BC Society of Transition Houses

Technology-Facilitated Gender Based Violence:

BC Anti-Violence Worker Technology, Safety and Privacy Survey Summary Report

September 2022

ACKNOWLEGMENTS

Research, Writing and Editing:

Alexandra George
Rhiannon Wong

We gratefully acknowledge Police Victim Services of British Columbia, the Ending Violence Association of British Columbia and the 137 anti-violence programs, who participated in our survey, for their contributions to making this report possible.

BCSTH acknowledges the Safety Net Project at the National Network to End Domestic Violence, United States for letting us adapt their survey.

BC Society of Transition Houses

Table of Contents

Background

The BC Society of Transition House's (BCSTH) Technology Safety Project provides anti-violence workers across British Columbia with information, resources and training about technology safety and technology-facilitated gender-based violence.

Technology-Facilitated Gender-Based Violence (TFGBV) occurs when digital spaces and devices are intentionally used to harass, abuse and or exploit others based on gender and/or sexuality. Similar to the LEAF definition, BCSTH defines TFGBV as the "spectrum of activities and behaviours that involve technology as a central aspect of perpetuating violence, abuse, or harassment [...]" against women and girls (Khoo, 2021). This can include restricting or limiting usage or access to technology, domestic violence, criminal harassment (stalking), sexual assault, impersonation and harassment. As Dunn points out, "Like other forms of gender-based violence, TFGBV is rooted in discriminatory beliefs and institutions that reinforce sexist gender norms. It intersects with racism, homophobia, transphobia, ableism and other discriminatory systems in many of its manifestations" (Dunn, 2020).

As technology evolves and becomes more prevalent in our daily lives, it is important to understand the impact of technology-facilitated gender-based violence in experiences of violence against women[1].

During the COVID-19 pandemic, BC anti-violence programs adapted their services in order to meet the needs of women, children and youth experiencing violence. This included addressing additional risks and safety concerns that arose due to pandemic restrictions, as well as shifting a significant amount of in person services to support provided over the phone or through virtual technology platforms such as Zoom and Doxy.me.

[1] **Women:** "Women and girls" refers to and is inclusive of all self-identified women. While we recognize that gender-based violence has significant impacts on cis-gender women and girls in Canada, we also acknowledge that 2SLGBTQQIA+ and gender non-conforming people are disproportionately impacted by experiences of violence and continue to experience significant barriers to anti-violence supports and services.

In August 2021, BCSTH surveyed British Columbia's anti-violence organizations to get a better understanding of:

- The prevalence of technology-facilitated gender based violence experienced by women, children and youth accessing anti-violence programs;
- Any new or increased ways organizations are connecting with their program participants under COVID-19 restrictions;
- Whether organization's use of technology to provide services has increased;
- If moving to online support has created barriers or improved anti-violence services for women, children and youth;
- Whether organization's use of technology has improved the provision of services for staff and/or created barriers for staff to provide service;
- The issues and concerns that programs are facing when it comes to confidentiality, privacy and use of technology, both for staff and service users.

Anti-violence organizations *provide a continuum of services, which share a common mission: to support* women, children and youth *who experience domestic and/or sexual violence.*

The anti-violence program respondents to the 2021 BCSTH survey were: Transition House (23.31%), Second Stage House (1.50%), Safe Home (6.02%), PEACE Program (24.06%), Stopping the Violence Counselling (16.54%), Community Based Victim Services (4.51%), Police Based Victim Services (17.29%), Outreach (3.76%), Sexual Assault Program (0.75%) Children's services outside of PEACE and VIP (0.75%), Family Preservation and Reunification Program/Family Services (1%).

This report summarizes the findings from BCSTH's August 2021 "BC Anti-Violence Program Technology Safety and Privacy Survey." The survey results summarize the scope and method of technology-facilitated gender-based violence experienced by women accessing anti-violence programs in BC and provides recommendations and discussion about the needs of women, children, youth and anti-violence workers when responding to technology-facilitated gender

based violence. All BCSTH Technology Safety Project resources are published on the BCSTH website at www.bcsth.ca

TECHNOLOGY-FACILITATED GENDER BASED VIOLENCE:
BC Anti-Violence Technology, Safety and Privacy Survey

Survey Respondent Information

BCSTH's Technology-Facilitated Gender Based Violence: BC Anti-Violence Technology, Safety and Privacy Online Survey recorded 137 responses in total.

The data shows that 48.46% of programs are receiving funding from the Ministry of Public Safety and Solicitor General while 28.46% continue to receive funding from BC Housing. Only 1.54% recorded that they receive funding from Indigenous Services Canada and the Ministry of Child and Family Development (Figure 1).

ANSWER CHOICES		RESPONSES	
BC Housing		28.24%	37
Ministry of Public Safety and Solicitor General		48.09%	63
Indigenous Services Canada		1.53%	2
Ministry of Child and Family Development		1.53%	2
Not Sure		15.27%	20
Other (please specify) (i.e. particular grants, community donations, etc.)	Responses	5.34%	7
TOTAL			131

Figure 1: Where does this program receive its funding from? (n = 131)

In terms of location, the majority (20%) of programs are in the Vancouver and the Lower Mainland region. Given that, 17.78% are located in the North and Vancouver Island. Other regions included Fraser Valley, Kootenays, Okanagan, and Cariboo.

The data shows that 32.84% of agencies are located in a smaller town whose population is between 5,000 and 29,999 people. Also, 27.61% stated that they are located in a small community with a population up to 5,000 people. Other programs (around 19.40%) are located in a medium to large city (Figure 2).

ANSWER CHOICES	RESPONSES	
Small community (population up to 5,000 people)	27.41%	37
Small town (population between 5,000 and 29,999);	33.33%	45
Medium city (population between 30,000 and 99,999);	17.78%	24
Large city (population of 100,000 and over)	19.26%	26
Other (please specify)	2.22%	3
TOTAL		135

Figure 2: What size best describes the community where your agency is located? (n=135)

Technology-Facilitated Gender Based Violence in BC

When asked if women and/or children have disclosed if they have experienced technology-facilitated gender-based violence such as threats and harassment via text messages or social media, sharing of non-consensual nude images, location tracking and/or stalking, 89.06% of participants responded “yes” (Figure 3).

ANSWER CHOICES	RESPONSES	
Yes	89.06%	114
No	10.94%	14
TOTAL		128

Figure 3: Have women and/or children and youth disclosed to you that they have experienced technology-facilitated gender-based violence? (n = 128)

Devices and Methods

When participants were asked how often different forms of technology were misused against women, children and youth, the majority responded that **assistive technology** such as preventing or breaking hearing aids, screen readers, or teletypewriter machines are "never" misused as a form of violence. However, it is important to note that this does not mean that this form of TFGBV does not ever happen. One explanation for this result may be because according to DAWN Canada, "there are various barriers [to accessing anti-violence programs] that specifically affect women with disabilities such as; difficulty in making contact with shelters or other intervention services, lack of access to information about available services, difficulties in accessing transportation, fear of losing their financial security, their housing or their welfare benefits and fear of being institutionalized[2]." This means that it may often be the case that women with disabilities do not necessarily reach out and access anti-violence resources and report their experiences of TFGBV.

However, what anti-violence did report is that the majority of participants disclosed to them that smartphones and laptops are "often" misused. It is interesting to note that landlines and desktop computers are rarely improperly used against women, children, and youth (Figure 4).

