Privacy, Security, and Confidentiality: Database Considerations for Violence Against Women Programs

Safety Net Canada 2013

SAFETY NET
CANADA

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:	
	Cynthia Fraser
	Laurie Parsons
	Rhiannon Wong
	National Network to End Domestic Violence Safety Net Project
French Translation:	*Jose Beaudet*
Graphic Design:	*Hannah Lee*

FINANCIAL

This project has been funded by the Office of the Privacy Commissioner of Canada. The views and opinions expressed herein are those of the BCSTH and CIPPIC and do not necessarily reflect those of the OPC.

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

SAFETY NET CANADA

cippic

NNEDV NATIONAL NETWORK TO END DOMESTIC VIOLENCE

TABLE OF CONTENTS

1. Introduction

The electronic collection of data has been an emerging topic for discussion amongst Violence Against Women (VAW) agencies/programs across Canada. Some VAW agencies/programs are moving towards standardization through such processes as accreditation; during these processes, databases are being suggested as possible tools to help promote consistency in how women, youth, and children's personal information is collected, stored, aggregated, shared, and/or protected.

There is also increased discussion about the use of biometric data collection (collecting fingerprints and facial features for recognition) and how it can increase privacy and safety risks for some women, while increasing safety and security for other women and anti-violence workers. Though biometric identification is being marketed as a "state of the art" security feature, we encourage VAW programs thinking carefully about this option and to read this document first in order to make women and child-centered choices for your programs.

We would like to ensure that all agencies who serve women surviving family and domestic violence, sexual and dating violence, stalking, harassment, and abuse—and their children—are informed about the risks and benefits of various methods of data collection. We hope that this guide will help agencies to consider their options and weigh the risks and benefits, so that they can make informed decisions that not only work for their programs, but ensure that the safety, privacy and confidentiality of women, youth, and children are protected.

Finally, this guide should be used in conjunction with many resources including:

- Assessing Technology in the Context of Violence Against Women & Children. Examining Benefits & Risks. (Safety Net Canada, 2013)
- Canadian Legal Remedies for Technology-Enabled Violence Against Women. (Safety Net Canada, 2013)
- Organizational Technology Practices for Anti-Violence Programs. Protecting the Safety, Privacy & Confidentiality of Women, Youth & Children. (Safety Net Canada, 2013)
- Records Management Guidelines: Protecting Privacy for Survivors of Violence
  www.bcsth.ca/content/general
- Privacy Toolkit
  www.bchousing.org/Partners/H_S_Op/Privacy_tools
- Non Profit Records Management Toolkit
  www.bchousing.org/Partners/H_S_Op/Administration/Records_management
- Provincial and territorial privacy laws
- Freedom of Information and Protection of Privacy Act
- Provincial and Territorial Child Protection Legislation
- Criminal Code of Canada

2. What Problem Does A Database Solve?

For many organizations, the appeal of a database is the apparent ease through which outcomes can be tracked and measured and used to demonstrate program "effectiveness" and/or to identify areas for program improvement. For other organizations, it is a way through which staff activity can be statistically monitored from a distance.

When considering purchasing or developing a database for the storage of resident/participant information, it is helpful to clearly identify the problem your agency is trying to solve within your anti-violence programs.

- Are you having difficulty locating information that you need?
- Is there an alternative way to find it?
- Is it information that will always be useful to track, or is your need for the information temporary?

If the benefits of databases were self-evident, they would sell themselves. Remember that database companies must establish a need, to create a demand, for them to fill. Consider the following questions before deciding if your agency/program needs a database:

- How will a database help you to fulfill your organization's mission statement?
- Is it congruent with your organization's values?
- Could it result in staff/volunteers working more with computers and less with residents/participants?
- Will it require staff to ask questions of residents/participants that may influence either negatively or positively the nature of their relationship?
- Will it cause staff to sit across a desk from residents/participants as they type information into a computer?
- Are you able to ensure the security, privacy, and confidentiality of the data collected?

Some database companies provide for the sharing of information between agencies. Remember that sharing information about residents and/or former residents and participants could be in direct violation of your agency's contracts with most funders, without the explicit request from, and/or informed consent of, a resident/participant.

When considering databases, think about:

- Upholding a resident's/participant's right to privacy and the ethical implications of using databases.
- Women's safety and security, and the impact databases may have on safety.
- Do databases help eliminate violence? At times, can databases help abusers/stalkers further perpetrate violence?
- What are the direct benefits of databases for the women and children you serve?

3. Risks for Women, Youth, and Children

When considering the liability that databases can cause agencies, it is critical to think and consider the implications that databases have on the safety, privacy, and autonomy of women, youth, and children. Here are questions to consider:

- What happens if Citizenship and Immigration Canada subpoenas or provides a court order for your data and finds women without immigrant, refugee, and/or Canadian citizenship status accessing your program?
- What if the data you collect is run against a police database and the survivor has charges against her? What would this mean in terms of protecting the confidentiality and privacy of women?
- Some databases ask programs to collect unnecessary information about a woman, youth, or child. The collection of irrelevant information into a database, such as information about women’s abusers, can put women at risk for legal complications such as libel and "Defamation of Character."
- The collection of biometrics does not allow the flexibility to protect a woman’s confidentiality. If your agency has a security system that requires a resident to provide her fingerprints in order to access transition housing/shelter, there will always be a record that she accessed services at your program on a specific date.
- Does an agency’s decision to use and store biometric data as a form of safety, outweigh the possibility of putting women, youth, and children at risk of "unintended consequences"? *See Biometrics, page 9.*
- What are the risks for women’s safety if a woman’s ex-partner, or an associate of her ex-partner, works for the database company that is hosting her data?
- Consider the significant privacy and civil liberty implications of collecting too much data—such as social media accounts, pictures of residents/participants and their children, Social Insurance Numbers, and immigration statuses.
- How vulnerable is your database to theft, hacking, or abuse? Is it located on a computer connected to the Internet?
- If a resident/participant file is subpoenaed, how will you ensure that all other records on the database are not compromised?
- What are the implications of having an electronic trail of your service that essentially can never be completely deleted?

4. Other Things to Consider When Using a Database [1]

Necessity

What problem is your agency trying to solve? Is a database really the answer? For example, a community experiencing difficulties with protection orders being served, may want to create a database—thinking that it will make the process more efficient. Creating a database doesn't address the problem of orders not being served, if the problem is not having enough officers to serve the orders.

Functionality

Is the database you choose, user friendly? Has your agency allocated sufficient money, resources, and staffing to keep the database up to date and useful? Has the agency allocated funding and staff time to conduct annual privacy assessments? Has the agency allocated sufficient resources for training existing and new staff (turnover), and for providing ongoing technical support?

