

**Online Harassment and Cyberstalking: Victim Access to  
Crisis, Referral and Support Services in Canada  
Concepts and Recommendations**

by Randy McCall

President

Victim Assistance Online Resources  
info@vaonline.org  
<http://www.vaonline.org/>

October 5, 2003  
(Updated May 11, 2004)

## **Abstract**

The explosive growth in Internet use, as well as in other forms of electronic communications, in Canada – with more than 16.84 million Internet users in over two thirds of all Canadian households – has brought with it an equal explosion in the misuse of these new forms of communication, including the crimes of online harassment and cyberstalking. These crimes directly impact individual Canadian victims, creating:

- Fear for personal safety and security;
- Anxiety for the future and a loss of quality of life;
- Uncertainty and unpredictability, as the uncontrolled acts intrude upon the lives of victims in a random fashion, making the re-establishment of a normal life difficult.

At the same time, familiarity with the Internet and a sense of distance created by electronic communications causes society believe that such communications are not dangerous, are easily ignored and are therefore unimportant.

Technology is presently outpacing both society's understanding and the law itself. To help victim needs be understood, this paper:

- Examines the laws, policies and procedures surrounding these technological crimes and how they compare to harassment and stalking in the real world;
- Examines the lack of automatic and immediate access to crisis, support and referral services; how the needs of these victims can best be served;
- Recommends the creation of an independent, non-profit organization which can act as an information clearinghouse and reporting, referral and support service for victims of Internet crimes against the person such as online harassment and cyberstalking, which would liase closely with law enforcement agencies and commercial Internet Service Providers; and
- Makes additional recommendations based on consultation with law enforcement personnel, Internet Service Provider staff, victim advocates and victims themselves.

## **Introduction**

The explosive growth Internet use, and in other forms of electronic communications, in Canada – with more than 16.84 million Internet users (CIA World Factbook, 2003) in over two thirds of all Canadian households (Internet Use in Canada, 2002) – has brought with it an equal explosion in the misuse of these new forms of communication.

While most people are have at least heard of, if not personally encountered, the more common forms of electronic crime – commonly known as cybercrime – involving: money or property cybercrimes such as online fraud, identity theft and white collar cybercrime; technologically-based cybercrimes such as hacking, denial-of-service computer attacks, viruses and Trojan horses; or morals-based cybercrime such as online child luring or child pornography, there exists a group of cybercrimes which has become so common as to be overlooked and underestimated by both the public and government services. These are the crimes of online harassment and cyberstalking.

These cybercrimes directly impact the individual lives of Canadian victims (Cyberstalking – A New Challenge for Law Enforcement and Industry, 1999), creating in them:

- Fear for personal safety and security;
- Anxiety for the future and a loss of quality of life;
- Uncertainty and unpredictability, as the uncontrolled acts intrude upon the lives of victims in a random fashion, making the re-establishment of a normal life difficult. (Miller, 2001).

Technology is presently outpacing both societies' understanding of the technology, and the law itself. We need to re-examine the policies and procedures surrounding these technological crimes, and how we should best be serving the needs of victims.

## **Defining Online Harassment and Cyberstalking**

There is no simple definition of the terms “online harassment” and “cyberstalking”. Indeed, the terms are often used interchangeably. One of the simplest definitions of cyberstalking is: “...the use of electronic communication including, pagers, cell phones, emails and the internet, to bully, threaten, harass, and intimidate a victim.” (Maxwell, 2001)

Online harassment can be divided into direct and indirect harassment. Direct harassment include: threats, bullying, or intimidating messages sent directly to the victim via e-mail or other Internet communications mediums, and/or the use of technological means to interfere with a victim's use of the Internet – such as hacking or denial of services attacks. Indirect harassment includes – but is not limited to: spreading rumors about the victim in various Internet discussion forums; subscribing the victim to unwanted online services, posting information about the victim in online dating or sex services, or sending messages to others in the victim's name (Harvey, 2003)(Ellison, L., & Akdeniz, Y., 1998)

Online harassment can be seen as an element of cyberstalking, which has the additional factor of pursuit via electronic means. “The distinction between harassment and cyberstalking is that cyberstalking is characterized by pursuit and fear.”(Harvey, 2003).

Thus, generally speaking, online harassment becomes cyberstalking when repeated unwanted communications, whether direct or indirect, takes place over a period of time, via one or more mediums of Internet or electronic communications. The messages themselves must be unwanted, and the content can be – but is not limited to—threatening, sexually harassing, emotionally harassing or bullying, or general misinformation. Provided the messages create reasonable fear in the victim, they fit the definition for cyberstalking.

In Canada, these offences are covered by the charge of Criminal Harassment, “Criminal harassment is an offence in the *Criminal Code*. It is *harassing* behaviour that includes *stalking*” (Stalking is a Crime Called Criminal Harassment, 2003). As Canadians use the Internet every day, at both work and home, there has been bred a certain familiarity and comfortableness with this new medium. Electronic communications, with the lack of physical contact and confrontation, in the safety of a home or office, creates a feeling of distance and security; a feeling which may be misplaced, as statistics suggest that more than 70% of women and 60% of men are stalked by people they know, and that online harassment and cyberstalking can lead to stalking in the real world. (Tjaden & Thoennes, 1998)(WHO@ Online Harassment Statistics, 2003)

“The fact that cyberstalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true. As the Internet becomes an ever more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information. In addition, the ease of use and non-confrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to cyberstalking. Put another way, whereas a potential stalker may be unwilling or unable to confront a victim in person or on the telephone, he or she may have little hesitation sending harassing or threatening electronic communications to a victim. Finally, as with physical stalking, online harassment and threats may be a prelude to more serious behavior, including physical violence.”