[2] https://dawncanada.net/issues/women-with-disabilities-and-violence/

	ALWAYS	OFTEN	SOMETIMES	RARELY	NEVER	TOTAL	WEIGHTED AVERAGE
Smartphones	22.11% 21	51.58% 49	25.26% 24	1.05% 1	0.00% 0	95	2.05
Landlines	1.11% 1	5.56% 5	23.33% 21	45.56% 41	24.44% 22	90	3.87
Tablets	7.37% 7	26.32% 25	50.53% 48	10.53% 10	5.26% 5	95	2.80
Laptops	5.38% 5	29.03% 27	51.61% 48	10.75% 10	3.23% 3	93	2.77
Desktop Computers	2.20% 2	18.68% 17	41.76% 38	29.67% 27	7.69% 7	91	3.22
IoT: Internet of Things (e.g. everyday devices such as thermostats, cars, appliances, smart watches, lights, clocks, security systems that are connected to the internet)	2.20% 2	8.79% 8	32.97% 30	21.98% 20	34.07% 31	91	3.77
GPS enabled location tracking device (separate from a smartphone)	5.38% 5	18.28% 17	30.11% 28	19.35% 18	26.88% 25	93	3.44
Assistive Technology (e.g., hearing aid, screen reader, Teletypewriter (TTY machine)	1.14% 1	2.27% 2	9.09% 8	17.05% 15	70.45% 62	88	4.53
Gaming Consoles	2.27% 2	4.55% 4	27.27% 24	19.32% 17	46.59% 41	88	4.03

Figure 4: How often are these kinds of technology misused against the women, children and youth you work with

(not just during the pandemic)? (n= 97)

Anti-violence workers also responded that the use of texting (29.17%), WhatsApp, Facebook Messenger, and Signal etc. are always misused even before the pandemic. In addition to texting, the misuse of social media was also ranked in the "always" category.

In contrast to these two forms of technology misuse, the majority responded that gig economy apps (i.e., Uber, Skip the Dishes, Airbnb) are never misused by abusers in their community (1.10%). However, again this does not mean that it does not happen.

The data also shows that the most common type of tech misuse women, children and youth report to staff members is harassment (59.77%), followed by threats (13.48%) and online monitoring/surveillance and stalking (5.06%). Doxing (i.e., when someone posts personally identifying information (e.g., name, address, phone number, email address, passport/SIN numbers) on social networks or websites without a woman's consent), was the least common (0.00%) (Figure 5).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Harassment	59.77% 52	18.39% 16	8.05% 7	3.45% 3	3.45% 3	1.15% 1	0.00% 0	0.00% 0	0.00% 0	0.00% 0	0.00% 0	1.15% 1	2.30% 2	0.00% 0	2.30% 2
Threats	13.48% 12	49.44% 44	15.73% 14	7.87% 7	4.49% 4	3.37% 3	0.00% 0	1.12% 1	2.25% 2	1.12% 1	0.00% 0	0.00% 0	1.12% 1	0.00% 0	0.00% 0
Monitoring/Surveillance	5.06% 4	2.53% 2	26.58% 21	12.66% 10	15.19% 12	7.59% 6	7.59% 6	8.86% 7	5.06% 4	5.06% 4	2.53% 2	0.00% 0	0.00% 0	0.00% 0	1.27% 1
Virtual Services Abuse (i.e. harassment/threat/coercion during virtual court, counselling, support services)	5.13% 4	2.56% 2	0.00% 0	7.69% 6	5.13% 4	10.26% 8	6.41% 5	6.41% 5	10.26% 8	5.13% 4	2.56% 2	6.41% 5	3.85% 3	10.26% 8	17.95% 14
Impersonation/Fraud	0.00% 0	1.35% 1	5.41% 4	4.05% 3	10.81% 8	2.70% 2	12.16% 9	8.11% 6	4.05% 3	14.86% 11	5.41% 4	12.16% 9	6.76% 5	6.76% 5	5.41% 4
Stalking (criminal harassment)	5.06% 4	7.59% 6	16.46% 13	13.92% 11	13.92% 11	10.13% 8	11.39% 9	3.80% 3	3.80% 3	7.59% 6	1.27% 1	3.80% 3	1.27% 1	0.00% 0	0.00% 0
Location Tracking	2.47% 2	7.41% 6	4.94% 4	18.52% 15	7.41% 6	7.41% 6	16.05% 13	9.88% 8	7.41% 6	3.70% 3	9.88% 8	2.47% 2	0.00% 0	1.23% 1	1.23% 1
Abuser limiting tech access	0.00% 0	2.50% 2	8.75% 7	10.00% 8	6.25% 5	18.75% 15	11.25% 9	15.00% 12	10.00% 8	7.50% 6	3.75% 3	2.50% 2	2.50% 2	1.25% 1	0.00% 0
Restricted speech (i.e. social media censorship)	2.70% 2	0.00% 0	1.35% 1	4.05% 3	2.70% 2	8.11% 6	1.35% 1	18.92% 14	17.57% 13	9.46% 7	14.86% 11	6.76% 5	2.70% 2	4.05% 3	5.41% 4
Damaging tech (physical and/or digital destruction)	2.56% 2	5.13% 4	6.41% 5	3.85% 3	11.54% 9	6.41% 5	8.97% 7	5.13% 4	12.82% 10	8.97% 7	10.26% 8	5.13% 4	3.85% 3	2.56% 2	6.41% 5
Non-Consensual Distribution of intimate Images	4.60% 4	3.45% 3	1.15% 1	10.34% 9	8.05% 7	3.45% 3	5.75% 5	3.45% 3	9.20% 8	10.34% 9	16.09% 14	8.05% 7	9.20% 8	3.45% 3	3.45% 3
Doxing (i.e. abuser posts her personally identifying information online without consent)	0.00% 0	0.00% 0	2.60% 2	5.19% 4	5.19% 4	2.60% 2	2.60% 2	2.60% 2	5.19% 4	10.39% 8	7.79% 6	23.38% 18	16.88% 13	10.39% 8	5.19% 4
Online sexual exploitation (perpetrator builds trust online for the purposes of sexual violence, abuse/trafficking)	1.32% 1	0.00% 0	2.63% 2	2.63% 2	1.32% 1	3.95% 3	2.63% 2	5.26% 4	1.32% 1	2.63% 2	7.89% 6	7.89% 6	19.74% 15	27.63% 21	13.16% 10
Online services and benefits abuse (abuser applies for benefits like CERB under her name and her funds go into his bank account)	0.00% 0	1.22% 1	1.22% 1	2.44% 2	4.88% 4	4.88% 4	4.88% 4	3.66% 3	2.44% 2	1.22% 1	7.32% 6	7.32% 6	18.29% 15	18.29% 15	21.95% 18
Online gender-based hate speech (i.e. slut shaming, target of gender-based racist or homophobic comments/posts.	2.33% 2	1.16% 1	8.14% 7	3.49% 3	6.98% 6	6.98% 6	4.65% 4	6.98% 6	3.49% 3	10.47% 9	1.16% 1	9.30% 8	12.79% 11	9.30% 8	12.79% 11

Figure 5: Please rank the most common kinds of tech misuse women, children and youth report to staff? Please rank 1 being the most common, 15 being the least. (n= 96).

