Mind the Gap: A New Model for Internet Child Pornography Regulation in Canada

Sara M. Smyth*

CANADA'S CHILD PORNOGRAPHY PROVISIONS WERE ENACTED just as the "computer revolution" was building momentum. At that time, very few policy makers had any idea about what the internet was, how it could be used, and its vast potential for facilitating criminal activity on an international scale. Although Parliament has proven to be both willing and able to respond to the child pornography problem, our legislators have not implemented appropriate regulatory measures to combat the circulation of these materials on the internet.

Domestic legislation is clearly necessary to target child pornography offenders; however, various problems with the way that child pornography is now collected and distributed make the use of domestic regulation *by itself* unworkable. Parliament must focus on effective systemic enforcement of internet content by securing the cooperation of service providers at home and abroad. The Council of Europe's *Convention on Cybercrime*, which Canada signed but did not ratify, provides an ideal framework for the implementation of new regulatory measures to achieve this goal. It enables many countries to work together by pursuing a common criminal policy based on international cooperation and the harmonization of domestic legislation. It requires signatory states to update their technological capabilities for combating digital crime by implementing sophisticated evidence gathering techniques to lawfully intercept online communications, share resources, and obtain information about those who use the internet for criminal purposes. Parliament must ratify this treaty and work with other nations to target the proliferation of real child pornography on the internet.

LES DISPOSITIONS RELATIVES À LA PORNOGRAPHIE JUVÉNILE ONT ÉTÉ ADOPTÉES au Canada dans la foulée de la « révolution informatique ». À l'époque, peu de politiciens étaient au courant de ce qu'était Internet, de son mode de fonctionnement et de sa profonde capacité à faciliter les activités criminelles à une échelle internationale. Bien que le Parlement ait démontré sa volonté de réagir efficacement au problème de la pornographie juvénile, nos législateurs n'ont pas adopté les mesures réglementaires appropriées pour lutter contre la diffusion de ce type de documents sur Internet.

Il est donc devenu impératif d'édicter une législation nationale si l'on veut cibler les contrevenants de pornographie juvénile; cependant, les divers problèmes découlant de la manière dont ces images de pornographie juvénile sont recueillies et distribuées rendent la réglementation impossible à appliquer. Le Parlement doit concentrer ses efforts sur des méthodes visant une application systémique du contenu Internet en s'assurant la collaboration des fournisseurs de services aussi bien au Canada qu'à l'étranger. La Convention sur la cybercriminalité, du Conseil de l'Europe, que le Canada a signée mais non ratifiée, fournit un cadre idéal pour l'adoption de nouvelles mesures réglementaires destinées à réaliser cet objectif. Cette convention permet à bon nombre de pays de travailler de concert pour faire appliquer une politique criminelle commune fondée sur la coopération internationale et l'uniformisation des lois nationales. Elle impose aux États signataires la mise à jour de leurs moyens technologiques en vue de combattre la criminalité via Internet en instituant des techniques perfectionnées pour l'obtention d'éléments de preuve en vue d'intercepter, de façon légale, des communications électroniques, de partager des ressources, et de recueillir des renseignements au sujet de ceux et celles qui utilisent Internet à des fins criminelles. Le Parlement doit donc ratifier ce traité et collaborer avec d'autres nations afin de cibler et juguler la prolifération de la pornographie juvénile sur Internet.

---

* Assistant Professor, Department of Criminal Justice, Rochester Institute of Technology. BA, LLB, LLM, PhD (of the British Columbia Bar). I am indebted to everyone who provided comments on this paper, which draws on my PhD thesis. I am most grateful to Jamie Cameron, who supervised the thesis, and whose advice and encouragement were invaluable over the years. Bruce Ryder, Hamish Stewart, Margaret Beare, Liora Salter and Andrea Slane also provided thoughtful comments at the thesis oral defense.

61 1. INTRODUCTION

64 2. THE MODERN HISTORY OF CHILD PORNOGRAPHY

69 3. SPECIFIC MEASURES FOR EFFECTIVE INTER-JURISDICTIONAL COOPERATION

70 *3.1. Offences Relating to Child Pornography*

72 *3.2. Search and Seizure*

73 *3.3. Extradition and Mutual Assistance*

75 4. PURPOSIVE CONSTRUCTION OF OBVIOUSNESS

75 *4.1. Detection and Reporting*

80 *4.2. Lawful Access*

82 5. PROPOSED LAWFUL ACCESS PROVISIONS

82 *5.1. Requirement to Ensure Intercept Capability*

88 *5.2. Requirement to Provide Subscriber Information*

91 *5.3. Orders for the Preservation of Data*

94 *5.4. Orders for the Production of Data*

95 6. THE PRIVACY AND *CHARTER* IMPLICATIONS OF LAWFUL ACCESS

96 *6.1. The Charter of Rights and Freedoms*

104 *6.2. The Personal Information Protection and Electronic Documents Act (PIPEDA)*

106 7. CONCLUSION

Mind the Gap: A New Model for Internet Child Pornography Regulation in Canada

Sara M. Smyth

1. INTRODUCTION

IN THE LAST TEN YEARS OR SO, the internet has rapidly expanded from a little known communications medium into a worldwide product of mass consumption. The internet has opened up new communication channels and created exciting new learning opportunities for those who have access to it. At the same time, it has enabled individuals to perpetrate crimes on an unprecedented scale, with vast distances between themselves and their victims. The internet has become a breeding ground for many different kinds of criminals, including hackers, thieves, child pornography enthusiasts, terrorists, fraud artists, and others who have the technical knowledge and opportunity to commit their crimes through high-tech means. The entry costs are now far lower than those required to commit crime in the real world and one of the biggest advantages claimed by those committing digital crimes is the anonymity they are granted in cyberspace.

This is particularly true with respect to child pornography, which was previously available to a small number of individuals who were able to penetrate highly secretive networks. Until the mid-1990s, there was little child pornography available in Canada and most of it was imported from elsewhere.[1] Those who sought to purchase or trade child pornography images were primarily restricted to small, clandestine networks, through advertisements in magazines, newspapers, or mail solicitations. Much of this distribution was informal and fragmented; yet, in order to import and distribute child pornography in Canada, one needed to evade law enforcement and customs officials who were monitoring the mail system and seizing incoming materials at the border.[2] This suggests that for the past several decades, child pornography distribution mechanisms have been at

1. Donald MacDonald, "Sexual Offences Against Children: The Badgley Report" (Library of Parliament Research Branch, Ottawa, 1988), at p. 13.
2. MacDonald, *supra* note 1 at p. 13. The Badgley Committee reported that the amount of child pornography seized in Canada by customs officials between 1979 and 1981 was very small. There were over 29,000 seizures of obscene materials during this time-period; however, only 1.3%, or 377 items, were child pornography.

least somewhat coordinated and systematic. In addition to the commercial importation and sale of child pornography, there has also been an informal network of private production, mainly designed to serve the sexual interests of those producing it.[3]

By the late 1980s, law enforcement officials were able to significantly reduce the distribution of child pornography through the mail and other commercial avenues. At the same time, many child pornography enthusiasts began to use computer technology to facilitate the exchange of these materials. Since then, the child pornography market has grown rapidly from a small, underground, highly secretive "cottage" industry into one in which very large volumes of pornographic images of children, some of which are extremely violent and sadistic, are widely available on the internet at little or no cost. The child pornography epidemic provides a vital opportunity to consider how internet policy can be further developed to confront computer-related crime in Canada.[4]

Although child pornography is an old and deeply rooted problem in our society, the laws to combat it are surprisingly new.[5] It was not until 1993 that Parliament created a number of offences relating to child pornography in s. 163.1 of the *Criminal Code of Canada (Criminal Code)*.[6] Its broad definition of child pornography includes fantasy materials, which involve no real children in their production,[7] and imposes severe penalties upon those who are convicted of child pornography crimes in Canada. This includes making it an offence punishable by up to ten years in prison for making, distributing, or possessing child pornography for the purpose of distribution and criminalizing simple possession, which is punishable by up to five years imprisonment.[8]

The child pornography provisions were enacted just as the "computer revolution" was building momentum. At that time, very few policy makers had any idea about what the internet was, how it could be used, and its vast potential for facilitating criminal activity on an international scale. While Parliament has proven to be both willing and able to respond to the child pornography problem,

---

3. MacDonald, *supra* note 1, at p. 14.
4. Philip Jenkins, *Beyond Tolerance: Child Pornography on the Internet* (New York University Press, 2001), at p. 5.
5. Amy Adler, "The Perverse Law of Child Pornography," (2001) 101:2 *Columbia Law Review* 209–273, at p. 212.
6. *Criminal Code*, R.S.C. 1985, c. C-46, <http://laws.justice.gc.ca/en/ShowFullDoc/cs/C-46///en>.
7. *Criminal Code*, *supra* note 6, at s. 163.1(1).

> 163.1 (1) In this section, "child pornography" means
>
> (a) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means,
>
> (i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or
>
> (ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years;
>
> (b) any written material, visual representation or audio recording that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act;
>
> (c) any written material whose dominant characteristic is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act; or
>
> (d) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act.

8. *Criminal Code*, *supra* note 6, at ss. 163.1(3) and (4).

Canadian legislators have not implemented appropriate regulatory measures to combat the circulation of these materials on the internet. Concerns about child sexual exploitation have preoccupied Canadian courts and the media in recent years, and have led to demands for justice by an outraged but largely misinformed public. Parliament has consistently responded to the public outcry by broadening the child pornography provisions. Yet the distribution and use of online child pornography has escalated along with increased regulatory attention.

Domestic legislation is clearly necessary to target child pornography offenders; however, various problems with the way that child pornography is now collected and distributed make the use of domestic regulation *by itself* unworkable. There is an urgent need for inter-jurisdictional cooperation because the internet has no boundaries and law enforcement agents must also be given the technical tools to conduct effective cyber-investigations. The Council of Europe's *Convention on Cybercrime* (the *Cybercrime Convention*)[9] provides an ideal framework for the implementation of new regulatory measures to facilitate international cooperation and the harmonization of domestic legislation.

The *Cybercrime Convention* is the first multilateral treaty aimed at facilitating international cooperation in the prosecution of computer crimes. It was signed in Budapest on November 23, 2001 by member states of the Council of Europe and by several non-member states, including Canada, Japan, South Africa, and the United States, that participated in its development.[10] As of September 27, 2006, there were forty-three signatory states.[11] Of the 43 countries that signed the *Cybercrime Convention*, 22 countries have ratified it and entered it into force, including the United States but not Canada.[12]

Parliament must ratify the *Cybercrime Convention* in order for it to take effect in Canada. Several amendments to the *Criminal Code* are needed for Parliament to bring the law into conformity with it, including enabling the interception of online communications, as well as new search and seizure provisions.[13] An important question is whether these measures are feasible in Canada from a technological, budgetary, and constitutional standpoint. There are a number of issues currently facing Canada with respect to the ratification of the *Cybercrime Convention*: Parliament's interest in combating computer crime, particularly online child pornography, which is an international problem of great urgency and importance; the feasibility of implementing new search and seizure methods involving private third parties and digital networks; and the need to safeguard the existing privacy rights and civil liberties of Canadians, particularly those protected by sections 8 and 2(b) of the *Canadian Charter of Rights and Freedoms* (the *Charter*). [14]

---

9. Council of Europe, *Convention on Cybercrime*, Budapest, 23.XI.2001, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> [*Cybercrime Convention*].
10. Laura Huey and Richard S. Rosenberg, "Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention," (2004) 46:5 *Canadian Journal of Criminology and Criminal Justice* 597–606.
11. Council of Europe, Chart of signatures and ratifications for Convention on Cybercrime, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG >.
12. Council of Europe, Chart of signatures and ratifications for Convention on Cybercrime, *supra* note 11.
13. Government of Canada, *Lawful Access Consultation Document*, Department of Justice, Industry Canada, and Solicitor General Canada, 25 August 2002, at p. 10, <http://www.canada.justice.gc.ca/eng/cons/la-al/la-al.pdf> [*Lawful Access Consultation Document*].
14. *Canadian Charter of Rights and Freedoms,* <http://laws.justice.gc.ca/en/charter/index.html> [*Charter*].

Using child pornography as a critical case study, this article will assess how the *Cybercrime Convention* can be successfully implemented in Canada. Part 2 will begin with a general overview of the internet child pornography industry. This is important because we must define the crime that we are seeking to target before we can consider how to successfully combat it. Part 3 will provide a general overview of the provisions contained in the *Cybercrime Convention*. Specific attention will be given to the provisions relating to child pornography. Part 4 will discuss how existing laws must be updated, in order for Canada to ratify the *Cybercrime Convention*, which will enable law enforcement agents to achieve the goals of suspect identification and evidence gathering online. Analogies will be made to existing legislation in other jurisdictions, as well as to legislation that has already been implemented in Canada to combat other emergent threats in the law, such as money laundering and terrorism financing. Part 5 will closely examine how Canada can implement new measures to enable law enforcement agents to lawfully intercept online communications and seize evidence from Internet Service Providers (ISPs). Part 6 will examine whether the proposed initiatives will infringe upon existing privacy rights and constitutional guarantees.

*

2. THE MODERN HISTORY OF CHILD PORNOGRAPHY

IN THE EARLY DAYS OF THE CHILD PORNOGRAPHY TRADE, photographs and films of children in many forms of sexual poses and acts, particularly from the Netherlands and Scandinavia, became available for sale in underground markets in North America.[15] A trusted client could purchase child pornography in a variety of magazines, including those devoted to music and politics, from bookstores in major cities such as New York and Los Angeles or through the underground mail-order market.[16] There was little child pornography available in Canada, with virtually no commercial production of it, and most of what did exist was imported from the United States and appeared to originate in Southeast Asia and other third world countries, as well as Denmark.[17] In the late 1970s, news stories began to focus on pedophiles as violent and predatory monsters who were deliberately and repeatedly photographing or filming children in sexual contexts.[18] The media coverage helped to provoke intense societal reaction and led to child pornography being considered a serious social stigma, associated with the activities of pedophiles and child sex rings. In addition, a vigorous social and legal campaign against many forms of pornography ensued in the late 1970s. Law enforcement officials became actively engaged in prosecutions and seizures of pornography materials, and the availability of child pornography declined dramatically in North America.

---

15. Philip Jenkins, *Moral Panic: Changing Concepts of the Child Molester in Modern America* (Yale University Press, 1998), at p. 146.
16. Jenkins, *supra* note 4, at p. 32.
17. Sharon Moyer, "A Preliminary Investigation Into Child Pornography in Canada," a working document of the Department of Justice Canada, May 1992, at p. 7.
18. Jenkins, *supra* note 15, at p. 145.

The spread of video technology was a significant factor that led to the anti-pornography campaign in the late 1970s and early 1980s.[19] Many anti-pornography feminists became concerned about the lack of regulation and classification of video cassettes and video stores, believing that this would lead unsuspecting consumers, and even children, to become exposed to sexually explicit material.[20] Canadian police also expressed concern that new technologies could widen public exposure to sexually explicit materials.[21] Due to various law reform initiatives and the mobilization of police resources to combat the problem, by 1986 virtually all traditional means of obtaining child pornography had been eradicated, and the entire business was nearing extinction.[22] Those with an interest in child pornography needed to find a more secretive means to distribute and acquire these materials. This is how the internet became essential to the child pornography trade, surprisingly early, in the mid-1980s.[23]

While considerable law enforcement attention was being given to preventing the distribution of child pornography images through the mail, some enthusiasts began using computers to communicate with each other and exchange images. The invention of the modem made it possible for individual users to access bulletin board systems, which allowed them to form discussion groups and share information confidentially.[24] Computer bulletin boards were sometimes used to pass on mailing lists of collectors and other paper-based sources of child pornography, such as magazines and books, which the individual could obtain through mail or courier services rather than online.[25] Although running a bulletin board service was time consuming and expensive, it offered child pornographers an anonymous and speedy means to exchange images, as well as a means to communicate and connect with one another.

At that time, law enforcement agents were not yet aware that child pornographers were using these tools to facilitate the buying, selling, and trading of images. As a result, computer technologies provided an obscure and highly secretive means to share illicit materials out of sight from law enforcement officials.[26] The growing reliance on digital technologies resulted in a significant increase in the quantity of child pornography images circulating online and the number of individuals involved in this illegal enterprise. By the late 1980s, producers and consumers of child pornography were among the most sophisticated users of computer technology and their accumulated technical skills and expertise enabled them to master many useful innovations.[27] Before long, it became possible for child pornographers to access materials from a wide range of sources online and to create, store, and disseminate large files containing both pictures and movies.[28] With each technological advancement, the child pornography trade continued to thrive and flourish, and the law

19. Dany Lacombe, *Blue Politics: Pornography and the Law in the Age of Feminism* (University of Toronto Press, 1994), at p. 75.
20. Lacombe, *supra* note 19, at p. 75.
21. Lacombe, *supra* note 19, at p. 76.
22. Jenkins, *supra* note 4 at pp. 40–41.
23. Yaman Akdeniz, *Sex on the Net* (Reading, UK: South Street Press, 1999), at p. 49.
24. Jenkins, *supra* note 4, at p. 41.
25. Moyer, "Preliminary Investigation," *supra* note 17, at p. 5.
26. Jenkins, *supra* note 4, at p. 43.
27. Jenkins, *supra* note 4, at p.47.
28. Jenkins, *supra* note 4, at p.47.

enforcement officials who pursued the perpetrators were left increasingly far behind.

