested. Again it was a Laval University system that was compromised. The university had hired a security expert to put a stop to the intruders who routinely were breaking into its systems. He was able to do quite a good job of it, which of course was considered a challenge to a few of the better crackers. Once it was determined that crackers were using the system for Internet access the RCMP was brought in. In order to catch the crackers the phone lines were monitored and logging of all Internet activity was enabled. “SubHuman Punisher” was charged with theft of telecommunications (which was dropped), illegally using a computer and copyright infringement. As punishment all of his equipment was taken.

In September 1995 Jesse Hirsh was charged with unauthorized use of a computer system. He was caught using his stepbrother’s University of Toronto computer account, as well as the account of a friend to publish a newsletter on the Internet. On the morning of the trial, the prosecution dropped the charges. Hirsh agreed to pay the university $400.00.

April 2000 saw the first time a person was sentenced for computer cracking. Pierre-Guy Lavoie was found guilty under the *Code* for fraudulently using computer passwords to break into many government and corporate sites. Lavoie, and two of his friends who were discharged, listed the passwords on a website they created and invited others to penetrate the systems. Lavoie was sentenced to 12 months of community service, placed on 12 months probation and ordered not to touch a computer for 12 months.

In January 2001, the infamous Mafiaboy plead guilty to 56 charges for launching Distributed Denial of Service (DDoS) attacks. These attacks hit high-profile websites, such as CNN, Ebay and Yahoo causing them to be inaccessible to authorized users. During his cracking rampage, Mafiaboy had accessed 75 computers in 52 different networks in 4 countries. It is interesting to note that 48 of the 52 networks belonged to universities. Once he gained access to the networks, he planted a DoS tool onto their systems. Now he was able to command those systems from his computer to flood sites with

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

bogus traffic. The tool used by Mafiaboy apparently was able to send 10,700 phoney requests in 10 seconds. Most of the charges against Mafiaboy were related to illegal use of computer systems and the remaining were for mischief against the websites. He was eventually sentenced to 8 months in a youth detention centre, 1 year of probation after his release and was required to donate $250.00 to a charity. While in the detention centre, he would be allowed to attend school and have a part-time job.

Antiquated Laws?

How could laws that have been on the books for over 15 years possibly cover the requirements of a rapidly expanding computer world? That is the obvious question of those who believe the laws need to be changed.

Information Technology Association of Canada (ITAC) has been calling for stronger computer laws since 1999. Specifically they advocate stiffer penalties and criminalizing possession of virus dissemination devices. They advocate that the maximum sentence of 10 years imprisonment is not harsh enough to deter potential offenders. They would also like to see the mere possession of virus instruments or devices criminalized, whether or not they were used to actually disseminate a virus.

In April of 2001 a private member's motion (Motion No. 80) was made to the House of Commons. This motion requested that the government amend the *Code* so that a separate category of offences and punishments for computer criminals be created. According to one House member, an RCMP constable of the Commercial Crimes Division he contacted as part of the research for the motion, advised him there was a vacuum in the Code and in most cases of computer crime, the charges laid fell under mischief to data.

It's the Canadian Way eh!

Historically, Canada is known to draft legislation in such a general manner so that it is not particular to any one thing. "Theft is theft, fraud is fraud, libel is libel, hate is hate and porn is porn" is a popular refrain among those that believe this to be true in regards to computer crime. It does not matter that the fraud was perpetrated with the use of a computer, therefore a separate law for computer fraud is not required.

Another uniquely Canadian feature is the clear definition of a jurisdictional boundary for computer crime. All computer crime falls under the jurisdiction of the Information Technology Security Branch (ITSB) of the RCMP, which is responsible for the information technology security of the country.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Canada has been recognized as being very aggressive in implementing computer crime legislation. How may other countries had the same foresight as far back as 1985? In fact, some libertarians would say Canada has been too aggressive with its laws.

McConnell International, the consulting firm that advises on e-commerce, reported in a recent news release that Canada's computer crime laws are among the strongest in the world. Harris N. Miller, President of the World Information Technology and Services Alliance (WITSA), a sponsor of the report added "we hope that more countries will follow Canada's lead by updating their laws to ensure criminals are not getting ahead of law enforcement".

Discussion

Just because the laws were written in 1985 does not necessarily mean that they are out of date. Yet that seems to be the attitude of many of the critics. It is interesting to note that even McConnell International originally got it wrong in their report Cyber Crime… and Punishment? Archaic Laws Threaten Global Information of December 2000, when they characterized Canada as a laggard in creating laws that dealt with computer crime. They had to revise the report after the Canadian Department of Justice took exception and ITAC called for a retraction. Again, it was the perception that the laws were old and as such could no longer be relevant.

As seen in the cases documented above, Canada has been dismissing crackers as mischievous pranksters. The laws were there, but the enforcement wasn't. What good would a change to the laws do, if the existing laws weren't even being used? Even in the notorious Mafiaboy case the sentence was light. The most Mafiaboy could have been sentenced with was 2 years in detention and a $1000.00 fine. This is because Canada has an Act called the Young Offenders Act that treats juveniles charged with a crime (ages 12 – 17) differently than adults in Canada. This is the most serious case Canada has prosecuted, and yet the sentence was almost laughable. But even if the *Code* were changed it would not have made a difference in this case.