BCSTH defines some of the most common types of TFGBV:

Harassment: perpetrator intentionally targets a woman with behavior that is meant to alarm, annoy, torment.

Monitoring/Surveillance (voyeurism): perpetrator monitoring and/or watching a woman via technology.

Threats: perpetrator makes threats via phone call, video call, email, text message and/or social media platforms.

Doxing: when someone posts personally identifying information (e.g. name, address, phone number, email address, passport/SIN numbers) on social networks or websites without a woman's consent.

Abuse of Assistive Technology: perpetrator destroying, breaking, taking away assistive technology devices such as hearing aid, screen reader, Teletypewriter (TTY) machine.

Supporting Women and Girls Experiencing TFGBV

When participants were asked how confident they felt when helping women, children and youth navigate technology in safety plans, 39.39% stated they are very confident talking about supporting her in making safety plans if an abuser finds out that she is planning to leave the relationship (Figure 6).

The following chart shows how confident anti-violence workers are when asked to support women, children and youth with various aspects of technology safety planning.

	VERY CONFIDENT	SOMEWHAT CONFIDENT	NEUTRAL	NOT AT ALL CONFIDENT	N/A	TOTAL	WEIGHTED AVERAGE
Securing their mobile devices (i.e., phone, laptop)	15.84% 16	45.54% 46	15.84% 16	20.79% 21	1.98% 2	101	2.42
Developing a technology safety plan	13.86% 14	50.50% 51	22.77% 23	11.88% 12	0.99% 1	101	2.33
Changing basic privacy settings in common apps and devices	26.73% 27	43.56% 44	15.84% 16	12.87% 13	0.99% 1	101	2.15
Talking with their kids about online and device safety and privacy	26.00% 26	52.00% 52	14.00% 14	7.00% 7	1.00% 1	100	2.02
Talking about plans if their partner finds out that she is planning to leave the relationship	40.00% 40	43.00% 43	5.00% 5	6.00% 6	6.00% 6	100	1.76
How to protect oneself from online harassment and stalking	15.00% 15	59.00% 59	16.00% 16	10.00% 10	0.00% 0	100	2.21
Documenting harassing messages, posts, or images	31.68% 32	47.52% 48	12.87% 13	7.92% 8	0.00% 0	101	1.97
Providing support on how to best address harassing messages, posts, or images	24.75% 25	47.52% 48	15.84% 16	11.88% 12	0.00% 0	101	2.15

Using social media content moderation and safety features (i.e., reporting, blocking, taking down content, regaining control of an account)	20.00% 20	44.00% 44	18.00% 18	18.00% 18	0.00% 0	100	2.34
Create new accounts or devices (including assistive tech)	19.19% 19	40.40% 40	18.18% 18	20.20% 20	2.02% 2	99	2.40
Communicating with service users about not exposing program staff's personal information	26.26% 26	41.41% 41	12.12% 12	16.16% 16	4.04% 4	99	2.19
Keeping information private when relocating (e.g., avoiding location tracking)	20.79% 21	40.59% 41	17.82% 18	18.81% 19	1.98% 2	101	2.35
Dealing with being monitored or surveilled online	4.00% 4	35.00% 35	25.00% 25	34.00% 34	2.00% 2	100	2.91
Making decisions about working in the gig economy	3.03% 3	18.18% 18	16.16% 16	48.48% 48	14.14% 14	99	3.28
Securing existing online accounts (including bank, utilities, etc.)	14.00% 14	33.00% 33	26.00% 26	24.00% 24	3.00% 3	100	2.62

Dealing with economic abuse (fraud, credit reports, etc.)	8.00% 8	33.00% 33	24.00% 24	32.00% 32	3.00% 3	100	2.82

Figure 6: How confident do you feel when helping women, children and youth navigate these tech safety steps? (n= 101).

Using Technology to Communicate with Women, Children and Youth

The COVID-19 pandemic has sparked many anti-violence programs to rethink service provision and had many increase their use of technology to communicate with women, children and youth. This section of the survey asked questions about the ways in which organizations understand the risks and benefits of using technology in its work with women, children and youth experiencing violence.

When participants were asked what technology they used for their agency crisis line, 76.34% responded landlines at their agency location and 3 responded "other" which included answers such as (Figure 7):

1. "Smart voice used on staff laptops"
2. "Work cellphones and zoom"
3. "We do not have a crisis line at our specific agency"

ANSWER CHOICES		RESPONSES	
Landlines at agency location (i.e., at the transition house)		76.34%	71
Cell phones dedicated to the crisis line provided to staff		47.31%	44
Routing voice calls to staff working from home		10.75%	10
Added web chat service		8.60%	8
Added text messaging service with phones provided to staff		45.16%	42
Added text messaging service with staff using personal phones		4.30%	4
Answering service		24.73%	23
Forwarding calls to another local, provincial, or national crisis line		9.68%	9
N/A		13.98%	13
Other (please specify)	Responses	3.23%	3
Total Respondents: 93			

Figure 7: What technology are you using for your agency crisis line? (Please choose all that apply). (n= 93).

When asked how participants provide ongoing support or intake with service users, 98.92% stated they use phone calls to communicate. In addition to phones, there are a variety of different forms of communication via technology used by programs when providing ongoing support as seen in (Figure 8).

ANSWER CHOICES		RESPONSES	
Phone calls		98.92%	92
Video calls		54.84%	51
Web chat		11.83%	11
Voice calls		45.16%	42
Text		75.27%	70
Messaging app (i.e., iMessage, WhatsApp, Signal, etc.)		8.60%	8
Email		87.10%	81
Contact via social media messaging (Facebook Messenger, Direct Message on Twitter or Instagram)		11.83%	11
Electronic document signing		23.66%	22
Meeting in person with health safety precautions		78.49%	73
Other (please specify)	Responses	4.30%	4
Total Respondents: 93			

Figure 8: How are you providing ongoing support or intake with service users? (n= 93).

Support groups play a big role in anti-violence programs. Many programs that offered group counselling or support also adapted their programming to offer groups online. The data from our survey shows that 31.52% of respondents continued to hold support groups in person but with health safety precautions. The other 31.52% of respondents suspended all groups during the pandemic. Others facilitated groups via video conferences (Figure 9).

ANSWER CHOICES		RESPONSES	
Conference calls (voice)		14.13%	13
Video conference		29.35%	27
Web chat rooms		5.43%	5
Meeting in person with health safety precautions		31.52%	29
Suspended all groups during the pandemic		31.52%	29
N/A		27.17%	25
Other (please specify)	Responses	0.00%	0
Total Respondents: 92			

Figure 9: How are you holding support groups? (n= 92).

Remote Work during the COVID-19 Pandemic

According to the data, 26.47% of respondents stated that funding and the costs of devices and services are challenges to starting and continuing to use technology to communicate with women, children and youth. In terms of the least challenging, 23.94% reported that there was insufficient quality of internet or WI-FI for staff. The data also shows that 89.89% of staff mainly used email accounts for remote working along with 76.40% of people who used mobile phones.

When participants were asked which tools they use if their program uses a cloud-based service for documents, email, calendars, or other office purposes, most (46.15%) stated that they use Microsoft 365 (Figure 10).