Privacy and Safety

What confidentiality and privilege laws/regulations/obligations apply? Who will have ultimate responsibility for ensuring that confidential data is protected? Is there a designated privacy officer within the organization? Do users sign documents acknowledging their responsibilities for protecting the confidentiality of data, such as a data confidentiality agreement or an employment agreement with data confidentiality provisions? Are these incorporated into agency policy?

Resident/Service Recipient Information

What factors will agencies use in establishing collection, modification, use, and disclosure procedures for identifiable data? Are women and children informed about the security and data sharing policy? What is the process for residents/participants to opt-out, inspect, withdraw, or correct their data/records? How will agencies inform women and children about this process? How will they ensure that the data is completely gone if a woman/child opts-out of having her personal information collected in a database?

Cost

Has the agency priced multiple options and received at least two bids for the project? Has the agency done a cost-benefit analysis to assess the balance between ongoing costs and ultimate benefits? Has the agency designated appropriate funds for the project? While modest expenses for outcomes measurements are part of any grant, a direct services grant should primarily fund services and not outcomes measurement.

Security

Best practice is to secure backups at the same level of security as the original source. Has the agency included plans for system backup and security? How will they ensure all data is encrypted? Consider contracting with a computer security professional to assess the penetrability/security of the system, and to recommend improvements.

[1] National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. USA. Retrieved from: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf

5. What Is a Database?

Databases are computer programs used to organize information in a way that can make information easy to locate, access, and update. Databases can be organized in a variety of ways (alphabetically, numerically) and can include text, words, and images. Databases can be searched using a “query” like a name, place, date, etc. to find information about groups of people. Databases have a “report” function that allows the user to run reports on such things as the number of new residents/participants in the last month, or the most popular resource accessed, etc.

Databases generally allow "administrators" (it is best practice to have one person in your office responsible for the database, such as the Executive Director, program manager, Information Technology (IT) staff, or member of your administration team) to set usernames, passwords, access levels, and permissions. Additionally, well-designed databases incorporate audit trails to provide a detailed record of the queries and actions of each user. Databases can be designed at the outset to automatically purge or delete certain data elements after a certain time period, and only retain the elements necessary for reporting purposes.

- **Access levels**
  Access levels enable an administrator to access database information and to set a variety of access levels. For example, the system administrator could establish access levels so that a few staff see all the information in a database, and other users only see the information relevant to the role of the user (volunteer, staff, attorney, etc.). Before the database is put into place, it is important to determine who needs to access the data, what level of access is appropriate, and how access to the data will be limited to these authorized persons.

- **Data storage**
  Some databases are hosted locally, while others are hosted off-site. A locally hosted database means that the data remains in the agency, on the agency’s server. A remotely hosted database is often a commercial package, whereby the agency pays a monthly fee and the database is hosted by a third party, outside the agency. (See Section 4.)

Pre-packaged, commercial databases are often less expensive up front, but may not be adaptable or may require additional costs to modify the database, or create a new type of report, etc. If agencies choose to contract with someone to have a database developed especially for the agency, a limited number of modifications can be written into the initial contract. The costs to develop, implement, and maintain a database can range widely, from $5,000 to over $50,000.[2]

[2] National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. USA. Retrieved from: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf

6. What Is Biometric Data Collection?

Biometric data collection aims to automate personal identifiers such as eye colour, fingerprints, and face shape by comparing "information scanned in real time against an 'authentic' sample stored digitally in a database."[3] For example, Jane will be staying at your transition house/shelter for 30 days. At intake, the intake worker "scans" Jane's fingerprint into your agency's security system. The security program is set to allow Jane to leave and return to the house, after Jane scans her finger every time she wants to leave or return (in real time) and the security program recognizes her fingerprint as a match (authentic sample) in the system.

VAW programs have access to this option when purchasing some security systems. Options to collect and store a woman, youth, or child's fingerprints and facial features are marketed to VAW programs as ways to control access to physical facilities, such as housing programs.

Since 9/11, biometric security systems have increased in popularity and aim to identify individuals and track movement. The cost of these systems has decreased significantly, and can be included in a comprehensive security program for approximately $10,000.

Each VAW program must consider the unintended consequences of collecting biometric data, in addition to the database considerations listed in Sections 2 and 3. Agencies must work through the questions below, before making an informed decision that puts women's privacy and safety first.

There are major risks to consider when choosing biometric databases:

- Have you ensured that biometric data cannot be intercepted or stolen?
- Is all data, especially biometric data, encrypted? How have you ensured that all encrypted data cannot be "unencrypted"?
- Do all users have strong passwords?
- Because biometric data is inherently personal, any interception, hacking, or loss of biometric data can have detrimental consequences to women and children. How will you ensure that biometric data is deleted permanently once a resident/participant has left your program? Is this possible?
- Do you have informed consent from residents/participants to collect and store their biometric data? How have you ensured that they understand the unintended consequences of providing your program with biometric data?
- What happens if a survivor does not consent to you collecting or storing her biometric data? Women should not be refused access to any of your services, just because they exercise their right to refuse to have biometric data collected.
- Is your agency prepared for any legal implications that could happen if data, privacy, and confidentiality are breeched?
- Has your agency allocated funding to conduct regular privacy assessments, ensure encryption is up to date, and have Information Technology (IT) consultants/staff available for any immediate concerns?

[3] Electronic Privacy Information Center. (n.d.) "Biometric Identifiers." USA. Retrieved from: http://epic.org/privacy/biometrics/#bg

7. Data Collection Security

A) Data Storage Options

Data security, confidentiality, and privacy breach policies need to be in place before utilizing electronic databases; an agency data breach can be life threatening for women, youth, and children who are fleeing and/or living with the effects of domestic or family violence, sexual or dating violence, stalking, harassment, or abuse. Data breaches can also be financially costly to an agency.

Personal information can be stored in a database in two ways:

- Remotely, through the Internet.
- Locally, in your agency on your agency's server.

There are safety implications for both:

i) Database platforms that require Internet access have a variety of security risks that need to be considered:

- The risk of unauthorized third parties (some of whom may be hackers or advertisers) potentially accessing information through the Internet about the individual residents/participants your agency serves. Ensuring that all files are encrypted is one safety measure. However, someone could still get unauthorized access to your files if they get hold of an agency staff's user name and password.
- If staff have access to the database outside of their workplace, it is important to consider the possibility that their user names and passwords are being stored on public and personal computers, compromised by other people accessing the computer or simply by a third party watching a staff member enter their user name and password.
- There is always a possibility that computers get misplaced or stolen. Are the user names and passwords stored on these computers?
- Database companies often have access to an agency's database in order to solve any "glitches" or make any changes required. The confidentiality of residents/participants can be compromised if the database company can access your database any time, without restrictions. Ideally, database company employees will only ever see "Jane Doe" test records; they should be barred from viewing any of your agency's confidential client-level information.

ii) Databases that are hosted on an agency's server and do not require Internet access to be used, also have security concerns

- o If your agency server is connected to the Internet, abusers, stalkers, and hackers will still be able to find ways to access your database.
- o Consider who has access to the space where your agency's server is stored. Do volunteers, staff, outside janitorial staff, utility companies, residents/participants or other service providers have access to the space where the server is stored? Can someone walk into your space and pick up your server, and walk out with it?