(Cyberstalking: A New Challenge for Law Enforcement and Industry, 1999)

“In 1999, 42% of Canadian households had at least one regular user of the Internet. As more and more people are using the Internet, they are becoming vulnerable to a new and increasing crime — cyber crime. Cyberstalking, also known as on-line harassment, is closely related to real-life stalking. Chat rooms, message boards and e-mail are places in which a victim may be particularly vulnerable to cyberstalking. An individual may use a chat room to meet other people and subsequently harass them. A cyberstalker may also use e-mail to send threatening or obscene messages to their victim. In some cases, the stalker and victim might know one another. Other incidents have involved the cyberstalker campaigning against the victim by posting information about the intended target on discussion groups or poster boards (possibly by pretending to be the victim). In these incidents, the cyber-stalker may elicit a third party to harass and threaten the victim. In some incidences, stalking that takes place on-line remains on-line. It is also possible for cyberstalking to extend to real-life. The stalker may use a chat room discussion to obtain sufficient information about the target and/or gather information from other Internet sites. The stalker can then use the information to locate the victim and engage in ‘real-life’ stalking behaviours. Like real-life stalking, cyberstalking can cause extreme fear in the victim. The threats made on-line have the potential to carry over into real life. The stalker’s threats over the Internet may become more severe because barriers may be lowered as a result of the lack of contact and the anonymity provided by the Internet.”

(Hackett, 2000)

In her paper on Cyberstalking, Maxwell (2001) reported that Working to Halt Online Abuse’s 2000 statistics showed 19.5% of online harassment and cyberstalking cases reported to them in 2000 lead to offline stalking incidents.

Indeed, Victim Assistance Online has received numerous help requests from cyberstalking victims whose harasser’s activities have crossed over from the Internet to the real world, such as sending e-mail or Instant Messenger postings containing details of the victim’s daily activities, dress or movements. Any case where stalking activities cross over from the Internet to the “real world” suggests an extremely high level of physical threat. (Fein, Vossekuil and Holden, 1995)

As previously noted, attacks of targeted violence may be preceded by a series of preparatory behaviors including selection and location of the target, securing a weapon, subverting security measures, etc. Behaviors of concern include: (1) an unusual interest in instances of targeted violence, (2) evidence of ideas or plans to attack a specific target (e.g., diary notes, recent acquisition of a weapon), (3) communications of inappropriate interest or plans to attack a target (although direct threats to the target may be rare, subjects may communicate information about intentions to family, friends, co-workers, etc.), (4) following a target or visiting a possible location of an attack, and (5) approaching a target or protected setting. (Borum, Fein, Vossekuil, and Burglund, 1999)

The feeling of distance and safety created by the apparent anonymity of the Internet may be one of its most dangerous illusions.

### **Harassment and Stalking in Canada: How Criminal Harassment Charges Work**

In Canada, the crimes of harassment and stalking, both on and off-line, are covered by the charge of Criminal Harassment, section 264 of the Criminal Code (A Handbook for Police and Crown Prosecutors on Criminal Harassment, 1999, p. 21):

264(1) No person shall, without lawful authority and knowing that another person is harassed or recklessly as to whether the other person is harassed, engage in conduct referred to in subsection (2) that causes that other person reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them.  
(2) The conduct mentioned in subsection (1) consists of  
(a) repeatedly following from place to place the other person or anyone known to them;  
(b) repeatedly communicating with, either directly or indirectly, the other person or anyone known to them; besetting or watching the dwelling-house, or place where the other person, or anyone known to them, resides, works, carries on business or happens to be; or  
(d) engaging in threatening conduct directed at the other person or any member of their family.

The “Handbook” (1999, p. 23) lists the key elements that must be met to qualify for this charge:

1. The offender engaged in **conduct** described in subsection 264(2).
2. The offender did not have **lawful authority** to engage in the prohibited conduct.
3. The offender knew that the victim was **harassed** or he/she was **reckless or wilfully blind** as to whether the victim was harassed.
4. The conduct caused the victim to **fear for her/his safety** or that of someone known to her/him.
5. The victim’s **fear was reasonable** in all of the circumstances.

The “Handbook” (1999, pp. 28-29) goes on to clarify the **fear** clauses, showing that:

- “The victim must actually fear for her/his safety or that of someone known to her/him as a result of the defendant’s conduct”
- “The victim’s fear for her/his “safety” or that of someone known to her/him is not restricted to fear of physical harm but rather, includes fear for her/his mental, psychological and emotional safety”
- “In assessing the reasonableness of the victim’s fear, consideration may be given to the victim’s sex, race and age, but section 264 did not require that the victim have knowledge of what the defendant is capable”
- “Victims of harassment do not have to ‘suffer ill health or major disruption in their lives before obtaining the protection of section 264’”
- “One incident of threat is sufficient and need not be of a repetitive nature to satisfy subsection 264(2)(d)”.

Thus a single incident of harassment, provided it creates reasonable fear in the victim, is sufficient to invoke Criminal Harassment charges.

This then is the charge used when the crimes of online harassment or cyberstalking are reported. The government's own publication on stalking and the use of the charge of Criminal Harassment include suggested actions to be taken when stalked or harassed online, including reporting the crime to police for the laying of Criminal Harassment charges. (Stalking is a Crime called Criminal Harassment, 2003, p. 10)

## **Accessing Crisis Intervention and Referral Services – a Comparison**

### **Real World Harassment and Stalking – Accessing Crisis Intervention and Referral Services**

When a victim is physically harassed or stalked in the real world, they report directly to law enforcement. When a victim makes a report to the police of a case of stalking or criminal harassment, victim interview guidelines recommends that police (A Handbook for Police and Crown Prosecutors on Criminal Harassment, 1999, p. 7):

- Conduct a thorough interview of the victim. Advise the victim to be specific and accurate and to neither minimize nor exaggerate. Police also must not minimize the situation. The possibility of stalking and the future risk of physical violence should be considered whenever a harassing-type offence is reported (e.g., harassing or obscene phone calls, following, or unusual incidents involving mischief or vandalism).
- Be sensitive to the personal situation of the victim and her/his state of mind, including the psychological and emotional distress that she/he is likely experiencing. The victim may require the assistance of a support person and/or interpreter.
- Inform the victim that criminal harassment is a criminal offence. Emphasize the seriousness of the offence. Be clear with the victim regarding the potential threat.

Once in touch with law enforcement, the most provinces require the victim be presented with an option of referral to a local VCARS or similar victim crisis assistance program:

“The Victim Crisis Assistance & Referral Services (VCARS) program is a community response program providing immediate on-site service to victims of crime or disaster, 24 hours a day, seven days a week. With the consent of a victim, police officers call on VCARS to send a team of trained volunteers to provide on-site, short-term assistance to victims and make referrals to community agencies for longer-term assistance.”

(Victim Crisis Assistance & Referral Services)

<http://www.attorneygeneral.jus.gov.on.ca/English/about/vw/vcars.asp>

Why is referral important? Community service agencies supply personalized and specialized support, counseling and information services, which the victim of crime is very likely to need.

“The victims at the focus group emphasized that although the response of law enforcement and victim service providers is important, stalking victims need a wide range of services from doctors, mental health providers, day care providers, welfare and child protection workers, school staff, and employers. In addition, the focus group participants indicated that community awareness and understanding of what constitutes stalking behaviour is critical to the support and well-being of stalking victims.” (Cyberstalking: A new Challenge for Law Enforcement and Industry, 1999)

As can be seen, policy requires that a victim of a real world case of stalking or criminal harassment: a) be met with information on the seriousness of the crime and warnings of possible future risk, posed by officers with sensitivity to the victim's state of mind, and b) be given helpful support and referral to local agencies for long-term support and information. Why is this critical?

“Crime victims interact more with law enforcement officers than they do with any other criminal justice professional. In the United States, about 21 percent of all major crimes result in an arrest. This means that only 21 percent of victims have an opportunity to become involved in a criminal case through their local prosecutor’s office, which often can provide assistance to them. In other words, unless victims are assisted by law enforcement, nearly 80 percent of them may never learn about, let alone receive, the services that are available to them, at a time when these services are desperately needed.” (Gillis, 2003)

In those cases where arrest and conviction are not possible, these counseling and support referrals may be even more important, as support the victim will direly need services and safety information.

### **Online Harassment and Cyberstalking – Accessing Crisis Intervention and Referral Services**

“Make no mistake: this kind of harassment can be as frightening and as real as being followed and watched in your neighborhood or in your home.” Vice President Al Gore  
(Cyberstalking: A New Challenge to Law Enforcement and Industry, 1999)

There are no hard and fast rules for the reporting of online harassment/cyberstalking. Generally, Internet Service Providers (the company which supplies a user with access to the Internet and Internet services, noted hereafter as “ISP”) and online anti-harassment/cyberstalking organizations have four main suggestions for action when a person is harassed or stalked online. These often used in a incremental step-by-step process, progressing to the next step only when multiple attempts at the previous step failed, or if the seriousness of the offence or the level of fear generated in the victim increases. For example, if the first message received makes a direct threat to bodily safety, or creates exceptional fear for personal safety, all services recommend contacting law enforcement immediately. The four suggested actions are:

1. Report the offender to the victim’s own Internet Service Provider, to see if they can take any action to stop the perpetrator
2. Report the offender to his/her Internet Service Provider, as they are likely in violation of their ISP’s Acceptable Use Policy, or AUP (The AUP is a part of the contract agreed to when a user subscribes to an Internet Service Provider. It defines acceptable uses of the provided Internet connection. Violations of terms of the AUP can result in the termination of a violator’s Internet access. Use of the Internet to harass or threaten others is a violation of almost every ISP’s usage policy)
3. Report the offender to a third-party online service organization which can investigate and/or report to the police, or which can supply safety information. (Recommended by some organizations)
4. Report the offender to law enforcement.

“Report harassing e-mail or chat room abuse to your ISP. If you know the ISP of the person, tell that ISP too. They can cut off the person’s account if it is being used to harass others. Ask about tools to block unwanted communication. Do a Web search on cyberstalking. You will find many sites with tips and information. Some can help track down harassers, document their origin and send reports to you or the police.”

(Stalking is Crime Called Criminal Harassment, 2003)

“An email message that is sent to you implying harm to you or others you know is considered to be a threatening message. You must report this activity to your local law enforcement agency as they are in the best position to find the sender of the message and attend to any other questions or concerns you may have about your safety. Again, it is imperative that you keep the message and that all headers are readable and exposed for investigation and tracking.”

(Other Forms of Internet Abuse, 2003)

## Examining these Options

### Reporting the Offender to Internet Service Providers

Each ISP maintains an Abuse and Security department. The staff of these departments are normally computer and network specialists whose major training and focus is on the resolution of technical issues, not victim support; their responsibility is to maintain the ISP's hardware and software security, defend the overall network against computer viruses and hackers, and to ensure the ISP's customers/users are abiding by the ISP's AUP. While Abuse Department representatives at every ISP attempt to resolve all complaints, they are often constrained by a wide area of responsibility, limited personnel, as well as by the company's own privacy policies regarding user/customer information. "ISPs are not investigators. ISP Abuse Departments are only able to take action against their own subscribers for violation of AUP." (Anonymous Abuse Department Representative, September 11, 2003).

"In practice, however, ISPs have focused more on assisting their customers in avoiding annoying online behavior, such as receiving unsolicited commercial electronic mail ("spamming") or large amounts of electronic mail intentionally sent to an individual ("mail-bombing"); relatively less attention has been paid to helping victims of cyberstalking or other electronic threats. For some ISPs, the procedures for lodging complaints of online harassment or threats were difficult to locate, and their policies about what does or does not constitute a violation of service agreements were generally unhelpful. In addition, many ISPs do not inform their customers about what steps, if any, the ISP has taken to follow-up on their customer's complaint. These problems—hard-to-locate complaint procedures, vague policies about what does and does not constitute prohibited harassment, and inadequate follow-up on complaints—may pose serious obstacles to cyberstalking victims who need help."

(Cyberstalking: A New Challenge for Law Enforcement and Industry, 1999)

If a user is found in violation of an ISP's user agreement, they can have their Internet account/access cancelled. This does not prevent the violator from simply opening an Internet access account with another ISP and continuing the harassment. Anecdotally, it isn't unusual for victims to be told to repeatedly try and contact an ISP's Abuse Department, over a long period of time, to see if they can get action on their situation. In other words, they are told to solve their own problem.

### Reporting Offenders to Third Party Online Services

There are a number of third party online reporting and assistance services to be found on the Internet. Some of the most common to be found when searching for such organizations are:

- AntiStalking Web Site: <http://www.antistalking.com>
- CyberAngels: <http://www.cyberangels.org/stalking>
- End Stalking in America: <http://www.esia.net/>
- National Center for Victims of Crime Stalking Resource Center: <http://www.ncvc.org/src/>
- Network Abuse Clearinghouse: <http://www.abuse.net/>
- Sanctuary: <http://www.stalkingvictims.com/>
- Wired Patrol: <http://www.wiredpatrol.org/>
- Working to Halt Online Abuse (WHO@): <http://www.haltabuse.org/>

It will noted that none of the services are actually based in Canada, and are all being run by non-profit or voluntary organizations. Many supply only safety and security information and few have direct liasons to law enforcement for reporting purposes. While these services make the utmost effort to help, there is no officially recognized law enforcement or government related service, and no guarantee of referral to recognized crisis or support services. Why? The best explanation is taken from the "Report on Cyberstalking: A New Challenge for Law Enforcement and Industry" (1999):

“Because cyberstalking is a relatively new criminal phenomenon, very little public attention and resources have been committed to addressing this crime. Consequently, victims of online harassment and threats, often in collaboration with victim service providers and advocates, have had to step in to fill the void by developing their own informal support networks and informational web sites to exchange information about how to respond to these crimes effectively.”

### Reporting to Law Enforcement

Unless they receive the most drastic of threats, victims of online harassment or cyberstalking may have to make numerous attempts – over a lengthy period of time – to resolve the situation themselves before it is recommended they contact law enforcement. Only when reporting to law enforcement are victims likely to be placed in touch with local crisis and support services.

While law enforcement agencies make every effort to deal with Internet crime swiftly and efficiently (Meeting Law Enforcement’s Responsibility, 2001), the result is not always positive for victims, for a number of reasons. They may meet with officers who are unfamiliar with the crimes or technology in question, or who may be uncertain of how to proceed. “Unfortunately many law enforcement departments do not have the training or the funding to train their officers in Internet crime.” (Internet Safety, Help and Education, 2003)

“Unless directly reported to... and accepted by... police services, there is little or no direct community support for victims of online cyberstalking or online harassment, leaving the fearful and anxious victims of these crimes. Anecdotally, even when reporting to law enforcement, there seems to be gaps in service.

“The disparity in the activity level among law enforcement agencies can be attributed to a number of factors. First, it appears that the majority of cyberstalking victims do not report the conduct to law enforcement, either because they feel that the conduct has not reached the point of being a criminal offense or that law enforcement will not take them seriously. Second, most law enforcement agencies have not had the training to recognize the serious nature of cyberstalking and to investigate such offenses. Unfortunately, some victims have reported that rather than open an investigation, a law enforcement agency has advised them to come back if the cyberstalkers confront or threaten them offline. In several instances, victims have been told by law enforcement simply to turn off their computers.”

(1999 Cyberstalking – A new challenge to Law Enforcement)

It can also happen that the case will prove to be unsolvable. Reasons for this can include a variety of issues (D’Ovidio & Doyle, 2003): jurisdiction, including international, state/provincial and agency issues (McConnell International, 2000); lawful access to ISP user information; offender anonymity/identity issues (Kleinknecht, 2001), and technological issues.

In those cases where law enforcement and ISPs are unable to successfully locate, identify and prosecute/stop an online harasser or cyberstalker, the victim will be even more in need of emotional support and information on protecting their security and safety, as the harassment may well continue.

Victim Assistance Online has itself received (unverified) messages (personal communications, anonymous victims) from dozens of Canadian victims of cyberstalking and online harassment who report that their local law enforcement services seemed unfamiliar with cybercrime and online harassment in general, that they were often either referred them back to the Internet Service Provider’s Abuse Department, or told to just “change their e-mail addresses”. In several cases the victim reported being repeatedly referred back-and-forth between the ISP Abuse Department and their local police service, with no police report being taken at any point.

Two reports our organization received (unverified) suggested extremely high risk to the victim: in the first, the victim reported they had received a number of graphic descriptions or torture and death by e-mail, which including personal details of their daily lives. In the second, full descriptions of their daily dress and activities were sent to them by e-mail and other electronic means. In both cases, victims said they had reported the threats to their local law enforcement agency repeatedly, who told them they were unable to help with their situations. Both cases suggest high risk to the victims in question. (Fein, Vossekuil and Holden, 1995), (Borum, Fein, Vossekuil, and Burglund, 1999)

The fact such victims are contacting Victim Assistance Online, which is not a direct service agency, suggests they were desperate enough to reach out for any assistance possible. Staff of other Canadian victim service organizations with online presences such as web sites, mailing lists, etc., have informed us that they also receive many such help requests from victims of online harassment/cyberstalking, who reported they had no other avenue of aid left in their own regions.

### **Why Crisis Intervention and Long Term Support are Important**

It's generally agreed that there is little-to-no difference in the effects of being stalked/harassed on-or-offline. Maxwell (2001) quotes the Australian Minister for Justice and Customs: "Although the majority of studies have focused on the offline stalking victims, there is no evidence to suggest that cyberstalking is any less of an experience than offline stalking". Given this, victims of online harassment and cyberstalking will suffer the same crisis effects (Young, 2001) and long-term effects as victims of real world harassment and stalking.

While it is not within the scope of this paper to detail the many and varied possible short-or-long term effects of being stalked, many researchers suggest stalking can result in extensive psychological, social, physiological and behavioural effects or changes in the victim, including PTSD (Post Traumatic Stress Disorder), depression, panic attacks, sleep disturbances, substance abuse, suicidal thoughts and social or employment issues. (Tjaden, 1997), (Miller, 2000) (Prevalence and Health Consequences of Stalking, 2000, July), (Maxwell, 2001)

The sooner crisis intervention – and, if needed, longer term support or counseling – the sooner the victim can start to reestablish a sense of normality and safety. The sooner both technical and online safety information is supplied, the sooner the victim can start protecting themselves from their harasser or cyberstalker.

### **Online Harassment and Cyberstalking in Canada – A Growing Problem**

Statistics Canada police and court data for 1997 from "A Handbook for Police and Crown Prosecutors on Criminal Harassment" – which include online crime – reveals that:

- 8 out of 10 victims were female (79%)
- 9 out of 10 accused were male (88%)
- 67% of victims were criminally harassed by a current or former intimate partner or close male friend
- 43% of male victims were criminally harassed by a casual acquaintance, almost half of whom were male; only 13% were stalked by a former spouse or girlfriend
- 59% of all incidents occurred at the victim's home
- Although victims almost always suffered emotional harm, physical injury was recorded by the police in less than 1% of all cases

## Online Harassment and Cyberstalking Statistics in Canada

We could find no comprehensive public statistics kept on victims of online harassment or cyberstalking by ISPs, government or law enforcement. Both Canadian and other statistical sources agree that the number of Internet and electronic communication users in Canada are growing (Internet Use in Canada, 2002). We also know that the number of incidents of Criminal Harassment in the Canada has been growing (Hackett, 2000), thus we can presume this holds equally true for online harassment and cyberstalking. This trend may be even worse for Internet users, due to ease of communication, advanced technology and anonymity,

“Electronic communications technologies also lower the barriers to harassment and threats; a cyberstalker does not need to physically confront the victim. While there are many similarities between offline and online stalking, the Internet and other communications technologies provide new avenues for stalkers to pursue their victims. A cyberstalker may send repeated, threatening, or harassing messages by the simple push of a button; more sophisticated cyberstalkers use programs to send messages at regular or random intervals without being physically present at the computer terminal.

(Cyberstalking: A New Challenge for Law Enforcement and Industry, 1999)

Other indicators of increases in online harassment comes from the Forensic IT Trends Survey (2002) by Fox-IT, which shows that online harassment cases now comprise approximately 6% of all consulting done by computer forensic and information technology experts around the world.

While there are no precise statistics on the number of online harassment or cyberstalking cases in Canada, we can attempt a rough approximation. In “Stalking in America – Findings from the National Violence on Women Survey” (Tjadens & Thoennes, 1998) it is reported that:

- In the United States, one out of every 12 women (8.2 million) and one out of every 45 men (2 million) has been stalked at some time in their lives.
- One percent of all women and 0.4 percent of all men were stalked during the preceding 12 months.

Presuming:

- These statistics hold approximately true for Canada, with its similar society, and for Internet users as a body.
- The number of Internet users in Canada is approximately 16 million, (CIA World Factbook – Canada, 2003), confirmed by the Statistics Canada report “Internet Use in Canada” (2002) of 8 million Internet enabled households for the same year, presuming an average of two users per household.
- There is one user of each sex in each household
- We can estimate an approximate total of 8 million male and 8 million female Internet users in Canada

Then we can calculate:

- 8 million women x 1% (ratio for women stalked in the US within the past year) = 80,000 women harassed/stalked online in Canada in the past 12 months
- 8 million men x .4% (ration for men stalked in the US within the past year) = 32,000 men harassed/stalked online in Canada in the past 12 months

These rough and approximate figures suggest then that, at the low end, that 100,000 or more Canadians suffer online harassment or cyberstalking each year, with women making up more than 60% of all victims. Note that these calculations do not include those people who may also be being harassed or cyberstalked via text messaging on their cell phones, only those on the Internet.

An additional indicator of the seriousness of the situation can be found in a small, unscientific survey conducted by Victim Assistance Online. This survey asked Canadians suffering victimization from online harassment, online threats or actual cyberstalking to describe their situations, actions and results.

Respondents were self-selecting and their information was unverifiable, but indicative of the seriousness of these crimes. Of those who choose to participate:

- 66% reported being cyberstalked
- 25% reported being harassed online
- 8% reported threats of death or physical harm
- 42% reported that harassment/stalking crossed-over from the Internet to the real world, or vice-versa
- 30% reporting case duration at 1-3+ years, 50% at 2-6 months.
- 58% of respondents reporting that the online harassment or cyberstalking was still ongoing.
- Respondents were given a range of possible actions they could have taken to help resolve the situation, and then asked to rate the effectiveness of these actions on a scale of one to five, with one being the lowest. The actions offered, and percentage of respondents who took those actions were:
  - No Action Taken – 17%
  - Wrote Offenders – 42%
  - Changed Address/Name/ISP – 58%
  - Reported Offender to Your ISP – 33%
  - Reported Offender to Their ISP – 33%
  - Reported Offender to Law Enforcement – 42%
  - Reported Offender to Voluntary Online Reporting Service – 17%
  - Hired Private Investigator or Computer Forensics Expert – 8%
- All actions, with two exceptions, were rated as having an effectiveness of 1. The two exceptions were “Changed Address/Name/ISP”, which one person rated at 2, and “Hired Private Investigator or Computer Forensics Expert” which one victim rated as 4.
- When asked how they would like to be able to make reports of online harassment or cyberstalking, 90% of respondents selected via E-mail, 75% selected via Web page reporting form, and 42% selected via telephone.

Respondents were given an option to make comments on their cases or the issue. These included:

“The issue in this case goes beyond criminal harassment.”

“I have no idea where to get help.”

“The lack of assistance in this has disgusted me. Governments are ignoring a problem that has the potential to cause great emotional harm to individuals.”

“The police are not taking the issue seriously. No follow up completed - officer went on holidays for 5 straight weeks and when I call to request assistance, I’m told to wait until he returns (and that he has the ‘right’ to take holidays). I requested forms to make a complaint - the officer who gave them to me was sarcastic and rude.”

## The Need for Specialized Crisis and Referral Services

Viewing the above statistics, it becomes apparent that there is a large and underserved population of Internet users who are suffering under various degrees of Internet harassment, threats or cyberstalking without formal or specialized support. The question then becomes, what services are available to these victims? It would seem that, unless the victim takes the initiative and contacts agencies in their own towns, they are unlikely to be referred to local social service and support agencies until a report is taken by their local law enforcement service.

Victims of online harassment and cyberstalking need both the traditional support services for local counselling and support, but also effective safety information, technological and peer support. (Stalking is a Crime Called Criminal Harassment, 2003).

Just what is it that victims need? Participants at a focus group held in 1998 by the US Office for Victims of Crime asked just that question of victims of both on-and-offline stalking.

“The victims at the focus group emphasized that although the response of law enforcement and victim service providers is important, stalking victims need a wide range of services from doctors, mental health providers, day care providers, welfare and child protection workers, school staff, and employers. In addition, the focus group participants indicated that community awareness and understanding of what constitutes stalking behaviour is critical to the support and well-being of stalking victims. Finally, all of the stalking victims reported that the consequences of not being believed or supported, or having their fears viewed as exaggerated or unrealistic, can be devastating. Some victims feel isolated and alone, are made to believe that the stalking is their fault, lose primary relationships, or fear losing their jobs. These issues are just as relevant to cyberstalking victims as they are to victims of offline stalking.”  
(Cyberstalking – A New Challenge for Law Enforcement and Industry, 1999)

In 1999, the International Association of Chiefs of Police held a summit on victims of crime, and produced “What Do Victims Want? Effective Strategies to Achieve Justice for Victims of Crime” (2000) which listed the needs of victims; these needs are echoed in both Canada’s Solicitor-General’s “National Consultation with Victims of Crime” (2000) and the United Nation’s “Handbook on Justice for Victims” (1999):

- **Safety:** Protection from perpetrators and revictimization; crime prevention through collaborative problem solving; a restored sense of individual and community safety
- **Access:** Ability to participate in the justice system process and obtain information and services, regardless of individual or family circumstances
- **Information:** Verbal and written information about justice system processes and victim services that is clear, concise, and user friendly
- **Support:** Services and assistance to enable participation in justice processes, recovery from trauma, and repair of harm caused by crime
- **Continuity:** Consistency in approaches and methods across agencies; continuity of support through all stages of the justice process and trauma recovery
- **Voice:** Empowerment to speak out about processing of individual cases; opportunities to influence agency and system-wide policies and practices

It would appear that many Canadian victims of online harassment and cyberstalking are going with these needs unmet, mainly due to: the rapidity of technology development and change on the Internet; the lack of staff familiar with these technologies and their common uses, and; a social mindset that views Internet communication as safe and harmless. Victims not only need the traditional referral services for local counselling and support, but also effective safety information, legal resources, technological and peer support. They desire a simple and effective means of reporting online harassing and stalking to ISPs and law enforcement, while at the same time accessing social and support services.