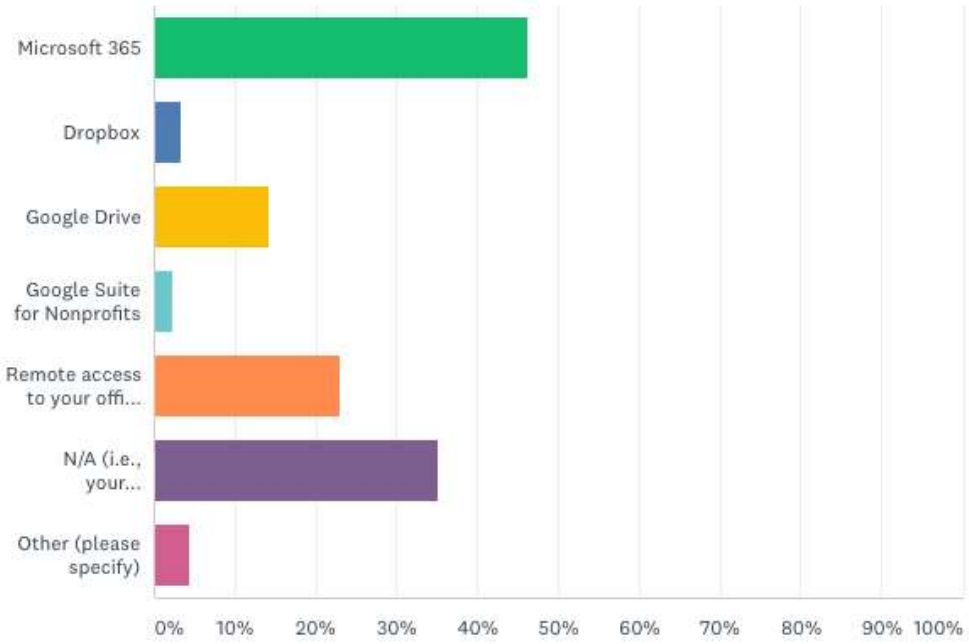

Figure 10: If your program is using cloud-based services for documents, email, calendars, or other office purposes, what tools are you using? (n= 91).

During the pandemic, there were many different forms of communication used in order to collaborate with other staff and community members (Figure 11). Email (97.85%), voice or conference calls (95.7%) and meetings via web based video conferencing (93.55%) were the top three forms modes of online communication.

ANSWER CHOICES		RESPONSES	
Email		97.85%	91
Voice calls/conference calls		95.70%	89
Meetings via web video conferencing		93.55%	87
Moved documents to cloud-based services		13.98%	13
Communication apps (i.e., Microsoft Teams, Slack)		46.24%	43
Accessed database remotely through secure network or VPN		22.58%	21
Participated in community tools to share available resources/capacity (e.g., availability of bed space)		8.60%	8
Other (please specify)	Responses	4.30%	4
Total Respondents: 93			

Figure 11: During the pandemic, how have you been collaborating with other staff and community partners? (n= 93).

Interestingly, 77.17% of participants responded that their program would continue to use technology to offer support and conduct intake after the COVID-19 pandemic.

Electronic Data Collection and Practices

BC and the Canadian government have proposed changes to various privacy and technology use laws and the creation of new ones. This section of the survey was to receive a better understanding of anti-violence program's use of technology to advocate for meaningful change by collecting practices as they relate to grant requirements and best practices for maintaining service user confidentiality.

Whether an anti-violence program is storing the confidential personal information of service users electronically or on paper, programs must develop policies and practices to ensure personal information of service users is protected and cannot be breached or intercepted. In order to safeguard the privacy and safety of service user's personal information when providing services through devices used by staff, 83.7% stated that passcodes are required on all devices. Only 2.17% responded that they do not have any protocols in place. As one participant in the

survey stated, “we have no protocols, but my impression is that staff are just using their varying levels of common sense” (Figure 12) which may or may comply with BC Privacy Laws.

ANSWER CHOICES	RESPONSES	
Passcodes required on all devices	83.70%	77
Different passcodes for each device	51.09%	47
Install and regularly update anti-virus/anti-malware software	68.48%	63
Only allow agency-owned devices for communication or work related to survivors	70.65%	65
Strictly limit the use of an agency-owned device to the staff member who uses it (no use by family, friends, etc.)	70.65%	65
Require use of a secure network or VPN to connect with the office, communicate with clients, or share client files	47.83%	44
Strictly limit app downloads on devices to only those that are necessary for work	47.83%	44
Regularly check privacy and security settings, of all apps, accounts, and devices	42.39%	39
Limit location sharing	18.48%	17
Prohibit location sharing	34.78%	32
Prohibit mingling of personal and professional data or accounts on devices	48.91%	45
Educate survivors about risks related to communicating with advocates over mobile devices	47.83%	44
Ensure devices can be remotely wiped in case of loss or theft	18.48%	17
Regularly purge data from the device	21.74%	20
Prohibit the use of backups	9.78%	9
Specific policies for the use of backups	13.04%	12
Prohibit / restrict the linking of a device to cloud accounts like iCloud or Google Cloud	20.65%	19
Only utilizing secure software (end to end encryption)	28.26%	26
Regularly delete all incoming and outgoing text messages	32.61%	30
Regularly delete all incoming and outgoing call logs	30.43%	28
Regularly delete all voicemails	58.70%	54
When getting rid of old devices, restore them to factory settings to ensure all information is deleted	54.35%	50
Notify survivors if voicemails are transcribed into emails or text messages so that they can make informed decisions about risk and safety	14.13%	13
Limiting or prohibiting recording of participant information (i.e., name, phone number, contact details, etc.) on mobile device	42.39%	39

Figure 12*: If applicable, what protocols do you have in place to help safeguard participant’s privacy and safety when providing services through devices used by staff? (n= 92).*

The data shows that 68.13% of respondents stated that their program explains the privacy risks to service users when using technology to provide services (i.e., email, text, web chat, video call) to receive informed consent. When the participants were asked if there are times when privacy and confidentiality statutory obligations (BC PIPA, Privacy Act, etc.) conflict with program participant centered service provisions, 40.22% responded "no" and 11.96% responded "yes." Other participants (47.83%) did not know. For those who stated "yes," a few barriers included the following:

1. "A client agrees to privacy laws then chooses to want her file destroyed prior to what law dictates"
2. "More consent forms to read, sign and collect"
3. "Participants are resistant to using new technology/programs that provide security as outlined by the privacy act"
4. "Sometimes receiving no response from client and at the same time not being able to give them any useful information until they do"

When asked what solutions, if any, have their organization developed to address these barriers, a few participants responded the following:

1. "Consultations about the law and limitation to our organization"
2. "None"
3. "Educating clients on the technology and making it as easy as possible to use. If they are still resistant but want to continue using technology/programs they are comfortable with letting them know the risks as well as limiting the topics that are discussed"
4. "Communicating with client first through other method like phone call or in person and discussing the use of technology with them so that they understand"

When asked which privacy act or regulation does their program follow, 35.87% stated BC Personal Information and Privacy Act (BC PIPA), 5.43% stated Personal Information Protection and Electronic Documents Act (PIPEDA), 13.04% stated BC Freedom of Information and Privacy Act (BC FOIPA), 1.09% stated BC government Ministries - such as the Ministry of Children and Family Development (MCFD) and 40.22% stated that they are "not sure." Also, 42.39% stated

that they are “not sure” if their agency has a designated privacy officer, 33.70% responded “yes,” and 23.91% stated “no.”

Privacy Breach

1. 64.13% of participants responded that their program has not experienced a privacy breach (for example, personal information sent to the wrong email address, online server or database has been hacked, staff from an external organization or program has access to case management files). 8.70% responded “no” and 26.09% stated that they are “not sure”. For those who responded “yes,” their organization’s protocol and who they inform is as follows: “Executive Director”
2. “Not sure of the protocol but HR/manager would be informed”
3. “Our IT department is very involved with protocols, and we also have to take internet security tests frequently”
4. “No PEACE client information goes on electronic devices. Paper files are triple locked in secure files. CEO would activate protocols”

When asked if any transition housing programs or victim service locations are confidential, 59.78% responded “yes” and 19.57% responded “no” (Figure 13).

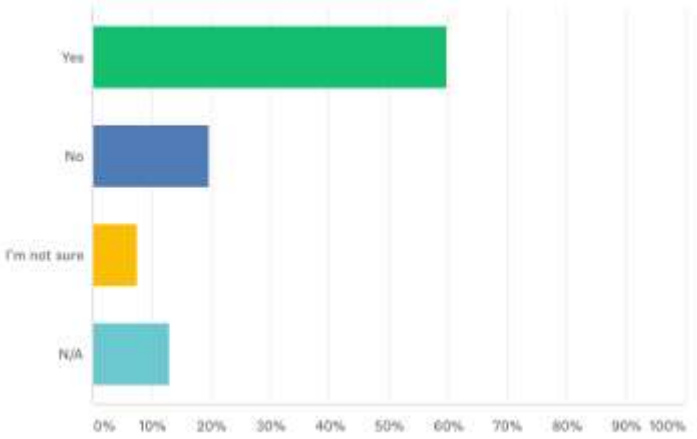

Figure 13: Are any of your transition housing programs or victim service locations confidential? (n= 92).

Having access to technology while participating or residing in an anti-violence program can empower a woman, child or youth and positively affect their self-determination. 37.08% of participants stated “yes,” they do have specific guidelines or restrictions on how participants

use technology and mobile devices while staying in a transition housing program. 17.98% stated "no" and 44.94% did not know.

For those who responded "yes", a few guidelines included:

1. "Location services turned off, no FaceTime or cell phone use in common areas of the home, phone on silent during sessions"
2. "No GPS using apps, change personal e-mail passwords"
3. "Possibly close old social media accounts"
4. "No taking pictures"

Use of Electronic Database Systems

Online case management systems, also known as databases have been an increasing inquiry of anti-violence programs. In this survey we asked if anti-violence programs were using electronic databases and what programs they are using.

3.70% of participants currently use Empower DB database, 11.11% use WISH, 3.70% use Share Vision, 43.21% stated that they do not use an electronic database. Other responses included:

1. "VSIS"
2. "Nucleus"
3. "Silent Partner"
4. "RCMP"
5. "Prime"
6. "WEB DAV"
7. "COAST"

When asked the purpose of the database, 41.98% of participants responded that the database helps them to complete case management, 39.51% stated service tracking, 11.11% stated room assignments, 17.75% stated outcome tracking, 14.81% stated grant reporting and 30.86% stated historical record keeping. For those who stated "others" these included:

1. "Quarterly reports, family goal plans"

2. “Stats”
3. “Donor data”

When asked what participant information is collected and stored in their program’s database or stored online in a different method such as an Excel spreadsheet or Google doc, answers varied from name, phone number, date of birth etc. (Figure 14).

ANSWER CHOICES		RESPONSES	
Name		63.10%	53
Date of birth		57.14%	48
Social Insurance Number		2.38%	2
Address		51.19%	43
Phone number		58.33%	49
Email address		48.81%	41
Citizenship		13.10%	11
Immigration Status		19.05%	16
Indigenous Status		28.57%	24
Abuser's name		36.90%	31
Children's names		44.05%	37
Children's ages		46.43%	39
Case notes		53.57%	45
Health related information		17.86%	15
Court related information		38.10%	32
Law enforcement related information		29.76%	25
Photographs		3.57%	3
N/A		32.14%	27
Other (please specify)	Responses	4.76%	4
Total Respondents: 84			

Figure 14: What participant information do you collect in your database or store online in a different method such as an Excel spreadsheet or Google doc? (n= 84).

For those who responded "Other," responses included:

1. "Resident file number and dates of stay"
2. "Cultural needs"
3. "Goal setting and tracking"
4. "Experiences and needs"
5. "Preferred service language, physical description, and alternate names"

45.98% of participants responded that their organization has data retention guidelines for both electronic and paper files that specify how data is maintained and when it is purged or disposed. 31.03% have data retention guidelines for paper files only and 1.15% for electronic files only. Also, 5.75% responded that their organization does not have data retention guidelines and 12.64% responded that they are not sure.

When asked if service users are informed about their right to opt out of having data entered or their right not to answer certain questions. 58.62% responded "yes", 26.44% responded "no," and 14.94% responded that they are "not sure" (Figure 15).

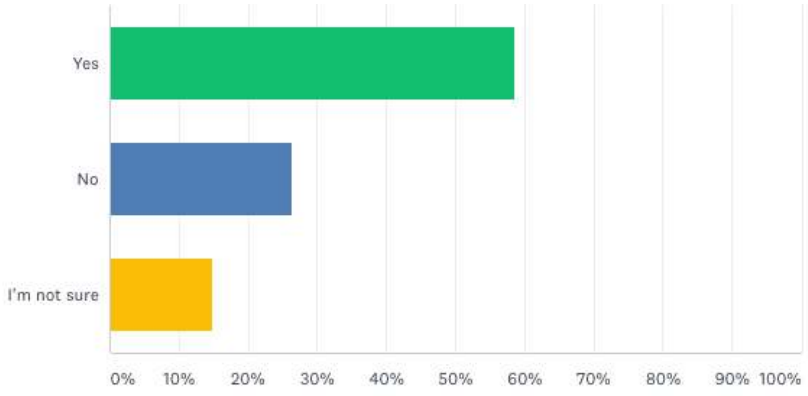

Figure 15: Are participants informed about their right to opt out of having data entered or their right not to answer certain questions? (n= 87).

When respondents were asked how long they kept personally identifying information about a service user (both paper and electronic), answers varied (Figure 16).

ANSWER CHOICES	RESPONSES	
We keep all personally identifying data for as long as is necessary to complete a specific task	12.20%	10
We keep all personally identifying data for the duration of time spent providing services and dispose once the person is no longer receiving services	10.98%	9
Once services are complete, we purge everything but the service user's name and the fact that they were served	3.66%	3
We regularly purge personally identifying information but maintain financial records for a specific amount of time	3.66%	3
We keep everything, including personally identifying information, and do not purge files.	15.85%	13
We keep all personally identifying data for a specific amount of time. Please tell us how long you keep that information Responses	64.63%	53

Figure 16: *How long do you keep personally identifying information about a service user (both paper and electronic)? (n= 82).*

For those who choose "Other," (64.63%) responses included:

1. "7 years"
2. "10 years"
3. "6 years"
4. "10 years or until the youngest child in file reaches 19"
5. "Hard client files are archived for 30 years"
6. "6 years after minor coming of age"

When asked if respondents have protocols to ensure that electronic files that contain service user information (i.e., resumes, court forms, etc.) are regularly purged from all agency devices, including computers, scanners, copiers, and mobile devices, 50.57% stated that they are not sure. However, 27.59% responded "yes" and 21.84% responded "no" (Figure 17).

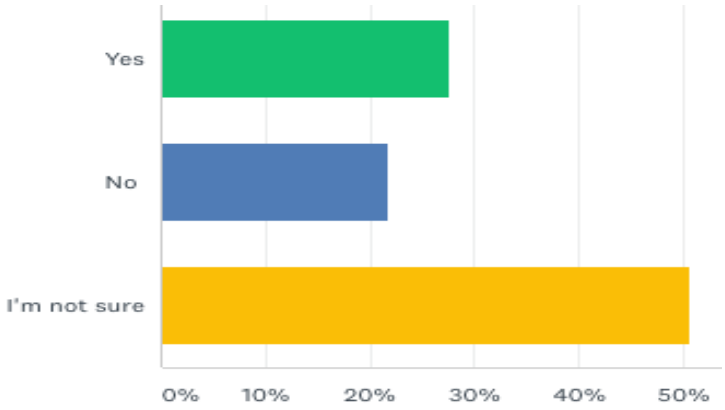

Figure 17: *Do you have protocols to ensure that electronic files that contain service user information (i.e., resumes, court forms, etc.) are regularly purged from all agency devices, including computers, scanners, copiers, and mobile devices? (n= 87).*

Community Partnerships and the Sharing of Personal Information

70.11% of participants stated that their agency participates in collaborations where information about individual participants might be requested or is expected to be shared (e.g., ICAT tables, community coordination committees, Violence Against Women in Relationships (VAWIR) committees). 11.49% stated "no" and 17.24% stated that they are "not sure." 1.15% do not participate in any community collaborations or partnerships.

Anti-violence programs were asked if their program had been or is currently undergoing third party accreditation. This question was asked as some accreditation agreements require access to the person information and records of women, children and youth experiencing violence. Figure 18 demonstrates whether or not certain programs are accredited or in the process of being accredited (e.g., CARF or COA certified).

ANSWER CHOICES	RESPONSES	
Yes	22.99%	20
No	29.89%	26
In progress	4.60%	4
We have been talking about it	2.30%	2
My program is not, but other programs within our agency are	5.75%	5
I'm not sure	34.48%	30
TOTAL		**87**

Figure 18: *Is your program accredited or in the process of being accredited? (e.g., CARF or COA certified) (n= 87).*

According to the data, some funders of anti-violence programs require programs to report the demographic information of the service users they work with. Responses varied in terms of what kind of demographic information funders required. For instance, 25.29% stated their funders only required aggregate demographic totals, 1.15% stated their funder only required aggregate demographic totals only if a certain number of people per demographic category has been reached, 12.64% stated funders required individual level demographic data, 13.79% stated that their funders do not require them to report demographic information, and 44.83% stated that they are not sure.

For those who selected "Other" (2.30%) responses included:

1. "We only supply general non-identifying demographic information"
2. "Age and sex only"

Privacy, Confidentiality and Social Media

Many organizations have social media accounts as a way to provide another avenue for women, children and youth in their community with information about available resources and supports. When respondents were asked if their organization has protocols to ensure that program participants retain control over whether and how personally identifiable information is and is not used on their social media, outreach, fundraising and other promotional activities, 42.53% of participants stated that their organization does not use the stories of people who have received our services for these purposes. 31.03% stated "yes,"2.30% stated "no," and 24.14% stated that they are "not sure." Protocols included:

1. "We do not share participant information"
2. "Any identifying information is removed from any promotional material"
3. "Permission required, documented and signed on release forms"
4. "Consent for story to be shared and where/how"
5. "Waivers they can consent and sign"
6. "Maintain paper files, not electronic files"

36.78% stated that their organization has protocols to ensure that staff and volunteers retain control over whether and how personally identifiable information is and is not used in their social media, outreach, fundraising and other promotional activities. 5.75% stated "no," 28.74% responded that they are "not sure" and 28.74% stated that their organization does not use the stories of program participants who have received our services for these purposes (Figure 19).

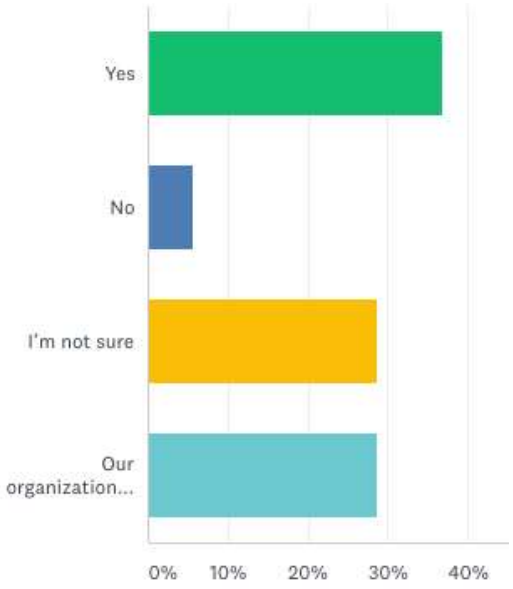

Figure 19: Does your organization have protocols to ensure that staff and volunteers retain control over whether and how personally identifiable information is and is not used in your social media, outreach, fundraising and other promotional activities? (n= 87).

When asked what the biggest challenges organizations are face in maintaining the privacy of women, children and youth, responses varied:

1. "The women talking to other women in the house"
2. "It's a small community and people talk"
3. "Keeping up with technology"
4. "Making sure clients don't disclose the location of transition houses"
5. "Emails. Online social media"
6. "Confidentiality of the address and location"
7. "Tech-savvy abusers"
8. "Lack of policy and procedures for electronically stored information and a lack of attention to policy and procedure on file"
9. "Guest not respecting the privacy of each other"

10. “Spyware, location tracking, doxing, etc.”

Connectivity

Program participants reported that a lack of access to technology and/or concerns that their abuser may be monitoring their use of technology has negatively impacted their ability to access domestic and/or sexual violence support (78.21%), employment (44.87%), housing (52.56%), education (24.36%), benefits and/or insurance (i.e., CERB, EI, IA,) (42.31%), civic participation (6.41%), social connection and support (76.92%).
For those who specified “Other,” (8.97%) this included:

1. “None”
2. “Connection with family and friends”
3. “Parental Alienation”

When asked what issues may arise from the lack of technology (mobile devices, computers, Internet, WI-FI) for women, children and youth experiencing violence, 93.98% stated increased isolation of the participant (e.g. separation from family and peers, digital and technological isolation, etc.). Also, 89.16% stated decreased ability to seek support, 83.13% stated decreased likelihood of seeking support/accessing services, 28.92% stated increased intensity of technology-facilitated violence, and 56.63% reported increased intensity of violence other than tech abuse (e.g. physical, emotional, financial, sexual abuse).
For those who selected “Other,” (4.82%) these included:

1. “Lack of education on tech security”
2. “Lack of WI-FI services around town”
3. “Harassment”
4. “Unaware of any”