- If the database company is hosting your database on their own server, essentially they have access to the files your agency uploads to the server.
- If your database is stored on your own server, consider how the database company has access to your database for maintenance purposes.

Note: databases can be used to store non-personal information; in fact, if you are going to use a database, try to design it as best you can to collect information about requested and provided services versus personally identifying information.

B) Security for Paper Files

Paper files also pose a security risk when storing personally identifying information. Programs should:

- Ensure that filing cabinets are secure places to store paper copies of resident/participant records, and that removable hard drives are also locked inside filing cabinets, desk drawers, or an office/bank safe. Agencies should have plans in place if the filing cabinet key is lost or stolen.
- Filing cabinets should be in locked rooms with limited access.
- Clearly defined access levels should identify who has access to the keys for the filing cabinets, storage rooms, and offices. Access should be defined based on the person's job role and a "need-to-know" basis.[4]
- Consider who has access to the paper files and filing cabinets. Volunteers, staff, outside janitorial staff, utility companies, service recipients, or other service providers accessing your space? Can someone walk into your space and wheel out your filing cabinet?

For more information, see "Records Management Guidelines"
www.bcsth.ca/sites/default/files/Records%20Management%20Guidelines%20April%202006.pdf

[4] Field, Julie. (2008). Securing Paper and Electronic Information for Co-Located Sexual Assault/Domestic Violence Programs and Partners. National Network to End Domestic Violence. Washington DC.

8. Different Ways of Using a Database

There are many ways of utilizing a database. It is important that an agency considers what it really needs, before purchasing one.

Personal Information Database
Some agencies prefer a database to collect personal information only. This type of database is usually one that is hosted on an agency's server and can be developed easily in software applications such as Microsoft Access. These databases might collect basic personal information, such as a resident's/participant's name and contact information.

Another option for personal information only databases, is to use the database as "more of a 'card catalog' to reference paper files. Here the data is entered with a non–identifying code instead of a name. Paper files are labeled with the same code and this helps staff know which filing cabinet to go to in order to find the paper file."[5]

If connected to the Internet, personally identifiable information in these databases remains at risk of being compromised by unauthorized third parties, not to mention subpoenas/court orders, and other persons who may have access to the database.

Case Management Database
Some agencies use resident/participant databases as the primary means of information storage. This might include inputting personal information and more extensive details, such as which programs were accessed; background information, such as abuser information and child information; programs accessed; and case notes and referrals. Programs might create database fields to collect funder-required statistics, and output aggregate reports for monthly and quarterly reporting. In many Internet-connected or interagency database systems, the risks of breaching confidentiality and privacy is high. Personal details inputted into databases put the lives of women and children at risk. *See page 16 for the risks associated with databases.*

Biometrics Storage
Some agencies consider using biometric identification and authentication methods. These tend to be marketed as ways to ensure building security. However, using biometric methods to enter a program/shelter does not necessarily ensure the safety of the women, youth, children, and staff.

When using biometrics, it is important to consider where biometric data is being stored, and how. Is it encrypted? How can a perpetrator hack into the biometric database and steal personal information? What happens when biometric data is deleted? When the computer security program compares biometric information, what happens if there are false positives (allowing access to an unauthorized service recipient/staff) or false negatives (denying access because a software program has misread a fingerprint)? Biometric authentication is often quite a privacy-invasive technology; because the data collected is of the body (e.g. iris scan, fingerprint), breaches of biometric systems can create new, significant, and irreversible privacy and safety risks for women, youth, children, and

[5] National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. USA. Retrieved from: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf

staff. For example, in 2005, car thieves in Malaysia cut off a finger of the owner of a Mercedes Benz in order to get around the owner's high tech security system.[6]

[6] Kent, Jonathan. (2005). Malaysia car thieves steal finger. BBC Online. Kuala Lumpur. Retrieved from: http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

9. Data Collection In Accordance To BC's Personal Information Protection Act: An Example

From the example listed in Section 5, we know that collecting too much data on an electronic database can increase danger and risks for women, youth and children. It is suggested that agencies choosing to use an electronic database follow privacy legislation such as BC's Personal Information Protection Act (PIPA). Though this is a BC-specific example, provincial and territorial privacy legislation can be incorporated.

Below is a table that outlines the legal privacy requirements for BC organizations collecting personal information on databases, and what to consider before inputting service recipient's personal information into one.

According to PIPA Agencies:	Database Implications to Consider
Must receive consent in order to collect, use, and/or disclose personal information.[7]	Informed consent is best practice. Let the resident/participant know that their personal information will be uploaded to a database, and who has access to this database (IT, developer, staff members/volunteers) and the risks associated with this.
Must not, as a condition of supplying a…service, require an individual to consent to the collection.[8]	Have plans in place for when a resident/participant decides they do not want to have her personal information collected. If you are using your database to input statistics, how do you do so? Are paper files an option for backup?
On request of an individual, an organization must provide the individual with the following: • the individual's personal information under the control of the organization; • information about the ways in which the personal information...has been and is being used by the organization; • the names of the individuals and organizations to whom the personal information...has been disclosed by the organization.[9]	• Is your database capable of printing off the resident/participant information/electronic case file without jeopardizing other women's information? • Have information ready about how your organization is using personal information in the database. • Remember to include the database developer and their staff, if they have access to your database.

[7] Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

[8] Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

[9] Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

Must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks.[10]	Are your database files individually encrypted (e.g. is each person's data separate? How strong is the encryption you are using? What happens if the encryption can be "decrypted" by third parties? Does your agency have firewalls and anti-virus software? What policies do you have in place if third parties do access your files, or your agency server is physically removed? What access levels will staff have? What security plans do you have in place for backups or disposal of old hard drives?
Must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that: • the purpose for which that personal information was collected is no longer being served by retention of the personal information, and • retention is no longer necessary for legal or business purposes.[11]	A computer's data can almost always be recovered. Have a plan to physically destroy all computer hard drives that have access to the database when your agency decides to upgrade hardware. Have a plan in place for when to delete a resident/participant file after their file has been closed and the retention period for records is over. (Discuss with the developer if deleting a file permanently is possible, if your agency is still utilizing the database.)

For more information on BC's Personal Information and Privacy Act:
http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

Other considerations:

- Data and privacy laws vary from province, territory, and country. Know what laws apply to your data if your participant's files are stored in a jurisdiction other than your own. Ask who owns the records, if they are being stored offsite.
- Have a plan in place for if your whole database gets subpoenaed/court ordered, instead of the individual file sought in a court case or by law enforcement.

