CYBERSEXUAL VIOLENCE

What is Cybersexual Violence?

Although there is currently no universally-accepted definition, cybersexual violence or CSV can be described in simple terms as using social media and other communication technologies for the purpose of:

- Sexual comments or advances
- Attempts to obtain a sexual act
- Unwanted sexual acts
- Sexual coercion

CSV can also be about spreading rumours online, sending messages, photos, and/or videos that are damaging to one's reputation, impersonation, and much more.

All of these behaviours aim to damage a person's feelings, self-esteem, reputation, and mental health.

DRCC
DURHAM RAPE CRISIS CENTRE

Adapted from the University of Ottawa

COMPARISONS TO CONSIDER

Online Hate, Cyberbullying, and Cybersexual Violence

Online Hate is generally rooted in hatred of a specific group, based on gender, identity, race, religion, nationalist, sexual orientation, or other characteristics.

Cyberbullying is often associated with children and youth being harassed online, although when it is used to describe violence against women and girls, it does not always address the root causes of gendered violence and harassment.

Cybersexual Violence or CSV has varying definitions, and includes online harassment, as well as threats of physical harm such as sexual assaults, murders, and suicides. According to the United Nations, CSV is as damaging to women and girls as physical violence.

DRCC
DURHAM RAPE CRISIS CENTRE

Adapted from the
Canadian Women's Foundation

RELATED TERMINOLOGY

Covert Surveillance (Stalkerware) - monitoring software or spyware that is used for cyberstalking

Culture of Visibility – refers to how posting information to the Internet has become a normalized practice

Cyber Misogyny – acknowledges that women and girls are more likely to face online hate speech or harassment, and how digital tools are used to harass women and girls because of their gender

Cybersex Trafficking - a cybercrime involving sex trafficking and the live streaming of coerced sexual acts and/or rape on webcam

Cyberstalking - repeated and unwanted e-mails, texts, or social media messages, and can involve posting inappropriate or personal information or pictures on social media

Deepfake - a video of a person in which their face or body has been digitally altered so that they appear to be someone else, typically used maliciously or to spread false information

Denial-of-Service Attacks - an attack meant to shut down a machine or network, making it inaccessible to its intended users

Doxing - the practice of digging up information on a person to post online to websites that will often encourage participants to harass their target

Flaming - messages, often containing offensive, abusive, and/or discriminatory language, posted on online discussion forums to offend other forum members

Hacking - gaining illegal access to an individual's or organization's online services for reasons such as to acquire or alter personal information, slander, or create harm

DRCC
DURHAM RAPE CRISIS CENTRE

RELATED TERMINOLOGY

Impersonation - situations where someone maliciously uses another person's online identity for their benefit

Non-Consensual Sexting - sending intimate photos or messages without permission

Online Abuse & Harassment - using technology to continuously contact, annoy, threaten, and/or scare the victim

Rape/Death Threats - a threat made against another person of rape, sexual assault, or murder

Revenge Porn - occurs when individuals post intimate photographs or videos of another person online to humiliate them or negatively impact their life

Sextortion - the practice of extorting money or sexual favors from someone by threatening to reveal evidence of their sexual activity

Sexual Exploitation/Luring of Minors - being coerced into removing clothing and posing sexually for a webcam or being solicited for sex as a minor

Sexual Privacy - a distinct privacy interest that warrants recognition and protection of the human body, sex, sexuality, gender, and intimate activities

Swatting - making a prank call to emergency services in an attempt to bring about the dispatch of a large number of armed police officers to a particular address

Weaponization of Visibility - refers to how our visibility, or the availability of our personal information, is weaponized by online vigilantes as a form of violence

DRCC
DURHAM RAPE CRISIS CENTRE

ROOT CAUSES OF CSV

Gendered forms of hate and violence, such as cybersexual violence, are rooted in **social inequality**, and based on **patriarchy** and **heteronormativity**.

Misogyny, which is "hard baked" into social norms, influences how people behave online and in real life. Perpetrators of hate and violence are often motivated by power and the desire to dominate. Often directed at those who transgress patriarchal stereotypes and expectations, cybersexual violence controls peoples' behaviour by creating discomfort, anxiety, and fear.