When asked, "according to your program's service users, what have you been told regarding barriers to access services that you provide?" participants recorded a variety of responses. Lack of access to childcare (78.57%), lack of access to transportation (76.19%) and Affordability of devices, phone plans, internet plans, and tech repair (59.52% were the top three barriers to accessing anti-violence services (Figure 20)

ANSWER CHOICES	RESPONSES	
Lack of access to transportation	76.19%	64
Lack of access to childcare	78.57%	66
Lack of access to culturally informed services (social, religious, personal accommodations and understanding from employees to clients)	30.95%	26
Language barriers/translation (i.e., virtual and in-person content/services not available in multiple languages)	32.14%	27
Lack of access to legal aid (e.g., costs of applications and forms, legal counseling, legal representation)	46.43%	39
Personal status concerns (e.g., using technology to evoke deportation fears, limited knowledge on rights and freedoms, financial sponsorship undertakings/abuse, etc.)	22.62%	19
Tech literacy	45.24%	38
Format of service delivery (i.e., virtual or in person complications, ex. access to virtual services through ZOOM)	35.71%	30
Privacy concerns (e.g., Sheltering at home with an abuser, shared devices, barriers to evidence preservation, etc.)	48.81%	41
Tech Affordability (i.e., devices, phone plans, internet plans, tech service repair, etc.)	59.52%	50
Lack of consistent access to devices	51.19%	43
Lack of infrastructure for connectivity (e.g., no cell reception in the area)	42.86%	36
Low quality of signal and/or reliability (e.g.,there is a basic internet connection, but it only works at certain times of day).	54.76%	46
Stigma surrounding affordable internet programs (not wanting to go through government agencies to receive reduced monthly rates)	11.90%	10
Other (please specify) Responses	5.95%	5
Total Respondents: 84		

Figure 20: According to your program's service users, what have you been told regarding barriers to access services that you provide? (n= 84).

Other responses (5.95%) included:

1. "Long waitlist"
2. "We don't always have this information"
3. "Stigma and visibility of seeking services in a small community"
4. "Lack affordable housing"

5. “Clients feel like they are not valued, isolated marginalized because our shelter does not have WI-FI”

55.29% of respondents stated that service user’s lack of technology has made their program’s service delivery more difficult. However, 28.24% responded “no” and 16.47% stated that they are not sure if technology was a barrier to accessing service.

For those who stated “yes, “connectivity issues impacted the service delivery process in many ways such as the following:

1. “Some clients don’t have phones which makes it difficult to reach them”
2. “I have mostly been meeting people in person and when doing things, we have done them over the phone or the computer – whatever clients are most comfortable with”
3. “We provide service to a lot of outlying areas where internet is either not available or very unreliable at best”
4. “Patchy internet for rural clients, interrupted service, and safety concerns”
5. “Being unable to attend counseling sessions due to pandemic, transportation and lack of connectivity”
6. “Out of service range”

At the start of the pandemic, some anti-violence programs struggled to meet remote work tech needs for a variety of reasons. When participants were asked if their program’s lack of technology made their program’s service delivery more difficult, 77.38% responded “no”, 14.29% responded “yes” and 8.33% responded that they are not sure.

In terms of technology being incorporated into service delivery, 84.71% of participants agreed with the fact that technology played a positive role in their program’s service delivery. 3.53% stated “no” and 11.76% responded that they are not sure. For those who stated “yes”, it has helped in ways such as:

1. “Allows to connect with others. It became particularly important during the pandemic when all face-to-face meetings and home visitations were not allowed”
2. “Fast and reliable connection to various services and resources”
3. “Sending emails has been beneficial when reinforcing conversations with clients that may be overwhelmed”
4. “Provided zoom meetings during the pandemic”
5. “Reminder texts have decreased no- shows”
6. “Reduce barriers related to anxiety about leaving home”
7. “Connection with wider community through social media”
8. “Better organized case notes accessible for all staff in multiple locations”

Training and Resource Development

When participants were asked if their employee training and educational material provided sufficient awareness and comprehension of diverse topics, the data within the chart below shows how anti-violence workers perceive the following training topics (Figure 21):

	SUFFICIENT	SOMEWHAT SUFFICIENT	NOT SUFFICIENT	TOTAL	WEIGHTED AVERAGE
Service users with different legal status (e.g., immigrant, migrant worker, refugee, non-status/ legally unrecognized, etc.)	19.51% 16	40.24% 33	40.24% 33	82	2.21
Service users from/in rural and remote communities	38.75% 31	45.00% 36	16.25% 13	80	1.77
Technology safety planning (e.g., using technology safely, legal remedies for TFV, etc.)	25.93% 21	53.09% 43	20.99% 17	81	1.95
Technology literacy (e.g., Using appropriate software and programs, basic privacy and safety knowledge, data collection, navigating video conferencing software, etc.) Sufficient Somewhat sufficient	32.10% 26	44.44% 36	23.46% 19	81	1.91
Privacy and confidentiality obligations (BC PIPA, records keeping, etc.)	53.09% 43	33.33% 27	13.58% 11	81	1.60

Best practices for culturally informed services (e.g., understanding community's diverse Indigenous and newcomer cultures, understanding sexuality and what is considered sexually explicit content in various cultures, diverse training materials such as Newcomer power and control wheel and Indigenous distinction based training and resources)	41.98% 34	45.68% 37	12.35% 10	81	1.70

Figure 21: Does your employee training and educational material ensure sufficient awareness and comprehension of the following? (n= 82).

When participants were asked what type of training and technical assistance, they would prefer related to understanding obligations/ information sharing, 79.73% stated they would benefit from "Better understanding of privacy obligations under provincial laws" and 77.03% stated "Better understanding of privacy obligations under federal laws". Other responses were scattered (Figure 22).

ANSWER CHOICES		RESPONSES	
Better understanding of privacy obligations under federal laws		77.03%	57
Better understanding of privacy obligations under provincial laws		79.73%	59
How to work with community partners to understand our shared privacy obligations		48.65%	36
How to share information with community partners		55.41%	41
How to work with accreditation organizations such as CARF and/or COA to ensure privacy obligations are followed		27.03%	20
How to work with funders to ensure privacy obligations are followed		27.03%	20
How to work with organizations' board of directors to ensure privacy obligations are followed		21.62%	16
How to work with staff to ensure privacy obligations are followed		50.00%	37
How to work with volunteers to ensure privacy obligations are followed		17.57%	13
Other (please specify)	Responses	1.35%	1
Total Respondents: 74			

Figure 22: What kind of training and technical assistance would you like for the tech topic: UNDERSTANDING OBLIGATIONS/ INFORMATION SHARING? (n= 74)

For the participant who selected "Other," they specified:

1. "How to encourage local RCMP to take tech-related violence seriously"

When participants were asked the same question below but for the topic of "technology, communication with participants, and confidentiality," text message privacy practices and polices (71.25%), how to help participants increase their knowledge and personal agency on

privacy related issues (70%) and email privacy practices and policies (68.75%) were the top three responses as shown. in figure 23.