[10] Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

[11] Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

10. Database Benefits For Programs

Agencies are likely to choose a database based on a variety of benefits:

- Databases allow agencies to analyze relationships between data and run reports on service usage.[12]
- Resource databases eliminate the need to recreate materials or resources and generally offer keyword searches to provide quick results.[13]
- Databases offer agencies the benefit of standardizing their method of data collection.
- Databases provide service providers with one system that is hopefully easily accessible to users.

[12] National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. USA. Retrieved from: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf

[13] National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. USA. Retrieved from: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf

11. Database Risks For Programs

Before purchasing a database, agencies must consider the safety risks in order to maintain the privacy and confidentiality of its residents/participants.

VAW Program Database Considerations

- Data kept on a computer that has Internet access is vulnerable to interception or breaches. A security breach can happen on many levels. Agencies need policies on who has access to the database, physical security of the agency's server, and security against third party breaches such as "hacking."
- Agencies are often served with subpoenas and/or court orders for the records of residents/participants. Agencies need policies in place for this occurrence, including how not to put other residents'/participants' records at risk and how to let the residents/participants know that their records have been subpoenaed or court ordered.
- Remember that any information entered into a database could exist for perpetuity. Even if the database owner promises to delete it after a certain number of days, data can be backed up, removed, exported, a screenshot taken, etc. It's important to carefully consider what is collected, and what the future implications may be. This is important to consider after the woman leaves shelter. Does she own or have access to her data?
- Although it's highly unethical, there is always a risk that data collected for one purpose will be used for secondary purposes (such as intake information being used by researchers for research studies). Additionally, there is a risk that current or former employees will purposely or accidentally share confidential information, or take advantage of their access to the database to perform searches for personal use.
- Untrained users may accidentally delete or alter data.
- Would you refuse service if a woman does not want her data stored in a database?

12. Database Vendor/Developer Considerations

- It is best practice to ensure that database vendor/developer employees DO NOT have access to your database. Often, database vendors will confirm that vendor employees do have access, but that they have signed a confidentiality waiver. It is important to ask the vendor questions on what happens if a vendor employee breaches that confidentiality agreement.
- If a vendor hosts an agency's data, can a vendor deny agencies their data if their business closes down, they experience technical problems, etc.?
- Agencies must clarify in a legal written contract who owns your agency’s data, once it is stored on the vendor’s server or in a cloud database system.
- Does the vendor have policies on what happens if they get subpoenaed/provided with a court order for your resident/participant records, and will they let your agency know if they do?
- Ask the vendor what security measures are in place to protect your agency’s data and services. For example, is the data encrypted, and if so, who has the encryption key?
- If the provider goes out of business, what happens to your agency’s data and services?
- Your agency is liable for the personal information uploaded into a database. Have legal contracts written to ensure that survivors’ privacy, confidentiality, and personal information is being upheld.

13. Recommendations For Database Privacy And Women’s Safety

- If your agency is using a database, agency staff must obtain ***Written, Informed and Time Limited Consent*** from residents/participants acknowledging that they know their information is being stored in an electronic database, and are informed about the security and confidentiality risks associated with this method of data collection.
- Ensure all data is encrypted. Have plans in place for if data becomes “unencrypted.”
- Individualize ***Levels of Access*** for each member of staff and volunteers who have access to the database. Do administrators, volunteers, and management need access to all files if they are not working with women, youth, and children directly?
- Have a plan in place if the main administrator of the database leaves, takes unexpected time off, or is sick. Who knows how the database works?
- Have a plan in place with the database developer for if they are no longer in business, or if there is staff turnover. Who owns the files? What happens to women’s information if it is hosted on the developer’s server?
- Work with the Database Developer to plan for potential subpoenas/court orders for confidential files/records. Ensure in a legal written contract that the developer will let you know that files have been subpoenaed/court ordered, and whose file it is. Is there a time frame they will contact you by? What is the policy around this? Note that your agency is liable for the developer’s actions with the personal information.
- Organizations should protect any personally identifiable information collected about a resident/participant, since any data leaks or breaches could be fatal.
- For safety reasons, we recommend that organizations not store confidential or personally identifiable information about residents/participants on any computer that is connected to the Internet. Without an Internet connection, there is significantly less risk that an abuser/stalker will hack in and access your organization's data, or, that a virus will infect your computer and automatically email confidential files out to others.
- Collect only information necessary to do the job. Database sales representatives typically showcase database perks such as storing photos, Facebook account information, names, and addresses of the abuser and immigration/refugee/First Nations/Metis/Inuit or Non Status information. Collecting unnecessary information can pose risks to women’s safety. Work with the Database Developer prior to launching your database in order to ensure that only necessary fields are in your database.
- Have plans in place for if there is a privacy complaint made against your agency. Consider what potential outcomes there could be if data has been breached or hacked, and if the lives and safety of women and children are put at risk.

14. Resources

- Organizational Technology Practices for Anti-Violence Programs. Protecting the Safety, Privacy & Confidentiality of Women, Youth & Children. (Safety Net Canada)
- www.nnedv.org/docs/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf
- www.nnedv.org/docs/SafetyNet/NNEDV_DataSecurity.pdf
- www.bcsth.ca/content/general
- www.bchousing.org/Partners/H_S_Op/Privacy_tools
- www.bchousing.org/Partners/H_S_Op/Administration/Records_management
- Provincial and territorial privacy laws
- Freedom of Information and Protection of Privacy Act
- Provincial and Territorial Child Protection Legislation
- Criminal Code of Canada

15. Bibliography

This bibliography is divided into content-specific sections and is inclusive of all sources used in the following:

- Assessing Technology in the Context of Violence Against Women & Children. Examining Benefits & Risks.
- Canadian Legal Remedies for Technology-Enabled Violence Against Women.
- Organizational Technology Practices for Anti-Violence Programs. Protecting the Safety, Privacy, & Confidentiality of Women, Youth, & Children.
- Privacy, Security and Confidentiality: Database Considerations for Violence Against Women Programs.
- Privacy, Security and Confidentiality: Social Media Considerations for Violence Against Women Programs.

Note: Sources will only appear once throughout the document.

SECTION A. VIOLENCE AGAINST WOMEN AND CHILDREN

Baum, K., Catalano, S., Rand, M., and 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. USA.

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. USA.

Canadian Centre for Justice Statistics. (2005). Family Violence in Canada, A Statistical Profile 2005. Statistics Canada. doi: 85-224-XIE. Page 9. Ottawa, Ontario. Retrieved from: www.statcan.gc.ca/pub/85-224-x/85-224-x2005000-eng.pdf , and, Centre canadien de la statistique juridique. (2005). La violence familiale au Canada : un profil statistique 2005. Statistique Canada. Ottawa, Ontario. Retrieved from: www.statcan.gc.ca/pub/85-224-x/85-224-x2005000-fra.pdf

Canadian Women's Foundation. (2013). Fact Sheet: Moving Women Out of Violence. Retrieved from: http://www.canadianwomen.org/facts-about-violence

Office of the Chief Coroner. (2011). Domestic Violence Death Review Committee—2010, Eighth Annual Report. Toronto, Ontario.