The internet now offers a wide variety of child pornography materials, including erotic images and stories, video clips, and live sex images and discussions, ranging from the relatively harmless to the exceptionally hardcore. It is difficult to say precisely how much child pornography is internet-based because its production and collection are highly secretive and the available material is constantly changing.[29] Yet we do know that the internet has become the primary medium for the distribution of child pornography.[30] This appears to be a trend that developed over time in North America. It was not until 1993, during an investigation into the kidnapping of a ten-year-old boy from the Baltimore-Washington area that the Federal Bureau of Investigation (FBI) discovered, for the first time, evidence of pedophiles trading pictures of child sexual abuse online.[31] After subsequently discovering a large ring of men using American Online (AOL) to exchange child pornography images, the FBI established the Innocent Images Child Pornography Task Force in 1995, which is one of the first law enforcement centres in the United States dedicated to online child exploitation.[32] The US Postal Inspection Service, the federal law-enforcement branch of the US Postal Service which investigates crimes involving the US mail, including child pornography, reported that in 1999, 81% of child pornography cases it investigated involved computers, compared with 43% in 1998 and 33% in 1997.[33]

The increasing availability of and access to child pornography on the internet in the last decade or so led to a rapid increase in the number of complaints received and cases processed by law enforcement. The National Center for Missing and Exploited Children (NCMEC) reports that in 1998 when it set up a Cyber Tipline to allow the public, police, and ISPs to report online images of child sex abuse, the Tipline averaged about 200 reports per year.[34] By the year 2000, the number of reports had climbed to more than twenty thousand

---

29. Ethel Quayle and Max Taylor, "Paedophiles, Pornography and the Internet: Assessment Issues," (2002) 32 *British Journal of Social Work* 863–875 at p. 868, <http://www.innovationlaw.org/AssetFactory.aspx?did=234>.
30. Max Taylor, Ethel Quayle and Gemma Holland, "Child Pornography, the Internet and Offending," (2001) 2:2 *ISUMA: The Canadian Journal of Policy Research* 94–100 at p. 97.
31. Julian Sher, *Caught in the Web: Inside the Police Hunt to Rescue Children from Online Predators*, (Carroll and Graf Publishers, 2007), at p. 73.
32. Sher, *supra* note 31, at p. 15. The Innocent Images Task Force is a component of the FBI's Cyber Division at FBI headquarters in Washington, DC. It undertakes multi-agency investigative operations to combat the proliferation of online child exploitation and child pornography. It coordinates with state, local, and international governments, as well as FBI field offices and Legal Attachés. See <http://www.fbi.gov>.
33. Eva J. Klain, Heather J. Davies and Molly A. Hicks, "Child Pornography: The Criminal-Justice-System Response," National Center for Missing and Exploited Children, Washington, D.C., March 2001, at p. 2, <http://www.missingkids.com/en_US/publications/NC81.pdf>.
34. NCMEC is a powerful non-profit organization in the United States, headquartered in Alexandria, Virginia, that works in cooperation with the US Department of Justice's Office of Juvenile Justice and Delinquency Prevention to help find missing and abducted children. It receives financial support from the United States Government and from private industry. NCMEC's congressionally mandated CyberTipline, a reporting mechanism for child sexual exploitation, has handled more than 519,300 leads. CyberTip is operated by NCMEC in partnership with the Federal Bureau of Investigation, US Immigration and Customs Enforcement, US Secret Service, U.S. Postal Inspection Service, US Department of Justice's Child Exploitation and Obscenity Section and the Internet Crimes Against Children Task Forces, along with state and local law enforcement. Since its establishment in 1984, NCMEC has assisted law enforcement with more than 135,800 missing child cases, resulting in the recovery of more than 118,700 children. See <http://www.missingkids.com>.

per year.[35] The FBI reports that between 1996 and 2006 there was a 1789% increase in cases opened (113 to 2135), with a 2174% increase in arrests, locates, and summons (68 to 1546), and a 1397% increase in convictions and pretrial diversions (68 to 1018).[36] Similar statistics have also been reported by the Canadian cyber-reporting initiative, known as Cypertip.ca, which was launched on September 26, 2002, and operates as a national cyber-reporting regime.[37] On average, Cybertip.ca now receives over 700 reports and 800,000 hits to its website per month and as of January 2008, the reports to the tipline have resulted in 44 arrests and the removal of 2,850 websites from the internet.[38]

The computer and the internet now facilitate the child pornography industry in numerous ways. An individual can copy traditional paper-based images using a scanner and store them electronically, on a hard disk, USB drive or CD-ROM, where they can be disseminated to others at virtually no cost. Many pictures from thirty or forty years ago, or even longer, which were once distributed privately or commercially through sex shops and mail order services, have been digitized and are currently circulating on the internet.[39] High quality pictures and film clips can be downloaded into a computer within seconds and will not deteriorate over time in the same way as magazine images or photographs do.[40] Encryption software is also used to increase anonymity and reduce the chances of detection by "scrambling" data so that it cannot be easily read by others. Individuals who download images can also use "anonymizers," or "anonymous remailers," which makes it difficult to locate them, much less prove that they possessed or downloaded the images. As a result of these developments, individuals are now acquiring extremely large collections of child pornography from the internet on an unprecedented scale.[41]

Until the mid to late 1990s, the internet commercial child pornography industry was not considered widespread and it was even regarded by some legal scholars as non-existent.[42] Since that time, media reports have indicated that the international commercial child pornography industry has been steadily growing, offering easy access to child sex abuse images to anyone with a credit card. The industry appears to thrive on the fact that the images can be created, accessed, and distributed easily and anonymously in cyberspace. The production of child

---

35. Sher, *supra* note 31, at p. 76.
36. See Federal Bureau of Investigation, "Innocent Images National Initiative," <http://www.fbi.gov/publications/innocent.htm>.
37. See <http://www.cybertip.ca> [Cybertip.ca]. Cybertip.ca receives the majority of its reports from provinces outside Manitoba, including Ontario, British Columbia, Québec, Alberta, and Saskatchewan. It also receives a number of reports from outside of Canada, including the United States, England and Denmark. Some readers might be surprised to learn that in the six month period between its official launch on January 24 and July 30, 2005, Cybertip.ca received 2,297 reports of child sexual exploitation on the internet. This was up from 743 reports for the six months prior to the launch, representing a 200% increase. Over the same period, reports of child pornography increased more than 300%, from 516 to 2,132. See "Press Releases [Media Releases], "Child Pornography Reports Continue to Climb, Canada's National Tipline Releases Second Quarter Statistics, September 1, 2005 (Winnipeg, MB).
38. Cybertip.ca, *supra* note 37, at "About Us [About Cybertip.ca]."
39. Max Taylor, "The Nature and Dimensions of Child Pornography on the Internet," (1 June 2002), at p.7, <http://www.ipce.info/library_3/files/nat_dims_kp.htm>.
40. Taylor, *supra* note 39, at p. 7.
41. Tony Krone, "International Police Operations Against Online Child Pornography," (April 2005) 296 *Trends & Issues in Crime and Criminal Justice* at p. 4, <http://www.aic.gov.au/publications/tandi2/tandi296.pdf >.
42. Lise Gotell, "Inverting Image and Reality: R. v. Sharpe and the Moral Panic Around Child Pornography," (2001–2002) 12:1 *Constitutional Forum* 9–22 at p. 14.

pornography is relatively inexpensive and there is an endless source of children to exploit. There also appears to be a vast consumer market for child pornography materials, with millions of dollars to be made, and entrepreneurs can hide from the authorities by establishing their businesses in countries where the laws are weak and then funneling the profits through financial institutions in multiple jurisdictions. A number of researchers, including Eva J. Klain, have argued that criminals who do not have a sexual interest in children, but who are simply trying to make fast and easy money, are central to the commercial child pornography industry, as are mainstream ISPs, banks, and credit card companies.[43]

The international commercial child pornography industry has become extremely lucrative for profit-motivated criminals who are not necessarily interested in child sexual exploitation themselves. In one recent case, an American couple created a Web portal called Landslide from their home in Texas, where they took credit card payments from subscribers and merchants from around the world for access to websites which contained images of children being sexually abused. During a two year period, from September 1997 to August 1999, Landslide generated revenue of close to US$9,275,900.[44] In its last month of operation, the business reportedly earned up to US$1.4 million.[45] According to Julian Sher, the Landslide website had an estimated 300,000 members in thirty-seven states in the US and sixty countries worldwide, who paid US$29.95 each for a monthly subscription to the service.[46] An estimated thirty to forty percent of the total revenues generated from the business came from child pornography images.[47]

The Regpay case provides another example of the international scope of the commercial online child pornography industry and the immense profits to be made from it. According to Sher, Regpay was a company based in Minsk, Belarus, which operated a network of child pornography sites, including "Redlagoo.com," "lust-gallaery.com," and "lolittas.com," all of which were hosted by ISPs operating in other countries, including the United States.[48] The sites provided customers with easy access to online child pornography using their credit cards.[49] Sher describes how Regpay used a Florida-based company called Connections USA to collect and transfer the money for it,[50] making it difficult for law enforcement officials and the credit card companies to connect Regpay with the online child pornography purchases. According to Sher, American investigators discovered the child pornography sites, began making purchases, and found that the name "Iserve" appeared on their credit card statements.[51] This led them to Connections USA and helped them to discover that Morgan Stanley Trust was the bank receiving the money from the company.[52]

43. Klain, Davies and Hicks, *supra* note 33, at p. 5. See also Sher, *supra* note 31, at p. 117.
44. Sher, *supra* note 31, at p. 45.
45. CBC News: The Fifth Estate, "Landslide Profile of a Pornographer," (5 November 2003), <http://www.cbc.ca/fifth/landslide/profile.html>, and CBC News, "RCMP Tracks Thousands in Child Porn Crackdown," (10 August 2001), <http://www.cbc.ca/canada/story/2001/08/09/child_porn010809.html>.
46. Wendy McAuliffe, "Commercial Child Porn Ring Bust Leads to 100 Arrests," ZDNet UK, (9 August 2001), <http://news.zdnet.co.uk/internet/0,1000000097,2092866,00.htm>.
47. Sher, *supra* note 31, at p. 46.
48. Sher, *supra* note 31, at p. 182.
49. Sher, *supra* note 31, at p. 182.
50. Sher, *supra* note 31, at p. 183.
51. Sher, *supra* note 31, at p. 183.
52. Sher, *supra* note 31, at p. 183

They eventually figured out that the money was being transferred from Morgan Stanley Trust to a bank in Germany and from there to a bank account in Latvia owned by Regpay. There was plenty of money being made by Regpay. Sher reports that in the one year period from June 2002 to June 2003 it received at least US$3 million in payments, not including the eleven percent commission it paid to Connections USA for collecting the payments and wiring the money overseas.[53] According to Sher, in the year 2002, Regpay was generating profits of up to US$200,000 per month and in 2003, it was making as much as US$800,000 in a single month.[54]

The Regpay and Landslide cases illustrate that the international commercial child pornography industry has been thriving during the last decade or so. The internet has also become the primary medium by which child pornography is distributed throughout the world. This is largely due to the fact that communication networks are easy to access, wide-reaching, inexpensive to use, and private. Technology has enabled those with an interest in child pornography materials to access other like-minded individuals from around the globe to share very large amounts of material freely and anonymously. As technology improves, the online child pornography trade will likely continue to grow in sophistication and complexity. The fact that a large amount of child pornography is exchanged through internet websites and newsgroups suggests that law enforcement officials can successfully target child pornography offenders and collect valuable evidence through online surveillance and interception. These issues are further explored below.

*

3. SPECIFIC MEASURES FOR EFFECTIVE INTER-JURISDICTIONAL COOPERATION

IT IS SIGNIFICANT THAT THE TRANSMISSION of child pornography over the internet is a borderless crime because it cuts across international boundaries. Virtually every country is threatened by child sexual exploitation and it will require a collaborative effort on the part of law enforcement and industry players from around the world to attack this problem on a global scale. The *Cybercrime Convention* seeks to overcome these obstacles by facilitating international cooperation. Its central purpose, which is stated in the preamble, is "[…] to pursue […] a common criminal policy aimed at the protection of society against cybercrime, [especially] by adopting appropriate legislation and fostering international co-operation."[55] The *Cybercrime Convention* achieves this goal by requiring state parties to adopt legislation against computer crime, to ensure that their law enforcement officials have the necessary procedural tools to investigate and prosecute these offences, and to work with other signatory states against individuals who perpetrate crimes across multiple jurisdictions.[56] The structure of the *Cybercrime Convention* consists of three major elements: it identifies a list of offences, including offences related to child pornography, that

53. Sher, *supra* note 31, at p. 182.
54. Sher, *supra* note 31, at p. 182.
55. *Cybercrime Convention, supra* note 9.
56. *Cybercrime Convention, supra* note 9 at chaps. II–III.

each signatory state must criminalize;[57] it requires each signatory state to grant new powers of search and seizure to its law enforcement officials, including the power to require an ISP to preserve a citizen's internet activity records and the power to monitor user activity in real time;[58] and it requires law enforcement officials in each signatory state to assist those in other participating states by cooperating with "mutual assistance requests" from police "to the widest extent possible."[59]

3.1. Offences Relating to Child Pornography

Online child pornography is a particularly difficult type of crime to confront on an international scale because it requires many countries to agree on a variety of difficult questions. For example, the very idea of what constitutes "child pornography" is a controversial issue. Owning pedophilic materials is not illegal in Sweden, although it is a crime to market or transmit them, whereas in areas of the Middle East, a picture of a girl in a bikini is considered scandalous.[60] The lack of an international consensus on these issues has led to inconsistent standards and practices around the world and a lasting difficulty in defining what types of material should be prohibited.

A recent study by the International Center for Missing and Exploited Children[61] illustrates how important it is for there to be an international agreement requiring countries to draft legislation defining child pornography and establishing criminal offences relating to it.[62] The study reveals that only 5 out of the 184 Interpol member countries (the United States, France, Belgium, and South Africa) have national legislation that includes specific reference to child pornography; provides a definition of child pornography; criminalizes computer-related crimes; criminalizes the possession of child pornography regardless of whether the offender intends to distribute the materials; and requires ISPs to report suspected child pornography to law enforcement officials, or some other agency.[63] Only 22 countries, including Canada, have all but the last criteria. However, 54 of these countries do not define child pornography; 27 countries do not establish computer-facilitated offences; and 41 countries do not criminalize simple possession, regardless of intent to distribute. A surprising 95 countries have no legislation that specifically addresses the problem of child pornography.[64]

The issue of whether or not a country has legislation defining child pornography and establishing offences relating to it is important because it correlates to the willingness and ability of its law enforcement officials to

57. *Cybercrime Convention*, *supra* note 9, at arts. 2–11.
58. *Cybercrime Convention*, *supra* note 9, at arts. 16–22.
59. *Cybercrime Convention*, *supra* note 9, at arts. 23–35.
60. Frances Cairncross, *The Death of Distance* (Harvard Business School Press, 1997) at p. 183.
61. The International Centre for Missing & Exploited Children (ICMEC) was founded in 1998 and launched by the US-based National Center for Missing & Exploited Children (NCMEC). It works to identify and coordinate a global network of organizations fighting child-sexual exploitation and abduction. See <http://www.icmec.org>.
62. International Center for Missing & Exploited Children, "Child Pornography: Model Legislation & Global Review," (2006), <http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf> [ICMEC, "Child Pornography"].
63. ICMEC, "Child Pornography," *supra* note 62, at p. iv.
64. ICMEC, "Child Pornography," *supra* note 62, at p. iv.

investigate and prosecute offenders. The failure of even a single nation to enact effective child pornography regulations can hamper law enforcement efforts to combat the problem because unlawful materials can be moved to servers in less strict countries, creating "safe havens" for harmful and offensive materials to be distributed around the globe. Even if law enforcement officials can determine the originating location of the material, there can be no meaningful prosecution if the person who is running a child pornography website is operating from a country which does not consider the possession or distribution of the material a criminal offence or treats it as a very minor infraction.[65] This is why it is essential for countries to harmonize their laws with respect to what constitutes child pornography.

Article 9 of the *Cybercrime Convention* requires signatory states to adopt legislative and other measures to establish criminal offences under their domestic law for the following conduct: producing child pornography for the purpose of distribution through a computer system; offering or making available child pornography through a computer system; distributing or transmitting child pornography through a computer system; procuring child pornography through a computer system; and possessing child pornography in a computer system.[66] Article 9 is essential because it establishes a comprehensive framework for the prosecution of child pornography offences throughout the world. By enacting a common list of offences into their penal codes, member states will make it easier to combat child pornography on the internet because they will have a universal basis upon which to approach these crimes.

Article 9 provides a definition of child pornography. Section 2 states that "[…] the term 'child pornography' shall include pornographic material that visually depicts: a minor engaged in sexually explicit conduct; a person appearing to be a minor engaged in sexually explicit conduct; and realistic images representing a minor engaged in sexually explicit conduct."[67] The *Cybercrime Convention* does not provide a definition of "sexually explicit conduct," leaving it up to the various signatory states to come up with their own definition. Section 3 states that "[…] the term 'minor' shall include all persons under 18 years of age."[68] Given that there are vast differences between countries on the question of what constitutes a child, this provision can assist in the investigation and prosecution of online child pornography offences by establishing a universal standard to work from. As the *Criminal Code* already defines a child for the purpose of child pornography, as someone under the age of eighteen years,[69] Canada will have no difficulty meeting its requirements under this aspect of the *Cybercrime Convention*.

---

65. Jenkins, *supra* note 4 at p. 196, who notes that many of the former Communist countries, such as Russia, tend to be lenient in this regard, which has contributed to the fact that there is now a wealth of hardcore child pornography being produced in Russia and other Eastern European countries, which is being transmitted throughout the world using the internet.
66. *Cybercrime Convention*, *supra* note 9, at pp. 5–6.
67. *Cybercrime Convention*, *supra* note 9, at pp. 5–6.
68. *Cybercrime Convention*, *supra* note 9, at p. 6. A state may, however, require a lower age-limit, which must not be less than 16 years, *Cybercrime Convention*, *supra* note 9, at p. 6.
69. *Criminal Code*, *supra* note 6, at s. 163.1.

With respect to its broad definition of child pornography, it is important to note that the *Cybercrime Convention* contains a number of reservations and exceptions. Although Canadian law prohibits fictional representations of minors engaged in sexually explicit conduct,[70] other countries, such as the United States, do not. In order to resolve this conflict, the *Cybercrime Convention* permits state parties to reserve the right not to apply the part of the definition as it relates to "a person appearing to be a minor engaged in sexually explicit conduct" and "realistic images representing a minor engaged in sexually explicit conduct."[71] In addition, states reserve the right to not apply the requirements of "procuring child pornography through a computer system" or "possessing child pornography."[72] Other important issues relating to these reservations and exceptions are discussed below.

3.2. Search and Seizure

The main thrust of the *Cybercrime Convention* is to require participating states to enact legislation granting broad search and seizure powers to law enforcement authorities, including the power to compel ISPs to intercept data transmissions, to provide assistance to police in the storage and search of data transmissions, and to provide information about their individual customers to police. Article 16 requires signatories to adopt legislation requiring ISPs to preserve computer data, including traffic data, for up to 90 days, if it is relevant to an investigation.[73] Article 18 requires signatories to draft regulations that permit law enforcement officials to request computer data as well as individual ISP subscriber information.[74] Article 20 requires that signatory states draft legislation to compel ISPs to permit law enforcement officials to monitor and collect the data of their subscribers in "real-time."[75] Article 21 requires signatories to draft legislation requiring ISPs to intercept and store data, or to assist law enforcement officials in doing so.[76] Together with the mutual assistance provisions discussed below, these provisions facilitate the collection, retention, and dissemination of computer data not only within a single jurisdiction, but also between signatory states. They are useful for targeting a wide range of cybercrime offences committed inter-jurisdictionally, including hacking, identity theft, and fraud, and not just child pornography.

It is noteworthy that some critics of the *Cybercrime Convention* have argued that the privacy interests of individual users are undermined by the real-time interception and recording of data. However, the *Cybercrime Convention* contains provisions to protect civil liberties and human rights in accordance with local state laws. Article 15 requires each state party to "[…] ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human

70. *Criminal Code*, *supra* note 6, at s. 163.1(1).
71. *Cybercrime Convention*, *supra* note 9, at p. 6.
72. *Cybercrime Convention*, *supra* note 9, at art. 9.
73. *Cybercrime Convention*, *supra* note 9, at art. 16.
74. *Cybercrime Convention*, *supra* note 9, at art. 18.
75. *Cybercrime Convention*, *supra* note 9, at art. 20.
76. *Cybercrime Convention*, *supra* note 9, at art. 21.

rights and liberties […]."[77] As I discuss in the next section, it is clear that the *Cybercrime Convention*'s procedural requirement to enable the real-time interception of data can be implemented in accordance with Canada's existing privacy laws, as well as the *Charter*. Article 16 also requires state parties to consider the impact of the powers and procedures provided for in the *Cybercrime Convention* upon the rights, responsibilities, and interests of third parties.[78]

Since 2002, Parliament has been considering how it should design and implement electronic surveillance rules, including production and preservation rules, which would require ISPs to collect and store traffic data and share it with law enforcement authorities. As yet, no workable data retention scheme has been enacted.[79] Canada has not ratified the *Cybercrime Convention* largely because it has not been able to draft workable data retention rules including production and preservation orders, which the *Cybercrime Convention* requires signatory states to adopt. In the next section, I discuss how Canada can ratify the *Cybercrime Convention* by drafting workable legislation in this respect.

3.3. Extradition and Mutual Assistance

Much of the treaty deals with extradition and mutual assistance between nations in investigating and gathering evidence in cybercrime offences. The extradition provisions, contained in Article 24, supplement any formal extradition agreements or treaties that exist between the state parties.[80] Article 24 is critical to the investigation and prosecution of online child pornography offences, which can involve the apprehension of suspects who live in one country but are under investigation or are charged in another. This might occur in the case where an individual operates a website from one country and makes child pornography available in another country for a fee. This provision will help to prosecute child pornographers who set up their operations in countries with weak laws and escape prosecution in the host country, as well as those to whom they disseminate their illegal materials.

Similarly, the "mutual assistance" provisions contained in Article 25 obligate countries to help out other countries in cross-border investigations to the "widest extent possible."[81] This can include drafting mutual assistance treaties with specific nations or responding to requests for "mutual assistance" from states with respect to specific investigations (in conformity with the requirements specified in the *Cybercrime Convention*). Specific requests for "mutual assistance" include expedited preservation of stored computer data, expedited disclosure of preserved traffic data, accessing stored computer data, and interception of content data.[82] This means that officials in one state can request those in another to access, seize, preserve, and make available stored computer data as well as to intercept data in real-time. This is important because

77. *Cybercrime Convention*, *supra* note 9, at p. 8.
78. *Cybercrime Convention*, *supra* note 9, at art. 15.
79. See the Canadian Internet Policy and Public Interest Clinic, <http://www.cippic.ca>; these government proposals will be discussed further in Part 4.
80. *Cybercrime Convention*, *supra* note 9, at art. 24.
81. *Cybercrime Convention*, *supra* note 9, at art. 25.
82. *Cybercrime Convention*, *supra* note 9, at p. 14. See also *Cybercrime Convention*, *supra* note 9, at pp. 18–19 (Articles 30–34).

the physical evidence needed to arrest and prosecute a child pornography suspect can be located anywhere in the world.

The *Cybercrime Convention* does not require dual criminality for mutual assistance with respect to the expedited preservation of stored computer data.[83] Dual criminality occurs when two countries both have statutes prohibiting the same criminal behaviour. Some critics of the *Cybercrime Convention* have voiced concern that a country might be asked to hand over information about its citizens to other countries investigating actions that are illegal in the other country but perfectly legal within their territory.[84] The result, they fear, is that law enforcement officials and ISPs might be forced to cooperate with foreign officials in conducting investigations on citizens in their country who have not committed a crime under their laws.

Yet the *Cybercrime Convention* allows states to require dual criminality as a condition for responding to some requests for mutual assistance. Article 25, which sets out "general principles relating to mutual assistance," provides that in some cases, "[…] the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality […] irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws."[85] Article 29 allows states to require dual criminality as a condition for responding to a request for mutual assistance for the search, seizure, or disclosure of stored computer data and further provides that a state may refuse the request for the expedited preservation of stored computer data if the requirement for dual criminality cannot be fulfilled.[86] This might apply in a case where the government of one country asks law enforcement agents in another country to seize imaginary representations of children, which are perfectly legal in the requested state.

It is curious that dual criminality is such an important issue given that one of the primary objectives of the *Cybercrime Convention* is to harmonize the laws of the signatory states with respect to computer crimes. When states enact the necessary laws to comply with the *Cybercrime Convention*, they will be prohibiting the same criminal acts. It is thus difficult to imagine that a state would not want to assist another state party to the *Cybercrime Convention* on the basis that the conduct at issue is not illegal in both jurisdictions. However, differences between the laws of the signatory states may be relevant because the *Cybercrime Convention* allows parties to reserve the right not to apply certain provisions, as discussed earlier with respect to the definition of child pornography in Article 9.

It is likely that the reservations contained in the *Cybercrime Convention* were necessary to encourage a large number of countries to sign it without drastic changes to their domestic laws, which may have been constitutionally

83. *Cybercrime Convention*, *supra* note 9, at p. 18: "For the purposes of responding to a request [for the expedited production of stored computer data] dual criminality shall not be required as a condition to providing such preservation."
84. Declan McCullagh, "Perspective: Fuzzy Logic behind Bush's Cybercrime Treaty," CNET News (28 November 2005), <http://www.news.com/Fuzzy-logic-behind-Bushs-cybercrime-treaty/2010-1071_3-5969719.html>.
85. *Cybercrime Convention*, *supra* note 9, at p. 15.
86. *Cybercrime Convention*, *supra* note 9, at art. 29.

unworkable. Yet the issue of dual criminality illustrates the need for countries to establish uniform standards for the definition and prosecution of child pornography offences. A common understanding of what constitutes a "child" and "child pornography" is critical in order to ensure that relevant information can be gathered and shared in cross-border child pornography investigations and that offenders can be prosecuted.

The *Cybercrime Convention* is perhaps not the perfect solution to the global problem of online child pornography because it fails to require signatory states to define a common set of offences. The fact that it permits parties to preserve their existing laws undermines its central goal of harmonizing legislation to combat computer crime on a global scale. Yet despite these flaws, it is currently the best way to achieve international harmonization and cooperation. One of its most critical shortcomings is the fact that not every country has agreed to be bound by it. As of February 17, 2009, of the 46 states that signed the *Cybercrime Convention*, only 23 have ratified it.[87] If global participation in the *Cybercrime Convention* cannot be obtained, cyber-criminals will continue to relocate their criminal enterprises to "safe-haven" countries. Other states, including Canada, will be forced to investigate and prosecute these offenders without assurance that the host state will cooperate, making it difficult to recover evidence, locate child victims, and secure convictions. Thus, not only does Parliament need to implement the domestic measures necessary to ratify the *Cybercrime Convention* and thus set a good example for other states, but it also needs to encourage non-participating countries to join the *Cybercrime Convention* by signing, implementing, and ratifying it. The next section of this article examines the various measures that are needed for Canada to achieve this important goal.

*

4. PROPOSED METHODS OF REGULATORY CONTROL

4.1. Detection and Reporting

ONE OF THE FEW MECHANISMS THAT CURRENTLY EXISTS in Canada to ensure the cooperation of ISPs in the investigation of child pornography suspects, and to facilitate the removal of illegal content from ISP networks, is a voluntary agreement entered into by the members of the Canadian Association of Internet Providers (CAIP). [88] CAIP was formed in 1996 and represents a broad range of internet providers, including large telephone companies, telephone carriers, and independent ISPs of all sizes. CAIP reports on its website that approximately 80% of Canadian internet users subscribe to a CAIP-member ISP for their internet service.[89] The mission of the association is to foster the growth of a healthy and competitive internet service industry in Canada through cooperation on both local and international issues. CAIP established a code of conduct for its ISP members, which includes the following: cooperating with government officials,

87. Information about the current status of the *Cybercrime Convention* can be found on the Council of Europe's website, <http://conventions.coe.int/>.
88. See Canadian Association of Internet Providers, <http://www.caip.ca> [CAIP].
89. CAIP, *supra* note 88.

international organizations and law enforcement, as well as all applicable laws (this includes developing internal practices to comply with legal standards); promoting public education regarding internet issues and technology; protecting the privacy of their users (which entails only disclosing private customer information when required by law); refusing to host illegal content (which includes sharing information about material that is illegal); and investigating complaints regarding illegal content or network abuse (which includes undertaking internal reviews of complaints, consulting with legal authorities and notifying the content provider or abuser of the complaint).[90]

While these are clearly laudable goals, the major disadvantage of this system is that it is entirely voluntary. Canadian ISPs who are not members have not signed up to abide by the code of practice and CAIP cannot force them to comply with any of its requirements. CAIP members are also not legally required to fulfill any of the commitments they set out in their code of conduct and do not even obligate themselves to remove harmful or illegal content from their networks.[91] While we might assume that the members of this voluntary association would want to comply with the law and remove harmful materials from their servers, there is no legal obligation to do so. Parliament would have to pass legislation to compel ISPs to comply with these requirements because they are not legally enforceable under Canadian law.

In order to address this gap between the law and technology, Parliament should enact legislation requiring ISPs to monitor their networks for child pornography and disclose their suspicions of illegal content to a centralized law enforcement agency. A number of countries, including South Africa, the United States and the United Kingdom, have established this type of regime. In South Africa, the *Films and Publications Amendment Act, 1999* requires ISPs to "take all reasonable steps to prevent the use of their services for the hosting or distribution of child pornography," and to report any incidents of child pornography to the police, along with the particulars of the person maintaining, hosting or distributing those materials.[92] In addition, ISPs are required by this provision to preserve the evidence for the purposes of investigation and prosecution by law enforcement officials. A violation of this section can lead to fine or imprisonment for up to five years.

In the United States, the *Protection of Children from Sexual Predators Act*[93] requires ISPs to report to law enforcement any knowledge of facts or circumstances involving the violation of child pornography offences. It establishes fines for initial and subsequent failures to make a report. Another US federal law[94] requires ISPs to report online child pornography to the NCMEC's CyberTipline,[95] a congressionally mandated mechanism for reporting child exploitation and abuse, where analysts are required to forward reports to the appropriate law enforcement agency. An ISP's failure to make a report can result

90. CAIP, *supra* note 88.
91. CAIP, *supra* note 88.
92. *The Films and Publications Act*, (1999) Parliament of the Republic of South Africa, <http://www.fpb.gov.za/docs_publications/acts_regulations/docs/Act%20and%20Regs.pdf> at s. 27A(1)(b).
93. *Protection of Children from Sexual Predators Act* (USA 1998), P.L. 105-314, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ314.105>, at s. 604.
94. 42 U.S.C. 13032(b) (1).
95. See *supra* note 34.

in a substantial fine.

In a recent press release, the NCMEC announced that since the CyberTipline was established in 1998, reports of child pornography images by ISPs and members of the public have increased each year.[96] NCMEC believes the growth in reports can be attributed to several factors: new technologies; an increased public awareness about the issue; and the federal law requiring ISPs to report incidents of child pornography to the CyberTipline. However, it also reported that only 142 of the more than 3,000 ISPs in the US comply with the federal law, suggesting that while the law has been effective, it needs stronger enforcement.[97]

In the UK, an ISP Association (the ISPA) was established in 1995 to promote self-regulation of the internet industry.[98] ISPA helped to establish the Internet Watch Foundation (IWF) in 1996. Members agree to abide by the ISPA UK Code of Practice which provides, in section 5.2, that ISPA members will cooperate with the Internet Watch Foundation in an effort to remove illegal material from internet websites and newsgroups.[99] The IWF works with UK government departments and is funded by the EU and the UK internet industry. The IWF set up a hotline to receive reports of illegal content from the public, with the focus on internet child pornography. ISPA members provide twenty-four hour point of contact with the IWF to receive notices of illegal material, which they immediately remove from their servers after they are reviewed by IWF staff to see whether they are illegal under Britain's child protection laws.[100] The IWF also reports this information to the police, allowing for further investigation and prosecution. If the content provider is located outside the UK, the IWF provides the information to the National Criminal Intelligence Service, which forwards it to the relevant authorities in the host country. The IWF also recommends to ISPs that they not carry certain newsgroups. In its first year of operation, the IWF handled 615 reports and in 2006 it processed as many as 27,750 reports.[101]

The UK regime is far more effective than the one established in Canada because it incorporates a reporting mechanism, whereby ISPA members commit to reporting illegal material to the IWF and removing them from their networks. In Canada, the members of CAIP have only agreed to investigate complaints about illegal materials, consult with law enforcement agencies, and notify content providers about complaints. There is no legal requirement for ISPs in Canada to monitor their networks and report suspicions of illegal content to law enforcement. The major disadvantage of the British model is that, like its Canadian counterpart, membership in the ISPA is voluntary.[102] The strongest sanction that the ISPA can impose upon its members for non-compliance is

96. National Centre for Missing & Exploited Children, "Reports of Child Pornography to the National Center for Missing & Exploited Children Continue to Rise," (27 January 2005), <http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=1865> [NCMEC, "Reports"].
97. NCMEC, "Reports," *supra* note 96.
98. See the ISPA Website, <http://www.ispa.org.uk>.
99. ISPA Code of Practice, adopted on 25 January 1999, <http://www.ispa.org.uk/about_us/page_16.html#IWF>.
100. Sher, *supra* note 31 at 228.
101. Sher, *supra* note 31 at 227.
102. Sher, *supra* note 31 at 229.

suspension or expulsion from membership,[103] which is an ineffective and inadequate response to the child pornography problem.

The proposed measures to address child pornography in Canada, which would require ISPs to monitor their networks for child pornography and disclose their suspicions of illegal content to a centralized law enforcement agency, are very similar to those which have already been implemented in response to other significant threats, including terrorism and money laundering.[104] The new *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (Money Laundering and Terrorism Financing Act)*[105] authorizes FINTRAC to detect and deter money laundering and the financing of terrorist activities and to disclose this information to law enforcement. FINTRAC operates at arms length from the police and other departments and agencies of government to whom it provides financial intelligence. It receives reports from financial institutions, as well as other businesses, law enforcement agencies, and other government institutions. It analyzes the reported information and discloses suspicions of money laundering or terrorist financing activities to the relevant law enforcement authorities.[106]

The most important aspect of this regime is that it imposes reporting requirements upon private third parties in cases where they have reason to suspect that their clients are engaged in illegal activities. Since June 12, 2002, a number of entities must disclose suspicious transactions to FINTRAC where there are *reasonable grounds to suspect* that transactions are related to either a money laundering or terrorism activity financing offence.[107] They must also report to FINTRAC if they have property in their possession or control that they know is owned or controlled by or on behalf of a terrorist group. Since January 2003, these institutions and entities also have to report to FINTRAC large cash transactions involving amounts of C$10,000 or more and, as of March 2003, international electronic funds transfers of C$10,000 or more.[108]

The *Money Laundering and Terrorism Financing Act* also places responsibilities upon these entities to implement a compliance regime, keep certain transaction records (for large transactions of $10,000 or more), verify the identity of clients with whom they are conducting these transactions, and make "third party determinations," where a third party is instructing the individual

---

103. See the ISPA Code of Practice, *supra* note 99 at s. 8.4, <http://www.ispa.org.uk/about_us/page_16.html#IWF>.
104. Parliament established the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which is a government agency responsible for the collection, analysis, assessment and disclosure of information in order to assist in the detection, prevention and deterrence of money laundering and financing of terrorist activities in Canada and abroad <http://www.fintrac-canafe.gc.ca/intro-eng.asp>.
105. *Proceeds of Crime (Money Laundering) and Terrorist Financing Act,* (2000) *Statutes of Canada* ch. 17, <http://canlii.com/ca/sta/p-24.501/>.
106. *Proceeds of Crime (Money Laundering) and Terrorist Financing Act, supra* note 105.
107. Financial entities (includes banks, credit unions, caisses populaires, trust and loan companies and agents of the Crown that accept deposit liabilities); life insurance companies, brokers or agents; securities dealers, portfolio managers and investment counselors who are provincially authorized; persons engaged in the business of foreign exchange dealing; money services businesses; agents of the Crown when they sell money orders; accountants and accounting firms (when carrying out certain activities on behalf of their clients or receiving fees for such activities); real estate brokers or sales representatives (when carrying out certain activities on behalf of their clients); and casinos (including those authorized to do business in Canada, with slot machines or roulettes or card games, but excluding certain temporary charity casinos). *Proceeds of Crime (Money Laundering) and Terrorist Financing Act, supra* note 105 at s. 5.
108. *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, Canada Gazette,* Part II, SOR/2002-184, <http://www.gazette.gc.ca/archives/p2/2002/2002-05-14-x/html/sor-dors184-eng.html>.

making the transaction, as well as keep related records.[109] All reporting entities are protected from civil and criminal legal liability when they submit transaction reports and terrorist property reports in good faith to FINTRAC. However, a failure to comply with record keeping and reporting requirements can lead to criminal charges being brought.[110]

According to the most recent Annual Report issued by FINTRAC, this system has been successful at combating money laundering and terrorist activity financing in Canada.[111] FINTRAC made 168 case disclosures to law enforcement, or to the Canadian Security Intelligence Service (CSIS), in the 2005/2006 year.[112] These cases involved over C$5 billion, which was more than double the value from the previous year. The total value of case disclosure of suspected terrorist activity financing and other threats to Canadian security was approximately C$256 million.[113] The Minister of Finance, Jim Flaherty, announced that the increase in the dollar value of disclosures is the direct result of coordinated financial intelligence, which is being reflected in investigations, charges and prosecutions.[114]

In addition, section 83.1(1) of the *Criminal Code* provides:

> Every person in Canada and every Canadian outside Canada shall disclose forthwith to the Commissioner of the Royal Canadian Mounted Police and to the Director of the Canadian Security Intelligence Service (a) the existence of property in their possession or control that they know is owned or controlled by or on behalf of a terrorist group; and (b) information about a transaction or proposed transaction in respect of property referred to in paragraph (a).[115]

Section 83.11(1) of the *Criminal Code* places specific reporting and disclosure requirements upon financial institutions, of the same sort as those listed under the *Money Laundering and Terrorism Financing Act*, to determine on a continuing basis whether they are in possession or control of property owned or controlled by or on behalf of a entity (or acting on its behalf) that has knowingly carried out, attempted to carry out, participated in, or facilitated, a terrorist activity.[116]

The reasoning behind these measures is that financial service providers, and other related entities, are often the first to come into contact with a financial transaction that may be linked to money laundering or terrorist financing. They are the "gatekeepers" of highly secretive information, including client identification and transactional details, which is essential to providing law enforcement officials with the tools they need to investigate and prosecute serious crimes. Similar to FINTRAC, Parliament must establish an independent agency to operate at arms length from the police and other departments and

109. See ss. 3, 4, 5 of Guideline 6, June 2005, <http://www.fintrac-canafe.gc.ca/publications/guide/Guide6/6-eng.asp>.
110. See Guideline 1, March 2003, <http://www.fintrac-canafe.gc.ca/publications/guide/Guide1/1-eng.asp>.
111. FINTRAC News Release, "Canada Shedding More Light on Money Laundering and Terrorism Financing, FINTRAC Reports," 4 October 2006, <http://www.fintrac-canafe.gc.ca/publications/nr/2006-10-04-eng.asp> [FINTRAC News].
112. FINTRAC News, *supra* note 111.
113. FINTRAC News, *supra* note 111.
114. FINTRAC News, *supra* note 111.
115. *Criminal Code*, *supra* note 6.
116. *Criminal Code*, *supra* note 6.

agencies of government by receiving reports from third parties, analyzing and assessing the reported information and disclosing evidence of illegal activities to the relevant law enforcement authorities. Once the evidence has been carefully analyzed and determined to be illegal, law enforcement agents must be able to proceed with obtaining production and preservation orders to seize it for use in a criminal investigation. They must also be able to compel ISPs to provide them with the names and addresses of content providers for the purposes of investigation and prosecution. The preservation of the illegal material is also critical to provide evidence for a prosecution. The measures relating to production, preservation and the provision of subscriber information are discussed below.

4.2. Lawful Access

Lawful access applies to the lawful interception of communications, as well as the search and seizure of information by law enforcement authorities, either with or without a judicial warrant. In 2002, after the federal departments of Justice, Industry and the Solicitor General conducted extensive consultation with members of the law enforcement community, the telecommunications industry, and the public, Parliament tabled a *Lawful Access Consultation Document,*[117] which addressed the need to enact new regulations to enable law enforcement officials to lawfully intercept online communications and seize evidence from ISPs. Parliament maintains that lawful access provisions are necessary to provide law enforcement agencies with "modern and effective capabilities to support their investigative or intelligence gathering efforts" and to "bring the law into accordance with the current state of telecommunications technology."[118] One of the principal reasons behind this initiative was to ratify the *Cybercrime Convention*, which requires Parliament to draft provisions for "production and preservation orders" and the lawful interception of online communications into the *Criminal Code*. The United States recently implemented these measures into its federal legislation, whereas Canada has not yet taken these important steps.

In 2005, Parliament tabled Bill C-74, or *The Modernization of Investigative Techniques Act* (MITA).[119] The purpose of this Act was,

> to ensure that telecommunications service providers have the capability to enable national security and law enforcement agencies to exercise their authority to intercept communications, and to require service providers to provide subscriber and other information, without unreasonably impairing the privacy of individuals, the provision of telecommunications services to Canadians or the competitiveness of the Canadian telecommunications industry.[120]

The Bill passed first reading in November 2005, but died on the order paper

117. *Lawful Access Consultation Document*, *supra* note 13.
118. *Lawful Access Consultation* Document, *supra* note 13 at p. 4.
119. *The Modernization of Investigative Techniques Act*, 38th Parl., 1st Sess. 4 October 2004 – 29 November 2005, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=2334024&file=4> [MITA].
120. MITA, *supra* note 119 at s. 3.

when the 38th Parliament dissolved at the end of that month.[121] A federal Liberal Member of Parliament, Marlene Jennings, recently introduced a private members bill, Bill C-416, which is virtually identical to the one proposed by the previous Liberal government in 2005, through which she hopes to get the current Conservative government to pass the MITA.[122]

The MITA would require ISPs to have intercept-capable networks, which means that when an ISP introduced new technologies into its network, such as installing new equipment or software, it would be obligated to include an interception capability.[123] This would provide law enforcement officials with the ability to intercept and isolate information concerning a particular suspect, including the ability to simultaneously intercept communications of multiple users, and to provide the intercepted communication to law enforcement officials, and to remove, where possible, any measures taken to preserve the anonymity of a communication, such as encryption, compression, or encoding.[124] The MITA would also require ISPs to disclose basic information about subscribers to law enforcement officials, including an individual's name, address, and internet protocol (IP) address, without the need for a warrant or judicial order.[125] Other provisions contained in the *Cybercrime Convention*, such as those relating to production and preservation orders, were not introduced as legislation; however, they were raised by the Government in its extensive consultations on the issue of lawful access legislation.[126]

Given the challenges of combating cybercrime offences, Parliament must establish an effective model for lawful access to data held by ISPs. Canada is in a good position to implement lawful access legislation because it has already undertaken an extensive consultation process and drafted legislation, which could serve as a model for new regulatory initiatives.[127] In addition, lawful access legislation already exists in many other countries, including the United States and the United Kingdom, which provided the starting point for Bill C-74.[128] Given that other major western nations have already dealt with many of the difficult issues surrounding the implementation of a lawful access regime, including cost and competition concerns, which are discussed below, Canada has several excellent models from which it can develop its own workable legislative scheme.

The regulatory framework must be broader than the one set out in Bill C-74 because Parliament neglected to address all the provisions contained in the *Cybercrime Convention*, including orders for the preservation and production of data, discussed below, which were proposed by Parliament in its *Lawful Access Consultation Document* but not included in Bill C-74. Implementing these measures will enable Canada to keep up with legislative developments in other nations and cooperate with our partners in combating trans-border computer

121. Dominique Valiquet, *Telecommunications and Lawful Access: II. The Legislative Situation in the United States, The United Kingdom and Australia,* (28 February 2006), Library of Parliament, <http://dsp-psd.pwgsc.gc.ca/collection_2007/lop-bdp/prb/PRB0566-e.pdf> [Valiquet, *Telecommunications and Lawful Access II*].
122. CBC News, "Harper Government Should Adopt Liberal Bill on Surveillance: MP," (29 March 2007), <http://www.cbc.ca/canada/montreal/story/2007/03/29/interception-bill.html>.
123. Valiquet, *Telecommunications and Lawful Access: II*, *supra* note 121 at p. 2.
124. MITA, *supra* note 119 at s. 6(1).
125. Valiquet, *Telecommunications and Lawful Access: II*, *supra* note 121 at p. 2.
126. *Lawful Access Consultation Document, supra* note 13.
127. Valiquet, *Telecommunications and Lawful Access: II*, *supra* note 121 at p. 2.
128. Valiquet, *Telecommunications and Lawful Access: II*, *supra* note 121 at p. 12.

crime, as called for by the *Cybercrime Convention*. Parliament must, of course, be mindful of balancing existing privacy protections and *Charter* guarantees against the need to develop workable internet data policies, both independently and in conjunction with other nations. Following a detailed review of the provisions relating to the lawful access of data, I will examine how this can be done in a manner that safeguards fundamental privacy interests and *Charter* guarantees.

*

5. PROPOSED LAWFUL ACCESS PROVISIONS

5.1. Requirement to Ensure Intercept Capability

LAW ENFORCEMENT OFFICIALS IN CANADA CURRENTLY have powers under Part Six of the *Criminal Code* to intercept private communications.[129] However, since the legal provisions relating to lawful interception were drafted in the early 1970s, Canadians have witnessed significant changes in information technologies, including the widespread use of the internet. The *Criminal Code* must be updated to reflect the changes that have occurred with respect to recent advances in communications technologies. Since 1995, the Canadian Association of Chiefs of Police (CACP) has urged Parliament to enact legislation to compel telecommunications service providers to maintain the technical capabilities to enable law enforcement officials to conduct lawful interceptions on their networks.[130]

In 2002, the CACP released a response to Parliament's *Lawful Access Consultation Document* in which they maintain that there are a number of examples where the safety of victims of crime has been jeopardized by the refusal of carriers to comply with existing legislation and warrants" and "non-compliance and delays pose serious threats to public safety.[131] They further state that some ISPs have "refused to cooperate with court ordered surveillance."[132] For example, some ISPs in central Canada are "very reluctant to make their networks compliant to judicially authorized interception" and some ISPs "steadfastly ignore the requests of police to work with them to create an effective intercept capability."[133]

Further, under the current regime, ISPs are not required to have interception capabilities, so when a new technology or communication service is introduced, law enforcement agents must develop innovative methods to gain access to the networks.[134] Canadian police are frustrated because they have no

---

129. Part VI of the *Criminal Code* sets out procedures for how to obtain judicial authorizations to conduct electronic surveillance in criminal investigations. These provisions are discussed below.
130. Dominique Valiquet, *Telecommunications and Lawful Access: I. The Legislative Situation in the United States, The United Kingdom and Australia*, PRB 05-65E, Library of Parliament, 21 February 2006, <http://www.parl.gc.ca/information/library/PRBpubs/prb0565-e.pdf> [Valiquet, *Telecommunications and Lawful Access I*].
131. Canadian Association of Chiefs of Police, "Response to the Government of Canada's Lawful Access Consultation Document," (16 December 2002) <http://www.cacp.ca/media/library/download/215/CACPResponse.pdf> [CACP, "Response"] at p. 2.
132. CACP, "Response,"*supra* note 131.
133. CACP, "Response," *supra* note 131 at p. 8.
134. Paul Weinberg, "Wiretaps Could Raise the Cost of Web Access," (28 July 2005) *The Globe and Mail*, <http://intperspectives.wordpress.com/2005/07/28/wiretaps-could-raise-costs-of-web-access/>.

standard means by which to intercept a suspect's online communications.[135] This is why they are asking for legislation to compel ISPs to have a technical means to enable law enforcement officials to intercept communications built into their network technology from the outset.[136]

As I discussed in Part 1, in 2001, Canada signed the *Cybercrime Convention* which requires all signatory states to adopt legislative measures compelling ISPs to permit the interception and seizure of both *traffic* and *content* data from their networks.[137] Canadian legislation must be updated, in conformity with this important international agreement, to reflect the increasing inter-jurisdictional nature of crime. Not only are these regulations workable in Canada, they are consistent with our international obligations and current international standards. By implementing these measures, Parliament will enable Canadian law enforcement agencies to harmonize their surveillance capabilities with other nations and work collaboratively with police in other jurisdictions.

Canada needs to expand existing intercept powers in two ways. First, Parliament must impose a legal obligation on ISPs to update their networks so that they can be intercepted by law enforcement agents. The standard should be for all new or significantly upgraded technologies to be intercept-capable by a specific date. Second, Parliament must update the *Criminal Code* to make it clear that law enforcement officials can intercept content data in real time on ISP networks. Canadian police must only be able to intercept online communications with prior court approval.

Judicial authorization can be required for all interceptions according to the same standards already set out in the *Criminal Code* for other forms of communication, such as telecommunications, as I discuss below. Part VI of the *Criminal Code* sets out the requirements that must be met to successfully apply for an authorization to intercept private communications and these conditions should apply to the interception of ISP networks. Only the Minister of Public Safety and Emergency Preparedness, or persons specially designated by the Minister or the Deputy Minister of Public Safety and Emergency Preparedness, may make an application for an authorization with regard to offences that may be prosecuted by or on behalf of the Attorney General of Canada. An application must be accompanied by an affidavit sworn by a peace officer or public officer. The affidavit must include information such as the facts relied on to justify the need for an authorization, details about the offence, and the names and addresses of the persons whose private communications would be intercepted.[138]

Before an authorization is issued, the judge hearing the application must be satisfied that it would be in the best interests of the administration of justice to authorize the electronic surveillance. Except in the case of certain specific

135. Weinberg, "Wiretaps Could Raise the Cost of Web Access," *supra* note 134.
136. Weinberg, "Wiretaps Could Raise the Cost of Web Access," *supra* note 134.
137. *Cybercrime Convention*, *supra* note 9, Articles 20 and 21. Traffic data is defined as including any data relating to the routing of a communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service. This includes information about an email (including those that are located in a "draft" box, an "inbox," or are in transit), the sender, recipient, size, subject line, as well as the URLs visited, time spent online, requests to search engines for specific information and downloads. Content data is not defined in the *Cybercrime Convention*; however, it might include the content of Internet web pages visited, as well as messages sent and received.
138. *Criminal Code*, *supra* note 6 at s. 185.

offences, such as a terrorism offence, the judge must also be satisfied that other investigative procedures have been tried and failed, that other investigative procedures are unlikely to succeed, or that there is an urgency which renders other investigative procedures impractical. The judge may impose terms and conditions on the authorization, including conditions to ensure that the privacy of individuals is respected as much as possible during the surveillance.[139]

Authorizations are not issued for a period of time longer than 60 days.[140] However, designated persons may apply to a judge to have the authorization renewed, which extends the period of time during which police can lawfully conduct electronic surveillance. Before the judge may renew the authorization, he or she must be satisfied that the same circumstances that applied to the original application for authorization still apply.[141] Provisions also exist to obtain authorizations in emergency situations. Under section 188 of the *Criminal Code*, a peace officer may apply to a judge for an authorization if the urgency of the situation requires interception of private communications, but there is not enough time to use the regular application process to obtain an authorization.[142] In these circumstances, authorization may be issued for a period of up to 36 hours and the judge may impose terms and conditions upon it.

In addition to applying for an authorization to intercept private communications, law enforcement officials may also apply to a judge for a "general" warrant under section 487.01 of the *Criminal Code*.[143] This section enables the issuance of a warrant for the use of any device or investigative technique that is not contemplated elsewhere in the *Criminal Code* or any other Act of Parliament. As with other judicial authorizations, certain requirements must be met before a warrant can be issued. In the case of warrants issued pursuant to section 487.01, these requirements include: the judge must be satisfied by information provided under oath and in writing (i.e. a sworn affidavit) that there are *reasonable grounds to believe* that an offence has been or will be committed, and that *information about the offence can be obtained* by the use of the technique; the judge must be satisfied that it is in the best interests of the administration of justice to issue the warrant; there must be no other provision in the *Criminal Code* or any other Act of Parliament that would provide for a warrant, authorization or order to allow the intended video surveillance to be carried out.[144] The judge may also impose terms or conditions on the warrant, including conditions to ensure that the privacy of individuals is respected as much as possible during the surveillance.

As previously mentioned, the requirement to ensure lawful intercept capabilities has been implemented by other nations, including the United Kingdom, which enacted the *Regulation of Investigatory Powers Act* in 2000,[145] requiring telecommunications service providers to maintain a reasonable intercept capability, and similar legislation was also enacted in the United States.

139. *Criminal Code*, *supra* note 6 at s. 186.
140. *Criminal Code*, *supra* note 6 at s. 186(4)(e).
141. *Criminal Code*, *supra* note 6 at s. 186(6).
142. *Criminal Code*, *supra* note 6.
143. *Criminal Code*, *supra* note 6 at s. 487.01.
144. *Criminal Code*, *supra* note 6 at s. 487.01.
145. *Regulation of Investigatory Powers Act*, 2000, ch. 23, Bill 64 of 1999-2000; in force October 2000, <http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1>.

On October 25, 1994, Congress enacted the *Communications Assistance for Law Enforcement Act* (CALEA).[146] CALEA sets out the interception capability requirements that telecommunications carriers[147] must establish and maintain within their networks to enable law enforcement officials to conduct electronic surveillance.[148] CALEA does not expand or modify law enforcement's authority to conduct electronic surveillance in the United States. It simply requires telecommunications carriers to modify and design their equipment, facilities, and services to ensure that they have the necessary capabilities to assist law enforcement officials with electronic surveillance and the collection of both content and traffic data.[149] In this sense, it is similar to Bill C-74.

Telecommunications service providers were required to comply with CALEA by June 30, 2002.[150] Congress addressed the issue of financial expense by ensuring that a substantial portion of the costs of implementing CALEA would be borne by taxpayers. Section 109 provides that the Attorney General may pay telecommunications carriers for all reasonable costs associated with updating their networks and Congress authorized a fund of $500 million to be set aside for this purpose.[151] This is similar to the legislation enacted in the United Kingdom which provides that the Secretary of State may make arrangements for contributions toward costs incurred by telecommunications service providers in maintaining intercept capability out of money provided by Parliament.[152]

The financial costs associated with the implementation of mandatory intercept capability requirements is an important issue for Canada because network upgrades could cost millions of dollars.[153] The CACP reports that even in cases where the technical ability to intercept exists, some service providers in Canada are frustrating police efforts, even in cases where prior court approval has been granted, by arbitrarily imposing substantial fees upon law enforcement agencies.[154] This has forced law enforcement officials in some cases to "negotiate" the terms upon which the ISP grants access to its networks, even where they have already obtained judicial authorization.[155] Clearly, no service provider should have the ability to frustrate a court ordered investigation by imposing arbitrary and inconsistent fees and other terms as a pre-condition of compliance, particularly

146. *Communications Assistance for Law Enforcement Act*, 1994, *Pub L. No. 102-414, 108 Stat. 4279*, <http://www.askcalea.net/docs/calea.pdf> [CALEA].
147. Although the definition of "telecommunications carrier" in CALEA, *supra* note 146 at 47 USC s. 1001, appears to apply only to telephone communications and not ISPs, the FCC issued a ruling in September 2005 to ensure that the Act would apply to ISPs and companies providing Internet telephone services, such as "voice over Internet Protocol" or "VOIP." See FCC 05-153, First Report and Order, CC Docket No. 04-295, 23 September 2005, <http://www.educause.edu/ir/library/pdf/EPO0528.pdf>.
148. Department of Justice, Federal Bureau of Investigation, CALEA Implementation Section, *Flexible Deployment Assistance Guide*, 3d ed. (May 2002), <http://www.askcalea.net/archives/docs/flexguide3.pdf>.
149. *Flexible Deployment Assistance Guide*, *supra* note 148 at p. 4.
150. Federal Communications Commission, FCC 02-108, CC Docket No. 97-213, April 11, 2002. CALEA also states that if a telecommunication service provider does not comply with the Act by the required date, it is liable to an enforcement action under s.108 and fines up to $10,000 per day. See CALEA, *supra* note 146 at sec.1007 and see *Enforcement of the Communications Assistance for Law Enforcement Act*, 18 U.S.C. s. 2522(c), <http://www.law.cornell.edu/uscode/18/usc_sec_18_00002522----000-.html>.
151. *Flexible Deployment Guide*, *supra*, note 148 at p. 6.
152. See the *Regulation of Investigative Powers Act*, *supra* note 145 at s. 14 and Gabrielle Garton Grimwood and Christopher Barclay, *The Regulation of Investigatory Powers Bill*, Research Paper 00/25, House of Commons Library, 3 March 2000, <http://www.parl.gc.ca/information/library/prbpubs/prb0566-e.pdf>.
153. Weinberg, *supra* note 134 at 2.
154. CACP, "Response," *supra* note 131 at p. 6.
155. CACP, "Response," *supra* note 131 at p. 6.

given that many agencies simply cannot afford these costs.[156]

If Bill C-74 had become law, ISPs would have been required to face the costs associated with implementing new transmission apparatus or software into their networks, as well as with storing and deciphering data, and providing it to law enforcement upon request. This would have had a significant impact on their cost of doing business. For this reason, some members of the Canadian telecommunications industry expressed reservations about the costs of complying with the proposed regulations.[157]

ISPs would have most likely addressed the problem by passing the costs on to their subscribers, through service fees, resulting in an increased cost to consumers for internet use in Canada. While the required costs may have been tolerable for large ISPs, smaller ISPs might have been put out of business and new providers may have been deterred from entering the marketplace altogether. A related concern is that this would significantly harm the telecommunications industry in Canada by impairing the ability of ISPs to compete with those in other jurisdictions that do not impose similar requirements. However, this is no longer likely to be a significant obstacle because many other nations, including the United States, the United Kingdom, Germany, France, Australia, New Zealand and South Africa have now implemented legislation regarding the interception of communications transmitted using new technologies.[158] Moreover, by not implementing lawful access legislation, Parliament risks Canada becoming a "safe-haven" for cyber-criminals from other jurisdictions. Parliament must take immediate steps to ensure that this does not happen.

Given that most other major industrialized nations have already enacted these measures into their domestic law, particularly since they are required by the *Cybercrime Convention*, the question is not whether or not Canada will implement interception capability requirements, but how quickly and on what terms. Canada's largest ISP, Bell Sympatico, recently opened the door for increased ISP interception capabilities through changes to its user agreement, although it emphatically denied that the modifications were related to the lawful access initiative.[159] Bell inserted a new clause into its user agreement, which took effect on June 15, 2006, informing customers that it had the right to "monitor or investigate content on your use of your service provider's networks and to disclose any information necessary to satisfy any laws, regulations or other governmental requests."[160] This change indicates that the ISP is willing to monitor network usage, including monitoring user content and disclose subscriber information to law enforcement.[161] This led to speculation that the change might have been in anticipation of legislative reform, as many have anticipated that the Conservative government will reintroduce lawful access legislation soon.

---

156. CACP, "Response," *supra* note 131 at p. 13.
157. Selma M. Lussenburg, "Security and the Economy: The North American Computer and Communication Infrastructure," (2003) 29 *Can-U.S. Law Journal* 237 at p. 242.
158. Valiquet, *Telecommunications and Lawful Access: II*, *supra* note 121 at p. 10.
159. Michael Geist, "Big Brother Bell," (6 July 2006) *Ottawa Citizen*, <http://www.canada.com/ottawacitizen/news/technology/story.html?id=91478922-9a40-488f-8dda-5a3e41359ed0>.
160. Geist, "Big Brother Bell," *supra* note 159.
161. Geist, "Big Brother Bell," *supra* note 159.

The implementation costs of reasonable interception capability and the impact of the proposed requirements on the competitiveness of the Canadian telecommunications industry remain important issues which will undoubtedly have an impact on how lawful access legislation is structured and implemented. Either ISPs (meaning their users) will have to pay for the costs or they will be imposed upon taxpayers. Parliament could commit to paying the costs by setting aside a substantial sum of money for that purpose, as was done in the United States. One group representing telecommunications service providers and members of the police in Canada recently proposed that a fund could be at least partially generated from the money seized from criminals.[162] Parliament could also make reimbursement for all costs discretionary, as is the case in the United Kingdom. Requiring ISPs to pay the full implementation costs is another option, although this might jeopardize Canada's ability to maintain a competitive and fair communications industry.

Parliament attempted to address the issues of cost and competitiveness by exempting telecommunication service providers with fewer than 100,000 subscribers from the requirements set out in Bill C-74 for a period of three years.[163] The Minister of Public Safety and Emergency Preparedness would also have been entitled to issue an order to suspend the obligation of a service provider to meet the operational requirements of implementing new apparatus or software.[164] The risks associated with this approach are that smaller ISPs, or those otherwise exempt from the requirements, will become havens for cyber-criminals, including child pornography offenders, who know that the networks cannot be intercepted by law enforcement officials.

Perhaps recognizing that placing significant financial impediments upon the Canadian telecommunications industry might not be beneficial, the Bill also provided that in cases where the Minister of Public Safety and Emergency Preparedness issued an order to a telecommunications service provider to comply with requirements to maintain intercept capability, the Minister would have been required to reasonably compensate the carrier for the costs of compliance.[165] This provision appears to provide a mechanism for the government to compel all ISPs to comply with the intercept capability requirements, as well as to ensure that at least some of the costs of implementing this regime would be borne by taxpayers, in a manner similar to CALEA in the United States.

We do not yet know what the financial and other business-related costs of implementing a lawful access regime will be for ISPs. We do know that other states in other jurisdictions, including the United States and the United Kingdom, have implemented legislation requiring their telecommunications service providers to update their networks to enable the interception and preservation of data. This suggests that the financial costs are not so significant that they make the implementation of this regime impossible. The lawful access regimes implemented in other jurisdictions can also serve as useful models for determining the best approach to take in Canada on these issues.

---

162. Valiquet, *Telecommunications and Lawful Access: II*, *supra* note 121 at p. 8.
163. MITA, *supra* note 119 at s. 12.
164. MITA, *supra* note 119 at s. 14.
165. MITA, *supra* note 119 at s. 15.

5.2. Requirement to Provide Subscriber Information

Currently, there is no mechanism by which law enforcement officials can compel ISPs to provide subscriber information, such as the name, address, telephone number, email, and IP address of an individual, without a warrant.[166] As with the interception of ISP networks, the CACP recently reported that the practices of ISPs with respect to the collection and disclosure of subscriber information are arbitrary and inconsistent.[167] The CACP maintains that subscriber information is critical to tracking criminals; however there are no established standards for collecting and maintaining it. Some ISPs have refused to comply with court orders and provide the requested information to police and in some cases, according to the CACP, "even willing companies cannot decipher their own records."[168]

The CACP further maintains that since there are no legal requirements for anyone who wants to subscribe to telecommunications services to provide accurate identification (or for the telecommunications provider to verify the identities) false information is often used.[169] While not all ISPs collect this information from their customers, every ISP has the contractual right to demand, collect and retain a wide range of personal information about its customers as a condition of service. This places ISPs in an ideal position to assist law enforcement agents with identifying the real-world identity and location of cyber-criminals. ISPs must be required by law to collect, verify and retain subscriber information from their customers as a condition of service.

With respect to the collection and disclosure of personal information by ISPs, two important concerns arise. The first is whether an ISP can *collect* private information about an individual and disclose it to law enforcement without the individual's knowledge or consent. As I discuss below, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to federal works and undertakings, which include ISPs. It permits the collection and disclosure of personal information without the knowledge and consent of an individual in certain circumstances, which includes for the purpose of making a disclosure that is required by law or in administering any law of Canada or a province.[170] Of course, an ISP would not need to collect information about its subscribers without their knowledge and consent. It could simply inform them up-front, as a condition of service, that this information will be collected, verified, retained, and disclosed to law enforcement, as required by law.

The second concern arises with respect to whether the ISP can *disclose* subscriber information to police without a warrant. Bill C-74 would have allowed the police and members of CSIS to obtain subscriber data from ISPs upon request, *without* judicial authorization.[171] In the case of the disclosure of basic subscriber information, such as an individual's name, address, telephone number, and IP address, the Supreme Court of Canada has stated that as the information

166. Valiquet, *Telecommunications and Lawful Access: II*, *supra* note 121 at p. 4.
167. CACP, "Response," *supra* note 131 at p. 2.
168. CACP, "Response," *supra* note 131 at p. 2.
169. CACP, "Response," *supra* note 131 at p. 5 (Appendix A).
170. *Personal Information Protection and Electronic Documents Act*, (2000) *Revised Statutes of Canada* ch.5 <http://laws.justice.gc.ca/en/showtdm/cs/P-8.6> at s. 7 [PIPEDA].
171. MITA, *supra* note 119 at s. 17.

collected by the state nears a certain type of "core" personal and "biographical" information about the individual, the privacy interest becomes more important and the requirement for judicial authorization increases.[172] In *R. v. Plant*,[173] the Supreme Court found that information collected by a public utility company about its customers without a warrant, in the form of computerized records, could be freely shared with police without an infringement of s. 8 of the *Charter*. The records about electricity consumption did not disclose "intimate details of lifestyle and personal choices of the individual" and revealed little about "the personal lifestyle or private decisions of the occupants."[174]

An important concern is whether subscriber information has a significant privacy element that goes to the core of personal information that the individual would not wish to disclose. In the case of *R. v. Plant*, the Court was asked only to consider computerized records about electricity consumption, not information about an individual's address and phone number, which might be said to relate to more directly to the "lifestyle and personal choices" of the individual.[175] Conversely, subscriber information includes only basic personal information about an individual, such as that which is published in a telephone book. These important issues would need to be considered by Parliament in drafting measures to compel ISPs to collect, verify, retain, and disclose subscriber information.

However, a recent case indicates that Bell is already fulfilling its promise to disclose customer information necessary to satisfy law enforcement requests. This case also stands for the proposition that a subscriber does not have a reasonable expectation of privacy in his or her name and address information when the service agreement entered into between the ISP and the user contemplates that this information can be shared with the police. In *R. v. Ward*,[176] the accused was charged with accessing and possessing child pornography, contrary to section 163.1 of the *Code*. The investigation of the accused began when German authorities transmitted information to the Canadian police that three numeric "Internet Protocol" (IP) addresses, which were later determined to be assigned to the ISP Bell Sympatico, had been used to access and download child pornography from a German website. A constable with the Royal Canadian Mounted Police contacted Bell and requested the information to identify the subscriber account associated with the three IP addresses. Bell complied and provided Mr. Ward's name and home address as the subscriber associated with each of the three IP addresses at the time the child pornography images were accessed and downloaded.

Mr. Ward argued at trial that the subscriber information (his name and address) obtained from Bell Sympatico was information in respect of which he had a reasonable expectation of privacy and that nothing gave police the authority to access the information in the absence of judicial authority. However,

172. *R v Plant*, <http://scc.lexum.umontreal.ca/en/1993/1993rcs3-281/1993rcs3-281.html>, 1993:3 *Supreme Court Reports* 281 [*Plant*].
173. *Plant*, *supra* note 172.
174. *Plant*, *supra* note 172.
175. Parliament briefly referred to this decision at p. 12 of its *Lawful Access Consultation Document*, *supra* note 13, maintaining that basic customer information "such as name, billing address, phone number and name of service provider," would not attract a "reasonable expectation of privacy" because it does not reveal intimate details of the individual's lifestyle and personal choices.
176. *R v Ward*, 2008 ONCJ 355, <http://www.canlii.org/en/on/oncj/doc/2008/2008oncj355/2008oncj355.html>.

the court stressed that the service agreement, code of practice and privacy statement contemplated that personal information could, in certain circumstances, be shared with police. Given the fact that the information was in the hands of a third party (the ISP) and considering the contract that he had entered into with Bell Sympatico, Mr. Ward did not have a reasonable expectation of privacy in his name and address. This information could be freely shared with the police without a warrant, in accordance with PIPEDA. This case indicates that the provision of subscriber information by ISPs is consistent with Canada's existing privacy legislation and the *Charter*, even when it is provided to law enforcement upon request without a warrant, provided that the ISP has notified the customer about the potential for this kind of information sharing up front.

There are good reasons why police might require subscriber information without a warrant in online child pornography cases. They might need it urgently in order to prevent a crime from occurring, such as a luring offence which can lead to the kidnapping or rape of a child. In these rare cases, law enforcement officials may not have time to obtain a court order for the information before the crime is committed. Access might also be needed when police cannot get a warrant given the little information available to them. This is particularly critical with respect to the investigation of online offences where extraordinary measures might be required to reveal the true identity and location of a suspect who is hiding behind an anonymous or fictional online persona.

These concerns were recently raised by law enforcement representatives on the Canadian Coalition Against Internet Child Exploitation (CCAICE), a multi-sector group of industry, government, non-government, and law enforcement stakeholders from across Canada.[177] These law enforcement representatives said that their first priority was to receive more timely access to ISP customer name and address information in order to quickly identify internet users who are the subject of criminal investigations involving online child exploitation.[178] It has been common ISP industry practice to disclose this information to law enforcement only when served with a judicial warrant; however, law enforcement officials stressed that obtaining a warrant for this purpose can be extremely time-consuming and the resulting delays could place a child at further risk.[179]

Notwithstanding these concerns, there must still be a check on the abuse of this power. There are a number of safeguards that can be implemented to protect the privacy rights of individual subscribers. If Parliament were to enact measures enabling police to access subscriber information without a warrant, it would need to ensure that the following conditions are met: the law enforcement agent requesting the information must be acting pursuant to a lawful authority; the law enforcement agent must be gathering information for the purpose of a specific, ongoing investigation relating to the enforcement of a law of Canada or a province or foreign jurisdiction; and the law enforcement agent requesting the information must require the information to obtain a warrant, which is required

177. See Cybertip.ca, *supra* note 37, at "Press Releases," <http://www.cybertip.ca/app/en/press_details>.
178. See Cybertip.ca, "Press Releases," *supra* note 177.
179. See Cybertip.ca, "Press Releases," *supra* note 177.

to obtain information relating to the subscriber.[180] Other safeguards that can be implemented by Parliament include criminal penalties for any unauthorized use or disclosure of the information under the ISP's control, the requirement for police to obtain a warrant or production order to obtain further information from the ISP, and the application of existing privacy legislation to the disclosure of subscriber information by ISPs.

5.3. Orders for the Preservation of Data

Not all ISPs are in the habit of collecting and storing data that passes through their networks. This means that information that could be valuable to the investigation of a suspect for a computer-related crime, such as online child pornography, can easily be destroyed or modified before it can be obtained and used for law enforcement purposes. Currently, under section 164.1 of the *Criminal Code*, if a judge is satisfied by "information on oath" that child pornography is stored on or made available through a computer, he or she can order the "custodian" of the system, such as an ISP, to give an electronic copy of it to the court; provide the information necessary to identify and locate the poster of the material; and ensure that the material is no longer stored, or made available, through the computer.[181] The judge can also order the custodian of the system to delete the child pornography,[182] and in cases where the court has an electronic copy of the material, the judge can order that it be deleted by the court.[183] However, this order will be rendered ineffective if the ISP does not retain the child pornography images being sought.

The CACP maintains that large-scale international child pornography investigations have been frustrated by the failure of Canadian ISPs to retain data. For instance, in 2002, the German Federal Police received hard-core child pornography images from a suspect who was using one of the largest ISPs in Canada.[184] Through Interpol, the Canadian police were informed and they requested the assistance of the ISP.[185] The ISP told the local police that it could not search for records that were over thirty days old and since the records had not been retained, the investigation reached a dead end.[186]

In light of these concerns, Parliament needs to enact legislation allowing for preservation orders to be made. This valuable procedural instrument is provided for in the *Cybercrime Convention* but it does not currently exist in Canadian law.[187] It was also proposed by Parliament in its *Lawful Access*

180. These requirements are consistent with an order made by the CRTC on 20 March 2001 (Order 2001-279) in which it found that the name of a telephone subscriber's local service provider identification does not reveal intimate details of the lifestyle or personal choices of the subscriber. See Canadian Radio-television and Telecommunications Commission (CRTC), "Provision of subscribers' telecommunications service provider identification information to law enforcement agencies" (20 March 2001), <http://www.crtc.gc.ca/eng/archive/2001/O2001-279.htm >.
181. *Criminal Code*, *supra* note 6 at s. 164.1.
182. *Criminal Code*, *supra* note 6 at s. 164.1(5).
183. *Criminal Code*, *supra* note 6 at s. 164.1(6).
184. CACP, "Response," *supra* note 131 at Appendix 8.
185. CACP, "Response," *supra* note 131 at Appendix 8.
186. CACP, "Response," *supra* note 131 at Appendix 8.
187. As mentioned above, Parliament must enact these measures into law, along with those relating to the production of data, before it can ratify the *Cybercrime Convention*. See the *Lawful Access Consultation Document*, *supra* note 13 at p. 13.

Consultation Document but not included in Bill C-74. Preservation orders can be used to permit the immediate and temporary safeguarding of volatile evidence that is specific to a particular internet transaction or subscriber. The order is temporary, only requiring an ISP to not delete or destroy the existing data of an individual who is the subject of an investigation until law enforcement officials can obtain a judicial warrant to seize it.[188]

The preservation order is not actually an "order" issued by a judge but merely a request made by law enforcement agents to an ISP to locate and preserve specific information for a limited time period. The CACP recommends that law enforcement officials be given the authority to issue data preservation requests to ISPs on a short-term basis, such as a certain number of days.[189] In order to extend the preservation period, police must be required to obtain prior court approval. Additional safeguards can be put in place to require a law enforcement officer to give written notice to the service provider demonstrating that the information is necessary for an ongoing investigation and linking the request to a specific individual, service account, IP address, or other defined criteria. Judicial authorization must also be required for law enforcement agents to seize the information from the ISP, as discussed below. There should be a financial penalty imposed upon the ISP if it refuses to comply with the request. There must also be a process for the service provider to challenge the request in a court of law. In this way, a judge can decide whether to enforce the penalty against the ISP and order it to disclose the requested information, or not.

The United States recently adopted a data preservation scheme to minimize the risk of the deletion of information that may be necessary for the investigation of a crime.[190] Under that regime, a law enforcement agent issues a written request to the ISP to preserve identified records or communications related to a particular person. The ISP then preserves the information for up to ninety days, until the law enforcement official obtains the lawful authority to gain access to the communications.[191] Using this model, Parliament could enact similar provisions into Canadian law. However, the request might only be made for a short-term period, such as a few days or hours, with the additional requirement that law enforcement officials obtain judicial authorization to compel the ISP to preserve the data for a longer time period.

These measures will help Parliament to work with other states, according to the provisions contained in the *Cybercrime Convention*, whereby law enforcement agents can request those in another jurisdiction to preserve data until it can be lawfully produced. For example, law enforcement officials in country A might ask Canadian law enforcement agents to issue a request to a Canadian ISP to preserve data relevant to the investigation of a particular suspect in their country. Canadian law enforcement officials might then issue a preservation order to the ISP requesting that the information be located and preserved. Canadian law enforcement officials could then obtain a production order from a judge in Canada to compel the ISP to produce the information, as

188. *Lawful Access Consultation Document*, *supra* note 13 at p. 13.
189. CACP, "Response," *supra* note 131 at p. 9.
190. United States Department of Justice, 18 *United States Code* s. 2703 (f) <http://www.usdoj.gov/criminal/cybercrime/usc2703.htm>.
191. U.S.C. s. 2703, *supra* note 190.

discussed below. Once the information has been produced, pursuant to a valid search warrant, it could be analyzed by Canadian law enforcement officials and provided to country A.

It is noteworthy that the term "data preservation" refers only to orders for the retention of some data about a particular individual who is the subject of an investigation.[192] This is different from the term "data retention" which has been used to mean general retention by ISPs of all their data with respect to all customers, not just those under suspicion of criminal conduct.[193] The European Union recently approved a data retention directive that will apply to its member states which requires providers of electronic communications, or telecommunications networks, to retain data for periods "of not less than six months and not more than two years from the date of the communication."[194] Only "traffic" and "location" data is to be retained, which can identify the sender, or the time and duration of the communication.[195] The directive is not concerned with the content of the communication, such as the text of an email.[196] In other words, content is not to be retained. The type of information to be retained by Canadian ISPs, when served with a preservation order, can also be limited to "traffic data," which would reduce the risk of sensitive information from being disclosed.[197] This information can be useful in linking a child pornography suspect to a child pornography website, or a child pornography ring; to an online request for child pornography images; or to the downloading of child pornography onto a computer, particularly in cases where the images have been deleted or otherwise erased.

Although it does not apply to the retention of content data, the European Union data retention directive is excessively broad. ISPs in the EU member states are required to retain data pertaining to *all of their users*, regardless of whether they are under suspicion for illegal conduct or not. However, the data retained will only be made available to national authorities in specific cases and in accordance with national law.[198] The data preservation initiatives that I propose are far less intrusive, and likely to be significantly less costly, as they only permit law enforcement officials to request ISPs to preserve records relating to *a particular individual*, for a specified time period, until they can obtain a judicial order to seize it.[199]

---

192. *Lawful Access Consultation Document*, *supra* note 13 at p. 14.
193. *Lawful Access Consultation Document*, *supra* note 13 at p. 14.
194. The European Parliament, 2005/0182 (COD), Directive of the European Parliament and of the Council on the Retention of Data, (3 February 2006) at art. 6, <http://www.ispai.ie/drfinal.pdf.> [EU Data Retention Directive].
195. EU Data Retention Directive, *supra* note 194 at art. 6.
196. EU Data Retention Directive, *supra* note 194 at art. 6.
197. This was what the government proposed in its *Lawful Access Consultation Document*. See *Lawful Access Consultation Document*, *supra* note 13.
198. EU Data Retention Directive, *supra* note 194 at art. 4. See also Out-Law.com, "Data Retention Receives Rubber Stamp," *The Register*, (24 February 2006), <http://www.theregister.co.uk/2006/02/24/data_retention_directive_ratified/>.
199. Valiquet, *Telecommunications and Lawful Access: I*, *supra* note 130 at pp. 9–10. In May 2005, the Office of the Privacy Commissioner of Canada reported that Canadians send more than 2.7 million text messages per day. This figure demonstrates that ISPs would need to retain an extremely large volume of data if they were to adopt the broad-based data retention initiatives implemented in the European Union. Given the cost and technical difficulties associated with collecting and storing such a large volume of data, this measure is not recommended.

It is noteworthy that the new rules on data retention implemented in Europe were designed to help EU member states form a united front in the fight against terrorism and organized crime. On July 13, the Council of Europe reaffirmed, in its declaration condemning the terrorist attacks against London, the need to adopt common policies toward data retention as soon as possible.[200] Earlier I discussed that Canada has taken significant steps toward the combating of terrorism and organized crime through the establishment of an independent agency (FINTRAC) to handle complaints, as well as a comprehensive regime mandating the reporting of suspicious transactions, as well as large cash transactions, by third parties, including financial services institutions. Yet Canada has failed to implement an effective, coordinated data retention and reporting scheme, involving users and ISPs, which could be enormously beneficial at combating a wide range of pressing legal concerns, including online child pornography, terrorism and organized crime. It is time that Canada establishes an agency which is similar to FINTRAC, in conjunction with the implementation of lawful access provisions, to target these crimes in the most effective way possible, similar to that which has already been implemented in the United States and Europe.

5.4. Orders for the Production of Data

A production order, which is a type of judicial order that is similar to a search warrant, can be issued by a judge to require an ISP to make data available to investigators within a specified time period.[201] There are a number of circumstances in which law enforcement officials obtain judicial search warrants against third parties but do not actually conduct the searches. The reason is that the third party is the custodian of the information and is often in a much better position to produce it, such as the way a corporation or bank is able to produce financial information in a money laundering or terrorism financing case. Allowing the third party to conduct the search is less intrusive and more efficient because there is no entry into the premises or search by law enforcement agents of the premises controlled by the third party. This can also be useful in situations where the documents are held outside Canada in another jurisdiction. ISPs can be viewed, like financial institutions, as maintaining exclusive control over the essential evidence, including information about where to locate an otherwise anonymous individual in the real world, as well as the data connecting the offender to the crime.

The relevant provisions governing the use of production orders are set out in sections 487.012 through 487.017 of the *Criminal Code*. In order to give law enforcement agents better procedural powers to deal with emerging technologies, Parliament could amend the *Criminal Code* to include express language specifying which data an ISP can be required to make available to investigators within a specified time period. More specific definitions would lessen the risk of capturing personal information, such as PIN numbers and passwords, or health and financial information.

---

200. EU Data Retention Directive, *supra* note 194 at art. 4.
201. Valiquet, *Telecommunications and Lawful Access I*, *supra* note 130 at pp. 9–10.

Production orders can be subject to the same legal requirements already set out in section 487.012(3) of the *Criminal Code*. That section provides that production orders can be issued against third parties who are not under investigation for any offence if a judge is satisfied that there are "reasonable grounds to *believe* that an offence [...] has been or is suspected to have been committed."[202] A specific production order for financial or commercial information, such as bank account information, can also be issued under section 487.013 on the lower threshold of "reasonable grounds to *suspect* that an offence […] has been or will be committed,"[203] as discussed earlier with respect to money laundering and terrorism financing. Parliament will need to decide which threshold is the most appropriate for the issuance of production orders for digital information.

As previously discussed, the *Criminal Code* contains a number of other provisions that allow for the collection, retention and disclosure of personal information by third parties, such as financial institutions, in cases where this information could provide valuable assistance to law enforcement in the investigation of serious crimes including money laundering and terrorism financing. For instance, section 83.11 of the *Criminal Code* places an obligation on financial institutions to monitor the property they maintain on behalf of their clients, keep records of their activities, and regularly report their findings to a regulatory body.[204] A judge of the Federal Court can authorize the seizure or forfeiture of the property maintained by the institution, if there are "reasonable grounds to believe" that the property is maintained by a terrorist group or being used to facilitate or support terrorist activity.

The logic behind these measures is that financial institutions are the sole gatekeepers of this information, which is essential to prevent serious crimes from being committed and to investigate and prosecute offenders when they do occur. A similar approach should be taken with respect to the investigation of serious computer-related offences, including online child pornography, where essential evidence is held in the exclusive domain of private third parties. ISPs can be viewed, like financial institutions, as maintaining exclusive control over the essential evidence, including information about where to locate an otherwise anonymous individual in the real world, as well as the data connecting the offender to the crime.

*

6. THE PRIVACY AND *CHARTER* IMPLICATIONS OF LAWFUL ACCESS

IT IS IMPORTANT TO ENSURE THAT LAWFUL ACCESS measures are implemented in a way that protects the right of Canadians to have their privacy respected and their personal information not subject to abuse or mistreatment. The legislation must also be consistent with the rights contained in the *Charter*, as well as other privacy guarantees. In this sense, the *Charter* and PIPEDA will be essential in determining the feasibility of any lawful access initiative.

202. *Criminal Code*, *supra* note 6 at s. 487.012 (emphasis added).
203. *Criminal Code*, *supra* note 6 at s. 487.013 (emphasis added).
204. *Criminal Code*, *supra* note 6 at s. 83.11.

6.1. The Charter of Rights and Freedoms

Freedom of expression is one of the most fundamental rights possessed by Canadians who prize a diversity of ideas and opinions for their inherent value both to the community and to the individual. We recognize that it is crucial to enable people to express a wide range of conflicting and divergent ideas in order to maintain our free, pluralistic and democratic society.[205] This means that we protect not only "good" and popular expression but unpopular and even offensive speech.[206] The freedom to express ourselves, no matter how unpopular or offensive our thoughts and beliefs might be, is critical to ensuring the full participation of individuals and groups in our society.[207] This was recognized by Canadian courts even before the enactment of the *Charter*.

Our commitment to freedom of expression has historically been rooted in the following values and convictions: that seeking and attaining truth is an inherently good activity; that participation in social and political decision-making is to be fostered and encouraged; and that diversity in forms of individual self-fulfillment and human flourishing ought to be cultivated in a tolerant environment for the sake of both those who convey a meaning and those to whom meaning is conveyed.[208] All of these values are critical to the maintenance of a free and democratic society, which requires the open exchange of ideas and viewpoints. Section 2(b) of the *Charter* guarantees everyone the "fundamental freedoms" of thought, belief, opinion and expression, including freedom of the press and other media of communication.[209] Section 52 of the *Constitution* provides that the *Charter* is part of the supreme law of Canada and any law that is inconsistent with it is of no force or effect, with respect to the inconsistency.[210] Yet our freedom of expression is not absolute, and Parliament or a provincial legislature may limit expression to prevent harm to vulnerable members of our society. Because of the importance of the guarantee of free expression, any attempt to restrict that right must be carefully scrutinized.[211]

The Supreme Court of Canada has developed a test to determine whether the freedom of expression guarantee has been infringed. The first step is to determine whether the activity can be characterized as falling within "freedom of expression" because if the activity is not protected by section 2(b), the government action cannot be challenged under that section.[212] The Supreme Court of Canada has interpreted the section 2(b) guarantee of freedom of expression broadly to mean that if the activity conveys or attempts to convey a meaning, it has expressive content and *prima facie* falls within the scope of the guarantee.[213] The exception to this general definition is that section 2(b) does not protect activity which conveys

205. *R v Sharpe*, 2001 SCC 2 <http://scc.lexum.umontreal.ca/en/2001/2001scc2/2001scc2.html>, 2001:1 *Supreme Court Reports* 45 at paras. 21–23 [*Sharpe (SCC)*].
206. *Sharpe (SCC)*, *supra* note 205 at para. 21.
207. *Sharpe (SCC)*, *supra* note 205.
208. *Irwin Toy v Quebec (Attorney General)*, <http://csc.lexum.umontreal.ca/en/1989/1989rcs1-927/1989rcs1-927.html> >, 1989:1 *Supreme Court Reports* 927 at p. 53 [*Irwin Toy*, cited to S.C.R.].
209. *Charter*, *supra* note 14 at s. 2(b).
210. *Constitution Act, 1982*, <http://laws.justice.gc.ca/en/const/annex_e.html>, s. 52 [*Constitution Act, 1982*].
211. *Sharpe (SCC)*, *supra* note 205 at para. 22.
212. *Irwin Toy, supra* note 208 at p. 45.
213. *Irwin Toy, supra* note 208 at p. 46.

a meaning in a violent form.[214] If the activity in question falls within the protected sphere of conduct, meaning that it conveys or attempts to convey a meaning in a non-violent form, the next step is to determine whether the purpose or effect of the government action is to restrict freedom of expression.

Child pornography does not generally contribute to the values that underlie freedom of expression, including the search for truth, self-fulfillment and the contribution to social and political discourse.[215] However, unlike in other jurisdictions, such as the United States, where it has been found that child pornography is not protected speech,[216] in Canada it is constitutionally protected and the burden lies with the Crown to justify an infringement.[217] The idea behind this requirement is that without the right to possess expressive materials, including those which are offensive to the majority, our freedom of thought, belief and opinion, as well as our liberty, would be severely impaired. Thus, while the offensive nature of child pornography might limit its constitutional worth, it does not negate it altogether.[218] Similar findings have been reached by the Supreme Court of Canada with respect to other forms of offensive speech including obscenity,[219] hate propaganda,[220] and defamatory statements.[221]

This does not mean that child pornography cannot be proscribed under certain circumstances. In fact, the more distant the expression is from the core values underlying the section 2(b) guarantee, the more likely it is that the governmental restriction can be justified.[222] One of the most important rationales, or objectives, for criminalizing child pornography is that children are a highly vulnerable group in our society who are in need of protection from physical and emotional abuse by adults. If child pornography causes harm to children, this provides a strong justification for prohibiting, or at least severely restricting, its production and dissemination.

If an individual alleges that his or her section 2(b) right has been infringed, the onus falls on the government to justify the intrusion by demonstrating on a balance of probabilities that the infringement is constitutionally justified and can be "saved" by section 1 of the *Charter*. This section provides that the rights and freedoms protected by the *Charter* are not absolute and may be subject to "such reasonable limits proscribed by law as can be demonstrably justified in a free and democratic society."[223] "The onus of proving that a limit on a right or freedom guaranteed by the *Charter* is reasonable and justified in a free and democratic society rests upon the party seeking to uphold the limitation."[224]

---

214. *Sharpe (SCC)*, *supra* note 205 at para. 147.
215. *Sharpe (SCC)*, *supra* note 205 at para. 24.
216. *New York v Ferber* (USA, Sup. Ct. 1982), <http://www.law.cornell.edu/supct/html/historics/USSC_CR_0458_0747_ZO.html >, 458 *United States Reports* 747.
217. *R v Sharpe*, 1999 BCCA 416, <http://www.courts.gov.bc.ca/jdb-txt/ca/99/04/c99-0416.html>, 69 *British Columbia Law Reports (3d)* 234, at paras. 149–153 [*Sharpe (BCCA)*].
218. *Sharpe (SCC)*, *supra* note 205 at para. 27.
219. *R v Butler*, <http://scc.lexum.umontreal.ca/en/1992/1992rcs1-452/1992rcs1-452.html>, 1992:1 *Supreme Court Reports* 452.
220. *R v Keegstra*, <http://scc.lexum.umontreal.ca/en/1990/1990rcs3-697/1990rcs3-697.html>, 1990:3 *Supreme Court Reports* 697.
221. *Hill v Church of Scientology of Toronto*, <http://scc.lexum.umontreal.ca/en/1995/1995rcs2-1130/1995rcs2-1130.html>, 1995:2 *Supreme Court Reports* 1130.
222. *Sharpe (SCC)*, *supra* note 205 at para. 181.
223. *Charter*, *supra* note 14 at s. 1.
224. *R v Oakes*, <http://scc.lexum.umontreal.ca/en/1986/1986rcs1-103/1986rcs1-103.html>, 1986:1 *Supreme Court Reports* 103 at para. 66. [*Oakes*].

In *R. v. Oakes*, the Supreme Court of Canada set out the analytical framework for determining whether the violation of a *Charter* right can be justified under section 1.

The analysis, which is commonly referred to as the "Oakes Test," provides that a constitutional guarantee can be limited if two conditions are met. First, the objective, which the legislative measures are intended to serve, must be sufficiently important to warrant overriding a constitutionally protected right or freedom.[225] It must relate to "pressing and substantial" concerns in a free and democratic society before it can be characterized as sufficiently important.[226] Second, the means chosen to attain this objective must be reasonable and demonstrably justifiable in a free and democratic society. This involves a "proportionality test" in which the courts must balance the interests of society against those of individuals and groups.[227]

There are three important aspects of the proportionality test.[228] First, the measures enacted (giving rise to the *Charter* violation) must be carefully designed to achieve the objective in question. In other words, they must be rationally connected to the objective.[229] Second, the means chosen should impair the right or freedom "as little as possible."[230] Third, there must be proportionality between the effects of the measures, which are responsible for limiting the *Charter* right or freedom, and the objective being sought.[231] "In all section 1 cases the burden of proof [rests with the Crown] to show on a balance of probabilities that the violation is justifiable."[232]

Section 163.1 of the *Criminal Code* already makes it an offence to access or distribute child pornography, through electronic means, or otherwise.[233] Assuming that criminal prohibition against accessing and distributing child pornography online constitutes a reasonable and justified limit upon freedom of expression, the question is whether measures implemented to enable law enforcement officials to conduct surveillance and seize information, which will enable it to better enforce these restrictions, are reasonable and appropriate, particularly given that section 8 of the *Charter* protects the right to be secure against unreasonable search and seizure.

The lawful access measures are aimed at protecting both children and society by attempting to eradicate the sexual exploitation of children, so they clearly have a pressing and substantial purpose. They are designed to serve the objective of targeting those who access and distribute material that poses a reasoned risk of harm to children. The means chosen are rationally connected to this objective because the internet is now the primary way that child pornography is supplied and consumed. Collecting electronic evidence from ISPs is one of the few tools that law enforcement agents have to gather valuable information about

225. *R v Big M Drug Mart Ltd.*, <http://scc.lexum.umontreal.ca/en/1985/1985rcs1-295/1985rcs1-295.html>, 1985:1 *Supreme Court Reports* 295 at para. 139.
226. *Oakes*, *supra* note 224 at para. 69.
227. *Oakes*, *supra* note 224 at para. 70.
228. *Oakes*, *supra* note 224 at para. 71.
229. This means that they must not be arbitrary, unfair or based on irrational considerations. See *Oakes*, *supra* note 224 at para. 70.
230. *Oakes*, *supra* note 224 at para. 70.
231. *Oakes*, *supra* note 224 at para. 70.
232. *Sharpe (BCCA)*, *supra* note 217 at para. 140.
233. *Criminal Code*, *supra* note 6 at s. 163.1.

suspects, which may have probative value in online child pornography cases, as well as to identify and locate child victims.

These law enforcement measures are minimally invasive because they will only be used to investigate serious crimes, such as those relating to a particular suspect's use of the computer to access and disseminate child pornography, which is already prohibited by the *Criminal Code* and lies far from the core of protected speech. A greater threat to freedom of expression is posed by the lawful interception proposals, particularly when one considers that even basic information about the sender of an online communication affects freedom of expression, which is an extremely important constitutional right in Canada. However, these measures will be narrowly tailored to ensure that an individual's freedom of expression rights are impaired no more than reasonably necessary to obtain necessary evidence for use in criminal investigations. The risk of capturing other types of information, such as private communications, personal records or PIN numbers, such as through the interception of communication involving several individuals, will be minimized because these measures will only be used in limited cases, with respect to particular information about specific individuals who are suspected of accessing or distributing illegal materials online.

Parliament must also ensure that the lawful access legislation protects the reasonable privacy interests of Canadians. A central question is whether the legislation infringes section 8 of the *Charter*. It is important to note that the restraints imposed on government to pry into the lives of its citizens are at the heart of the modern democratic state.[234] Early English common law protected an individual's home from unjustified intrusion by the sovereign, which was linked to property rights and the law against trespass.[235] The general protection against government encroachment later evolved into a broader right to be secure against unreasonable search and seizures; yet, it retained recognition for the sanctity and privacy of the home.[236] Nevertheless, the privacy protection in Canada is largely based on individual freedom and moral autonomy, rather than property *per se*, which, in the context of section 8 means that it protects "people, not places,"[237] and it has been recognized as being essential to maintain the state's respect for the dignity and well-being of the individual.[238] This has led to special protection being accorded to individual bodily sanctity and personal information about the lifestyle or intimate personal choices of the individual.

There is no express constitutional right to privacy in the *Charter*; however, section 8 provides that everyone "has the right to be secure against unreasonable search or seizure,"[239] and the Supreme Court of Canada has recognized this provision as protecting an individual's right to be secure against encroachment of a reasonable expectation of privacy in a free and democratic society.[240] Yet, as with other fundamental rights, the right to privacy is not absolute and the guarantee against unreasonable search and seizure only

234. *R v Dyment*, <http://scc.lexum.umontreal.ca/en/1988/1988rcs2-417/1988rcs2-417.html>, 1988:2 *Supreme Court Reports* 417 at para. 17 [*Dyment*].
235. *Hunter v Southam*, <http://scc.lexum.umontreal.ca/en/1984/1984rcs2-145/1984rcs2-145.html>, 1984:2 *Supreme Court Reports* 145 at para. 21 [*Hunter*].
236. *Hunter*, *supra* note 235 at para. 22.
237. *Hunter*, *supra* note 235 at para. 23.
238. *Dyment*, *supra* note 234 at para. 22.
239. *Charter*, *supra* note 14 at s. 8.
240. *Hunter*, *supra* note 235 at para. 24.

protects a "reasonable expectation" of privacy, when balanced against the other societal interests, including law enforcement.[241] This means that privacy rights can sometimes be limited when there is a reasonable and compelling state interest, in accordance with section 1 of the *Charter*.[242] The balance between the need to protect an individual's privacy from unjustified state intrusion and the interest in overriding the right can shift, depending on the nature of the privacy interest at stake.

The Supreme Court of Canada has established that privacy arises in three distinct domains: spatial and territorial; personal; and informational.[243] In the spatial or territorial realm, certain types of social interactions require a greater degree of privacy protection than others, and this requires shielding certain types of social interactions from public scrutiny, such as those which occur within the sanctity of the home. In the personal domain, privacy has been linked with surveillance and the individual's right to maintain control over his or her own bodily movements,[244] as well as bodily sanctity, in the sense that an unlawful search can constitute an affront to human dignity.[245] The last zone of privacy identified by the Court requires respect for personal information. The retention of personal information about oneself has been said to be a fundamental right because it should be left up to the individual to determine under what conditions personal information is disclosed to others.[246]

The protection of individual privacy against state intrusion is particularly important with respect to the state's power to monitor communications and conduct electronic surveillance, which concerns all three zones of privacy. The Supreme Court of Canada has stressed the need for even greater privacy protections to be accorded to the individual in light of new technological developments which enable more extensive encroachments on our personal privacy and fundamental liberties. Parliament now has many methods at its disposal by which it can collect information about us and conduct surveillance in previously unforeseen ways, including the sharing and cross-referencing of electronic records (medical, taxation, financial and business data about individuals), video, camera and satellite surveillance, as well as a range of electronic monitoring and interception techniques, including wiretapping.[247] Thus, the Court has stressed its need to carefully scrutinize the state's use of new technologies and has required compliance with the requirements for a "reasonable" search or seizure under section 8, including the need to obtain judicial authorization, such as a valid search warrant.

---

241. *Hunter*, *supra* note 235.
242. *Oakes*, *supra* note 224.
243. *Dyment, supra* note 234 at para. 19.
244. *R v Wong*, <http://scc.lexum.umontreal.ca/en/1990/1990rcs3-36/1990rcs3-36.html>, 1990:3 *Supreme Court Reports* 36 [*Wong*]. See also *Dagg v Canada (Minister of Finance)*, <http://scc.lexum.umontreal.ca/en/1997/1997rcs2-403/1997rcs2-403.html>, 1997:2 *Supreme Court Reports* 403, where the Court found that government employees have a reasonable expectation that workplace sign-in logs that reveal information about their movements and location at work should not generally be made available to the public.
245. This sense of privacy transcends the physical and provides protection against the indignity of a search, and its invasion of the person, in a moral sense (*Dyment*, *supra* note 234 at para. 21).
246. *Dyment, supra* note 234 at para. 22.
247. Such as through hidden video surveillance (See *Wong*, *supra* note 244) and the use of a thermal heat imaging device to take "heat" pictures of an individual's home from overhead aircraft (See *R v Tessling*, 2004 SCC 67, <http://scc.lexum.umontreal.ca/en/2004/2004scc67/2004scc67.html>, 2004:3 *Supreme Court Reports* 432.

The Court's insistence on legal authority for searches and seizures involving new surveillance technologies is consistent with its goal of preventing unjustified searches before they happen. In the words of Dickson J, in *Hunter v. Southam*, "this can only be accomplished by a system of prior authorization, not one of subsequent validation."[248] This approach has been consistently maintained by the Court and is reflected in many of the surveillance technology decisions dealing with the requirements for a reasonable search and seizure under section 8. Generally speaking, these cases stand for the proposition that unauthorized surreptitious electronic surveillance will violate section 8 where the target of the surveillance has a reasonable expectation of privacy.

In *R. v. Wong*, the Court found that unauthorized video surveillance of a hotel room offended the reasonable expectations of privacy of the occupants of the room and violated section 8.[249] The Court also refused to find authority for the issuance of surreptitious video surveillance warrants under the electronic surveillance provisions then contained in the *Criminal Code*. At that time, there was no legislation specifically authorizing video surveillance and Justice LaForest declined to "fill the lacunae" and read such authority into the *Criminal Code*, observing that the "common law powers of search were extremely narrow, and that the courts have left it to Parliament to extend them where need be."[250] In *R. v. Duarte*, the Court found that the recording of a private communication, without the consent of all parties, can only be reasonable where prior judicial authorization has been obtained.[251] Justice LaForest cautioned that:

> …the very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposes us, at the whim of the state, to the risk of having a permanent electronic recording made of our words, every time we opened our mouths might be superbly equipped to fight crime but would be one in which privacy no longer had any meaning.[252]

These cases suggest that there is a strong connection between electronic surveillance and the infringement of one's reasonable expectation of privacy. The Supreme Court of Canada has emphasized the need to restrict the government's ability to use sophisticated technologies to intercept private communications, stressing the requirement for prior judicial authorization and cautioning that the unfettered use of this power will greatly infringe or deny the fundamental rights and freedoms guaranteed in section 8. Parliament will need to be careful to ensure that the data interception, preservation, and production requirements are as minimally intrusive as possible so as to not impair the privacy rights of Canadians beyond that which is reasonably necessary to achieve the objective of collecting information that is necessary for the purposes of law enforcement investigations.