For folks who face other forms of discrimination on top of sexism, they are "doubly targeted", and the effects of CSV are multiplied.

CSV hurts communities as a whole, not just the individual. There is a cumulative harmful effect for women and girls as a group.

DRCC
DURHAM RAPE CRISIS CENTRE

Adapted from the
Canadian Women's Foundation

THE INTERNET IS ESSENTIAL

In the age of social media and COVID-19, Internet essentialism is non-negotiable.

The Internet is an important social resource that gives us access to friends, family, community, and politics. This is especially the case in the context of COVID-19 and social isolation.

This issue is urgent because the implied political goal of far-right vigilantes is to force marginalized women offline, to isolate women from their social connections, and to silence political dissent.

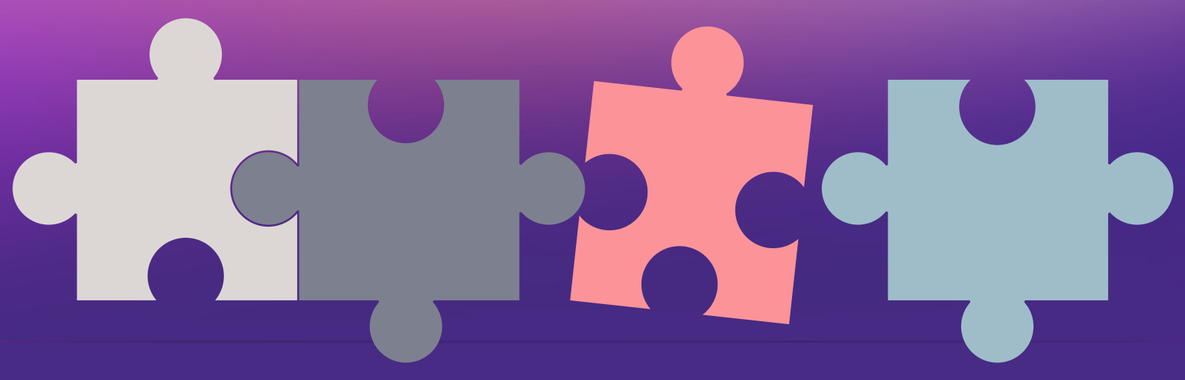
Since the pandemic began, **81% of Ontario sexual assault centres saw an increase in crisis line contacts** (phones, text lines, and crisis chat).

In 2021, Ontario sexual assault centres responded to over 37,500 crisis calls, including via phone, texting, and online crisis chat support, compared to 23,000 in 2019.

92% of Ontario sexual assault centres **provided prevention education via social media**.

"The trauma, the fear, the intimidation that goes with the course of harassment is harm itself."

– Justice Cioni, Alberta Provincial Court, R. v. Barnes, [2006] A.J. No. 965



DRCC
DURHAM RAPE CRISIS CENTRE

Adapted from Abigail Curlew, PhD (CA) and
The Ontario Coalition of Rape Crisis Centres

STATISTICS IN CANADA

Hate crimes and online hate in Canada have substantially increased in recent years, especially in digital spaces...

Between November 2015 and November 2016, online hate speech in Canada increased by **600%**.

Of reported hate crimes between 2010-2017, almost a third of the victims were females.

Cybersexual violence can have a more devastating psychological impact on victims than face-to-face interactions. It can have a global reach and can take place anytime, making it difficult to escape or stop.

According to a 2012 national survey of anti-violence support workers in Canada, 98% of perpetrators used technology to intimidate or threaten their victims. 72% hacked the email and social media accounts of women and girls they targeted, 61% hacked into computers to monitor online activities and extract information, and 31% installed computer monitoring software or hardware on their target's computer.

Adapted from the
Canadian Women's Foundation

DRCC
DURHAM RAPE
CRISIS CENTRE

GOVERNMENT POLICY AND LEGISLATION

In 2015, Bill C-13 came into effect to protect Canadians from online crimes. The Protecting Canadians from Online Crimes Act prohibits non-consensual distribution of images, empowers courts to tackle this type of online crime, and provides monetary reimbursements to victims.