Department of Justice Canada. (2004). A Handbook for Police and Crown Prosecutors on Criminal Harassment. Ottawa, Ontario. Retrieved from: www.justice.gc.ca/eng/pi/fv-vf/pub/har/index.html

Department of Justice Canada. (2012). A Handbook for Police and Crown Prosecutors on Criminal Harassment. Ottawa, Ontario. Retrieved from: http://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/har/EN-CHH.pdf

McCormack, C., and Prostran, N. (2012). "Asking for It." *International Feminist Journal of Politics* 4, no. 3: 410–414. USA.

McFarlane, J. et al., (1999). Stalking and Intimate Partner Femicide, *Homicide Studies* 3, no. 4. USA. Retrieved from: www.victimsofcrime.org/docs/src/mcfarlane-j-m-campbell-j-c-wilt-s-sachs-c-j-ulrich-y-xu-x-1999.pdf

Ministry of Justice. (2011). Safety Planning with Children and Youth: A Toolkit for Working with Children and Youth Exposed to Domestic Violence. British Columbia. Retrieved from: http://www.pssg.gov.bc.ca/victimservices/training/docs/child-youth-safety-toolkit.pdf

Mohandie, K., Meloy, J., McGowan, M., and Williams, J.. (2006). “The RECON Typology of Stalking: Reliability and Validity Based Upon a Large Sample of North American Stalkers." *Journal of Forensic Science* 51 no. 1: 147–155. USA.

National Center for Injury Prevention and Control, Division of Violence Prevention. (2013). The National Intimate Partner and Sexual Violence Survey: A Fact Sheet. Atlanta, USA. Retrieved from: http://www.cdc.gov/ViolencePrevention/pdf/NISVS_FactSheet-a.pdf

Perreault, S. (2012 December 12). Homicide in Canada, 2011. Statistics Canada. Ottawa, Ontario. Retrieved from: http://www.statcan.gc.ca/daily-quotidien/121204/dq121204a-eng.htm and http://www5.statcan.gc.ca/bsolc/olc-cel/olc-cel?catno=85-002-X201200111738&lang=eng

Sinha, M., ed. (2013 February 25). Measuring Violence Against Women: Statistical Trends. Canadian Centre for Justice Statistics, Statistics Canada. Ottawa, Ontario. Retrieved from http://www.statcan.gc.ca/pub/85-002-x/2013001/article/11766-eng.htm and http://www.statcan.gc.ca/pub/85-002-x/2013001/article/11766/hl-fs-eng.htm

Sophie’s Choice. Dir. Alan J. Pakula. Perf. Meryl Streep, Kevin Kline, Peter MacNicol. Artisan, 1982. Film.

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. USA.

Stalking Resource Center. Stalking Information. U.S. National Center for Victims of Crime. Retrieved from: www.victimsofcrime.org/our-programs/stalking-resource-center/stalking-Cinformation

Statistics Canada. (2011) Criminal Harassment in Canada, 2009. *Juristat*. Ottawa, Ontario. Retrieved from: www.statcanada.gc.ca/pub/85-005-x/2011001/article/11407-eng.htm

Statistics Canada. (2013 April 16) Family Violence. Ottawa, Ontario. Retrieved from: http://www5.statcan.gc.ca/subject-sujet/subtheme-soustheme.action?pid=2693&id=2696&lang=eng

Statistics Canada (2010). Family Violence in Canada: A Statistical Profile, 2010. Ottawa, Ontario. Retrieved from: http://www.statcan.gc.ca/daily-quotidien/120522/dq120522a-eng.htm

Statistics Canada. (2013 February 25). Violence Against Women, 2011. *The Daily*. Retrieved from: http://www.statcan.gc.ca/

Statistics Canada. (2011). Transition Homes in Canada: National, Provincial and Territorial Fact Sheets, 2009/2010. Ottawa, Ontario.
Retrieved from: http://www.statcan.gc.ca/daily-quotidien/111025/dq111025c-eng.htm and http://www.statcan.gc.ca/pub/85-404-x/2011000/part-partie1-eng.htm

Tjaden, P., and Thoennes, N. (1998). Stalking in America: Findings From the National Violence Against Women Survey, final report to the National Institute of Justice. National Institute of Justice and Centers for Disease Control and Prevention. NCJ 169592. USA.

United Nations. (1993 December 20). 48/104 Declaration on the Elimination of Violence Against Women. Retrieved from: www.un.org/documents/ga/res/48/a48r104.htm.

SECTION B: TECHNOLOGY AND VIOLENCE AGAINST WOMEN AND CHILDREN

Auld, A. (2013 April 12). “Don’t ‘Respond with Violence,’ Rehtaeh Parsons’ Mother Tells Vigil Through Tears.” The Canadian Press. Retrieved from: http://www.canada.com/news/Rehtaeh+Parsons+vigil+held+Halifax+people+urged+violence+against/8234427/story.html

Association for Progressive Communications. (2010 November). How Technology is Being Used to Perpetrate Violence Against Women—And to Fight it. South Africa. Retrieved from: www.apc.org/en/node/11452

CBC News. (2013 Mar 4). Man sentenced over B.C. rave rape photos. Canada. Retrieved from: www.cbc.ca/news/canada/british-columbia/story/2013/03/04/bc-rave-rape-photos-sentencing.html

Canadian Clearinghouse on Cyberstalking. What is Cyberstalking? Canadian Resource Center for Victims of Crime. Retrieved from: www.cyberstalking.ca/en/fact-sheets/what-is-cyberstalking

Canadian Resource Centre for Victims of Crime. (2002) Cyberstalking. Canada. Retrieved from: http://www.crcvc.ca/docs/cyberstalking.pdf

Carpenter, D. (2013 March 17). Text Messages That Led to the Convictions in the Steubensville Rape Trial. USA. Retrieved from: www.mobilebroadcastnews.com/NewsRoom/Don-Carpenter/Text-Messages-led-convictions-Steubenville-Rape-Trial

Finn, J. (2000). Domestic Violence Organizations on the Web: a New Arena for Domestic Violence Services, *Sage Journals*, 6 (1): 80–102. New Hampshire, USA.

Fraser, C., Olsen, E., Lee, K., Southworth, C., and Tucker, S. (2010). The New Age of Stalking: Technological Implications for Stalking. *Juvenile and Family Court Journal,* 61 (4): 39–55. doi: 10.1111/j.1755-6988.2010.01051.x. Retrieved from: http://onlinelibrary.wiley.com/doi/10.1111/j.1755-6988.2010.01051.x/full

The Globe and Mail. (2010 September 16). Photos of gang rape go viral on Facebook. The Globe and Mail. Canada. Retrieved from: http://www.theglobeandmail.com/news/british-columbia/photos-of-gang-rape-go-viral-on-facebook/article545448/

Goddard, A. (2013 March 18). I Am the Blogger who Allegedly “Complicated” The Steubensville Gang Rape Cases—and I Wouldn’t Change a Thing! USA. Retrieved from: www.xojane.com/issues/steubenville-rape-verdict-alexandria-goddard

Hand, T., Chung, D., and Peters, M. (2009). The Use of Information and Communication Technologies to Coerce and Control in Domestic Violence and Following Separation. ISSN: 1443-8496. Australian Domestic & Family Violence Clearinghouse. Australia. Retrieved from: http://www.adfvc.unsw.edu.au.

Hollier, S. (2011). Sociability: social media for people with a disability. Media Access Australia. Australia. Retrieved from: http://www.mediaaccess.org.au/sites/default/files/files/MAA2657-%20Report-OnlineVersion.pdf

Kranz, A.L. (2002). Helpful or Harmful? How Innovative Communication Technology Affects Survivors of Intimate Violence. Violence Against Women Online Resources. Retrieved from: http://www.vaw.umn.edu.

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

LoveisRespect.org. What is Digital Abuse? LoveisRespect.org. USA. Retrieved from: http://www.loveisrespect.org/is-this-abuse/types-of-abuse/what-is-digital-abuse

McDonald, S. (2012). The Darker Side of Technology. *Victims of Crime Research Digest* 5. Department of Justice Canada. Retrieved from: http://www.justice.gc.ca/eng/rp-pr/cj-jp/victim/rd5-rr5/rd5-rr5.pdf

MTV. (2011). AP-MTV Digital Abuse Study. USA. Retrieved from: www.athinline.org/pdfs/MTV-AP_2011_Research_Study-Exec_Summary.pdf

National Network to End Domestic Violence. (2011). Sexting. USA. Retrieved from: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_Sexting_2011.pdf.

Office of the Chief Coroner. (2011). Domestic Violence Death Review Committee—2010, Eighth Annual Report**.** Toronto, Ontario.

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

Perry, J. (2012). Digital Stalking: a Guide to Technology Risks for Victims. Network for Surviving Stalking and Women’s Aid Federation of England. ISBN: 978 0 907817 52 9. England. Retrieved from: http://www.digital-stalking.com/storage/digital-guidelines/Digital%20Stalking%20Guide%20V2%20Nov%202012.pdf

Province of Nova Scotia. (2013). Be A Responsible Digital Citizen. Canada. Retrieved from: http://antibullying.novascotia.ca/sites/default/files/DigitalCitizenship_Eng.pdf ; et, Nouvelle-Écosse. (2013) Le Civisme à l'ère numérique. Retrieved from: http://antibullying.novascotia.ca/sites/default/files/DigitalCitizenship-FR.pdf

Province of Nova Scotia, Canada. (2013 April 25) Cyberbullying Investigative Unit a First in Canada. Premier's Office. Retrieved from: http://novascotia.ca/news/release/?id=20130425001
Safety Net Canada. (2013). Survey of Anti-violence Workers on Technology Abuse, 2012. BC Society of Transition Houses. Vancouver, British Columbia.

Southworth, C., Dawson, S., Fraser, C., and Tucker, S. (2005). A High-Tech Twist On Abuse: Technology, Intimate Partner Stalking and Advocacy. *Violence Against Women Online Resources.* USA. Retrieved from: http://www.vaw.umn.edu and http://nnedv.org/safetynetdocs

Southworth, C., Finn, J., Dawson, S., Fraser, C., and Tucker, S., (2007). *Intimate Partner Violence, Technology, and Stalking. Violence Against Women* 13 (8): 842–56. USA.

Southworth, C., Fraser, C., Tucker, S., et al. (2003–2011). *NNEDV Safety Net Project Training-of-Trainers Core Curriculum Library*. National Network to End Domestic Violence. Note: this resource is not available to the public.

Southworth, C., Fraser, C., Tucker, S., et al. (2003 - 2011). *NNEDV Safety Net Project Handouts Collection*. 32 of the over 50 pieces are available online at: NNEDV's Technology Safety Resources. National Network to End Domestic Violence. Retrieved from: http://nnedv.org/resources/safetynetdocs.html

Statistics Canada. (2011). Canadian Internet Use Survey. Ottawa, Ontario. Retrieved from: http://www23.statcan.gc.ca/imdb/p2SV.pl?Function=getSurvey&SDDS=4432&Item_Id=66020&lang=en

Tomilnson, K. (2013 May 3.) Teacher "Powerless" to Stop Ex-Girlfriend's Cyberstalking. Court Order Fails to Prevent Comments from Being Posted Online. CBC News. Canada. Retrieved from: www.cbc.ca/news/canada/story/2013/05/03/bc-cyber-stalking.html

SECTION C: PRIVACY, TECHNOLOGY, AND DATA

BC Housing. (2012). Privacy Toolkit. BC Housing. British Columbia, Canada. Retrieved from: http://www.bchousing.org/Partners/H_S_Op/Privacy_tools

Brown, K. (2013 March) How to Back Up iPhone Voicemails to MP3. HowToGeek.com. USA. Retrieved from: http://www.howtogeek.com/141164/how-to-backup-iphone-voicemails-to-mp3/

Cavourkin, A., and Stoianov, A. (2007). Biometric Encryption: A Positive Sum-Technology that Achieves Strong Authentication, Security and Privacy. Information and Privacy Commissioner of Ontario. Toronto, Ontario. Retrieved from: http://www.ipc.on.ca/images/Resources/bio-encryp.pdf

comScore. (2013 February 22). 2013 Mobile Future in Focus. comScore. USA. Retrieved from:

http://www.comscore.com/Insights/Presentations_and_Whitepapers/2013/2013_Mobile_Future_in_Focus

El Akkad, O. (2011 March 8; rev. 2012 August 23). Canadians' Internet Usage Nearly Double the Worldwide Average. The Globe and Mail. Canada. Retrieved from: http://www.theglobeandmail.com/technology/tech-news/canadians-internet-usage-nearly-double-the-worldwide-average/article569916/

Fitzpatrick, J. (2011 June 14). How to Recover if Your Password is Compromised. HowToGeek.com. Retrieved from: http://www.howtogeek.com/66033/how-to-recover-after-your-email-password-is-compromised/

Hoffman, C. (2012 September 30). How To Check If Your Account Passwords Have Been Leaked Online and Protect Yourself From Future Leaks. HowToGeek.com. Retrieved from: http://www.howtogeek.com/125569/how-to-check-if-your-account-passwords-have-been-leaked-online-and-protect-yourself-from-future-leaks/