ITAC believes that harsher penalties serve as a deterrent to potential offenders. This is a poor excuse for wanting tougher laws, as it is a misconception that harsher penalties deter crime. As far as criminalizing the possession of a virus disseminating device, whatever that may be, it would in all likelihood be unconstitutional to do so.

There seems to be confusion, especially with politicians, as to what computer crime is all about. They recognize that something needs to be done because they hear the media reports of how bad things are in the computer world.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Unfortunately, they are misguided in thinking that changing the laws will make a difference. This stems from a lack of education. During the debate on Motion 80 in the House of Commons, a member actually admitted that he really didn't know what new laws should be added or what the penalties should be. In the end, the government denied Motion 80. The government's reasoning was that the motion was redundant and there is not a vacuum in the law. If a charge has to fall under the mischief of data section, as the RCMP constable complained about, what's wrong with that? If a law was made that was specifically targeted to computer crime, would that change anything?

Only two cases have been prosecuted under the newest Canadian computer laws. Of course cases such as these end up in the headlines only because the offenders got caught. Why don't we hear about the professional computer crackers such as agents for enemy intelligence groups or terrorist groups? Either they are not out there at all, they are out there but our systems are so secure they can't crack them, or they are out there cracking but have not been caught. What do you think the reason is? You can have the strictest laws on the books, but if you can't catch the criminal you can't prosecute them.

Conclusion

It is probably true that Canada is dreadfully behind in its preparedness for averting a major comprise to its systems, whether it be banking, air traffic control, defence, energy generation, or telecommunications. But changing the laws is not going to change that. The RCMP is falling behind because of the growing technology gap between them and the criminals. There are not many officers of the law or prosecutors who understand the technical aspects of computer crime and how illegal acts are committed. What is needed is education. Times have changed, and how crimes are committed has changed as well. If the officers of the law and the courts do not get up to speed on cyber crime now, they will have missed the chance to close that ever widening gap.

The Canadian laws as they pertain to computer crime are fine the way they stand. Sections 342.1 and subsection 430(1.1) were worded in such a way that could make them applicable to some still unknown form of computer mischief.

After the priority of ensuring we have a well-educated law enforcement agency, it is important that we work towards international co-operation in the form of treaties. Laws must be co-ordinated internationally and participation must exist between borders to trace the origins of viruses, worms, trojan horses, malicious code and whatever the next generation of computer crackers bestows upon us. And if and when the time comes that changing the existing laws as they pertain to computer crime would make a difference to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the number of people charged and convicted, Canada will make those changes and remain a world leader in the fight on computer crime.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References:

"Canadian Cyber Crime Laws Are Among the Strongest." McConnell International News Release. 2 Jan 2001. www.mcconnellinternational.com/pressroom/20010102.ctm (02 May 2002).

Department of Justice, Canada. "Canadian Law on Computer Offences and Investigation." 22 Nov 2001. http://www.legal.coe.int/economiccrime/cybercrime/ConfCY(2001)Nat14Canada.pdf (4 May 2002).

Halleck, Gurney. "What is going on in the 418 scene." Phrack Magazine. Volume Four, Issue Forty-four, File 26 of 27. 10 Apr 2001. http://phrack.org/phrack/44/P44-26 (4 May 2002).

Kim, Michael W. "How countries handle computer crime." (Fall 1997). http://www.swiss.ai.mit.edu/classes/6.805/student-papers/fall97-papers/kim-crime.html (4 May 2002).

"'Mafiaboy' Sentenced to 8 Months." Wired News. 13 Sep 2001. http://www.wired.com/news/print/0,1294,46791,00.html (26 Apr 2002).

Mladen, Caryn. "What's Law got to do with it? A reasonable judgement? Wow!" 28 May 2001. www.canadacomputes.com/v3/story/1,1017,6710,00.html (4 May 2002).

Criminal Code of Canada (R.S. 1985, c. C-46) Part IX. 31 Aug 2001. http://lois.justice.gc.ca/en/C-46/39387.html#section-342.1 (29 Apr 2002).

Criminal Code of Canada (R.S. 1985, c. C-46) PART XI. 31 Aug 2001. http://lois.justice.gc.ca/en/C-46/3960.html#rid-39684 (29 Apr 2002).

"Private Members Business – Motion 80, Amending the Criminal Code – Computer Hackers." Hansard. 37th Parliament, 1st Session. 26 Nov 2001. http://www.stephenowen.org/speeches/2001-11-26a.shtml (23 Apr 2002).

Shap, Daniel. "The Jesse Hirsh Case." LoGISTICS. Vol. 01 No. 01 Sept 1995. http://www.catalaw.com/logic/docs/log-late.htm (4 May 2002).

Stinnissen, Arni K. "Computer Crime, Search and Seizure." 11 Apr 2001. http://privacy.openflows.org/powerpoint/computercrime/sld003.htm (2 May 2002).

"Private Members' Business." Edited Hansard No. 045. 37th Parliament, 1st Session. 6 Apr 2001. http://www.parl.gc.ca/37/1/parlbus/chambus/house/debates/045_2001-04-06/HAN045-E.htm#LINK194 (26 Apr 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Evans, James. “Mafiaboy’s story points to ‘Net weaknesses.” 29 Jan 2001. www.computingsa.co.za/2001/01/29/analysis/ana01.htm (3 May 2002).

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced