Assessing Technology in the Context of Violence Against Women & Children. Examining Benefits & Risks.

Safety Net Canada 2013

ACKNOWLEDGEMENTS

We are indebted to many people for providing insights and other contributions towards this project. While the opinions expressed in these reports are ours alone, they are informed by years of collaborating with and learning from survivors, colleagues and communities.

We remain guided by the women, youth, and children experiencing violence at the hands of perpetrators. They often face high risks to their lives and wellbeing. We deeply appreciate all we continue to learn from these strong, brave, and creative individuals. Only by listening to the experiences and opinions of these women and youth, can Canada accurately identify and implement practices that best protect their safety, privacy, safety autonomy, equal rights and access to justice.

Thank you to the many anti-violence workers throughout Canada who contributed by sharing their experiences and knowledge for this report and for participating in our two national surveys of anti-violence workers on *Technology Abuse* and on *Organizational Technology Practices*. These individuals work in non-profit women's shelters, transition and interval houses, rape crisis centres, victim services agencies, counseling services, children exposed to violence programs, crisis lines, K-12 classrooms, college campuses, courts, income assistance offices, police stations, hospitals, mobile clinic vans, and many other places where a survivor of violence might request help. During this recession, many anti-violence programs face staff cuts, limited agency resources, and low salaries. These workers often volunteer time as crises arise and still took the time to fill out our surveys.

We gratefully acknowledge the Office of the Privacy Commissioner of Canada for providing funding for our research and this report and for their leadership. Privacy is priority concern for many women and youth, especially since it impacts their ability to maintain autonomy and access safety.

Thank you to CIPPIC legal interns Ken Dunham and Paul Holden for helping to review literature and compile findings and to CIPPIC Director David Fewer for supervising their work. Thank you to the U.S. National Network to End Domestic Violence's Safety Net Project for their ongoing leadership and support, and for providing a framework for our national technology surveys. A special thank you to Rhiannon Wong for her stewardship of this year-long project.

Thank you to Cynthia Fraser, founder of Safety Net Canada, who has been and continues to be an invaluable resource. We are grateful for having the opportunity to learn from you.

SAFETY NET CANADA

Safety Net Canada is a national initiative of the British Columbia Society of Transition Houses and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. Safety Net Canada addresses how technology impacts and can enhance safety, privacy, accessibility, autonomy, justice and human rights for women, youth, and other survivors of family and domestic violence, sexual and dating violence, stalking, harassment, and abuse.

Safety Net Canada est une initiative nationale de la Colombie-Britannique Society des Maisons de Transition (BCSTH) et la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC). Safety Net Canada étudie l'impact de la technologie et la façon d'accroitre la sécurité, la confidentialité, l'accessibilité, l'autonomie, la justice et les droits de l'homme à l'égard des femmes, des jeunes, des enfants et des victimes de violence familiale et conjugale, de violence sexuelle, de harcèlement et d'abus.

CONTRIBUTIONS BY

Research, Writing, Editing:	*Ken Dunham*
	David Fewer
	Cynthia Fraser
	Paul Holden
	Rhiannon Wong
French Translation:	*Jose Beaudet*
Graphic Design:	*Hannah Lee*

FINANCIAL

We thank the Office of the Privacy Commissioner of Canada for their financial contributions to this work and project.

Office of the Privacy Commissioner of Canada / Commissariat à la protection de la vie privée du Canada

In-kind contributions to this work by BCSTH, CIPPIC, the U.S. National Network to End Domestic Violence (NNEDV), and Safety Net Canada's founder Cynthia Fraser.

BC Society of Transition Houses · cippic · NNEDV National Network to End Domestic Violence · Safety Net

DISTRIBUTION PERMISSIONS

"Assessing Technology in the Context of Violence Against Women & Children. Examining Benefits & Risks." is one of three reports by Safety Net Canada addressing technology-enabled violence against women in Canada. The additional two reports are titled "Canadian Legal Remedies for Technology-Enabled Violence Against Women" and "Organizational Technology Practices for Anti-Violence Programs. Protecting the Safety, Privacy & Confidentiality of Women, Youth & Children."

It is beneficial to read these reports subsequently as each addresses equally important aspects of technology-enabled violence against women in Canada.

You may reproduce any portion of this report for non-profit training or educational purposes, provided that you:

- Do Not post **any of the contents of this report online**
- Do Not misrepresent the context or content of the work
- Acknowledge the source by including the following statement on each piece you reproduce:

"Reproduced (in whole or in part) from **Assessing Technology in the Context of Violence Against Women and Children. Examining Benefits And Risks. (2013)** By Safety Net Canada, a joint initiative of the British Columbia Society of Transition Houses (BCSTH.ca) and, the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC.ca)"

EXECUTIVE SUMMARY

Technology is evolving in dynamic ways. Rapid innovations in communications and connectivity are changing the way we socialize with loved ones and strangers, date and break up, work with colleagues, and express our views. New services and gadgets appear hourly, promising to make our lives easier, and some actually do.

Women report feeling safer carrying a mobile phone so they can call for help anytime[1]. The improved reliability of that call result of enhancing and upgrading telecommunications systems, emergency call centers, and mobile devices so that a location-enabled cell phone can help emergency services quickly find the 911 caller[2]. Mobile phones are also becoming great tools for documenting harassment and abuse. Cell phone cameras can videotape a woman's stalker as he violates his restraining order; screenshots can create date/time stamped images of his threatening text messages. After years of women pleading, "but he was here 5 minutes ago threatening me", cell phones now provide ways she can document the perpetrator's ongoing abuse.

While technologies can improve access to services and safety for women and children, they can also elevate danger by providing more tools for stalkers, abusers and other offenders to use in the context of domestic and dating violence, sexual assault, stalking and harassment. Most of this technology-enabled abuse is done using commonly available and popular technology like mobile phones, computers, email, cameras and online social networks. Even when abusers use more specialized surveillance technologies, they don't need to be a computer savvy or information technology expert, they simply need to be able to search and purchase tools and services online that promise to do the high-tech work for them. As part of harassing, stalking and perpetrating domestic and sexual violence, perpetrators hijack social media identities; eavesdrop and record phone conversations; intercept email and voicemails; log keystrokes and spy on computers or mobile phones; hack and sabotage online accounts; create fake online identities to harass, solicit and impersonate; track real-time locations; hack databases and computer networks and crack security.

Technology-enabled abuse is impacting the safety and well-being of Canadian women and children. The 2012 nationwide *Survey of Anti-Violence Workers on Technology Abuse* by Safety Net Canada documents many ways that women and youth are being abused, tracked, stalked,

[1] Lenhart, A. (2010) Cell Phones and American Adults. Pew Internet & American Life Project. At: www.pewinternet.org/Reports/2010/Cell-Phones-and-American-Adults/Part-3-Adult-attitudes-towards-the-cell-phone/Cell-owners-feel-safer.aspx

[2] Canadian Radio-Television and Telecommunications Commission (CRTC). 911 services for traditional wireline, VoIP and wireless phone services. By 2/2010, cell providers had to use GPS chip or triangulation technology to make location accurate at 10-300 metres from the phone; call centres services had to upgrade to support E-911 location. At: www.crtc.gc.ca/eng/info_sht/t1035.htm

monitored, impersonated, threatened, coerced and/or harassed through technology. A vast majority of perpetrators use technology to intimidate and threaten a woman (98%); impersonate her or others (72%) and, to hack into her email or social media accounts (72%).

Reports of Technology-Enabled Violence Against Women
Intimidation or threats via technology e.g. texts, email, and cell phone (98%).
Hacked into the survivor's email, social media and other online accounts (72%) **Hacked and monitored** Instant Messaging accounts (46%)
Impersonation using email, online profiles or other technologies to pretend to be the survivor or someone she knows, such as a friend (69%)
Hacked into computers to monitor her online activities and extract information (61%) Installed monitoring software / hardware spyware, keystroke loggers (31%)
Distributed or posted online pictures (60%) and videos (31%) of the woman/survivor without her consent. Used a hidden camera or her laptop's webcam to surreptitiously **spy on and record** her without consent (31%)
Tracked her location via GPS device or other location service (including showing up everywhere unexplained (50%)
Misused cell phones to track or monitor calls, location or other activities (49%)
Monitored conversations on landline phone (35%) or listening/recording devices (29%)
Misused caller ID to screen calls, or to spoof other phone numbers in order to call or text threats and abuse (44%)
Tampered with or destroyed assistive technology, e.g. hearing aid, screen reader, TTY machine in order to further isolate her (10%)
Source: Safety Net Canada. (2012) Survey of Anti-violence Workers on Technology Abuse.

While, research on technology-enabled violence against women is minimal, some studies do provide a glimpse at the world of technology misuse and digital abuse targeted at women and youth. On a global level, the United Nations estimates that 95% of aggressive behaviour,

harassment, abusive language and denigrating images in online spaces are aimed at women and come from partners or former male partners[3].

In Canada, 76% of criminal harassment and stalking victims are women.[4] 13% of Canadian women have experienced cyber bullying by a classmate or co-worker and 15% experienced cyber-bullying by a current or former family member or spouse[5]. Intimate partner stalking comprises two-thirds of all cases where women are stalked.[6]-[7]-[8] Of those stalked, more than one in four report their stalker used technology. Of the individuals stalked via technology, 83% reported being stalked through email, 35% through instant messaging, 46% via hidden cameras and 10% Global Positioning Systems (GPS) location tracking[9]. 7% percent of Canadian Internet users reported the misuse of their personal information online (e.g. misuse of pictures, videos or misuse of personal information uploaded on public websites).[10]

This report will examine how technology impacts women and children fleeing and/or living with the effects of sexual violence, domestic violence, harassment, stalking and other forms of violence against women. We will identify ways that information technologies can be used to undermine or enhance the privacy, security, and safety of women and children.

[3] Association for Progressive Communications. (2010 November) How Technology is Being Used to Perpetrate Violence Against Women – And to Fight it. www.apc.org/en/node/11452

[4] Statistics Canada. (2011) Criminal Harassment in Canada, 2009. *Juristat*. www.statcanada.gc.ca/pub/85-005-x/2011001/article/11407-eng.htm

[5] Perreault, S. (2011 September 15) Self-reported Internet Victimization in Canada, 2009. *Juristat.* Statistics Canada. www.statcan.gc.ca/pub/85-002-x/2011001/article/11530-eng.pdf

[6] Spitzberg, B., and Cupach, W. (2007) The State of the Art Stalking: Taking Stock of the Emerging Literature, *Aggression and Violent Behavior* 12: 64-86.

[7] Tjaden, P., and Thoennes, N. (1988) Stalking in America: Findings From the National Violence Against Women Survey. National Institute of Justice and Centers for Disease Control and Prevention, NCJ 169592.

[8] Black, M.C., Basile, K.C. et al. (2011) The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.

[9] Baum, K., Catalano, S. Rand, M., & Rose, K. (2009 January) Stalking Victimization in the United States. *Bureau of Justice Statistics Special Report*. NCJ 224527, 1-15. US Department of Justice, Office of Justice Programs.

[10] Statistics Canada. 2010 Canadian Internet Use Survey.

SOMMAIRE DE GESTION

La technologie évolue à la vitesse grand V. Des innovations constantes dans le domaine des communications et de la connectivité nous ont amené à modifier notre façon de socialiser autant avec nos proches qu'avec les étrangers : se donner des rendez-vous comme se quitter, travailler avec ses collègues, faire connaitre nos opinions. De nouveaux services et de nouveaux gadgets nous sont continuellement proposés en nous promettant de simplifier nos vies : cela s'avère dans certains cas.

Les femmes affirment qu'elles se sentent plus en sécurité si elles ont un téléphone cellulaire sur elles leur permettant d'appeler à l'aide en tout temps[1]. L'amélioration et la mise à jour des systèmes de télécommunications, des centres d'appels d'urgence et des appareils mobiles font qu'un téléphone cellulaire avec service de localisation peut permettre aux services d'urgence de repérer rapidement la personne qui a composé le 911[2]. Les téléphones cellulaires sont également des outils qui permettent de documenter les cas de harcèlement et d'abus. Avec un téléphone intelligent il est possible de faire une vidéo d'un homme qui viole son ordonnance restrictive ; avec des captures d'écran il est possible d'avoir des images indiquant la date et l'heure à laquelle une victime reçoit des menaces. Pendant des années, les femmes pouvaient affirmer en vain qu'elle recevait des menaces. Elles peuvent désormais appuyer leurs dires quant aux agissements de leur abuseur.

Même si les technologies améliorent l'accès à des services et offrent une sécurité aux femmes et aux enfants, elles peuvent aussi augmenter le danger en fournissant aussi des outils aux traqueurs, aux abuseurs et autres malfaisants qui les utilisent dans un contexte de violence conjugale et de violence dans les fréquentations, dans les cas d'agression sexuelle, de traque et de harcèlement. Une grande partie des abus générés par la technologie proviennent de moyens populaires et facilement disponibles comme les téléphones cellulaires, les ordinateurs, les courriels, les appareils-photos, Internet et les médias sociaux. Même en utilisant des technologies de surveillance plus sophistiqués, les abuseurs, sans être des experts dans le domaine, arrivent à leurs fins en achetant en ligne des outils et des services qui pallient leur manque de savoir-faire. Le harcèlement, la traque furtive et la violence conjugale et sexuelle prennent plusieurs formes : vol d'identité dans le dossier du média social utilisé par la victime ; écoute et enregistrement des conversations téléphoniques ; interception des courriels et de la messagerie vocale ; mémorisation de la frappe et espionnage d'ordinateurs et de téléphones cellulaires ; piratage et sabotage des comptes en ligne ; création de fausses identités en vue de harceler et de solliciter ; usurpation d'identité ; repérage de localisation en temps réel ; piratage des bases de données et des réseaux informatiques pour déjouer la sécurité.

L'abus de la technologie a un impact sur la sécurité et le bien-être des femmes canadiennes et des enfants. Le sondage national de 2012, intitulé : *Sondage concernant la technologie, auprès des personnes travaillant avec des femmes victimes de violence* par Safety Net Canada documente les nombreuses façons dont les femmes et les jeunes sont abusés, suivis, traqués, contrôlés, personnifiés, menacés, contraints et harcelés par le biais de la technologie. Beaucoup

d'auteurs de crimes utilisent la technologie à des fins d'intimidation et de menace envers les femmes (98 %) ; de vol d'identité – de la victime ou autre personne (72 %) et de piratage de courriels ou de comptes de médias sociaux (72 %).

Rapports d'abus de la technologie à des fins de violence envers les femmes
Intimidation ou menaces par le biais de la technologie ex. textos, courriels et téléphones cellulaires (98 %)
Piratage des comptes des courriels, médias sociaux et autres (72 %) **Piratage et contrôle** des comptes de messagerie instantanée (64 %)
Usurpation d'identité par courriel, profiles en ligne ou autres technologies pour personnifier la victime ou un ami de celle-ci (69 %)
Piratage d'ordinateurs pour contrôler les activités de la victime en ligne et extraire de l'information (61 %). **Installation de logiciels espions** (logiciels et matériel), enregistrement des frappes (*keylogging*) (31 %)
Distribution ou diffusion en ligne de photos (60 %) et vidéos (31 %) de la femme sans son consentement. Utilisation d'une caméra cachée ou de la webcaméra de son ordinateur portable pour l'espionner ou l'enregistrer à son insu (31 %)
Repérage de localisation par système GPS ou autre (incluant se manifester à tout moment sans explication) (50 %)
Mauvais usage du téléphone cellulaire pour retracer la localisation, écouter les appels ou autres méfaits (49 %)
Écoute des conversations sur téléphone fixe (35 %) ou appareils d'écoute/d'enregistrement (29 %)
Falsification de l'identité de l'appelant pour filtrer les appels ou pour usurper d'autres numéros de téléphone en vue d'appeler ou texter des menaces (44 %)
Altération ou destruction de la technologie d'aide, ex. aide auditive, lecteur d'écran, appareil télétype afin de l'isoler davantage (10 %)
Source: Sondage concernant la technologie, auprès des personnes travaillant avec des femmes victimes de violence par Safety Net Canada

Si la recherche sur les abus de la technologie menant à la violence envers les femmes est encore jeune, certaines études fournissent un aperçu des abus dans le monde de la technologie et du numérique dirigés envers les femmes et les jeunes. À l'échelle globale, les Nations Unies estiment que 95 % des comportements agressifs, du harcèlement, des propos injurieux et des images diffamatoires dans les espaces virtuels sont dirigés envers les femmes et proviennent de leur conjoint ou d'ex-conjoint.

Au Canada, 76 % des victimes de harcèlement criminel et de traque furtive sont des femmes[4]. 13 % des femmes canadiennes ont été la cible de cyberintimidation par un compagnon de classe ou de travail et 15 % en ont été victime de la part d'un membre de la famille ou conjoint[5]. Les deux tiers des cas de traque de femmes l'ont été par un partenaire intime[6,7,8.] Dans ces cas une femme sur quatre affirme que son traqueur utilisait la technologie. De celles-ci, 83 % ont été traquées par courriel, 35 % par messagerie instantanée, 46 % par caméras cachées et 10 % par système GPS[9]. 7 % des utilisateurs d'Internet au Canada rapportent un abus de leurs renseignements personnels en ligne (ex. photos, vidéos ou renseignements personnels téléchargés à partir de sites Internet publics). [10]

Ce rapport examine les impacts de la technologie sur les femmes et les enfants qui sont en fuite et/ou qui vivent avec les effets de la violence sexuelle et conjugale, le harcèlement, la traque furtive et autres formes de violence envers les femmes. Nous identifions comment les technologies de l'information sont utilisées pour miner ou améliorer la sécurité et la vie privée des femmes et des enfants.

TABLE OF CONTENTS

INTRODUCTION

PURPOSE OF "ASSESSING TECHNOLOGY IN THE CONTEXT OF VIOLENCE AGAINST WOMEN: EXAMINING RISKS AND BENEFITS"

The purpose of this research is to:

- Examine how technology impacts women and children fleeing and/or living with the effects of sexual violence, domestic violence, harassment, stalking and other forms of violence against women.
- Identify ways that information technologies can be used to undermine or enhance the privacy, security, and safety of women and children.
- Raise safety, identity and privacy concerns about mainstream, assistive, and emerging technologies.
- Explain the use of technology to threaten or re-victimize women and other survivors of domestic violence, sexual violence, harassment and stalking.
- Discuss ways that information technology can benefit survivors;
- Promote promising practices to protect the privacy and safety (identity) of participants.

This research informs the work of three related reports:

- Assessing Technology in the Context of Violence Against Women: Examining Risks and Benefits;
- Legal Remedies for Technology-enabled Violence Against Women; and
- Organizational Technology Practices for Violence Against Women Programs.

Terms

Violence Against Women is any act of gender-based violence against females which reflects or perpetuates women's subordinate status in society. Violence against women includes physical, sexual, emotional, economic, financial, spiritual and other harm or suffering to females including threats, coercion, and deprivation of liberty in public or private life.

Violence against women by intimate partners: also known as domestic violence, dating violence, intimate partner violence, battering, gender-based violence and family violence. Family violence tends to include: "*Physical, sexual and psychological violence occurring in the family, including battering, sexual abuse of female children in the household, dowry-related*

violence, marital rape, female genital mutilation and other traditional practices harmful to women, non-spousal violence and violence related to exploitation[11]*."*

Sexual violence, harassment and stalking are all types of violence perpetrated against women by their current or former intimate partners. Sexual violence, harassment and stalking are also commonly perpetrated against women and girls where there never was a romantic, marital, common law, or dating relationship.

Violence against women also includes *"Physical, sexual and psychological violence occurring within the general community, including rape, sexual abuse, sexual harassment and intimidation at work, in educational institutions and elsewhere, trafficking in women and forced prostitution; (c) Physical, sexual and psychological violence perpetrated or condoned by the State, wherever it occurs"*[12].

These reports reflect a wide range of technology-enabled violence perpetrated against women and girls but focus primarily on the following types of violence against women: domestic violence, sexual violence, harassment and stalking.

WHY TECHNOLOGY AND VIOLENCE AGAINST WOMEN?

Misusing technology to perpetrate violence against women is always changing with constant upgrades and developments of new technology. Women who experience violence through an offender's misuse of technology, and their advocates, often struggle to figure out how the abuser seems to always know her location, what she is saying on private phone calls, what websites she visits, and the emails she's sending and receiving. Women fleeing violence also report that abusers use technology like social networks to impersonate them or their children and to threaten and harass them, as well as their friends, and family. Without technology safety education, anti-violence workers struggle with knowing how to best incorporate technology into safety plans, knowing what the capabilities for each technology are and what evidence is needed for women and girls to take to law enforcement. For members of the justice system, including legal aid advocates, knowing how the Canadian Criminal Code and privacy and provincial legislation can be applied to cases of abuse, sexual assault, harassment and stalking through technology misuse can be life saving for many women.

The reality of technology use is it can help create paths to safety and it can be misused by abusers to terrorize and control. Women enduring violence don't necessarily have time to research each technology. In a crisis, they may rely on anti-violence workers to alert them to

[11] United Nations. (1993 December 20). 48/104 Declaration on the Elimination of Violence Against Women. www.un.org/documents/ga/res/48/a48r104.htm.
[12] United Nations. (1993 December 20). 48/104 Declaration on the Elimination of Violence Against Women. www.un.org/documents/ga/res/48/a48r104.htm .

safety risks and discuss strategies and options with them, so they can make informed decisions about which technologies work best for them.

As you read through this report, we encourage you to consider the privacy implications of technology and the vulnerabilities of technology in terms of privacy and protection of personal information and Canadian Law. Without thinking about how technology can jeopardize privacy and personal information, lives of women and their children are put at risk.

RESEARCH THAT INFORMED THE DEVELOPMENT OF THIS REPORT

An extensive literature review on technology available in Canada and the implications on women fleeing and/or living with the effects of violence was conducted. Articles and resources were reviewed which related to:

- The misuse of technology to harm women and children.
- The benefit of technology for women and children fleeing and/or living with the effects of violence.
- Issues relevant to technology and violence against women.

A twenty-eight question *on-line survey* was distributed in both French and English to anti-violence workers across Canada in domestic violence, sexual violence and other programs that support children exposed to violence in the home. 133 surveys were returned from a broad and diverse representation of staff.

Research Findings

Sixty-three percent of survey respondents indicated that they supported women and children who had experienced perpetrators misuse of technology to perpetrate violence against them. In answering the query “What are some of the things women have reported to you about what perpetrators have done or they believe the perpetrators have done to harass women using technology?” ninety-seven percent of the field survey respondents replied with “intimidation and threats via technology”. They responded that the majority of women are asking for support with safety and privacy while using social media and safety with cellular phones. Responding to their own concerns regarding privacy and confidentiality when working with women and children, workers across Canada fear perpetrators intercepting communication between advocates and women.

Conclusions Based on Research Findings

The research findings lead to the conclusion that advocates, law enforcement, members of the justice system, women and children are in need of education and resources about the ways technologies are being misused and can benefit Canadian women and children. We hope these three resources will be a starting point for the further development and implementation of Canadian educational resources.

We hope that these three initial resources will lead to:

- a better general understanding of the risks and benefits to privacy and identity security associated with the use of information technology in a violence against women context;
- a better understanding among survivors of domestic violence, sexual violence and stalking, and among the support community servicing this vulnerable group, of the risks and benefits to privacy and security associated with the use of information technology;
- a better understanding of the legal framework available to survivors and their advocates, as well as of the shortcomings of this framework; and
- greater compliance with the law as developers and distributors of information technologies come to understand the privacy and security implications of their own technologies.

OVERVIEW

For some women who experience intimidation and threats from an abusive ex/partner/husband or/and sexually violent stalker, the decision even to turn a mobile device on or off can feel like Sophie's choice[13]. As one anti-violence worker described:

> *I think the biggest thing is that perpetrators will continually text women and children with abusive messages. When they don't respond, he often becomes more abusive. In several cases, if they changed their number the perpetrator finds the new number and harassment starts again. [Some] police will not take this seriously and even after death threats were made against a woman and her children. She was told that unless he physically was there threatening her or caused her harm that they couldn't do anything about it.*

Most men who commit domestic violence will criminally harass for as long as they can get away with it. When police are not trained in interpreting and assessing danger in technology-enabled abuse cases, they may mistakenly assume that technology-enabled abuse might have a lower risk of injury or death. Sadly, this is not the reality, especially not when death threats are made.

The use of *"information and communication technologies to further abuse victims of domestic violence*[14]" was identified by Ontario's domestic violence death review committee as a theme that ran through several fatality cases. Technology-enabled abuse in these cases included: threats via online dating sites, monitoring her online journal and social networking activities, tampering with the victim's email, sending slanderous messages to people on the victim's address list, sending threatening, abusive and/or excessive messages to the victim and others using email and text services, and using tracking devices and/or spyware to monitor the victim's activities[15].

A number of deaths have also resulted from technology-enabled sexual violence against young women aged 14-17. In several cases, photos and videos were taken by peers or assailants while a girl was being sexually assaulted by several boys. Images of her assaults were shared with school peers who bullied, targeted and blamed the rape victim, calling her derogatory misogynist names, and doing sexualized online harassment and bullying. We are aware of four cases where the teenage girl found such violence too much and took her own life.

---

[13] In the movie *Sophie's Choice* (1982) Sophie is forced to choose which of her two children would be gassed at Auschwitz and which would live and be sent to a labor camp.

[14] Office of the Chief Coroner. (2011). *Domestic Violence Death Review Committee - 2010, Eighth Annual Report*. Toronto: Province of Ontario.

[15] Office of the Chief Coroner. (2011). *Domestic Violence Death Review Committee - 2010, Eighth Annual Report*. Toronto: Province of Ontario.

Given this disheartening reality, we are not surprised that three quarters of youth aged 14-24 believe that digital abuse is a serious problem. 41% of youth in a relationship have experienced some form of digital dating abuse, with about a 25% feeling pressured to constantly "check in" with their partner. 56% of surveyed youth have experienced abuse through social and digital media and a majority found the experience was "deeply upsetting."[16]

Tactics youth found helpful in ameliorating digital abuse included limiting the perpetrator's access to their social network accounts, passwords and digital contact information. Youth also said they are more likely now to intervene if they see someone else being abused online.

> "Privacy is one of the most enduring social issues associated with information technologies[1]" Privacy is also one of the most enduring needs for women who are fleeing technology-enabled harassment, stalking, and abuse.

Many technologies raise potential privacy risks and benefits for those who use them. But for survivors of violence and abuse, the ability to keep their identity, location, and plans private when using technology can be life-saving or life-threatening. The extent, to which a woman can control and keep her information private when using technology, has a direct impact on her safety and wellbeing. Women visiting VAW programs often requested safety and privacy planning around: mobile/cell phones (82%), social media (74%) online browsing and email accounts (73%) and location privacy (55%).

> Over 80% of surveyed anti-violence workers were concerned that perpetrators, or someone else, might intercept the communications between anti-violence workers and a woman/survivor

In this digital age, we can share information more quickly and easily than ever before, sometimes without even knowing it has happened. With communications and information technologies (mobile phones, email, social media sites) "so much is hidden and unclear about how they work, who can see and access the data, and who owns it[17]" that women, youth and children facing technology-enabled stalking can have a difficult time accessing the information they need to make decisions and calculate risks about the technologies they are using.

[16] MTV. 2011 AP-MTV Digital Abuse Study. At: www.athinline.org/pdfs/MTV-AP_2011_Research_Study-Exec_Summary.pdf p.1-4

[17] ONO the robot. At http://onorobot.org

New technology features, fixes, applications (apps) and updates get released daily that can effect individual security, privacy, safety, accessibility, security and autonomy. Ground-breaking devices, systems, and services improve the ways women can access help and support; they also increase the ways that women and youth can be stalked/monitored. Information technology in particular is innovating so quickly that it is hard for organizations and individuals, law and public policy to keep up.

Take photos and videos for example. Women have learned how to use privacy settings to restrict access for any digital pictures they take or upload to photo sharing sites. They have learned how to ask individuals and social media sites to take down photos of them that they had not consented to share. They have learned how to strip geotags from their images and from their tweets. They have learned that turning mobile phone location tracking off prevents new pictures from being geotagged. But now women and youth want to know how to prevent their photos are being run through facial recognition systems, because even though they may still want to post photos on Facebook, they don't want to be identified in a global facial recognition database.

Survivors can learn how to opt out for a while, but as we know, social media keeps changing and now it is collecting a biometric. What do individuals do in this situation? Leave all social media as we know it? By the time these sorts of technologies are able to be applied to mainstream uses, many survivors' biometric privacy might have already have been significantly compromised.

Solutions for protecting someone's individual biometric, such as their face geometry or iris, are systemic solutions. Individual survivors of violence can't currently choose to implement these protections. It takes collaborations between corporations and government, and buy in from technology developers and producers to plan to implement biometric encryption standards in social media sites that would much rather keep accessing more personally identifiable information. Ann Cavoukian details how biometric encryption could work effectively in health care and other settings. But we also need laws, regulations and implementation that clearly protect biometrics that have already been made vulnerable.

In this era of increasingly big data, new location tracking devices not only map our individual movements with uncanny levels of accuracy, but will soon be the size of a dot and have an IPv6 address assigned to them. Related geosocial services will continue to encourage and incentivise the sharing of these ever more precise locations for you and all that you own.

Internet-connected mobile devices have embedded themselves in our personal and work lives and leave a trail of data wherever we go. It is almost like that big cloud of dust that follows Charlie Brown's friend Linus. Except, that we can't see how big our data identify cloud has

become. If IPv6 can provide enough IP addresses to assign one to every item that you own or buy, abusers will take advantage of that to track many aspects of her life, unless we can enhance privacy before it implemented more widely.

This document has two sections. Section A describes technologies available in Canada that can and are being used to perpetrate violence against women. It describes how specific technologies are misused or can benefit women fleeing and/or living with the effects of violence.

In Section B, we describe ways that technology can be used to enhance the safety of women and their children fleeing and/or living with the effects of violence.

SECTION A: TECHNOLOGY INVENTORY

TELEPHONES AND VOICE MAIL

Home and business telephones once consisted exclusively of "land line" technology, hard-wired to the telephone company's central office or a business's internal telephone system (PBX switch). Fax machines also use traditional "land line" technology.

Today, many individuals and organizations use a variety of "cordless" and mobile telephones. Even wired telephones that are ostensibly "land lines" may not be based upon traditional telephone technology.

"Land Lines"

Home and business "land line" (i.e. traditional hard-wired) telephones are still in widespread use. Interception of communications using this technology requires physical access in order to install a traditional "wiretap" or recording device. An offender who lives with or otherwise can gain access to the woman's residence or place of work can readily install a tap or recording device.[18] As all "land line" communications are made "in the clear" (i.e. without being encrypted), any tap or recording will reveal the entire conversation.

"Cordless" Telephones

So-called "cordless" telephones use a variety of unlicensed radio spectrum to allow the user to move about the home or workplace without the restriction of being "wired" to a specific location within the building. Some cordless telephones transmit in the clear, much like a radio, and thus can be monitored by anyone in the vicinity with a common scanner including some baby monitors. More modern digital handsets may use simple techniques like DECT technology to prevent casual eavesdropping, but ultimately any cordless phone can be monitored.

Voice over IP (VoIP)

Although they may appear to be standard hard-wired telephones, many modern phones used in homes and businesses are based upon Voice over IP (VoIP) technology, rather than the

[18] While Canadian law permits a party to a call to record his or her own conversations, it is a criminal offence to record anyone else's calls, even if the person doing so owns the residence/business or is the person named on the telephone account.

traditional technologies used in the public telephone network. These transmit voice communications over the same IP data networks used for Internet traffic, rather than over dedicated telephone (PSTN) networks as in the past. Almost all VoIP telephones use simple encryption techniques to prevent casual eavesdropping.

Skype and similar software products use VoIP technology on computers and smart phones. A variety of "spyware" can be installed on these devices to record the user's conversations, regardless of which specific telephony software they are using.

For a description of spyware see page 32.

Caller ID and Dial Number Recorders

Most telephone lines today automatically display the number, and sometimes also the name, of the calling party using "Caller ID" technology. This is implemented by the telephone company and is independent of the subscriber. A caller may thus inadvertently reveal his or her location to the recipient of any calls he/she makes. The recipient can often use online directories, including reverse lookup and other Internet search tools to link the caller number displayed to a specific address or subscriber.

Some telephones log the caller ID of all incoming calls. A person who can gain physical access to the telephone can scroll through this log to see the origin of any incoming calls.

Note that you do need to have a caller ID enabled telephone in order to read the caller ID.

> After a few months of unemployment, one recently divorced woman decided to contact a few of the people who had interviewed her for some feedback. After asking them what she could improve on to have more positive results in another job process, the interviewers surprised her by saying she had been chosen for the position. They had left her a few messages, but figured she was no longer interested when they never heard back. After further investigation, the woman realised her ex-husband had been using a spoof card to access her home voicemail. By "spoofing" her landline number, the voicemail service would automatically recognize the number as its own. With granted access to the account, he would listen and delete her voice messages. Although he was charged for his conduct, the woman still suffered the financial consequences of having to go months with no income.

The originator of a call can block the caller ID on a per call basis by dialing *67 before dialing the number. Some telephone companies provide a special service (sometimes at additional cost), whereby a subscriber can permanently block caller ID on all outgoing calls.

A dial number recorder (DNR) can be installed on a telephone or line to record the telephone numbers of all incoming and/or outgoing calls.[19] This would allow an offender to monitor who another person is speaking with.

It is technically straightforward for a caller to "spoof" the caller ID for any given telephone call. A number of services are readily available to do this, or specialized equipment can be installed on a particular line. Such spoofing can be used for protective reasons (to conceal the name or location of the caller), or more commonly for malicious reasons (i.e. to conceal the identity or location of the caller, or to impersonate someone else).

An offender can use spoofing technology to trick a woman or child into answering the telephone (e.g. pretending to be calling from her lawyer's office), to transmit false messages that appear to be authentic (e.g. pretending to be calling from the local courthouse with a "new" (false) date for the next hearing), or to maliciously impersonate the victim while engaging in behavior that appears to be coming from her (e.g. making obscene phone calls that appear to be coming from her).

Voice Mail

Telephone messages can be recorded on both traditional "answering machines" (connected in a subscriber's residence) or on remote voice mail services provided by telephone companies. Callers may leave deeply personal messages on these devices, and the mere fact that someone called and left a brief message may convey intimate information to an offender (e.g. time and location of a meeting, or indication that she is in a new relationship).

A home machine may have no security (i.e. password). Commercial voice mail services are typically protected by simple passwords only (e.g. 4 digits). Such passwords can often be guessed or discovered through brute force attacks (i.e. trying all possible combinations until successful). An offender may also use social engineering techniques to trick the telephone company into resetting the password in order that he may listen to and/or delete messages left for the woman. Access may also permit the offender to leave a message for the woman without making a direct telephone call to her.

Some home answering machines can be easily configured to record all incoming calls. This may not be apparent to those in the home. A home answering machine could also be installed surreptitiously as a crude wiretap.

[19] Use of a DNR is not a criminal offence in Canada as it does not constitute an intercept of a private communication (telephone numbers are signaling information, not a conversation).

For more information on social engineering see page 35.

MOBILE TELEPHONES

Modern cell (mobile) phones use light encryption and other techniques to prevent casual eavesdropping; the interception of voice calls is only possible with specialized equipment that is generally not available outside government and law enforcement.

However, offenders can exploit modern cell phones, especially the more advanced "smart phones", in several significant ways.

Mobile Phones as Recording Devices

Most mobile phones can be configured to "auto answer" an incoming call. An offender may put a secret mobile phone in a person's home or office, and then dial into it for the purpose of using it as an eavesdropping device. If the phone's charger can be surreptitiously installed along with the phone, the "bug" can be left in place on a more or less permanent basis.[20]

Smartphone Apps

Thousands of "apps" (software applications) are available for smartphones such as Apple's iPhone, RiM's Blackberry, and other mobile phones based upon the *Windows Live* or Google's *Android* platforms to monitor women and children. These offer an infinite variety of functions, including such common functions as electronic mail, instant messaging ("chat"), and address books.

Through apps, an offender can gain access to a woman's smartphone and obtain personal private information in the form of e-mail, SMS text messages, chat logs, call histories, and the personal information of all those listed in the address book.

Malicious apps can also be installed on a smartphone. For example, the phone could be configured to surreptitiously record audio or video whenever the woman is using her phone.

[20] Other common household devices that are transmitters can similarly be exploited to become a listening device, for example baby monitors and FRS radios.

GPS / Location Tracking

All modern mobile telephones, not just smartphones, have GPS-based location technology tracking capability built in. Its intended purpose is to locate the user when a 911 call is made, however this capability can also be exploited to maliciously track the user. For example, there are tracking apps that purportedly are intended for parents to keep tabs on their children, but these can also be used by someone abusive to monitor their girlfriend, wife or children.

> Because cell phones often come with built-in Global Positioning Systems, they can serve as efficient tracking equipment. It is precisely with this type of tool that one man was able to track the movements of his former girlfriend. When their two-year relationship ended and the man's ex-girlfriend refused to get back together, he planted the device under the hood of her car. Shortly after, he started "randomly" bumping into her. His ex-girlfriend grew suspicious when it happened too frequently and under odd circumstances. Police were finally notified of his behaviour when he was spotted under the hood of his ex-girlfriend's car while trying to change the cell phone's battery. He was arrested and charged for his conduct.

An offender can exploit the GPS functionality in several ways:

- A GPS-equipped mobile phone can be secreted in a car or other thing that the offender wishes to track, and set to auto answer mode. The offender can dial into the phone whenever he wishes to track its location.

- An offender could use a variety of techniques to directly access the GPS tracking functionality in the woman's own phone.

- The offender could use the GPS tracking functionality of a child's phone to identify the location and/or movements of the other parent when the child is with her.

- The offender can use family finding services available through mobile phone providers to monitor the location/movements of the other parent/child on the same family plan.

Keyloggers

There are two types of keystroke loggers, or simply "keyloggers." The first is hardware that can be attached to a computer system. The second is software that can be downloaded onto computers, smartphones and tablets. Keyloggers record all keystrokes entered onto a smartphone, computer or tablet. Some variants also capture screenshots (e.g. web browsing)

and copy all e-mail and chat communications. This information is transmitted surreptitiously to the offender, typically via e-mail.

Keyloggers are often designed to remain hidden from the person being monitored. While they can be installed in seconds, the offender may need to gain access to the targeted smartphone in order to install the software. If the keylogger is hardware, the perpetrator would need physical access to the device in order to install it. The offender could also deliver the keylogger to the device by hiding it in an e-mail attachment or link to a malicious web page.

Given that many users employ their smartphones for a myriad of purposes, often intimate in nature, an offender who can deploy a keylogger can obtain an infinite variety of information about the woman, including most of her communications and many passwords.

Keyloggers are discussed in greater detail in the "special risks" section towards the end of this inventory.

FAX MACHINES

Fax machines and transmissions can be used to track a person in several ways:

- **Machine Identifiers**: Most fax machines can be programmed with the name and fax telephone number of the sending organization. The telephone number may be automatically acquired from the network. The name can be left blank, or substituted with something nondescript. This information is automatically transmitted to all other fax machines with which it communicates, and is also often displayed on the remote machine. A person present at the remote machine can read this information off its display.

- **Headers on Facsimile Transmissions**: Most fax machines will automatically print the identifiers described above at the top of each page of all incoming fax transmissions. Documents that are re-transmitted will thus include a trail of predecessor transmissions, unless this is manually removed. The headers can reveal the location of the victim. For example, if she is staying in a shelter and faxes something to her lawyer, who in turn re-faxes it to the perpetrator's lawyer or the courthouse, the perpetrator may be handed a document identifying which shelter the victim is staying at.

- **Machine Logs**: Fax machines log all incoming and outgoing transmissions, using the header information described above. Anyone who can obtain physical access to a machine can thus retrieve a record of all communications.

Shelters and other programs supporting women and children may wish to configure their fax machines to ensure no sensitive information is transmitted. Even the name of the VAW program is usually sufficient for someone else to identify its address. Lawyers may be reluctant to remove the identifiers from their own fax machines, but may need to cut away the previous headers from any fax transmissions they are forwarding on.

LOCATION TRACKING

Mobile Phones

As discussed previously, all modern mobile telephones, not just smartphones, have GPS-based location technology tracking capability built in.

Many "social networking" applications incorporate tracking information in their functionality. Many apps "geo-tag" photos with the location at which each photo was taken. Twitter and related apps do the same with "tweets". Many such apps allow the user to configure whether geo-tagging is turned on, which it often is by default. A user may not realize that an offender who has gained access to her smartphone has turned geo-tagging (back) on.

FourSquare and a range of other apps explicitly depend on location information to provide their functionality. A woman may inadvertently reveal her location through use of these apps/services.

> Geo-tagging consists of adding geographical information to a photo, video, or other form of media. Some applications are purely developed around this concept. One 16 year old girl was stalked and harassed by her ex-boyfriend through a smartphone application called Map my Run. The application allowed the GPS integrated in her smartphone to track and record her jog so she could later post the information and make it accessible to others. Because the young girl consistently ran the same course around the same time every day, her ex-boyfriend would "coincidentally" run into her. When she noticed these coincidences happening too frequently, she decided to change her route. Although this time, she chose not to map it.

Vehicles

Many vehicles now come with built-in GPS tracking systems, such as GM's *OnStar* service. A variety of legitimate (e.g. fleet tracking) and illegitimate ("spyware") devices can be attached to a vehicle in order to track its location. Many of these provide real-time tracking through a web browser interface (i.e. the stalker can be anywhere monitoring the movement of the woman in the vehicle from a computer or smartphone). Many of these devices are easy to conceal and may require a complete "tear down" of the vehicle in order to discover.

A mobile phone equipped with GPS functionality and set to auto-answer may be hard-wired into a vehicle's electrical system to serve as a GPS tracking device.

Other Items

A GPS tracking device can be attached or placed into almost any thing, such as a purse or child's toy, although such use may risk discovery.

GPS tracking devices are commonly found built into watches and fitness monitors.

COMPUTERS AND NETWORKS

All modern computers (whether Mac, *Windows*, or otherwise) use the same Internet Protocol (IP) communications technology as the Internet. Smartphones and tablet computers also use IP technology, except for voice calls made over cellular mobile networks.

Personal Computers

Personal computers of all types are usually designed to support multiple user accounts. A person with an administrator or "super user" account may be able to access all other accounts configured on the system. Any computer connected to the Internet may be accessible to such a person from a remote location.

User accounts (i.e. privacy) can also be compromised by obtaining or guessing the password. It is well known that many people use only very weak or otherwise easily guessed passwords. People also often re-use the same password across devices/accounts, so compromise of one may lead to the compromise of many.

Many users do not configure a password at all, either because they choose convenience (e.g. not being forced to enter a password when the system starts up), or as a result of ignorance (they either don't know how to, or don't understand why it is important).

Smartphones and Tablets

By comparison, smartphones and tablets are usually single-user devices; multiple accounts cannot be configured. Most such devices have weak or no security; a 4-digit unlock code is typical.

Some advanced devices (e.g. Apple's iPhone and iPad) can be backed up to a computer, and/or "wiped" clean in case of loss or theft. A malicious person who gains physical access to the device could duplicate its contents through an unauthorized backup, and/or delete all its contents through malicious use of the "wipe" function.

Wired Networks

A knowledgeable person who has physical access can monitor ("tap") a wired network, exposing much of the communications and other information transmitted over it. Financial transactions and some electronic mail services encrypt data to protect against this possibility.

Wireless Networks

Wi-Fi wireless technology is now widely deployed in homes, businesses, and meeting places (e.g. airports, hotels, and coffee shops). Most such systems support encryption to protect against unauthorized persons listening in, but this is often not actually enabled. Security technology known as "WPA2" represents the strongest such encryption method currently available, and should be configured whenever possible. Assuming a strong password is used, this also prevents an unauthorized user from impersonating a valid user on the network from a nearby location (e.g. car parked on the street).

A "rogue" wireless network can be placed nearby to trick a user into connecting to it rather than the legitimate network. By so fooling the user, data transmitted may be captured (e.g. passwords to online systems) or unauthorized access may be gained to the user's system.

ONLINE COMMUNICATIONS AND SOCIAL NETWORKING

A person's online activities, communications, and social networking may contain a great detail of personal identifying information about an individual. Some of these activities may include:

- Social networking: Facebook, LinkedIn, Twitter, Craigslist, etc.
- Online dating
- Electronic mail
- Real-time communications: instant messaging, chat, video-conferencing, *Skype* telephony.

In addition to any information posted by the user, many online activities create a trail of information than can be used to identify or locate the originator. For example, electronic mail messages usually contain the IP address of the sender, which in turn can be used to identify her location. Social networking sites such as FourSquare and Twitter may "tag" all posts with precise location information. A user may not be aware of this additional information that is being captured with every post. Log files and other caches of online activities can be accessed by anyone with physical access to the victim's compute or smartphone, or accessed remotely through a keylogger.

Social networking may also permit a stalker to obtain information about a victim from user accounts belonging to third parties. For example, a friend of a victim may reference her in a post online (for example, by describing an activity that both participated in). That friend may have configured less security on her own account (relative to the victim), thus exposing her postings to greater access from strangers.

A stalker can also masquerade as the victim and create social media, e-mail, etc. accounts in her name. These can be used to identify her friends, to gain access to their own social media posts, and/or to disseminate malicious information under her name. This is discussed further in the impersonation section below.

> As much as the online classified advertisement service known as Craigslist offers the opportunity for people to meet romantic partners, it is also what allowed one man to threaten and harass his ex-girlfriend. After one year of what had seemed to him like a serious relationship, his girlfriend told him she wanted to end things. In response, he posted her name and address on Craigslist and falsely advertised rape fantasies of hers. When men started trying to break into her apartment, all unsuccessfully, she found out what was going on and posted a notice on the door of her building warning people that the online advertisement was false. Her ex-boyfriend retaliated by mentioning in his post that the warning was all part of the game. She had to relocate in order to be safe once again.

GOVERNMENT AND COMMERCIAL DATABASES

Government and corporate databases contain vast arrays of information on individuals and their lifestyles. Basic biographical information (e.g. name and address) is routinely held by most businesses and government agencies. Some information can be highly detailed and intimate (e.g. mobile telephone call records and health records). The scope and quantity of information in these databases is increasing at a rapid rate as public and private sector organizations capture more and more details about us all.[21]

Anyone who can access even some of this information can learn a great deal of information about another person, especially when combined with other information that they may already know or be able to search out online. This includes for example Land Title Registry Databases that are accessible to the public and British Columbia's Integrated Case Management System.

As is often demonstrated by security breaches reported in the news, database security is often far less effective than it should be. Employees may "snoop" through databases (health, financial, and government assistance databases) in ways that have nothing to do with their legitimate work. Social engineering techniques (described more fully below) and hacking can be used to gain unauthorized access to someone else's information, especially as few frontline personnel may receive proper security training or oversight.

The increasing adoption of cloud computing means databases may be spread across multiple legal jurisdictions, and/or held by private sector service providers. The policies and procedures of more than one organization, and the laws of more than one jurisdiction, may impact privacy and confidentiality. These multiple layers may thus complicate accountability in the event of a breach of security.

ALARM SYSTEMS W/REMOTE CONTROL & VIDEO

Some advanced alarm systems are capable of remote control and/or remote video, both of which are transmitted over the Internet or a mobile data network.[22] The remote control function allows the user to arm/disarm the system from afar, and to receive alarm alerts. Remote video allows the user to observe the premises in real-time on their personal computer or smartphone. For example, the user could confirm that their child has indeed arrived home from school as expected.

While ostensibly offering additional levels of protection, there remains the potential for an offender to obtain access to the alarm system, including the remote video capability. The

[21] A recent *New York Times* profile of Axciom, one of the largest data marketing firms, indicated that it had records on 500 million people, with an average of 1500 data points each.
[22] Mobile data networks are sometimes labeled as 3G, 4G, or LTE.

password required for such access could be guessed (especially if weak), obtained from another compromised system via a keylogger, or obtained through social engineering techniques.

Most alarm systems include an installer passcode, which is supposed to be known only to a few trusted individuals. A perpetrator, who can obtain this pass code, by whatever means, can gain unlimited access to the premises.

HIDDEN CAMERAS

A wide variety of "spy cameras" are readily available through online or retail "spy shops". These are designed for covert installation in a home, workplace, or vehicle. Some are concealed within everyday objects such as a book, teddy bear, or clock radio, and thus may be hidden in plain sight. Others use "pin hole" technology, which permits the camera body to be hidden behind a wall while the separate lenses is so small that it can be easily overlooked.

> In 2002, a woman was shocked and terrified when she discovered her estranged husband, who still lived in the same household as her and their two children, had been video-taping her in her bedroom. What she had perceived as a small flaw in the wall of her bedroom actually turned out to be a pinhole camera. By using such a device, her estranged husband made sure it was easily overlooked by separating the camera lens from its body hidden in the wall. He connected the camera to his computer and watched her for weeks before being discovered. The woman notified the police and was granted a restraining order.

These cameras generally record the video in one of these ways:

- Saved to onboard flash memory: In this case, the perpetrator must (re)gain access to the camera in order to retrieve the memory card containing the stored video.
- Transmit over cellular or Wi-Fi networks to the remote perpetrator (in some cases, the perpetrator may need to be located nearby in order to be within range).
- Transmit the video in real-time over the Internet, using the existing data network on the premises.

It can be extremely difficult to locate these cameras once installed, and may require expert assistance. Cameras that transmit to a remote perpetrator can sometimes be detected by monitoring the data network on the premises, or by using detection equipment to locate unexplained wireless signals.

Recorded photos or video of a personal nature (e.g. nudity or sexuality) can be used to further victimize the target, for example, by sending to friends, family, or employers, or by posting on the Internet.

ID THEFT / IMPERSONATION

A stalker/abuser may steal a woman's identity for several reasons:

- To commit theft or fraud at her expense (e.g. purchase something on her credit card).
- To bring about negative financial consequences to her (e.g. negatively impact her credit rating).
- To embarrass or bring disrepute to her among family, friends, her employer, or professional colleagues. For example, a stalker could create malicious communications that (falsely) purport to come from her (e.g. create inappropriate e-mails to professional colleagues that appear to come from her).

An offender who can gain access to a woman's computer or smartphone (e.g. through use of a keylogger) can cause widespread harm in this manner. Since all such actions or communications apparently originate with the victim, it can be very difficult to "undo" the damage and establish that it all originated with someone else.

In some cases, the offender can readily impersonate the victim without requiring any special knowledge or technology. For example, Craigslist (an online classifieds ad service) offers personal ads, some of which express interest in casual "hook-ups". The offender may embarrass or even threaten the safety of the woman by posting a personal ad under her name, indicating (for example) that she likes to indulge in rape fantasies, and including her home address.

SPECIAL RISKS

This section outlines some special risks that can apply to (m) any of the above categories.

Keyloggers and other Spyware

Key logging software or hardware ("keyloggers") can be surreptitiously installed on a computer or smartphone, and can be very difficult to detect and remove. "Spyware" generically refers to keyloggers or other software that can be used to surreptitiously monitor a person's computer. These products can be readily procured from online or retail "spy shops", among other sources.

The offender does not necessarily need to gain physical access to the target device to install a keylogger, as many software variants can be surreptitiously delivered to the woman, either in the form of an e-mail attachment, or via a malicious web site link. In either case, the woman is tricked into downloading & installing the keylogger, usually without any suspicion that she has done so.

> In 2006, a man from Alberta was sentenced to one year in prison due to criminal harassment in the context of cyber-stalking. He used a type of computer monitoring software known as a keylogger to gain access to his ex-girlfriend's computer and monitor her activities. This particular type of spyware allowed him to record all keystrokes she entered, as well as receive electronically transmitted screenshots taken every few seconds. With this information, he created fake e-mail accounts under her name and sent her friends and co-workers embarrassing messages and nude pictures. He also hacked into her bank accounts, and cancelled her college enrolment. His ex-girlfriend was able to regain control of her personal accounts, but the damage caused by the leaked photos and forged e-mails was already done.

Keyloggers and other spyware can provide the offender with unfettered access to the woman's device and the information contained within it. Among other possibilities, keyloggers typically provide the following information to the offender:

- Screen shots taken every few seconds, which show all web browsing activities and other applications run on the device.
- Duplicates of all incoming and outgoing electronic mail, instant messaging and chat sessions.
- Web browser and other logs of online activities.
- Logging of all keystrokes, which reveal the passwords for social networking sites, bank accounts, and all security components.
- Some keyloggers permit remote control of a device's camera or audio recording capability without providing the usual external indication that these have been activated.

Access to the information provided by a keylogger will allow the offender complete access not only to the target device, but also to any online systems the woman accesses from that device. It does not matter if the woman changes her passwords or encrypts her communications on the compromised device, as all keystrokes are logged and this information will be forwarded to the offender (along with everything else the woman does).

The offender can also use the compromised passwords obtained to masquerade as the woman, to delete communications before she sees them, send false communications under her name,

and/or to commit financial crimes at her expense. Please refer to the "ID Theft/Impersonation" section above for additional information on this.

Bluetooth

Most portable computers and smartphones contain Bluetooth wireless technology, which permits short-range (3-5 meters) communication with peripheral devices such as cordless headsets. Many of these devices also allow "syncing" of information over Bluetooth. This can expose a victim's device to surreptitious access by the perpetrator whenever he or his device is in close proximity (e.g. ex-spouse while exchanging the children, or through a mobile phone provided to a child).

Users should disable any default access provided by Bluetooth, change any default password (to a strong password), or disable Bluetooth altogether if not otherwise required. The user should ideally also check her devices from time to time to ensure no one has made unauthorized changes to the Bluetooth or other configurations.

Search Engines and "Amateur Detective Work"

Search engines such as Bing or Google and online research techniques can allow a person to track and amass a great deal of personal information about an individual. Bits of information may have little value in isolation, but can reveal a great deal about a person once aggregated.

As just one example, a photo of a child on a social networking site may be tagged with a name, allowing an offender to easily find it using a standard Internet search engine. The photo may also be geo-tagged, indicating the approximate location where it was taken. Background details captured in the photo may provide very precise information about where the child is, and thus indicate where the child's parent is likely living.

Information contained within public records, news articles, and charity newsletters may similarly provide significant details to a stalker, especially when combined with other available information. It can be almost impossible for a person to avoid or erase these digital breadcrumbs.

Facial Recognition

Facial recognition software can be used to identify individual people in photos. Many personal digital albums now have this capability; once the user tags a single photo with the name(s) of those pictured, the computer will identify and tag all other photos containing the same person. Many social networking sites offer similar features. For example, a photo taken at a party may

include a woman or her child. Someone else could post that photo on a social networking site and tag it with her name, even though she would never do this herself. That photo and name may then be included in online search engines, so anyone else could discover it with a simple query.

While the technology remains less than perfect[23], facial recognition software is rapidly improving in capability and accuracy. Coupled with the proliferation of online photo albums and social networking sites, this is likely one more tool that will be used by offenders in their online "research" efforts.

Social Engineering

All security measures and legal protections ultimately depend upon people acting only as intended. A telephone company, for example, would probably have a policy that instructs employees to provide call records only to the account holder of record. Corporate policy and/or privacy legislation may prohibit disclosure to anyone else. However, none of these laws or policies are of any value if a person deliberately ignores them.

> In one 2007 case, a company executive was falsely accused of leaking classified information about employees, expenditures, and clients. Although recently divorced, the man in question never thought his ex-wife capable of going to the extent of hacking into his files and divulging confidential information under his name. His ex-wife, who had befriended his secretary on Facebook, found out the secretary had a relative fighting cancer, as well as her hobbies and favourite restaurants. His ex-wife called his secretary posing as a member of a charity raising money for cancer she often donated to, hence "explaining" how she had gotten her work number. When asked if she wanted to participate in a fund-raising draw and told that the prizes featured some of her preferred restaurants, the secretary did not hesitate to say yes. Without her knowledge, she allowed her boss' ex-wife to install spyware on her computer when she opened the fund-raiser "PDF", giving her access to all his files and contact information. Although he was not responsible for the harm done to the company, he felt he had no choice but to resign.

"Social engineering" refers to an infinite range of techniques by which an unauthorized person can gain access to a system or personal information by convincing an authorized person to do something that would otherwise be prohibited. These techniques may include outright deception (e.g. someone else masquerading as the account holder), or cajolery to encourage the employee to consciously ignore their instructions ("I need the call records to sort out a billing discrepancy"). An offender already in possession of some private information of the

[23] The Metropolitan Police in London found publishing CCTV images on "wanted" posters to be more effective in identifying rioters than current facial recognition software.

woman (however obtained) can appear particularly convincing, since they do not appear as a complete stranger.

Most people, especially those employed in customer service positions, want or are expected to be helpful to others, and may not appreciate the malicious potential of such queries. Constant training and reinforcement of privacy policies may be required to minimize the threat of social engineering.

Stalker in a Trusted Position

We depend upon other organizations (e.g. banks, service providers) to safeguard the personal information they legitimately hold about us. While these controls can potentially be defeated through social engineering techniques, an offender or someone in their network already in a position of trust may be able to gain significant quantities of personal information through their position employment.

> After ending what had been a serious five year relationship and moving cities, one woman started noticing unusual activity in her bank account. When unable to pay for a large bill with her credit card, she went to the bank and was told it exceeded her limit. Without too many problems, she was able to change it back to her original limit. Soon after, she noticed every one of her bills was being paid at least two or three times. She was always reimbursed for her "errors", but the process was long and she would often have to borrow money from her relatives to cover the time she spent waiting for her reimbursements. When she realised even her credit score had been altered, she asked for her situation to be investigated. She discovered that her ex-boyfriend had asked his friend, who was employed by the same bank, to make his ex-girlfriend "pay" for ending the relationship. Even though he worked in another city, he had access to confidential customer information and accounts. The ex-boyfriend and his friend were both charged for their actions; the friend in question lost his job; and the woman did not hesitate to change banks, a little too late.

For example, a police officer has direct access to a wide range of confidential databases, and can obtain additional information through enquiry (on the basis that many people and organizations will voluntarily cooperate with police "investigations"). A bank or telephone company employee can similarly access that organization's otherwise private databases. An offender may have a family member, friend or new partner with access to confidential databases that can relay information to them.

If a woman is concerned that a (potential) offender is employed in a position of trust, that organization should be approached directly with those concerns in order that specific oversight measures can be implemented (e.g. security audits of that person's database access). The woman may also wish to consider, if this is even possible, to switch her business to another provider.

Exploiting Children to Monitor the Other Parent

Parents no longer living together may engage in inappropriate monitoring of the other parent through their children.

A child's smartphone may have a keylogger or GPS tracking functionality installed by one parent in order to gain information on the other, or have Bluetooth configured to access the other parent's device(s) surreptitiously. A parent may ask a child to use the camera function of a laptop or smartphone to take photos or video of the other parent's residence, friends, workplace, etc. Some keyloggers permit remote control of a device's camera or audio recording capability without providing the usual external indication that these have been activated. A recording or GPS tracking device can be secreted inside a child's favorite toy.

> Spy equipment and other monitoring equipment are not hard to find. One divorced parent actually bought and installed a small commercial audio recording device in the ear of their son's favourite stuffed animal. A USB port in the stuffed animal's head would allow the parent to extract and access the audio data stored. The parent then asked the child to have the toy with him at all times when visiting their other parent. With this technology, the monitoring parent was able to listen to his/her ex's conversations with their son, track where they were going, and monitor the people they came in contact with.

Monitoring a child's online activities can also obtain information about other people. For example, the child's *Facebook* page may contain messages or photos involving the other parent.

A parent could also elicit significant information simply by questioning the child about activities with the other parent (e.g. where they went, who else was there, etc.).

Coerced "Consent"

A woman may be coerced into allowing an (future) offender access to her smartphone or computer, often while a relationship may still be in place. For example, the perpetrator may tell

her that since they're together, they should be sharing everything (including personal e-mail and bank accounts). Or, he may say that if she truly loves him, or has nothing to hide, she would have no reason not to provide him with access.

If he gains access in this way, he may already have her passwords. People often develop new passwords using patterns based upon personal information, and knowing one may greatly increase the probability of guessing others. Access to devices also provides complete opportunity to surreptitiously install keyloggers or other spyware, which can continue to be used long after a relationship ends. The offender could also claim that anything he did was with his victim's "consent".

One means of addressing is to have an expert erase and re-install ("wipe") any device(s) to which a stalker may have once had access. This will not eliminate any information already in his possession, but may reduce the possibility of him acquiring more.

Sex Tapes and Sexting

An offender may have intimate photos or video of a woman, especially if they were once in a relationship together, or if he has gained access to a computer or smartphone containing such images. Such recordings are not illegal so long as all participants consented.[24]

> It was only after she had broken up with her boyfriend that one 24 year old woman grew suspicious of her friends and co-workers' new behaviour towards her. Eventually, she found out from her family that her ex-boyfriend had sent out a sex tape they had consensually recorded. Feeling embarrassed and violated, she quit her job and tried to avoid people she knew. Although criminal laws exist in Canada that prohibits the recording of sexual activities made without the consent of all the participants, no crime prohibits the dissemination of such recordings. Her ex-boyfriend had therefore not broken any criminal law, and there was nothing she could do.

An offender may threaten to, or actually publish or distribute such recordings as a means of controlling or embarrassing her. A number of web sites and other Internet forums allow anyone to post pornographic content, and do not first require or verify informed consent from the persons depicted. Once posted online, anyone can copy or replicate the recordings.

[24] Any visual recording involving sexuality or nudity may constitute the crime of "voyeurism" if made surreptitiously or without the consent of any participant. Minors who record themselves are not committing any child pornography offences so long as all parties consent. However, any distribution to a third party automatically makes the recording illegal child porn as of that moment.

An offender may also distribute embarrassing content in ways that appear to make it come directly from her. For example, if he has access to her e-mail account, he could mail a sex tape to her family and professional colleagues under her own name.

It is not necessarily a crime in Canada for someone to maliciously distribute a private recording that was originally made consensually. For example, an “ex” could post a “sex tape” or picture on the Internet. Once distributed publicly, the damage may already be done, and continue to be done if others are able to replicate the recording further.

False Electronic Mail

It is very easy to fake the purported sender of an electronic mail message. While a technical expert can readily discern some methods, this may not be apparent to most recipients. An offender can thus send an embarrassing or other e-mail that appears to originate from her.

If the offender has access to the woman’s computer, smartphone, or e-mail account, he can send e-mail directly from her account. This would be much more difficult to detect and prove. For example, he could send false or embarrassing messages to her employer (e.g. a fake resignation letter) or family that appear to have been written by her, even though she actually has no knowledge of them. The recipient(s) may have no reason to question the messages’ authenticity, especially as they come directly from her e-mail account.

SECTION B: TECHNOLOGY SAFETY & PRIVACY PLANNING

INTRODUCTION

This section has two purposes. First, it provides tips on how to safely use technology to protect against violence against women. These are the kinds of systems that should become part of the every day practice of someone who has to contend with an offender. Second, this section provides a summary of some specific privacy-enhancing technologies (PETs) that can be used to help protect against violence against women.

There is some overlap between best practices and PETs. For example, WPA security on a wireless router may be characterized as a PET, but enabling it for use is a best practice. The overlapping suggestions have been left in the *Best Practices* section.

BEST PRACTICES FOR TECHNOLOGY USE

The following outlines some basic techniques anyone can implement to protect their privacy.

- Choose easy to remember but difficult to guess passwords. Most people choose passwords that almost anyone else can guess (e.g. birthdates or children's names). Choose a word or phrase that means something to you (i.e. is easy for you to remember), but no one else will think of. Longer is better. Capitalize random letters. Use a mix of letters and numbers. String multiple words together. Insert spelling mistakes or random spaces.
- Don't write down your passwords and then store in an obvious location (e.g. under your keyboard). Similarly, don't use the "remember me" or "auto-login" features offered by sites like Facebook and twitter. These features allow anyone with access to the computer to have full access to your accounts on those systems.
- Many systems now have "security questions" as backup to confirm your identity. Examples include the city where you were born, your birthdate, or the name of your first pet. Anyone who knows or has been stalking you will probably know this information too. Choose false answers (that only you would know) when you configure the responses to these security questions. For example, instead of saying you were born in City A (which you actually were); configure City B as the "answer" for that question. Just remember your false answers so you don't inadvertently lock yourself out of the system.
- Change your passwords regularly.
- If you're concerned that someone may have compromised your computer, use a safer one (e.g. at a public library) until you can have your concerns addressed. Don't use a

computer that may have been compromised to change passwords, as this will only allow the hacker to get the new passwords too.

- Do not use the same password on different sites or systems. If a password is compromised for whatever reason, it unlocks only one system, not your entire life.
- Do not share your password(s) with *anyone*. Once you've told someone else, it's out of your hands and control.
- Keep work and personal accounts separate, especially if your employer (or their staff) may be monitoring your computer use. For sensitive personal communications, choose user names and e-mail addresses that cannot be linked back to you (i.e. have no relation to your name or location).
- Get more than one e-mail account. There are a variety of free e-mail services (e.g. Gmail) that can be accessed from any computer. Use different accounts for corresponding with friends and family, for shopping, for social networking, online dating, etc. Keep a "private" account for ultra-sensitive communications, such as with your lawyer; don't give this account to anyone else. If it is necessary to communicate directly with the perpetrator (for example, to manage child visiting times) use a separate email account to communicate only with him, so that he will not have knowledge of personal accounts used to communicate with family or legal counsel.
- Remember that you have no idea who is at the other end when communicating by computer. The supportive person in a chat room could really be your stalker obtaining more information about you. An e-mail from a "friend" could be your ex masquerading online as your BFF. Use voice or face-to-face communications whenever possible.
- Configure startup and screen saver passwords on your computer, so someone who gains access to it can't simply start it up to gain access to everything.
- Keep your computer and other devices up-to-date with the latest operating system patches and security fixes. Unpatched security vulnerabilities are often exploited by "spyware". Install anti-virus software from a well-known vendor and keep the subscription current so that you always have the latest protection.
- Some smartphones and other portable devices now support a "remote wipe" function that allows the owner to erase all information if the device is lost or stolen. Enable this functionality if your device supports it, and know how to use it so you can do so quickly in an emergency.
- Don't use cordless phones for sensitive discussions, as these can be monitored by anyone in the area with a scanner. (This is not a concern with modern cell phones.)
- Beware of devices (e.g. smartphone) that can record audio or video, transmit, or identify location. These can be used surreptitiously to monitor or track you.
- Check your computer and smartphone regularly to ensure it is configured as you expect it to be. For example, don't enable Bluetooth if you have no reason to use it. Check regularly to ensure it remains off. Ensure it is protected with a password if you do. Do the same for other features that may be used to access your device or track your location (e.g. tracking services such as Google's *Latitude*, geo-tagging of tweets). Ask a trusted friend or colleague to assist you with these sorts of checks if you don't consider yourself "tech savvy".

- Remember that it only takes seconds for someone to install a keylogger on your computer or smartphone. Don't allow anyone to "borrow" your computer or phone, especially if you have reason not to trust them.
- Be cautious of (potential) offenders giving gifts such as smartphones or other items that
- Do not allow your children to use your computer. If you are not in a position to purchase additional computer(s) for them, configure separate accounts with limited access on your computer, and ensure you have logged out of your account before allowing them access.
- Be suspicious of e-mail attachments and web links, as these can be used to surreptitiously install spyware on your device. Install anti-virus software and keep it up to date.
- If you have Wi-Fi in your home, ensure it is configured with strong security (i.e. WPA2) and a strong password. Disable guest access. Configure your device to ask before connecting to new networks, so you don't inadvertently connect to a rogue Wi-Fi.
- Dial *67 or other applicable code before making each call to block Caller ID information from being transmitted to the recipient. Have your telephone company configure your lines (both landlines and mobile accounts) to block Caller ID from being sent back to anyone who calls you. Have your phone company configure your telephone number(s) as "unlisted" so they do not appear in online or other directories.
- While it won't protect you from a stalker, adding your telephone number(s) to "Do Not Call" registries may help limit the number of intrusive calls you receive from strangers.
- Name your computers, portable devices, and peripherals with labels that do not identify you. Many devices broadcast this information to everyone nearby. For example, it's probably no secret who "Joan's computer" belongs to. Or use false names.
- Share any safety concerns with trusted friends and family. Explain to them the importance of not sharing *any* information about you with *anyone*.
- Be suspicious of any "gift" that someone insists you keep with you at all times, or place in a particular location in your home, as it could contain a hidden camera or listening device.
- Be cautious about the private information you post on social networking sites, etc. A small bit of information may not mean much in isolation, but can be enormously useful to someone else when combined with other bits of information.
- Search online for your own name. Know what's out there about you, whether true or not.
- Trust your instincts. Someone who always seems to know more than they should about you, or always seems to be running into you, may be surreptitiously monitoring you. Ask yourself how they could have obtained that information. Could they be monitoring your phone calls? Have compromised your computer or are reading your e-mail? Installed a tracking device in your car so they can follow you?
- Be alert to the possibility that someone is using your children to monitor you, especially if your children have electronic devices or always have a favorite doll or toy with them.

- Never allow anyone to photograph you while nude or in sexual contexts. Think twice about sending a photograph of yourself while nude or in sexual contexts. You have no idea what they will do with the photos or how many copies may be made.
- Be aware of social engineering techniques and be on guard for them. Verify the source and authenticity of all information before acting on it, including e-mail attachments and web links, even when ostensibly from someone you know. If you receive a telephone call or message from a potentially doubtful source (e.g. the local courthouse), you can always verify the information by calling back using a number you've independently obtained from a public source (e.g. telephone directory or the organization's web site). Don't use the Caller ID or other information contained in the original message, as it may be bogus.
- Don't hesitate to seek professional help if you suspect someone is stalking you or may have accessed your computer or smartphone. Call the police and your lawyer. They have access to experts who can get to the bottom of your concerns.
- Consider installing an alarm system with a "panic button" feature.
- If someone whose behavior you are concerned about works at your bank, telephone company, or other business that holds sensitive information about you, consider switching your business to a different company. As an alternative, you may wish to discuss any concerns you have with the company's privacy officer, so that they may implement additional safeguards on your account.

Privacy Enhancing Technologies

Introduction

This section outlines some tools that can be used by women to protect themselves when using technology. It includes specialized tools as well as features of commonly used software such as Firefox, which could be useful. This section should be read in conjunction with the section above, *Technology Safety Planning*.

This is not meant to be an exhaustive list. These suggestions are compiled based on a broader category of privacy-enhancing technologies, many of which seek to protect users from online tracking by advertisers. Many of those tools do not target the kinds of invasion experienced by and which are most dangerous to victims of technology-enabled abuse. These suggestions focus on readily available and easy to use tools that will help protect victims from the most common types of technology-enabled abuse.

Use of these tools should not be regarded as protective armour that can repel all dangers. To see technology that way is a mistake and can, for victims of cyber-stalking, be very dangerous. These are tools, forming part of a broader package including good personal technology use habits, police and support networks that include professionals, friends, and family, which together can help protect victims of cyber-stalking.

Note: many of these tools can easily be defeated by a keylogger. See details on key loggers and social engineering in the previous section.

Web Browsing

Most web browsers include a "private browsing" function. This can be used to automatically wipe cookies and cached data when the browser is shut down. This can prevent other users of the same computer from knowing what sites were visited. This could be useful (unless spyware or a key logger has been installed) to someone living with a perpetrator, who is thinking about leaving, and needs to do online research about her options.

Similarly, there is a "portable" version of Firefox, which can be installed on a USB drive. When used, its cache files are kept separate from other installed web browsers making it more difficult for others to know what web sites were visited. None of the browser history or cache files are stored on the computer itself.

Finally, some Linux distributions make available a "live CD". Live CDs are used for evaluating an operating system before installing it on the computer. They allow the user to boot Linux from the CD, and use it as if it was installed on the computer, including the native Linux web browser. When the CD is removed and the computer is rebooted, the browsing history is not left behind.

Computer Security

A number of vendors provide anti-virus and firewall software for computers as well as mobile phones. Some of these are comprehensive home internet security packages. These aim to protect the computer from being infected with viruses, preventing unauthorized remote access to the computer and preventing keyloggers installed on the machine from "calling home" to the person who is controlling them.

Security software provides two types of protection particularly relevant to cyber-stalking. First, the anti-virus component can prevent email or web-based installation of key loggers on the computer. Note that this is only effective to detect well-known spyware tools and may not work for more targeted "spear phishing" attacks. Second, the firewall component can prevent key loggers that are already installed from sending any data back to the perpetrator.

Anti-virus and firewall tools are not perfect. The virus signatures must be kept up-to-date through paid subscription services, and even then there can be errors or deficiencies in the software. In addition, clever authors of malicious software are constantly finding ways to avoid their key loggers from being detected by anti-virus software.

Data Security

Certain sensitive files, for example, documents from a lawyer, must be treated with additional care in case the machine on which they're stored is compromised. The files must be stored properly, and they must be deleted properly. Some advanced computer skills are required to use these tools properly. If not used properly, the user will have a false sense of security which may be more dangerous than not using the tools at all.

For proper storage, there are free file encryption tools available, for example, *TrueCrypt*. This software, which is free, lets the user create encrypted "containers" on their hard disk or a USB drive. These can be hidden or visible. The sensitive files are stored in the container and are automatically encrypted. The user must never forget the password otherwise the files cannot be recovered.

For proper deletion, there are also free tools available for "wiping" sensitive files from the hard disk. Note that simply deleting files does not necessarily remove all traces from the hard disk, though it would require a highly skilled individual some time to recover them. Wiping tools, for example, *Eraser*, allow the user to completely wipe all data associated with a particular file or folder, from the hard disk. Other wiping tools, for example *DBAN*, can wipe an entire hard disk.

Email

Where email communication with the perpetrator is necessary, it's better to do it without supplying a real email address. This can be done using anonymous remailers or disposable email addresses.

Disposable email services offer a temporary email address which ceases to exist after a fixed amount of time, for example, 60 minutes. These can be used for one-time messages that need to be sent to a perpetrator, or with some services, for carrying on short email exchanges that are completed within the time limit. This provides a simple way for someone to communicate via email without revealing her real address. Note that some of these services do not guarantee the privacy of the emails.

Anonymous remailers allow the user to "mask" their real email address, by sending messages via the remailer. This lets them use their own email account, but without revealing the real address to the person at the other end of the communication. Anonymous remailers support sending and receiving emails. There is a wide variety of types of remailers with differing degrees of anonymity for their users.

As with the file encryption and wiping tools described above, these tools must be used properly to be effective. If not used properly, they may be more dangerous to the user than if not used at all.

RECOMMENDATIONS

Individuals and agencies can do their best to take necessary steps to safeguard their information. They can use good encryption and passwords, minimize collection of data and keep confidential the identity of survivors using VAW programs. But they can't decide how advertisers will be using facial recognition in shopping malls.

If technology developers, providers and users are serious about preventing technology from being wielded by perpetrators to further abuse and terrorize women, youth and children, then we need them to listen to how the lives of women and youth are impacted and then:

(1) Design and implement technology to ensure privacy rights and protections for everyone who uses it. By default, we should be opted out of any new feature that contains privacy intrusive features. Explanations about privacy risks should be clear.

(2) Demonstrate how each technology design provides sufficient protections for the privacy and safety rights of individuals who will face statistically higher risks to their safety and wellbeing. For example, women, youth, people with disabilities, the elderly, Aboriginal women, and other groups who face a statistically higher chance of experiencing violence if their privacy and security needs are not adequately anticipated.

(3) Have all privacy impact assessments of information technology identify and robustly address the specific risks faced by survivors of domestic violence, sexual assault, stalking, harassment and other types of violence against women and youth. This might be accomplished by incorporating a specific type of danger/risk assessment/analysis as a formal step in all standard privacy impact assessments and ongoing privacy management tools.

(4) Treat all personally identifiable information about abuse survivors as "highly sensitive information"

(5) Address any system functions, policies or practices that are known or can be anticipated to increase privacy and security risks for women, youth and children who are living with or have been impacted by sexual violence, domestic violence, harassment and stalking.

APPENDIX A

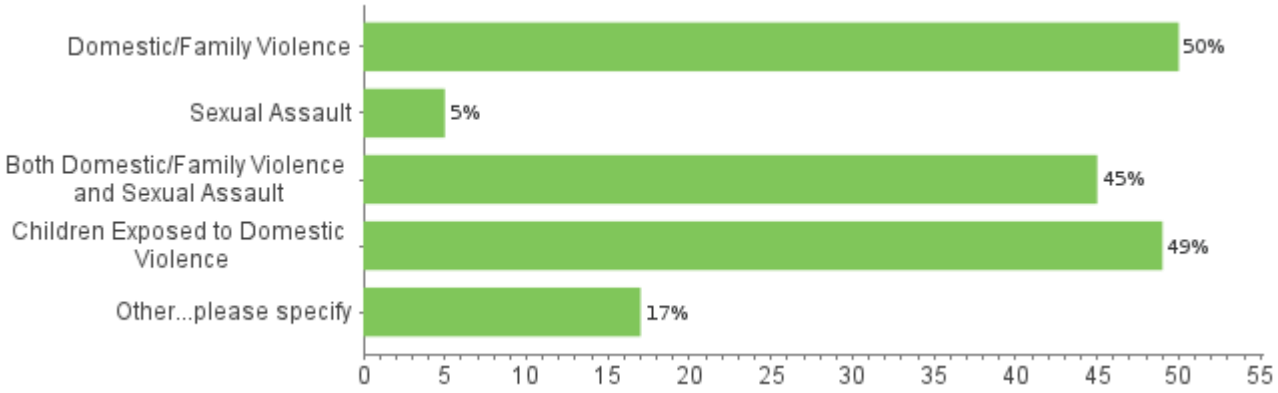
Summary Report: Organizational Technology Practices Survey for Violence Against Women Programs

Section A: Background Information about your VAW Program

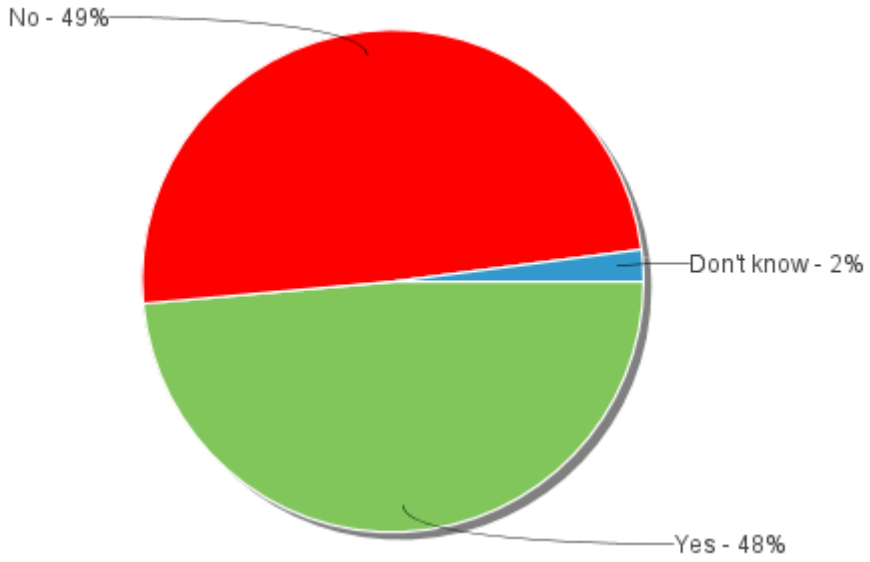
1. Canadian Province/Territory where you work:

Response	Chart	Percentage
Ontario		5%
Quebec		25%
Nova Scotia		7%
New Brunswick		1%
Manitoba		5%
British Columbia		46%
Prince Edward Island		0%
Saskatchewan		2%
Alberta		5%
Newfoundland and Labrador		1%
Northwest Territories		2%
Yukon		1%
Nunavut		0%

2. Type of VAW Program

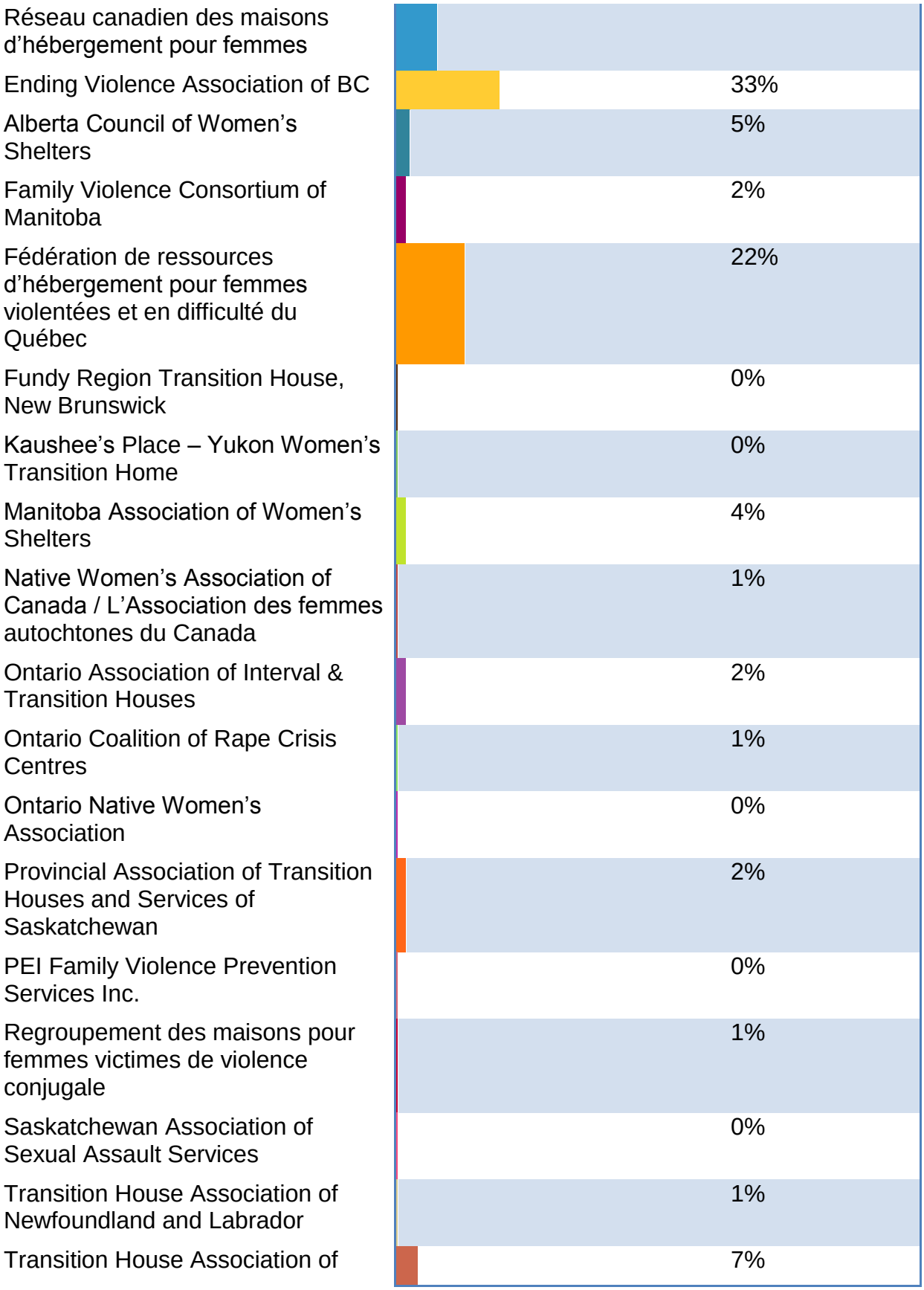


3. Is your VAW program part of a larger multi-service organization?



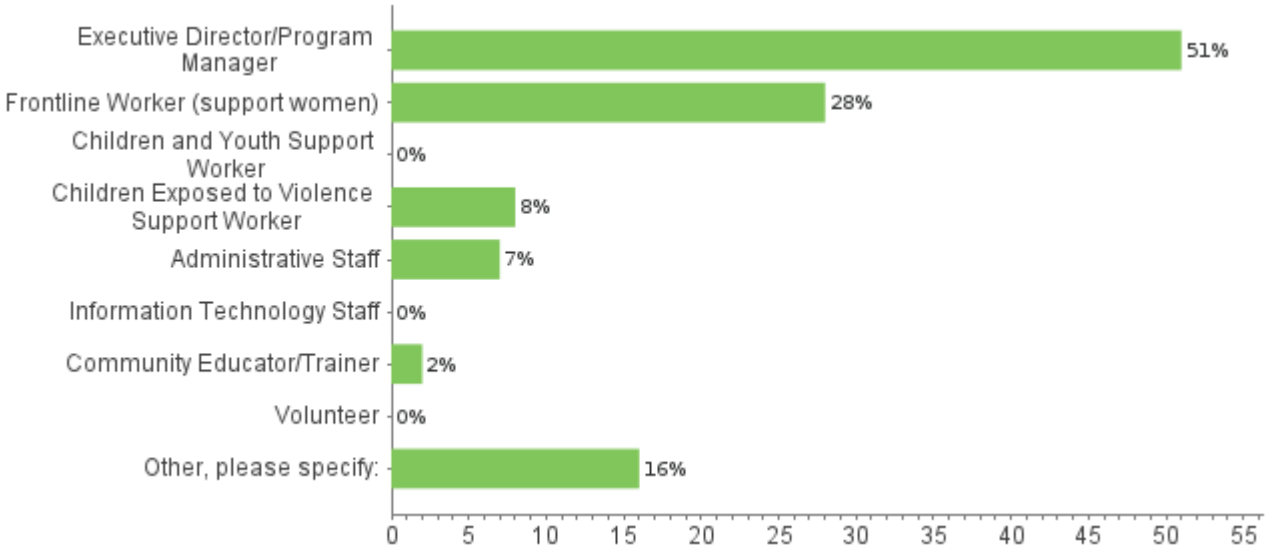
4. Is your VAW program a member of any of the following provincial, territorial, Aboriginal, or national association?

Response	Chart	Percentage
BC Society of Transition Houses		29%
Canadian Association of Sexual Assault Centres/Association Canadienne des centres contre les agressions à caractère sexuel		2%
Canadian Network of Women Shelters and Transition Houses /		13%


Réseau canadien des maisons d'hébergement pour femmes
Ending Violence Association of BC
33%
Alberta Council of Women's Shelters
5%
Family Violence Consortium of Manitoba
2%
Fédération de ressources d'hébergement pour femmes violentées et en difficulté du Québec
22%
Fundy Region Transition House, New Brunswick
0%
Kaushee's Place – Yukon Women's Transition Home
0%
Manitoba Association of Women's Shelters
4%
Native Women's Association of Canada / L'Association des femmes autochtones du Canada
1%
Ontario Association of Interval & Transition Houses
2%
Ontario Coalition of Rape Crisis Centres
1%
Ontario Native Women's Association
0%
Provincial Association of Transition Houses and Services of Saskatchewan
2%
PEI Family Violence Prevention Services Inc.
0%
Regroupement des maisons pour femmes victimes de violence conjugale
1%
Saskatchewan Association of Sexual Assault Services
0%
Transition House Association of Newfoundland and Labrador
1%
Transition House Association of
7%

Nova Scotia	
YWCA Yellowknife	1%
Other: please specify	13%

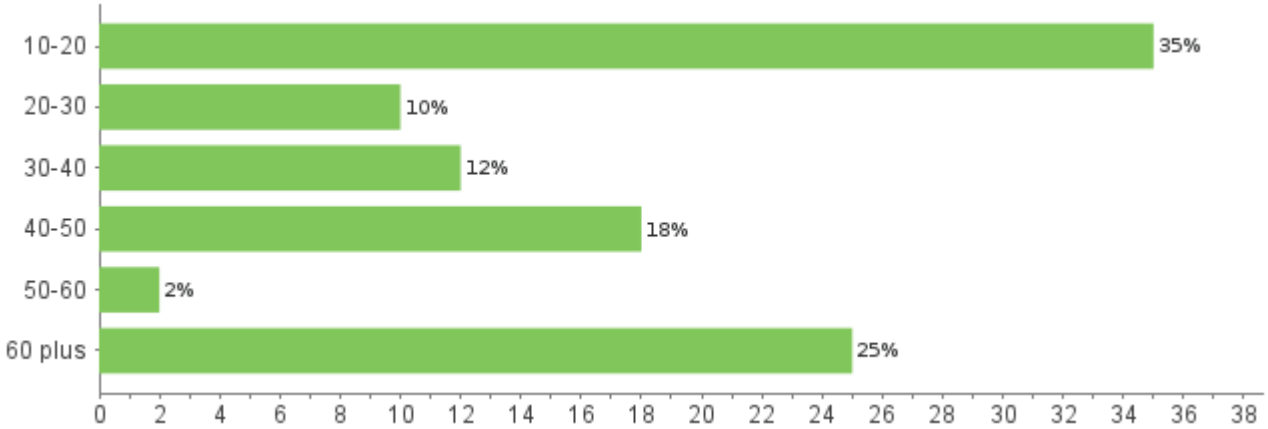
5. What best describes your role in your agency?



6. How many paid staff work in your VAW program/s?

The responses ranged from 1-225 paid employees.

If your VAW program/s is in a larger multi-service agency approxiamtely how many paid staff work in your entire agency?



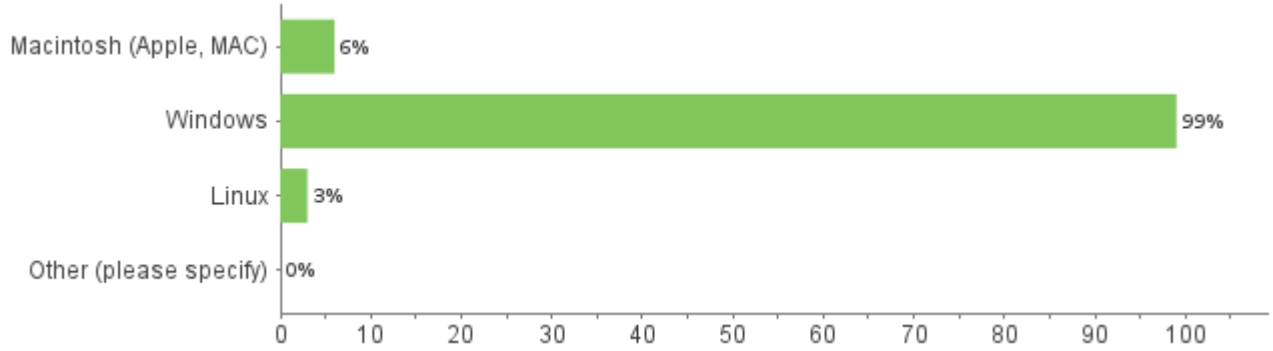
7. If we have questions about your survey response, may we contact you via email? If yes, please provide an email address:

67 respondents provided their email address.

Section B. What Types of Technology Does Your VAW Program Use?

You may need to ask your coworkers some of these questions. Your answers to this section will provide the VAW sector with a better understanding of the types of technology that our Canadian VAW Programs are using. We are interested in learning about technology: owned and maintained by your program/organization and personally owned by staff, volunteers and consultants who do work for your VAW program.

8. What Computer Operating Systems (OS) does your organization/VAW program use?



9. What types of Equipment/Devices does your VAW program use?

Response	Percentage
Laptops (and Netbooks)	78%
Desktop Computers	99%
Mobile Tablets (iPad, Android, etc)	13%
Computer Server	36%
USB sticks	81%
Memory Cards (often used in digital cameras)	41%
Portable or desktop backup	28%

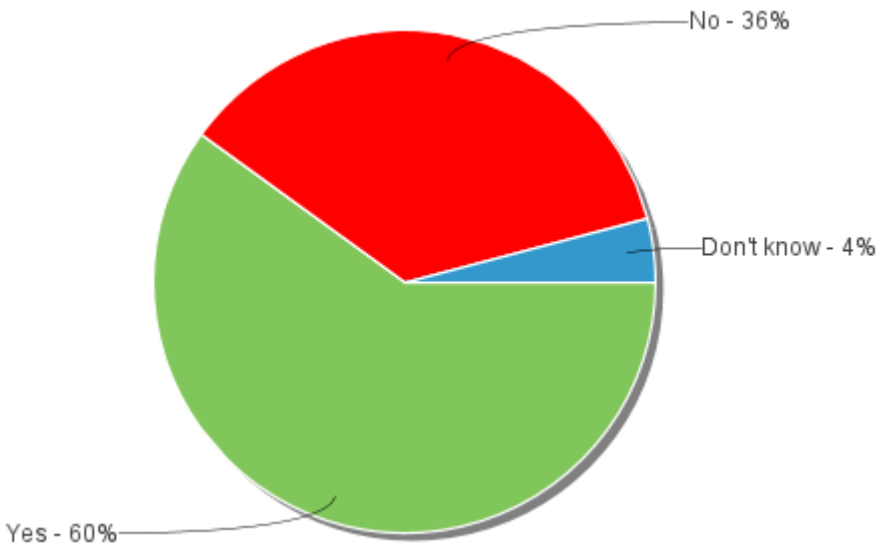
drives	
Office Phone System	85%
Individual voicemail boxes	60%
General voicemail box accessed by several people	31%
Corded Phones	85%
Cordless Phones	47%
Basic Mobile / Cell Phones (phone plan has calls, texts, voicemail)	55%
Mobile/ Cell “Smart” Phones like iPhones, Blackberry, Android that can access the Internet	44%
Pagers	5%
Multi-purpose copier and fax machine	88%
Stand alone fax machine	35%
Web camera (plug-in device or built into a computer/mobile phone or tablet)	29%
Security/Surveillance Camera for inside buildings	23%
Security/Surveillance Camera for outside buildings (entrances, parking, etc.)	59%
Video / Digital camera (take photos at events, create videos, etc.)	50%
Cameras (to record evidence of abuse)	21%
Alert Devices (accessibility and safety devices that vibrate or/and flash lights when sounds go off like fire alarms, alarm clocks, door bells)	41%
TTY / TDD (Teletypewriter or Telecommunications Device for the Deaf)	9%

Video phone (often used to communicate with sign language interpreters)	1%
Other (Please specify)	9%

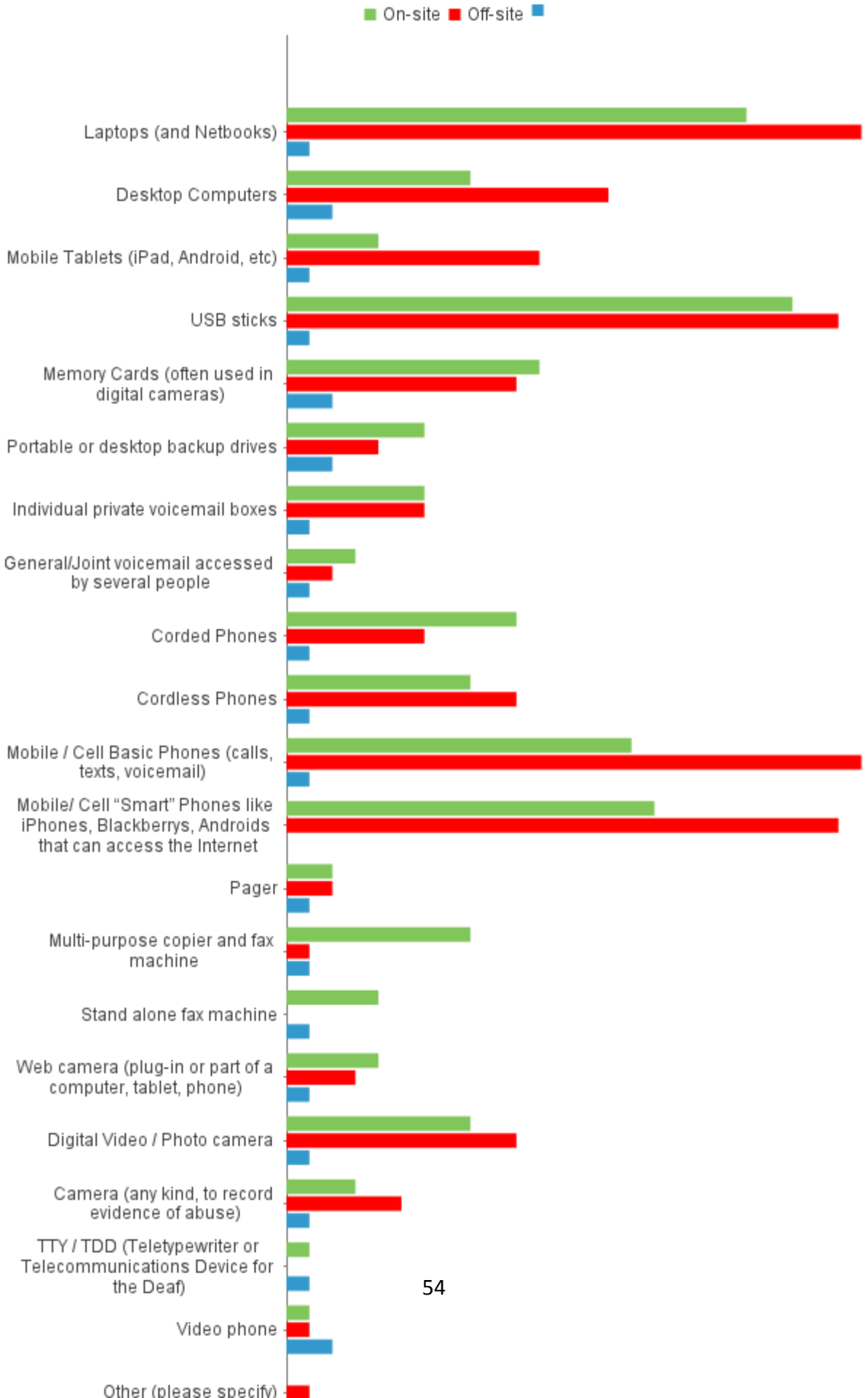
Other:

#	Response
1.	Panic buttons for staff. Press button and RCMP respond.
2.	panic button alarm systems
3.	appareil pour personnes sourdes à venir
4.	life line for staff security
5.	Lifeline Security Pendants x 3
6.	système de sécurité pour l'immeuble
7.	Projecteur

10. Does your VAW program's work ever involve using Equipment/Devices that are personally owned by staff, volunteers, or consultants?



11. If yes, which technology personally owned by staff, volunteers or consultants is used onsite (in VAW program offices) or/and offsite (at the person's home and elsewhere) for VAW program work?


On-site
Off-site
Laptops (and Netbooks)
Desktop Computers
Mobile Tablets (iPad, Android, etc)
USB sticks
Memory Cards (often used in digital cameras)
Portable or desktop backup drives
Individual private voicemail boxes
General/Joint voicemail accessed by several people
Corded Phones
Cordless Phones
Mobile / Cell Basic Phones (calls, texts, voicemail)
Mobile/ Cell "Smart" Phones like iPhones, Blackberrys, Androids that can access the Internet
Pager
Multi-purpose copier and fax machine
Stand alone fax machine
Web camera (plug-in or part of a computer, tablet, phone)
Digital Video / Photo camera
Camera (any kind, to record evidence of abuse)
TTY / TDD (Teletypewriter or Telecommunications Device for the Deaf)
Video phone
Other (please specify)

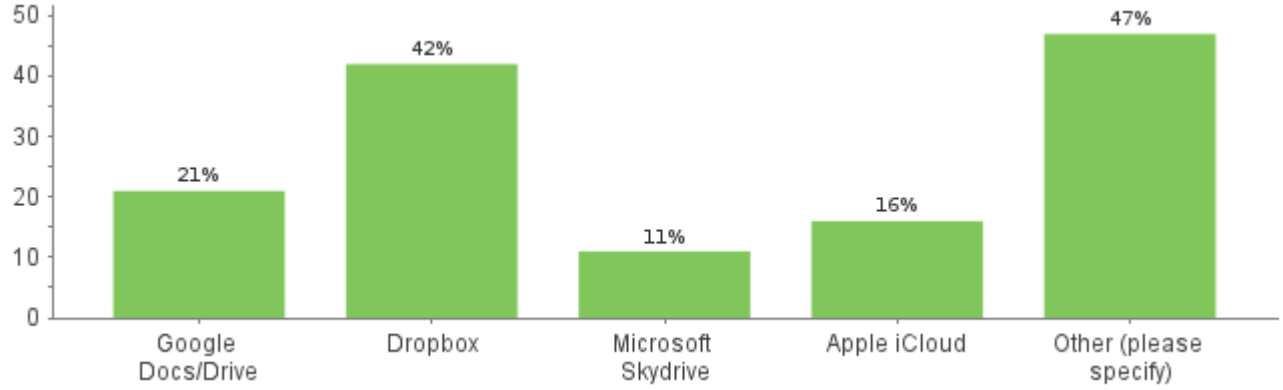
12. How do you store the information that your VAW program collects (financial files, participant records, etc.)?

Response	Chart	Percentage
Paper files in cabinets		95%
Individual computers only (not a network server)		37%
In-house Server (a computer server located inside your offices. Server stores some of the VAW program files or applications and provide access to them via your network.)		45%
Third-party Hosted Server (a server located offsite that you rent space on. Other people own the server and maintain your network security and access.)		15%
Cloud Computing or other Online Data storage		17%
Other (please specify)		8%

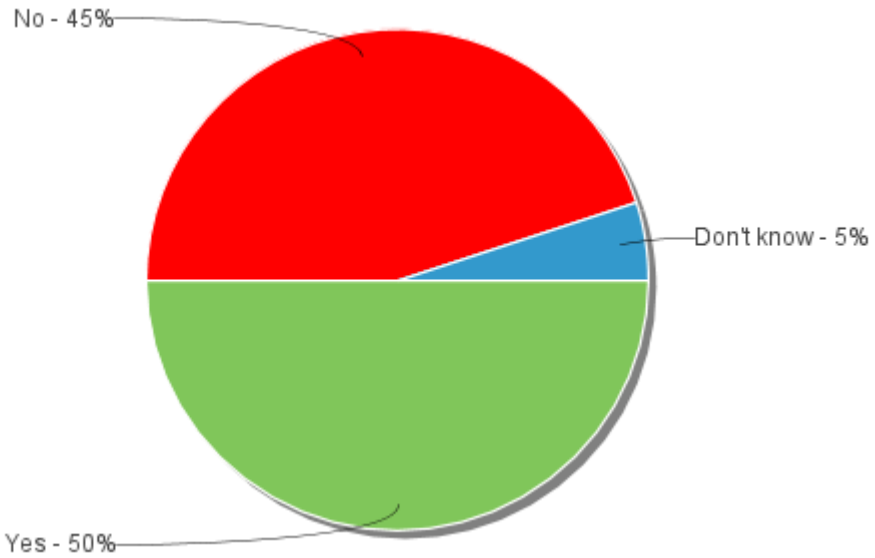
Other:

#	Response
1.	thumb drive
2.	data sticks
3.	moving to a server this year
4.	stats on flashdrives
5.	considering networking, have a nonfunctioning netweorker server, would like to have off site financial data storage
6.	Clé USB

13. If you use cloud computing or other online data storage to edit or store files, what do you use?



14. Does your VAW program (or broader organization) use databases to collect and store information about clients? (by client information, we mean information about women, youth and children who request and/or are provided services and support).



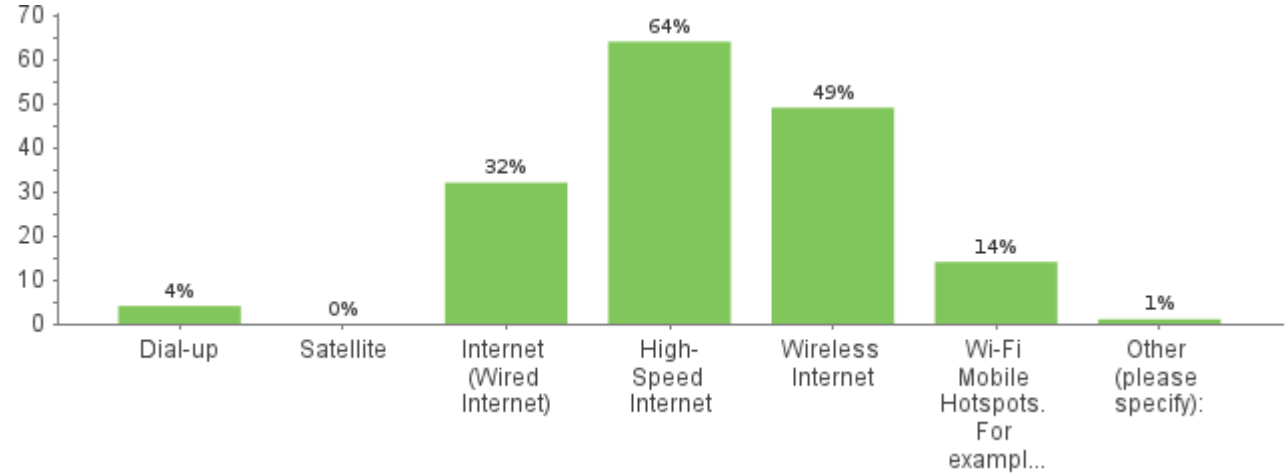
15. If yes, please describe the database/s your VAW program and/or organization uses to hold information about participant?

The 38 response(s) to this question can be found in the appendix.

Response	Chart	Percentages	Count

Databases Used		26%	10

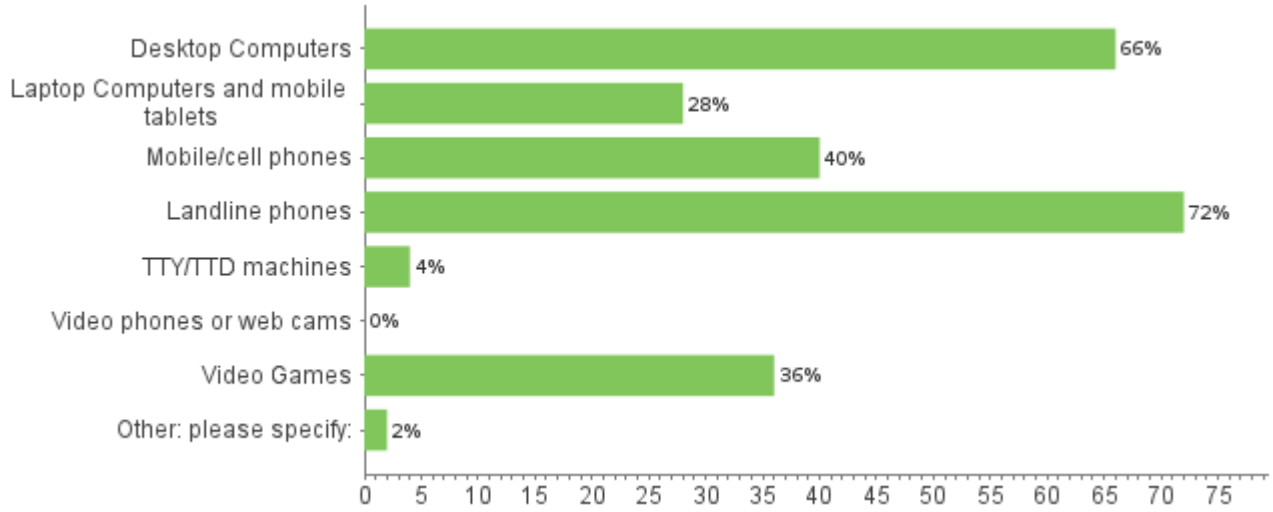
16. How does staff access the internet?



17. How do participants or visitors to your VAW program access the Internet?

Response	Chart	Percentage
We do not provide any Internet access to participants or visitors.		33%
We provide Internet access to people who visit or receive VAW program services.		22%
We run a women's shelter or transition/interval house, and only provide wireless Internet access for shelter/house residents.		30%
We provide participants/residents/visitors with access to an Internet network that is separate from our staff/employee network?		17%
Other		11%

18. Does your VAW program own or rent technology that you let participants use onsite or offsite?



19. Which online and social media platforms does your VAW program use?

Response	Chart	Percentage
Website		73%
Blog or Vlog (video online blog)		9%
Online discussion forum or chat rooms		3%
Facebook		44%
MySpace		1%
Google+		13%
Tumblr		0%
Pinterest		3%
Reddit		0%
Twitter		20%
YouTube or other video sharing site		13%
Flickr or other photo sharing site		1%
Online games or virtual worlds		3%
None		20%
Other (please specify):		4%

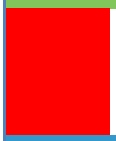
20. Why does your VAW program use social media?

Response	Chart	Percentage
Education/Awareness		91%
Fundraising		53%
Connect with other advocates, agencies, and allies		53%
Outreach to women		64%
Not sure		5%
Other (please specify):		7%

Other:

#	Response
1.	get picture of male partner form facebook
2.	we have not as of yet used only our web site
3.	We don't
4.	Connect with community members

21. How does your VAW program staff your social media presence?

Response	Chart	Percentage
Have a dedicated person to manage your social media		26%
Have a communications person whose job includes managing your social media		25%
Have one or more staff who share the job of updating your social media presence		42%
Other (please specify):		21%

Other:

#	Response
1.	
2.	pay honorarium, no one here has time

3.	Have hired someone to create a website
4.	outside resource
5.	We don't
6.	website is old, was put up years ago, not sure who maintains it but it's not all that in depth or useful
7.	Responsibility of ED
8.	self
9.	one staff as a side job
10.	usually me although I have farmed out to term staff a few times
11.	volunteer

22. Are any of these technologies used in office or offsite to communicate with or about the women, youth and children who are VAW program's service recipients?

	Yes	No	Don't know
Corded phones	91%	6%	3%
Cordless phones	50%	44%	6%
Cell/Mobile phones	80%	17%	3%
Internet-based phones (VoIP, Voice over Internet Protocol, calls like Skype, Vonage, Google Voice, use the internet rather than a traditional phone line)	18%	78%	5%
Text messages	57%	39%	4%
Pagers	3%	95%	3%
Caller ID (to screen, identify or sometimes block callers)	70%	30%	0%
Fax Machines	92%	6%	2%
Electronic Faxes (faxes received via email)	49%	44%	7%
Email	88%	12%	0%
Instant Messaging (online chats such as AIM, Google Chat)	5%	92%	3%
Relay Services (3rd party	22%	68%	10%

operator relays communications between the technology used by your worker and the offsite person who is Deaf, hard of hearing or has speech disabilities)			
Video Remote Interpreter Services (uses a web cam or video phone to connect the survivor/client and worker to an offsite sign language translator)	2%	92%	5%
Video Communication Software (such as iLink, GoToMeeting, Skype so survivors/service recipients can communicate with attorneys, friends, family, etc.)	8%	82%	10%

Section 3: Policies & Practices

These questions will help us understand the types of policies, practices, and procedures your agency has around using these technologies. The policies can be formal (agency policy manual) or informal (general understanding of proper protocol around using a particular technology).

23. What technology security and maintenance practices do you have to manage your VAW program's technologies?

	Yes	No	Don't know
anti-virus/anti-spyware protection installed on your individual office computers	97%	0%	3%
anti-virus/anti-spyware protection installed on your VAW program /agency server	67%	24%	9%
a dedicated Information Technology (IT) staff person or IT company/consultant who manages your VAW program's IT needs	53%	38%	8%
If your office has wireless Internet, is it protected with a password?	86%	5%	9%

If your office has wireless Internet, have you taken other security steps such as enabling strong encryption or limiting access to known computers/devices (by MAC address)?	24%	36%	40%
Does your agency provide a unique user name and password to each person who must access your agency's computers or networked server?	63%	32%	6%

24. If you have databases that store confidential, private and identifying information about people, does your organization do any of the following practices?

Response	Chart	Percentage
Password protect the database.		88%
Provide a unique user name and password to each VAW program worker who has access to use the database.		76%
Limit access to databases based on job roles. This may include limiting access to certain fields and client records.		73%
Ensure that third party IT consultants do not view the records in the database when fixing problems, doing routine maintenance or upgrades.		59%
Other		10%

25. Does your VAW program/organization have policies and practices that address safety, privacy, confidentiality and security for the following technologies?

	Yes	Being	Don't know

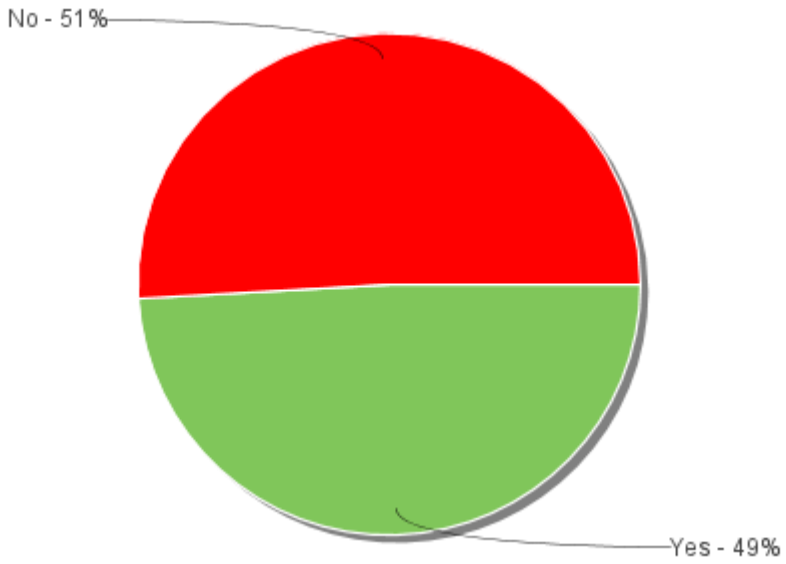
		developed	
Social media: regarding work-related social media use	40%	40%	21%
Social media: regarding personal (non-work-related) social media use	40%	38%	22%
Recording or retaining photo or video images (whether for evidence collection or security/surveillance)	42%	35%	23%
Staff/worker use of personally owned technology onsite or offsite for the VAW program's work	38%	31%	31%
Participants use of personally owned technology devices and services (laptops, cell phones, tablets, cameras, location sharing or mapping) onsite	41%	28%	31%
Participants use of technology the VAW program owns and makes available: desktop computers, mobile phones, video games, etc.	47%	26%	28%
Providing Internet access for participants	52%	26%	21%
Use of location mapping, tracking, sharing or tagging devices and services in all aspects of your work	23%	43%	34%
Using Virtual Private Networks (VPN's) to access files remotely	24%	39%	37%

26. Does your VAW program have policies and practices that address safety, privacy, confidentiality and security for using technology when communicating with or about the women, youth and children and others who contact you or receive services and support?

	Yes	N/A	Being developed	Don't know

Land-line Corded and Cordless phones	65%	12%	14%	11%
Mobile/cell phones	63%	15%	15%	8%
Fax machines and e-faxes	70%	14%	8%	8%
Text messages	32%	45%	13%	12%
Pagers	7%	77%	5%	12%
Pay as you go phones	14%	70%	5%	11%
Location mapping, tracking, sharing or tagging tools	17%	51%	17%	17%
Email	62%	19%	12%	8%
Instant Messaging	13%	57%	13%	19%
Web cams or Video phones	18%	58%	11%	15%
Social Media	32%	37%	18%	15%
Relay services	9%	69%	9%	15%
Remote Video Interpreter services	4%	79%	8%	12%
Online Counseling or Service Provision	18%	60%	9%	14%
Technology personally owned by staff	26%	42%	15%	17%
	16%	53%	16%	21%

27. If your organization is a provincial, territorial, Aboriginal or national association that has a primary purpose of representing and supporting local community-based VAW programs, are you working with your membership to develop policy and practice standards for VAW programs?



28. Which organizational technology policy and practice standards would your VAW program most like to see developed to address and protect safety, confidentiality, privacy, personal identity and security of workers, women and children.

Response	Chart	Percentage
Social media and networking		75%
Electronic communication (email, instant messages, texts, phones, VoIP, webcams, video conferencing, skype, etc.)		70%
Data and databases		57%
Technology use in counseling and service provision (email, real time instant messaging, live video, group chat rooms, video conferencing, Internet-based phone calls, etc.)		57%
Evidence Collection		38%

Mobile phones and other devices	58%
Location tracking, mapping, sharing and tagging devices and services	53%
Technology safety and privacy planning	60%
Identity protection planning	50%
Other (please specify):	8%

Other:

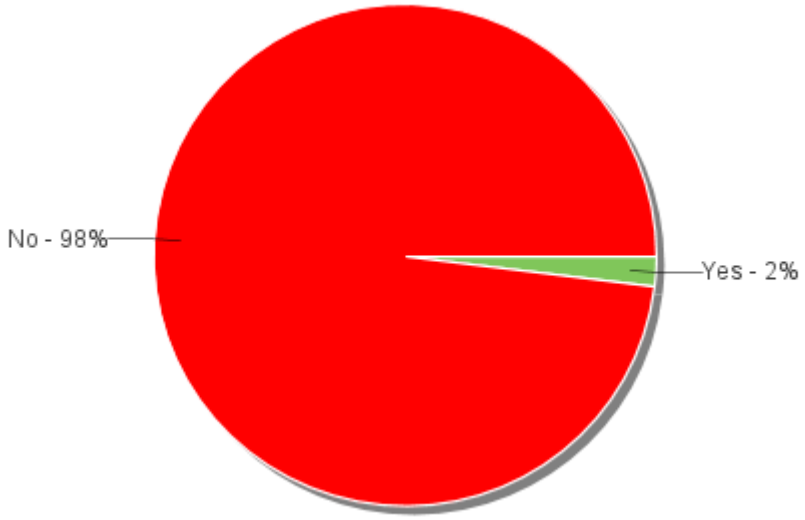
#	Response
1.	
2.	
3.	This is ongoing as tech. changes
4.	very uncertain what is needed
5.	education programs for clients so they are aware of technology use can put them at risk.

29. What barriers does your VAW program face in developing technology policies and practices that address safety, confidentiality, privacy, personal identity and security issues?

Response	Chart	Percentage
Lack of staff		49%
Lack of funding		68%
Lack of time		67%
How quickly technology changes and new technology appears		57%
How often technology companies (like Google, Facebook, Twitter) change their privacy policies		29%
Lack of knowledge or training on technology or on security steps		62%
Lack of knowledge or training on privacy and confidentiality laws and regulations		48%

Need more examples, samples or adaptable templates of technology policies and practices for VAW programs		61%

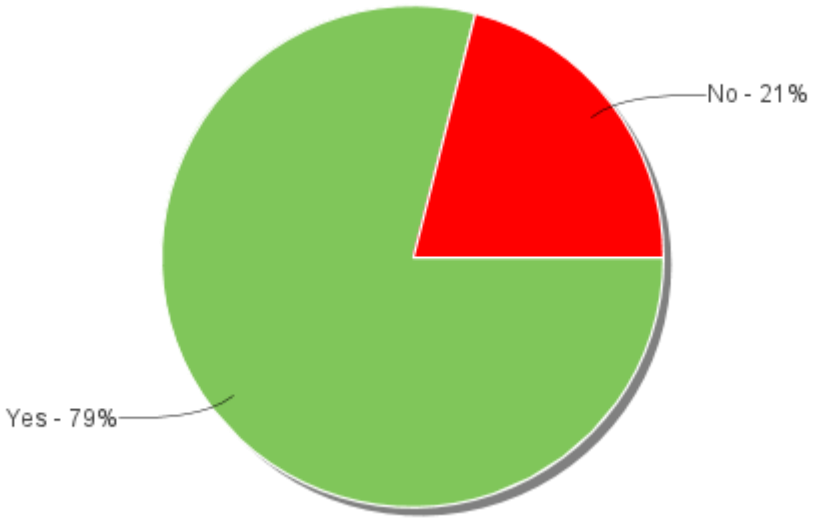
30. Do you have technology practices or policies you are using that you really like and would be willing to share as examples for other VAW programs?



31. Is there anything else you would like to share with us in this survey?

There were 7 responses to this question.

32. Would you like more information in the future when we have webinars and resource materials available?



If yes, please provide the email address(es) you want us to send announcements about future trainings and resources:

There were 52 responses to this question.

We thank you in advance and acknowledge NNEDV Safety Net for letting us adapt their survey. Your answers will help inform the work of Safety Net Canada.

APPENDIX B

Summary Report: Survey of Anti-Violence Workers on Technology Abuse

1. Canadian Province/Territory where you work:

Response	Chart	Percentage
Ontario		11%
Quebec		14%
Nova Scotia		3%
New Brunswick		1%
Manitoba		16%
British Columbia		36%
Prince Edward Island		2%
Alberta		11%
Newfoundland and Labrador		6%
Yukon		2%

2. Type of Program

Response	Chart	Percentage
Domestic/Family Violence		55%
Sexual Assault		5%
Both Domestic/Family Violence and Sexual Assault		38%
Other, please specify...		8%
	Total Responses	

3. What is your role in the anti-violence agency or program?

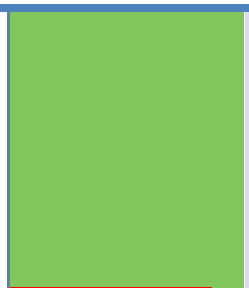
Response	Chart	Percentage
Executive Director/Program Manager		43%
Frontline Worker (support women, adult survivors)		40%
Children's Support Worker (support children and youth)		17%
Administrative Staff		3%
Information Technology Staff		0%
Community Educator / Trainer		6%
Volunteer		1%
Other		8%
	Total Responses	

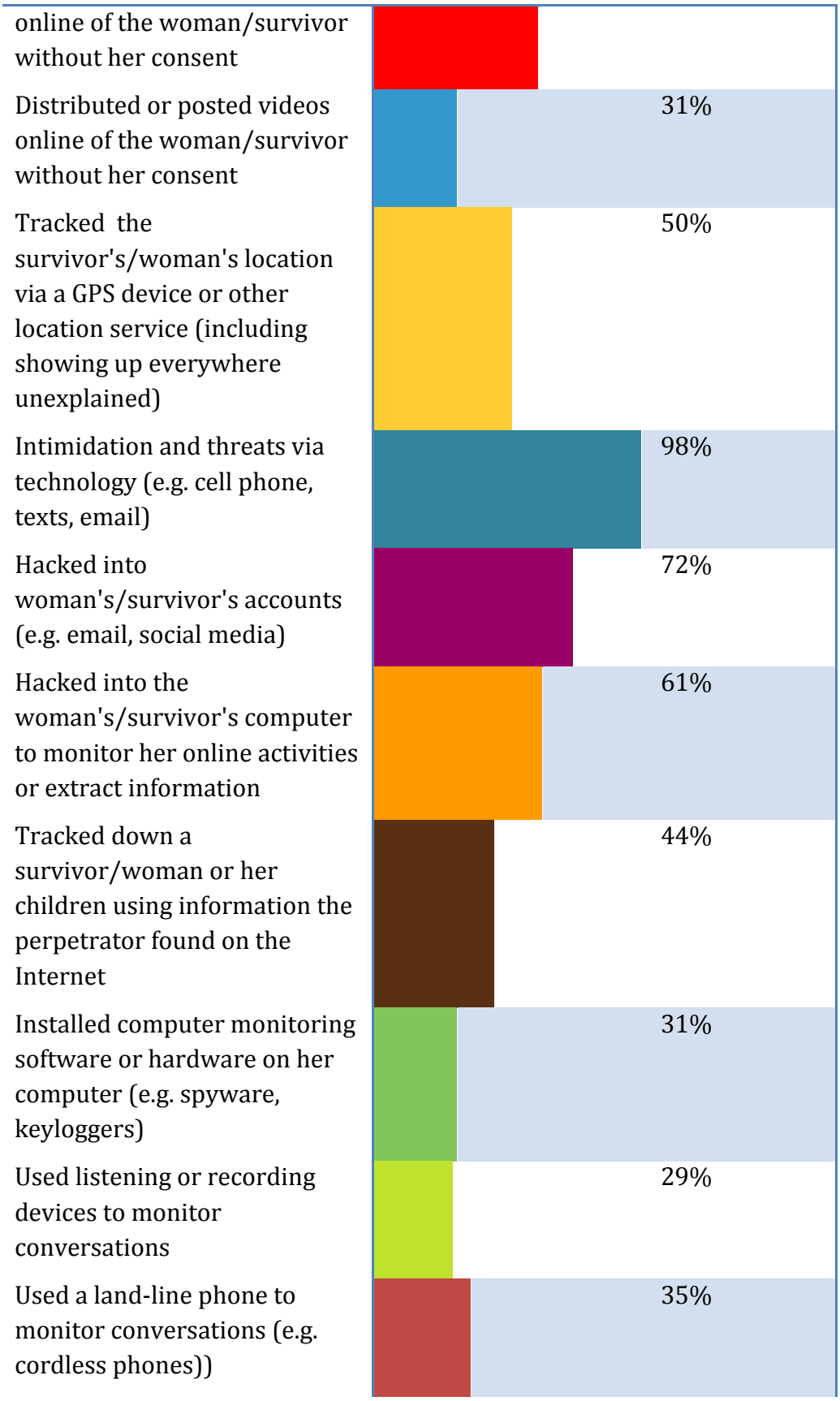
4. How many paid staff work in your anti-violence program?

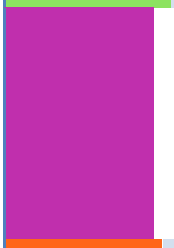
The average number of paid staff is 18.

5. Email Contact Information

6. What have women and other survivors told you about the ways that perpetrators have (or are believed to have) misused technology?

Response	Chart	Percentage
Impersonation (using email, online profiles or other technologies to pretend to be the survivor or someone the survivor knows such as a friend)		69%
Distributed or posted pictures		60%


online of the woman/survivor without her consent
Distributed or posted videos online of the woman/survivor without her consent
31%
Tracked the survivor's/woman's location via a GPS device or other location service (including showing up everywhere unexplained)
50%
Intimidation and threats via technology (e.g. cell phone, texts, email)
98%
Hacked into woman's/survivor's accounts (e.g. email, social media)
72%
Hacked into the woman's/survivor's computer to monitor her online activities or extract information
61%
Tracked down a survivor/woman or her children using information the perpetrator found on the Internet
44%
Installed computer monitoring software or hardware on her computer (e.g. spyware, keyloggers)
31%
Used listening or recording devices to monitor conversations
29%
Used a land-line phone to monitor conversations (e.g. cordless phones))
35%

Used VoIP (Voice over Internet Protocol) technology such as Skype or Google Talk to monitor or screen		9%
Misused a cell phone to track or monitor calls, location or other activities		49%
Misused Caller ID (e.g. to screen or identify calls, spoof other people's phone numbers to call or text threats and abuse.		44%
Used /hacked/monitored Instant Messaging accounts		46%
Tampered with or destroyed assistive technology (e.g. hearing aid, screen reader, TTY machine)		10%
Used hidden cameras or her laptop's webcam to secretly watch or record the woman/youth/survivor without consent (e.g. undressing, having sex)		31%
Other, please specify...		3%
	Total Responses	

7. What kinds of assistance are women/survivors requesting around their own technology use?

Response	Chart	Percentage
Safety and privacy with social media (e.g. Facebook, Twitter)		74%
Safety with cell phones (e.g. talking, texting)		82%

Safety online (e.g. email, web browsing, instant messages)	73%
Safety with location privacy (e.g. tracking cell phones, geo-tagging)	55%
Safety with computer use	61%
Safety and privacy with cameras, photos, videos (e.g. tags, removal, face recognition)	40%
Safety and privacy planning around technology use	55%
Safety and accessibility with technology (e.g. assistive devices and services, website, hotline and shelter accessibility, relay services)	34%
Other, please specify...	3%
Total Responses	

8. What are some privacy and confidentiality concerns you have about using technology when working with or communicating with women/survivors?

Response	Chart	Percentage
Perpetrators might intercept the communication		82%
Someone else might intercept the communication		60%
Support that is not face-to-face (e.g. lacks visual or verbal cues) might be misinterpreted or unclear		69%
Electronic communication might implicate our agency in		59%

ways that impact confidentiality (e.g. through a court order or a court case)		
How we communicate or maintain information might negatively affect the privacy and safety of a woman/survivor and her children		62%
Our agency has a confidential location that could be compromised		50%
Other, please specify...		5%

9. Do you feel you need more information and resources to best respond to requests from women/survivors about technology?

Response	Chart	Percentage
Yes		89%
No		11%

10. Are you aware of any complaints in your area involving technology-facilitated abuse where a law enforcement response was requested?

Response	Chart	Percentage
Yes		46%
No		54%

11. Was law enforcement in your community responsive to those complaints about abuse perpetrators misusing technology to harm?

Response	Chart	Percentage
Yes		47%
No		53%

12. If you think law enforcement is not responsive or prepared to address technology abuse, what do you think is the reason?

Response	Chart	Percentage	Count
Lack of awareness or understanding of technology and perpetrator misuse		54%	49
Lack of resources to investigate technology-related cases and crimes		60%	55
Minimization of cases associated with violence against women		62%	56
Lack of training about timely evidence collection regarding possible charges		40%	36
I don't know		21%	19
Others, please specify ...		9%	8
	Total Responses		91

13. Would you like more resources to help you work with law enforcement on issues related to technology abuse?

Response	Chart	Percentage
Yes		95%
No		5%

14. What are some ways technology is being used against women/survivors in court cases?

64 responses to this question.

15. What are some ways women/survivors have used technology to support their cases?

84 responses to this question.

16. What are some examples that you've seen in your community of technology evidence not being used or allowed by judges?

58 responses to this question.

17. Are you seeing judges mandate technology use between perpetrators and survivors/women?

Response	Chart	Percentage
Yes		40%
No		60%

18. Have women or other survivors been able to get civil legal recourse when a perpetrator has abused them through technology?

Response	Chart	Percentage	Count
Yes		8%	8
No		26%	27
I don't know		70%	73

19. Have you or your program worked with women/survivors who have had technology included in their protection or restraining orders?

Response	Chart	Percentage
Yes		54%
No		46%

20. What are some ways technology has been used against women, children or other survivors in family law cases?

50 responses to this question.

21. What are some ways technology has benefited women/survivors in family law cases?

51 responses to this question.

22. Would you like more information about legal protections and issues around technology and abuse?

Response	Chart	Percentage
Yes		97%
No		3%

23. If your anti-violence agency/program is involved in any community response teams or task forces, how are you using technology?

Response	Chart	Percentage
Our agency/program is part of a community task force or coordinated community response team		29%
Our agency/program and another agency currently shares the use of some technology (e.g. we use the same fax, wireless network, TTY machine, database , or, network		13%

server, etc.)	
Our agency/program does not currently share the use of any technology with another agency	59%
We have discussed how technology use in a community partnership impacts the safety, privacy and confidentiality of survivors/women.	39%
We would like more information on policies and practices to protect confidentiality, safety and privacy when using or sharing technology in community partnerships with other agencies	68%

24. Do you safety plan with women and other survivors around their own technology use and how the perpetrator might misuse technology?

Response	Chart	Percentage	Count
Yes		84%	88
No		16%	17

If yes, what types of technology do you most often safety plan about? What are recent technology issues that women/survivors have been concerned about?

77 responses to this question.

25. Do you have concerns regarding privacy and confidentiality when using technology?

Response	Chart	Percentage
Yes		76%
No		24%
	Total Responses	

26. What are other examples of technology misuse, concerns, issues that you would like to share with us?

33 responses to this question.

27. What are some innovative ways that women/survivors are using technology?

42 responses to this question.

28. This is the end of the survey. Thank you for sharing your insights. Is there anything else you want to share?

24 responses to this question.