Hoffman, C. (2012). Secure Access to Online Banking and Email on Untrusted Computers. How-To Geek.com. Retrieved from: http://www.howtogeek.com/139926/securely-access-online-banking-and-email-on-untrusted-computers-with-a-linux-usb-drive/

Hoffman, C. (2012). Why You Should Use a Password Manager and How to Get Started. HowToGeek.com. USA. Retrieved from: http://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/

Humphreys, T. (2012). TEDxAustin—Todd Humphreys. TEDx Talks. USA. Retrieved from: http://www.youtube.com/watch?v=wWLf4u2xJVM
Jacobi, J. (2012 May). The Best Encrypted Flash Drives. PC World. USA. Retrieved from: http://www.pcworld.com/article/254816/the_best_encrypted_flash_drives.html

OIPCA, OPCC, OIPCBC (2012 April) Getting Accountability Right with a Privacy Management Program. Canada. Retrieved from: http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf

Rodriguez, M. (2013 April 12). Facebook & Identity—Exploring Your Digital Self: Mario Rodriguez. TEDxTalks. Retrieved from http://www.youtube.com/watch?v=uFAigWTeX5Y

SHA-2. (n.d.) In Wikipedia. Retrieved from: http://en.wikipedia.org/wiki/SHA-2

Statistics Canada. (2011). 2010 Canadian Internet Use Survey. *The Daily*. May 25, 2011. Ottawa, Ontario. Retrieved from: http://www.statcan.gc.ca/daily-quotidien/110525/dq110525b-eng.htm

Statistics Canada. (2011). Individual Internet use and E-commerce, 2010. *The Daily*. Ottawa, Ontario. Retrieved from: http://www.statcan.gc.ca/daily-quotidien/111012/dq111012a-eng.htm .

Statistics Canada. (2013 January 30). "Dwelling Characteristics and Household Equipment, by Province." CANSIM, Table 203–0027. Ottawa, Ontario.

Tomkins, A. (2013 May 6). What Parents Need to Know About Instagram. Media Smarts. USA. Retrieved from: http://mediasmarts.ca/blog/what-parents-need-know-about-instagram

Voltage Security. (10 May 2013). Almost Half of Employees Admit to Bypassing Security Controls. InfoSecurity Magazine. Retrieved from:: www.infosecurity-magazine.com/view/32346/almost-half-of-employees-admit-to-bypassing-security-controls

SECTION D: TECHNOLOGY AND DATA STANDARDS, POLICIES, AND PRACTICES

B.C Association of Clinical Counsellors. (2011). Standard for the Use of Technology in Counselling. Adopted October 16, 2011. Canada. Retrieved from: http://bc-counsellors.org/wp-content/uploads/2011/02/7BCACC-Standard-Use-of-Technology-2011.pdf

Cavourkian, A. (2008). Privacy By Design…Take the Challenge. Information and Privacy Commissioner of Ontario. Canada. Retrieved from: www.ipc.on.ca and www.privacybydesign.ca

Cavourkian, A. (2009, rev. 2011) Privacy By Design. The 7 Foundational Principles. Information and Privacy Commissioner of Ontario. Canada. Retrieved from: http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Electronic Privacy Information Center. (n.d). "Biometric Identifiers." USA. Retrieved from: http://epic.org/privacy/biometrics/#bg

Field, J. (2008). Securing Paper and Electronic Information for Co-Located Sexual Assault/Domestic Violence Programs and Partners. National Network to End Domestic Violence. Washington, DC.

Fraser, C. (2009). Five Ways To Make Sexual Assault Services More Accessible Using Assistive Technology. / 5 Maneras de hacer los Servicios contra la Agresión Sexual más accesibles utilizando la tecnología asistencial. *Connections, a Biannual Publication of Washington Coalition of Sexual Assault Programs* 11 (4), 8–10. USA. Retrieved from: http://www.wcsap.org/connections and http://www.wcsap.org/technology-safe

Fraser, C. (2006. Rev. 2009). Free and Low Cost Tune-Ups: Some Accessibility Steps You Can Take With Little of No Money. Commissioned by *Project Access,* a U.S. national CALCASA training and technical assistance project for grantees of *The Education, Training, and Enhanced Services to End Violence Against and Abuse of Women with Disabilities Grant Program (Disability Grant Program)* of the US Department of Justice Office of Violence Against Women (US DOJ OVW): 1–18.

Fraser, C. (2006 January). The Cost of Waiting is High: Help Make Assistive Technologies More Accessible. *Access News, a publication from Project Access.* 3–6. USA.

Fraser, C., and Fribley, C. (2005). Assessing Organizational Readiness to Provide Online Advocacy & Services. *The Resource, A Newsletter of the National Sexual Violence Resource Center*. Retrieved from: http://www.nsvrc.org/publications/resource

Fraser, C., Field, J., Lee, K., Olsen, E., Southworth, C., and Tucker, S. (2011, September). Technology and Confidentiality Toolkit. For Agencies, Colocated Partnerships and Coordinated Community Response Teams working to end domestic violence, dating violence, sexual assault and stalking. National Network to End Domestic Violence and the Confidentiality Institute. This micro site provides access to 39 pieces created by the authors between 2008–2011. Retrieved from: http://nnedv.org/tools

International Society for Mental Health Online. (2000). Suggested Principles for the Online Service Provision of Mental Health Services. USA. Retrieved from: http://www.ismho.org/suggestions.asp

Kent, J. (2005). Malaysian car thieves steal finger. BBC Online. Kuala Lumpur. Retrieved from: http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm.

National Board for Certified Counselors, Inc. (2007). The Practice of Internet Counseling. USA. Retrieved from: http://nbcc.org/Ethics

National Network to End Domestic Violence; San Diego Family Justice Center Foundation; Office of Violence Against Women of the United States Department of Justice. (2005 August). The President's Family Justice Center Initiative. Confidentiality, Information Sharing and Privacy Protocol Recommendations. USA.

National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. USA. Retrieved from: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf

National Network to End Domestic Violence, Safety Net Project. (2008). Seven Ways to Add Technology Safety to Your Website. USA.

National Network to End Domestic Violence, Safety Net Project. (2007). Draft: Template Technology Safety Policies and Suggested Practices. USA.