ANSWER CHOICES	RESPONSES	
Email privacy practices and policies	68.75%	55
Text message privacy practices and policies	71.25%	57
Direct messages via social media (i.e., Facebook messenger) privacy practices and policies	46.25%	37
Messaging app (i.e., iMessage, WhatsApp, Signal, etc.) privacy practices and policies	36.25%	29
Online chat service privacy practices and policies	42.50%	34
Video Web Conferencing Call privacy practices and policies	60.00%	48
Website contact form privacy practices and policies	31.25%	25
Social media privacy practices and policies	42.50%	34
TTY privacy practices and policies	15.00%	12
Fax privacy practices and policies	21.25%	17
How to help participants increase their knowledge and personal agency on privacy related issues	70.00%	56
Other (please specify) Responses	0.00%	0
Total Respondents: 80		

Figure 23: What kind of training and technical assistance would you like for the tech topic: TECHNOLOGY COMMUNICATION WITH PARTICIPANTS, AND CONFIDENTIALITY? (n= 80)

When participants were asked what type of training and technical assistance would they like for the topic of "data collection," 78.08% stated "how to meet data collection requirements while also minimizing the amount of information collected", 71.23% responded "how to track progress, measure our program's effectiveness, and collect data about our work while also

providing participant centered services", 42.47% stated "how to work with funders or other partners when they demand excessive data about participants", and 65.75% stated "best practices related to how long we should retain participant data".

When participants were asked what type of training and technical assistance they would like for the topic of "databases and confidentiality," the responded were scattered. The majority (72.06%) responded "support understanding how different types of databases might support or compromise privacy obligations". The minority of people responded (30.88%) responded "how to work with a database vendor to ensure that the database used meets the agency's privacy obligations" (Figure 24).

ANSWER CHOICES		RESPONSES	
Support understanding how different types of databases might support or compromise privacy obligations		72.06%	49
Support understanding as to increasing database security using protocols (like encryption) or practices (such as internal policies)		52.94%	36
Figuring out if a specific database software meets best practice standards		54.41%	37
How to work with a database vendor to ensure that the database used meets the agency's privacy obligations		30.88%	21
Support in navigating privacy in databases in a co-located program (i.e., an organization has more than one program accessing information in one database)		35.29%	24
Support in navigating privacy in databases		45.59%	31
Other (please specify)	Responses	4.41%	3
Total Respondents: 68			

Figure 23: What kind of training and technical assistance would you like for the tech topic: DATABASE AND CONFIDENTIALITY? (n= 73)

In terms of BCSTH Tech Safety resources, 77.61% of respondents stated that they "attended webinars or recordings", 34.33% stated that they "attended an in-person training", 35.82%

stated they attended a "Tech Safety Training at our Annual Training Forum", 44.78% stated that they used "handouts shared by a colleague or partner organization or BCSTH", and 70.15% "accessed online resources at https://bcsth.ca/technology-safety-project-resources/ ".

When participants were asked what BCSTH can do to improve our technology safety resources, responses varied as followed:

1. "Maybe have resources available for parents, children and service providers. How to teach tech safety with young children and adolescents"
2. "Increased knowledge and awareness"
3. "I think they are great"
4. "More training on tech safety resources"

Recommendations and Discussion

i. Tech-Facilitated Gender Based Violence

The data shows that tech-facilitated gender-based violence has become a prevalent issue across BC. 89.06% of participants stated that women and/or children have disclosed that they have experienced technology-facilitated gender-based violence such as threats and harassment via text messages or social media, sharing of non-consensual nude images, location tracking and/or stalking (as shown in figure 3).

In comparison to last year's report "BC Anti-Violence Worker Survey Results Report," 87.6% of women have disclosed that they have experienced technology-facilitated violence. In last year's report 91.67% of survey respondents stated that women have experienced various forms of harassment. The data in that survey found that harassment, threats and criminal harassment are most commonly received via text, social media and email on women's smartphones, laptops and tablets. Location tracking through GPS enabled devices was also identified as a common way that perpetrators misuse technology to (criminally) harass and monitor women. Similar to this year's survey, harassment has been ranked the most popular form of tech related violence that increased significantly during the COVID-19 pandemic.

In order to decrease tech-facilitated gender-based violence, survey respondents stated that there should be more resources available for parents, children and service providers. Many found that there is a lack of education and resources that teach tech safety to parents, young children and adolescents. Awareness and consistent educational resources may help in supporting anti-violence workers to identify TFGBV and support women to safety plan for their experiences of TFGBV. An effort must also be made to prevent abusers from using technology as a form a violence. This may include working with law enforcement, judges and schools to enhance skills to hold abusers accountable and ensure that communicating through technology is not mandated.

ii. Using technology to communicate with Women, Children and Youth and Connectivity

The data shows that the misuse of technology to harm people and the strategies to increase safety and privacy of those targeted are constantly evolving. 26.47% of respondents stated that funding and the costs of devices and services are challenges to starting and continuing to use technology to communicate with women, children and youth. Also, 23.94% recorded that there was insufficient quality of internet or WI-FI for staff. According to the "Connectivity and Violence against Women in BC"[3] report, the key barriers to meaningful connectivity is affordability, access, infrastructure, and tech literacy. Similar to the data, affordability and the lack of funds plays a role in maintaining and developing proper communication and connectedness between staff, women, children and youth.

In order to use technology in a safe and efficient way, affordable internet and phone programs can be used. Simultaneous work could be conducted related to program equity. Also, there is a need to advocate for connectivity infrastructure (ex. cell phone towers, internet wiring, etc.) to expand availability of affordable access plans where they are most needed. In addition, "increase speeds offered in affordable access programs to meet targets in order to help

[3] Cahill, R., Kaya, Z. (2021). Connectivity and Violence Against Women in British Columbia: TFGBV, barriers, impacts, and recommendations. The BC Society of Transition Houses.

facilitate equitable and meaningful connectivity for all" (BCSTH, 2021). Interestingly, we cannot ignore the fact that programs (approx. 70%) will continue to use technology in a meaningful way even after the pandemic is over (BCSTH, 2021). In order for this programs to use technology meaningfully, funders must include and increase anti-violence program budgets to make room for updated technological devices, secure connections and the cost of internet and mobile phone plans.

iii. Electronic Data Collection and Practices (Privacy)

When survey respondents were asked which privacy act or regulation does their program follow, 35.87% stated BC Personal Information and Privacy Act (BC PIPA), 5.43% stated Personal Information Protection and Electronic Documents Act (PIPEDA), 13.04% stated BC Freedom of Information and Privacy Act (BC FOIPA), 1.09% stated BC government Ministries - such as the Ministry of Children and Family Development (MCFD) and 40.22% stated that they are not sure.

It is alarming and problematic that 40.22% did not know which privacy act or regulation their program follows. This means that they are unaware of the laws they must adhere by. By not knowing this crucial information, confidential information about women, children, and youth can be stored in an unsafe manner, exposing them to potential violence through a potential privacy breech.

To safely process and handle client's information, it should be recommended that all staff be trained on the privacy act and/or regulation that their program follows and its mandatory compliance rules to maximize security and privacy.

It is our hope that these BCSTH survey report findings will encourage BC's organizations to recognize the prevalence of technology-facilitated violence in violence against women. There is a need for change and for organizations to respond to this reality, especially after the consequences of the pandemic. This data provides crucial insight into current safety and privacy practices among anti-violence organizations while also helping the BC Society of Transition Houses design future resources and trainings.

We thank all the programs across BC for taking the time out of their busy days to fill out the BCSTH survey. These survey findings will guide the TFGBV work of the BCSTH Technology Safety Project.