## **Recommendations and Best Practices**

We submit therefore that the most efficient and effective method to serve Canadian victims of these crimes is through the creation of an independent, non-profit service organization, which would maintain a staff and volunteers with specific and detailed training in the areas of online harassment and cyberstalking. Depending on demand, the service could have a single office, or regional offices. It would be recommended that this organization should have both an online (Internet) and offline (office/telephone hotline) component. Areas of responsibility a proposed mandate could include are:

1. To create and maintain a library or database of safety and security information for victims of Internet crimes affecting the person – on online harassment and cyberstalking specifically – and act as a clearinghouse and information centre on these topics.
2. To create and maintain both an online and offline reporting capability for victims of these crimes, allowing victims to use the medium they are most comfortable with.
3. To develop an active and close relationship with local, regional and federal law enforcement agencies, and to refer cases to the appropriate agencies as warranted
4. To develop an active and close relationship with Internet Service Provider's Abuse Departments and to refer cases to them as warranted.
5. To act at need as a liaison between the victims, ISP Abuse Departments and law enforcement or High Technology Crime Units.
6. To act as a referral agency for victims of these crimes to regional social services, either through referral to existing programs via regional social services "Blue Book" directories, or by referring the victim to regional victim service organizations, who can then make local referrals.
7. To act as a referral agency for victims of these crimes to vetted online information and to support or peer discussion groups/ forums which can provide emotional support systems for victims. Due to the difficulty in vetting such services, the function of creating and maintaining such online information, support and peer discussion groups could be added to this mandate.
8. To act as an advocacy and advisory group on these issues.
9. To maintain current knowledge in Internet technologies, software, cultural and social uses, so as to remain knowledgeable on potential misuses of the Internet, and at the cutting edge of what can affect victims of online harassment and cyberstalking.

## **Best Practices Models**

As one best practice model for such an organization, I would recommend CyberTip.ca <http://www.cybertip.ca/>. A project of Child Find Manitoba, mandated by the Manitoba Department of Justice, this service was tasked with safeguarding Manitoba's children from being sexually exploited on the Internet. With extensive connections to child abuse investigation agencies and law enforcement service, staffed by personnel with specialized public education, prevention and advocacy information, this organization has been positioned to take reports through both on and offline means, and pass them on to the appropriate agencies quickly and efficiently.

“Cybertip.ca provides the public with a mechanism to report illegal content on the Internet, and facilitates the investigation and prosecution of those who use the Internet to victimize children. CFM’s Cybertip.ca is not an investigative entity, but rather a resource center and clearinghouse for the community and law enforcement.” (About Cybertip.ca)

Another model could be New Zealand’s “Netsafe: The Internet Safety Group” <http://www.netsafe.org.nz/> which is a non-profit organization designed to promote online safety and for all citizens, businesses and social groups in New Zealand. A national collaborative effort, its stakeholders include: law enforcement, the Ministry of Education, the Ministry of Justice, the Judiciary, the Department of the Interior, community organizations, businesses, teachers, parents and students.

### **Additional Recommendations**

In developing the following recommendations, Victim Assistance Online contacted ISP Abuse Department representatives, members of law enforcement or law enforcement associated High Tech Crime Investigation Units, as well as victim advocates and crime victims for their input and opinions. In general, most respondents agreed with the majority of these recommendations. These include:

1. More research into these crimes, including surveys of victims, need to be performed to discover precisely how extensive this problem is; these should include surveys of, or statistical research of reports on, cases reported to ISPs and law enforcement. The same research could help determine the best policies/procedures to be used in handling reports, as well as indicating victim support and information needs.
2. More training for law enforcement should be made available, to enable them to deal with victim reports of online harassment/cyberstalking efficiently and with sensitivity.
3. Many victims and victim advocates felt that ISPs needed larger, or more specialized, staff for dealing with these issues.
4. That some form of ISP Abuse Department and law enforcement High Technology Crime Unit database or contacts list be developed and maintained, to allow Abuse Department representatives and law enforcement officers to quickly locate and contact appropriate personnel in different regions/jurisdictions to resolve reports of online harassment/stalking. Anonymous ISP Abuse Department Representative, September 11, 2003), Canadian Cybercrime Project Mailing List (personal communications, January 2, 2002 – October 16, 2003)
5. That standardized reporting and response policies/procedures be used by all ISPs and law enforcement agencies, so that victims can follow and understand the progress towards resolving their situation.
6. That there be research into and development of combined online and telephone crime reporting systems, at least for online harassment and cyberstalking, to allow victims to report these crimes or seek information through the medium they are most comfortable with.

## **References**

A Handbook for Police and Crown Prosecutors on Criminal Harassment (1999). Department of Justice Canada [Online]. Available: <http://canada.justice.gc.ca/en/dept/pub/hpcp/complet.pdf>

About Cybertip.ca. Cybertip.ca Web Site [Online]. Available: <https://www.cybertip.ca/childfind/cybertip/930.html>

Borum, R., Fein, R., Vossekuil, B., and Burglund, J (1999). Threat Assessment: Defining an Approach for Evaluating Risk of Targeted Violence. Behavioral Sciences and the Law, 17, 323-337 [Online]. Available: [http://www.treas.gov/usss/ntac/ntac\\_bsl99.pdf](http://www.treas.gov/usss/ntac/ntac_bsl99.pdf)

CIA World Factbook – Canada – Communications (2003) [Online]. Available: <http://www.cia.gov/cia/publications/factbook/geos/ca.html - Comm>

Cyberstalking – A New Challenge for Law Enforcement and Industry (1999). United States Attorney General Report [Online]. Available: <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>

D'Ovidio, R., & Doyle, J. (2003). A Study on Cyberstalking – Understanding Investigative Hurdles. Law Enforcement Bulletin [Online]. March 72(3). Available: <http://www.fbi.gov/publications/leb/2003/mar2003/mar03leb.htm>

Ellison, L., & Akdeniz, Y. (1998), Cyber-stalking: the Regulation of Harassment on the Internet. Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet [Online], pp 29-48. Available: [http://www.cyber-rights.org/documents/stalking\\_article.pdf](http://www.cyber-rights.org/documents/stalking_article.pdf)

Fein, R., Vossekuil, B, and Holden, G. (1995, July). Threat Assessment: An Approach to Prevent Targeted Violence. National Institute of Justice: Research in Action [Online]. Available: [http://www.treas.gov/usss/ntac/ntac\\_threat.pdf](http://www.treas.gov/usss/ntac/ntac_threat.pdf)

Forensic IT Trends Survey (2002). Fox-IT [Online]. Available: <http://www.fox-it.com/survey/2002.pdf>

Gillis, J. (2003). Keynote Address, International Symposium on the Assistance for Victims of Crime: Identifying the Role of the Police in Meeting Victims' Needs [Online]. Available: <http://www.ojp.usdoj.gov/ovc/publications/infores/031803.htm>

Hackett, K. (2000). Criminal Harassment. Juristat - Statistics Canada [Online], Catalogue no. 85-002-XPE, Vol. 20, no. 11. Available: [http://www.statcan.ca/english/Dli/Metadata/justice/crim\\_harass\\_j\\_e.pdf](http://www.statcan.ca/english/Dli/Metadata/justice/crim_harass_j_e.pdf)

Handbook on Justice for Victims (1999). United Nations Centre for International Crime Prevention, Office for Drug Control and Crime Prevention [Online]. Available: <http://www.uncjin.org/Standards/9857854.pdf>

Harvey, D. (2003). Cyberstalking and Internet Harassment: What the Law Can Do. NetSafe II: Society, Safety and the Internet Conference Proceedings [Online]. Available: [http://www.netsafe.org.nz/downloads/conference/netsafepapers\\_davidharvey\\_cyberstalking.pdf](http://www.netsafe.org.nz/downloads/conference/netsafepapers_davidharvey_cyberstalking.pdf)

Internet Safety, Help and Education (2003). Wired Patrol Web Site [Online]. Available: <http://www.wiredpatrol.org/stalking/help.html>

Internet Use in Canada (2002). Statistics Canada [Online]. Available: <http://www.statcan.ca/english/freepub/56F0003XIE/index.htm>

Kleinknecht, S. (2001, November). Child Pornography on the Internet Session. Borders Conference – Rethinking the Line: The Canada-U.S. Border [Online]. Available: [http://canada.justice.gc.ca/en/ps/rs/rep/E\\_border.pdf](http://canada.justice.gc.ca/en/ps/rs/rep/E_border.pdf)

- Maxwell, A. (2001, June). Cyberstalking. Auckland University Department of Psychology [Online]. Available: <http://www.netsafe.org.nz/ie/downloads/cyberstalking.pdf>
- McConnell International. (2000) Cybercrime...and Punishment? Archaic Laws Threaten Global Information [Online]. Available: <http://www.witsa.org/papers/McConnell-cybercrime.pdf>
- Meeting Law Enforcement's Responsibility: Solving the Serious Issues of Today (2001, October). Major Cities Chiefs Association – Critical Issues Study Group [Online]. Available: <http://www.neiassociates.org/seriousissues.pdf>
- Miller, N. (2001). Stalking Laws and Implementation Practices: A National Review for Policymakers and Practitioners. Institute for Law and Justice [Online]. Available: <http://www.ilj.org/stalking/FinalRpt.pdf>
- National Consultation with Victims of Crime: Highlights and Key Messages (2001, July). Solicitor-General Canada [Online]. Available: [http://www.sgc.gc.ca/publications/ccra/200107\\_victimsofcrime\\_e.pdf](http://www.sgc.gc.ca/publications/ccra/200107_victimsofcrime_e.pdf)
- Other Forms of Internet Abuse (2003). Bell Sympatico Customer Service Web Site – Service Desk – Internet Security [Online]. Available: <http://www.service.sympatico.ca/ServiceDesk/ServiceDesk-Content.cfm?SDID=331&SDCategoryID=24&page=1>
- Prevalence and Health Consequences of Stalking --- Louisiana, 1998—1999 (2000, July). Morbidity and Mortality Weekly Report [Online] 49(29);653-5. Center for Disease Control and Prevention. Available: <http://www.cdc.gov/mmwr/preview/mmwrhtml/mm4929a1.htm>
- Stalking is a Crime Called Criminal Harassment (2003). Department of Justice Canada [Online]. Available: <http://canada.justice.gc.ca/en/ps/fm/harass-e.pdf>
- Tjaden, P. (1997, November). The Crime of Stalking: How Big is the Problem? National Institute of Justice Research Preview [Online]. Available: <http://www.ncjrs.org/pdffiles/fs000186.pdf>
- Tjaden, P. & Thoennes, N. (1998, April). Stalking in America: Findings from the National Violence Against Women Survey. National Institute of Justice Centers for Disease Control and Prevention Research Brief [Online]. Available: <http://www.ncjrs.org/pdffiles/169592.pdf>
- Victim Crisis Assistance & Referral Service (VCARS) (2003). Ontario Ministry of the Attorney General Web Site [Online]. Available: <http://www.attorneygeneral.jus.gov.on.ca/english/about/vw/vcars.asp>
- What Do Victims Want: Effective Strategies to Achieve Justice for Victims of Crime (2000, May). 1999 IACP Summit on Victims of Crime. International Association of Chiefs of Police [Online]. Available: <http://www.theiacp.org/documents/pdfs/Publications/victim.pdf>
- WHO@ Online Harassment Statistics (2003). WHO@: Working to Halt Online Abuse [Online]. Available: <http://www.haltabuse.org/resources/stats/index.shtml>
- Young, M. (2001). Psychological Trauma of Crime Victimization. Victim Assistance Frontiers and Fundamentals. National Organization for Victim Assistance [Online]. Available: <http://www.try-nova.org/Victims/Trauma.pdf>