---

248. *Hunter*, *supra* note 235 at para. 27.
249. *Wong*, *supra* note 244.
250. *Wong*, *supra* note 244 at p. 23. Note that Parliament subsequently responded by amending the *Criminal Code* to enable video surveillance.
251. *R v Duarte*, <http://scc.lexum.umontreal.ca/en/1990/1990rcs1-30/1990rcs1-30.html>, 1990:1 *Supreme Court Reports* 30 [*Duarte*].
252. *Duarte*, *supra* note 251 at p. 18.

With respect to the requirement imposed upon ISPs to ensure that they possess the technical capabilities to enable law enforcement officials to intercept their networks, it cannot be unconstitutional for Parliament to require that ISPs implement the necessary technological upgrades because Canadian police already have the power to conduct electronic surveillance pursuant to a well-established and rigorous legal framework in Part Six of the *Criminal Code*.[253] Since digital interceptions constitute a search or seizure, the statutory provisions authorizing them must conform to the minimum constitutional requirements required by section 8 of the *Charter*. Network data must only be intercepted by law enforcement officials, with prior judicial authorization, as is now required for the interception of other forms of communication. This will significantly lessen the risk of violating privacy guarantees under section 8 of the *Charter*.

In order to further protect the privacy rights of Canadians, ISPs must be required to put in place mechanisms and procedures that enable police to focus only on those individuals and that information to which the judicial authorization applies. In this way, interception will only be used in limited cases, with respect to particular information about specific individuals who are suspected of illegal online conduct. The risk of capturing other types of information, such as private communications, personal records or PIN numbers, such as through the interception of communication involving several individuals, will be minimized, thus safeguarding existing *Charter* rights and guarantees under sections 8 and 2(b) of the *Charter*. ISPs must also be required to ensure the privacy and security of the content of the data intercepted as well as the identities of the persons involved. If the search is found to be unreasonable under section 8, the evidence can be excluded under section 24(2) of the *Charter*.[254]

With respect to the disclosure of subscriber information by ISPs, the section 8 analysis turns on whether the information will be provided to law enforcement with or without a warrant. An important concern is whether subscriber information has a significant privacy element that goes to the core of personal information that the individual would not wish to disclose. As I discussed earlier, in the *Ward* case, the court found that as long as the ISP enters into a service agreement with the user about disclosing the information for law enforcement purposes, name and address information will not be considered "core personal information" that must be protected from disclosure without a warrant.

Turning to preservation orders, which I propose should be issued without a warrant, it is important to stress that this is merely a temporary measure in order to secure valuable information that would otherwise be deleted or destroyed by an ISP. Collecting electronic evidence from ISPs is one of the few tools that law

253. Pursuant to sections 185 and 186 (or section 487.01) of the *Criminal Code*, as discussed above. See *Criminal Code*, *supra* note 6 at ss. 185 and 186.

254. See *Charter*, *supra* note 14 at s. 24.

> 24 (1) Anyone whose rights or freedoms, as guaranteed by this Charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances.
>
> (2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

enforcement agents have to gather valuable information about suspects, which may have probative value in online child pornography cases, as well as to identify and locate child victims. Orders for the preservation of data will only be issued for a very short time period and they will only relate to specific information about a particular individual who is the subject of a law enforcement investigation, which will lessen the risk that they will contravene sections 2(b) and 8 of the *Charter*.

With respect to the constitutionality of permitting law enforcement officials to request an ISP to locate and preserve data for them, it is important to keep in mind that the actions of private parties, such as ISPs, are not generally implicated by the *Charter*. However, if ISPs are required by Parliament to play a significant role in data surveillance and search and seizure, the distinction between their role as private or public actors may become blurred and they may be characterized as "agents of the state."[255] This issue has been dealt with in only one Canadian case to date. In *R. v. Weir,*[256] an ISP discovered attachments to an email message that appeared to contain child pornography while repairing Mr. Weir's electronic mailbox. The ISP opened the attachments and found that they contained child pornography. It informed the police of its findings and, upon request, forwarded a copy of the message to the police. The ISP also provided the police with Mr. Weir's billing address. Mr. Weir argued that the ISP was acting as an agent of the state, and that the opening of the message and the forwarding of the message to the police were both warrantless searches.

The Alberta Court of Appeal held that the ISP was acting as an agent of the state when it forwarded a copy of the message to the police at the request of the police officer.[257] The Court was careful to distinguish between the ISP's role as an "agent of the state" before and after its contact with the police. The trial judge relied on *R. v. Broyles*[258] in finding that the ISP was not an agent of the state prior to its contact with the police. *Broyles* concerned the relationship between an informer and the Crown and the test set out by the Supreme Court was said to be applicable to this case: "[. . .] would the exchange between the accused and the informer have taken place, in the form and manner in which it did take place, but for the intervention of the state or its agents?"[259]

The Court of Appeal agreed with the trial judge and held that the ISP was not acting as an agent of the state before its contact with the police, when it was simply performing a routine repair of Mr. Weir's electronic mailbox.[260] However, the Court classified the forwarding of the email, upon the request of the police officer, as a "warrantless search" which is presumed unreasonable and in violation of section 8.[261] This case establishes that if a third party is collecting data for law enforcement purposes, or carrying out some other type of surveillance function, the provisions guarding against unreasonable search and seizure may be engaged and the need for a valid search warrant may arise. This

255. Valiquet, *Telecommunications and Lawful Access I*, *supra* note 130 at p. 13.
256. *R v Weir* (AB CA, 2001), 281 *Alberta Reports* 333 [*Weir*].
257. *Weir*, *supra* note 256 at para. 11.
258. *R v Broyles*, <http://scc.lexum.umontreal.ca/en/1991/1991rcs3-595/1991rcs3-595.html>, 1991:3 *Supreme Court Reports* 595 [*Broyles*].
259. *Broyles*, *supra* note 258 at pp. 3–4.
260. *Weir, supra* note 256 at para. 9.
261. *Hunter, supra* note 235; See also *R v Collins*, <http://scc.lexum.umontreal.ca/en/1987/1987rcs1-265/1987rcs1-265.html> 1987:1 *Supreme Court Reports* 265 at para. 22 [*Collins*].

will be an important issue for Parliament to consider when drafting legislation implementing the use of preservation orders for digital information. If the ISP is compelled to respond to police requests for the preservation of data, the need for a valid search warrant may be engaged.

It is important to keep in mind that the requirement for an ISP to disclose the data to law enforcement officials would only arise after the issuance of a production order by a judge. In child pornography investigations, the computer, its many components, and computer networks can contain a vast amount of information of various types that may provide valuable evidence of a crime. Police need to ensure that they, or any authorized third parties, are not perceived to be randomly combing through data looking for any information that might be useful. Before a specific production order can be issued, section 487.013(4) requires the justice or judge must be satisfied, on the basis of an *ex parte* application containing information on oath in writing, that there are reasonable grounds to suspect that (a) an offence against the *Criminal Code* or any other Act of Parliament has been or will be committed; (b) the information will assist in the investigation of the offence; and (c) the institution, person or entity that is subject to the order has possession or control of the information.

In order to satisfy these requirements, the application should define the meaning of the term "child pornography" pursuant to section 163.1 of the *Code* and also include general background information about the internet and explanations of the investigative and evidence-gathering techniques to be used by both police and the ISP, including the special relevance of ISPs in electronic evidence gathering, in descriptive, non-technical language.[262] Law enforcement officials must not assume that the justice or judge called upon to review them has knowledge of computer technology, the internet, or technical jargon.[263] Information explaining the nature of the internet, chat rooms, ISPs, email programs, or other detailed information, should be included in the information, in plain and descriptive terms. Descriptive computer search language must also be used in the warrant or judicial order to ensure they relate not only to the search and seizure of specific child pornography files, but also to the network data retained by an ISP in relation to the suspect, as well as the suspect's computer and any components or storage devices.[264] These safeguards will help to ensure that ISPs are not required to act as agents of the state without proper judicial authorization and oversight. They will also ensure that the information is only collected and used for a valid law enforcement purpose and that no more information than is reasonably necessary is disclosed in investigations concerning a particular suspect, such as health care information, banking records and PIN numbers.

6.2. The Personal Information Protection and Electronic Documents Act (PIPEDA)

When establishing a lawful access regime, Parliament must also keep in mind the requirements set out in PIPEDA. This federal legislation establishes rules for the

262. *Hunter*, *supra* note 235. See also *Collins*, *supra* note 261.
263. Susan S. Kreston, "Computer Search and Seizure Issues in Internet Crimes Against Children," (2004) 30 *Rutgers Computer and Technology Law Journal* 327 at 330.
264. *R v Morelli* (SK QB, 2005), 272 *Saskatchewan Reports* 282, <http://www.canlii.org/en/sk/skqb/doc/2005/2005skqb381/2005skqb381.html>, affirmed in *R v Morelli* (SK CA 2008), 310 *Saskatchewan Reports* 165, <http://www.canlii.org/en/sk/skca/doc/2008/2008skca62/2008skca62.html>.

collection, use and disclosure of personal information by private organizations involved in commercial activities.[265] It applies to federal works and undertakings, which include ISPs.[266] PIPEDA is important because the distinction between the "public" and "private" sectors has become progressively blurred. Private sector entities now have more resources and opportunities to collect information about individuals, and public sector organizations often require that data to fulfill their obligations. By drafting privacy legislation targeted specifically at the private sector, Parliament was able to facilitate the exchange of valuable information with private organizations and ensure that the privacy rights of Canadians are protected in both the public and private spheres.[267]

The purpose of PIPEDA is to establish rules for the collection, use, and disclosure of personal information in a manner that recognizes the privacy interests of individuals.[268] Personal information is defined in section 2(1) as "information about an identifiable individual but does not include, name, title, business address or telephone number of an employee of an organization."[269] The definition of "personal information" is very broad and does not refer to the concept of the "biographical core" of information that arises from the *Charter* jurisprudence.

PIPEDA seeks to establish fair information collection and management practices in the private sector, by ensuring that data is responsibly collected from individuals and, then appropriately held, used, or disclosed to a third party. One of the central principles behind PIPEDA is that consent must be obtained before information can be collected from an individual, and then used or disclosed. The "reasonable person" standard is used in that PIPEDA requires private organizations to collect, use, and disclose personal information "for purposes that a reasonable person would consider appropriate in the circumstances,"[270] in compliance with ten broad privacy obligations specified in Schedule 1 of the Act.[271]

However, PIPEDA also permits the collection and disclosure of personal information without the knowledge and consent of an individual in certain circumstances. An organization can collect personal information without the knowledge and consent of an individual under section 7(1)(e)(ii) if the collection is made for the purpose of making a disclosure that is required by law.[272] An organization can disclose personal information, without the knowledge and consent of the individual only if, pursuant to section 7(3)(c)(1), the disclosure is made to a government institution[273] and (iii), the disclosure will be made "for the

265. PIPEDA, *supra* note 170 at ss. 2(1) and 4(1).
266. PIPEDA, *supra* note 170.
267. The passage of PIPEDA marked a significant milestone in the development of Canadian privacy law because previous laws regulated only the public sector.
268. PIPEDA, *supra* note 170 at s. 3.
269. PIPEDA, *supra* note 170 at s. 2(1).
270. PIPEDA, *supra* note 170 at s. 3.
271. See PIPEDA, *supra* note 170 at sched. 1. These include the following: collection limitation (the parties should limit how information is collected; collection must be with consent and knowledge that the information is being collected); data quality (the data must be accurate and relevant); purpose specification (the party must specify the purpose for which the information will be collected); use limitation (once information is collected for one purpose it cannot be used for another purpose unless the individual consents or this is authorized by law); security safeguards (the information must be secured from risk, e.g. from attacks by hackers); openness (transparency, i.e. the individual should know what is being done with her information); individual participation (the individual should have access to her information and be able to look at it and correct inaccuracies); and accountability (there must be an oversight mechanism).
272. PIPEDA, *supra* note 170 at s. 7(1)(e)(ii).
273. PIPEDA, *supra* note 170 at s. 7(3)(c) (1).

purpose of administering any law of Canada or a province."[274] In this respect, PIPEDA is designed to both protect individual privacy and facilitate the sharing of information between third parties and government organizations, particularly for law enforcement purposes.

In terms of the collection and disclosure of basic subscriber information, Parliament needs to draft legislation requiring ISPs to collect this information and verify its accuracy. In order to collect and ascertain the reliability of the information, ISPs will need to notify their customers that they are collecting the information up front, perhaps as a condition of service, which means that section 7(1)(e)(ii) would not apply. Law enforcement officials can then request disclosure of the information, in compliance with section 7(3)(c)(1), with respect to a particular individual, when that information is required for law enforcement purposes only. In terms of orders for the preservation of data, section 7(1) of PIPEDA would authorize ISPs to collect and retain information from their networks, in response to a lawful request, without the knowledge or consent of the individual to whom the information pertains.[275] Once a search warrant is obtained, law enforcement officials could then compel disclosure of the data for law enforcement purposes, pursuant to section 7(3)(c)(1).

Section 7(1)(e)(ii) of PIPEDA appears to authorize an ISP to collect personal information, without knowledge and consent of the individual, *only* if the collection is made for the purpose of making a disclosure required by law.[276] In other words, if the request for disclosure has not already been made by law enforcement officials, with the lawful authority, the information cannot be collected. This appears to prevent the enactment of "data retention" legislation requiring ISPs to retain all of the data passing through their networks, pertaining to all subscribers, as discussed earlier. It is important to keep in mind that the lawful access measures proposed here do not include data retention policies, of the sort being implemented in the European Union, but merely data preservation, which would only apply to ISPs in a very limited number of cases, following the issuance of a judicial order. This would also avoid the risk of capturing more personal information than necessary, which might include information about financial transactions, health information, PIN numbers, private correspondence, and other sensitive information, and ensure that the information only relates to a particular suspect who has been identified by law enforcement officials.

*

7. CONCLUSION

DUE TO THE UNIQUE STRUCTURAL MAKEUP OF CYBERSPACE, ISPs have an essential role to play in targeting online child pornography. Parliament has recently been considering how it can enact legislation to require telecommunications service providers to retain data that moves across their networks, or make data in their possession available to law enforcement agencies on legally authorized request. Lawful access is a complex and delicate issue because it involves issues of

274. PIPEDA, *supra* note 170 at s. 7(3)(c)(1)(iii).
275. PIPEDA, *supra* note 170 at s. 7(1).
276. PIPEDA, *supra* note 170 at s. 7(1)(e)(ii).

financial costs and competitiveness, privacy, technical capability, and the need to enable law enforcement agencies to target criminals who use communications technologies to perpetrate serious criminal offences on a global scale. Canadian ISPs currently have different practices for how long they retain data flowing through their networks, if they even retain it at all. Most ISPs are members of voluntary associations that establish codes of conduct for their members. While these are helpful, they are insufficient to combat online child pornography in any significant way.

In August 2002, Canada tabled its *Lawful Access Consultation Document* which set out Parliament's argument in favour of modifying Canadian law to ensure that law enforcement agencies are able to engage in the lawful access of modern communications technologies, such as the internet. This initiative, which is essential to prevent, investigate, and prosecute serious offences, including child pornography and terrorism, was fueled by our international obligations in the struggle against global crime. This includes the *Cybercrime Convention*, which Canada signed but cannot ratify until important changes are made to the *Criminal Code*, including provisions for orders to be made for the production and preservation of computer data.

The *Cybercrime Convention* is an important response to the realization that while computer networks and digital information are often used for lawful purposes, they are also used to facilitate criminal activities. Due to the increased flow of data over trans-border networks, a harmonized approach to fighting cybercrime is required. Canada must enact a comprehensive legislative scheme for dealing with internet cases and establish requirements for facilitating cooperation between law enforcement agencies within Canada and abroad. The challenge is to implement new measures that respond to technological change and globalization while ensuring that the existing rights and freedoms guaranteed by the *Charter* are protected.

The *Criminal Code* already contains well-established procedures for the lawful interception of communications, including telephone networks. However, law enforcement officials are prevented from intercepting internet technology. A lawful access proposal would require ISPs to update their networks to facilitate lawful interception by law enforcement. Data preservation and production are also important to the implementation of a successful lawful access regime. The *Criminal Code* must be updated to enable law enforcement officials to compel ISPs to maintain, or not delete, records about a particular suspect for a specific time period and then provide them to the police for use in law enforcement investigations. Given the role of ISPs as agents of the state in the data preservation process, the need for a valid search warrant may arise with respect to *both* production and preservation orders. These important issues will need to be taken into account by Parliament when it seeks to close the gap between technological advances and Canadian child pornography legislation.