Nonprofit Tech 2.0. (2013 January 22). 11 Obvious Signs Your Nonprofit Needs Social Media Training. USA. Retrieved from: http://nonprofitorgs.wordpress.com/2013/01/22/11-obvious-signs-your-nonprofit-needs-social-media-training/

Office of the Privacy Commissioner of Canada. (2011). Securing Personal Information: A Self-Assessment Tool for Organizations. Canada. Retrieved from: http://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1

Ruebsaat, G. (2006). Record Management Guidelines: Protecting Privacy for Survivors of Violence. BC Association of Specialized Victim Assistance and Counseling Programs, and, BC / Yukon Society of Transition Houses. Retrieved from: http://bcsth.ca/sites/default/files/Records%20Management%20Guidelines%20April%202006.pdf

SECTION E: TECHNOLOGY AND THE LAW

A.B. v. Bragg Communications Inc. (2012). SCC46, [2012] 2 S.C.R.567. Retrieved from:

http://scc.lexum.org/decisia-scc-csc/scc-csc/scc-csc/en/item/10007/index.do

Adams, W. (2004). “There is no There: *Intel Corp v Hamidi* and the Creation of new Common Law Property Rights Online.” 40 Can Bus LJI 87 at 87.

Barnett v Collection Service Co, 242 NW 25 (la 1932).

Boothman v Canada, [1993] 3 FC 381.

Century 21 Canada Ltd. Partnership v Rogers Communications Inc., 2011 BCSC 1196.

Company of Canada Limited, 1999 CanLII 2863 (ON CA) and *Anderson v Wilson*, 1999 CanLII 3753 (ON CA).

CompuServe Inc. v Cyber Promotions, Inc., 962 F Supp 1015 (SD Ohio 1997).

EBay, Inc. v Bidder’s Edge, Inc., 100 F Supp 2d 1058 (ND Cal 2000).

Federation of the Law Societies of Canada: http://www.flsc.ca/

Griffin v Sullivan, 2008 BCSC 827 at paras 81, 113

Government of Canada. (2013). Criminal Code. Canada. Retrieved from: http://laws-lois.justice.gc.ca/eng/acts/c-46/

Government of Canada. (2007). Divorce Act. Canada. Retrieved from: http://laws-lois.justice.gc.ca/eng/acts/d-3.4/

Government of Manitoba. (2011). The Domestic Violence and Stalking Act. Canada. Retrieved from: https://web2.gov.mb.ca/laws/statutes/ccsm/d093e.php

Fillion v Fillion. (2011). BCSC 1593 at paras 160, 162 [*Fillion*].

Feldthusen, *supra* note **Error! Bookmark not defined.**. *Frame v Smith*, 1987 CanLII 74 (SCC). *Rahemtulla v Vanfed Credit Union*, 1984 CanLII 689 (BC SC) [*Rahemtulla*].

Handford, P., Mitchell, P., and Mullany, N. (2006). *Mullany and Handford’s Tort Liability for Psychiatric Damage*, 2d ed. Sydney.

Heckert v 5470 Investments Ltd. (2008). BCSC 1298 at para 6.

Intel v Hamidi, 30 Cal 4th 1342, 71 P.3d 296 (Cal Sup Ct 2003).

L.A.M. v J.E.L.I. (2008). BCSC 1147 at para 2.

Linden, A., and Feldthusen, B. (2012). *Halsbury's Laws of Canada—Torts*, LexisNexis Canada.

Mainland Sawmills. (2006). BCSC 1195 at para 13 [*Mainland Sawmills*].

McDermott v Ramadanovic, 1988 CanLII 2840 (BC SC) [*McDermott*]. *Rhodes Estate v Canadian National Railway*, 1990 CanLII 5401 (BC CA) [*Rhodes*]. *Beaulieu v Sutherland*, [1986] BCJ No 2325

Nunavut Court of Justice. (1999). Appendix D: Non-Publication Orders Nunavut Court Of Justice. Court Records Access Policy. Nunavut Judicial System Implementation Act, S.N.W.T. 1998, c.34, as enacted for Nunavut, pursuant to the *Nunavut Act*, S.C. 1993, c.28. Retrieved from: http://www.nucj.ca/rules/CourtRecords_AppendixD.pdf

Osborne, P. (2007). *The Law of Torts*, 3rd ed. Toronto: Irwin Law Inc.at 260, 261.

Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

Rahemtulla, *supra* note **Error! Bookmark not defined.** at paras 34, 47, 50, 55.

Sheridan, L., and Grant, T. (2007). "Is cyberstalking different?" 13:6 Psychology, Crime & Law 627
Passo Services, 2008 SKQB 356 at para 49 [*Passo Services*]
Solomon, R., et al. (2007). Cases and Materials on the Law of Torts, 7th ed. Thomson Canada Limited. Scarborough.

Supreme Court of Canada. (2009 February 9). Access to Court Records. Policy for Access to Supreme Court of Canada Court Records. Section 4.11 Sensitive Case Files. And 5 Creation of Court Records; 5.2.3 Responsibility of the Parties. Canada. Retrieved from: http://www.scc-csc.gc.ca/case-dossier/rec-doc/pol-eng.aspx

Tran v Financial Debt Recovery Ltd. (2000). 193 DLR (4th) 168 rev'd [2001] OJ No 4103.

Tsige, *supra* note **Error! Bookmark not defined.** at paras 4-7.

Watts v Klaemt. (2007). BCSC 662 at paras 3-4.

SECTION F: GENERAL RESOURCES

BC Society of Transition Houses: www.bcsth.ca

Canadian Association of Social Workers: www.casw-acts.ca
Canadian Association of Social Worker Education: www.caswe-acfts.ca

Canadian Clearinghouse on Cyberstalking: http://www.cyberstalking.ca/en

Canadian Judicial Council: http://www.cjc-ccm.gc.ca

Canadian Legal Information Institute (CanLII): http://www.canlii.org/

Centre Canadien d'Information sur le Cyber-Harcèlement www.cyberstalking.ca/fr

Educaloi. (2012 January). Family Violence. A Legal Information Toolkit for Service Providers. www.educaloi.qc.ca/en/familyviolence

Habilo Médias. Le centre Canadien d'éducation aux médias et de littératie numérique: http://habilomedias.ca

Kids Help Phone: www.kidshelpphone.ca

Media Smarts: Canada's Centre for Digital and Media Literacy: http://mediasmarts.ca

Northwest Territories Access to Information and Protection of Privacy Act, SNWT 1994, c 20: http://www.canlii.org/en/nt/laws/stat/snwt-1994-c-20/latest/snwt-1994-c-20.html

Nunavut Family Abuse Intervention Act, including application forms for emergency protection order or community intervention order: http://www.nucj.ca/FAIA.htm

Office of the Privacy Commissioner of Canada: http://www.priv.gc.ca/index_e.asp

National Network to End Domestic Violence: http://nnedv.org/

Need Help Now: http://needhelpnow.ca/app/en/

Nonprofit Tech 2.0: http://nonprofitorgs.wordpress.com/

Province of Nova Scotia Canada. What is Bullying and Cyberbullying?: http://antibullying.novascotia.ca

Rules of the Court for the Nunavut Court of Justice: http://www.nucj.ca/rules.htm

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC): http://www.cippic.ca

SexAssault.ca: http://www.sexassault.ca/index.htm