In 2018, Newfoundland and Labrador introduced the Intimate Images Protection Act to tackle revenge porn.

In 2018, an MP proposed a new judicial body to provide tickets or warnings to individuals that post hate speech online.

In 2019, the Federal Government announced a plan to introduce a new digital charter that will target hate speech, misinformation, and electoral interference.

In 2019, Statistics Canada launched a Gender, Diversity and Inclusion department to improve data collection on diverse communities to understand the barriers that intersect with gender, race and other social categories. The department will offer service providers and policy makers with relevant data on different topics, taking gender and other identity factors into account.

While these are good beginning steps, it is important to note that government policy and legislation are still catching up to the Internet, and how to hold perpetrators of CSV accountable.

DRCC
DURHAM RAPE CRISIS CENTRE

Adapted from the Canadian Women's Foundation

DEVICES AND WHAT THEY KNOW

What do your devices know about you?

Here are just a few things...

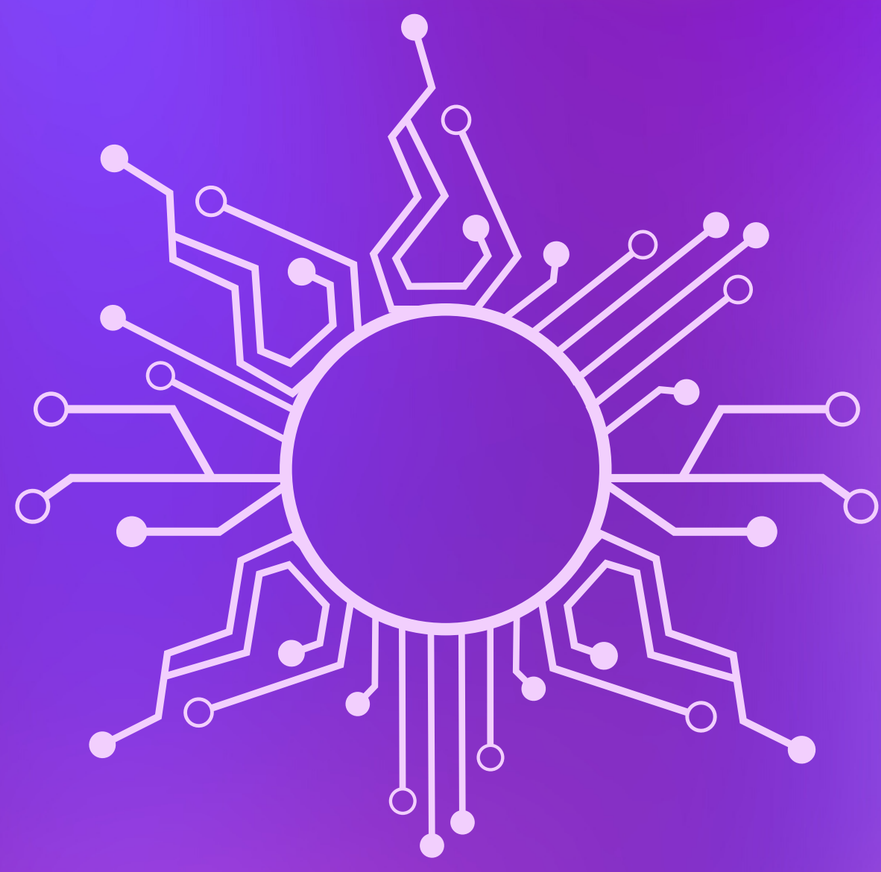
- Your name, age, gender, occupation, income, relationship status
- Your face, fingerprints, voice
- Words that you use in text messages and emails, screen captures of what you are doing on your devices, the sounds around your devices
- Your current location, the environment around your devices, how fast you are moving and in what direction, things around your devices that your camera/webcam can see
- A list of all the mobile and Wi-Fi networks, as well as cell phone towers that your devices have connected to
- And more...

Adapted from Raine Liliefeldt,
YWCA Canada

DRCC
DURHAM RAPE CRISIS CENTRE

DEVICES AND WHAT THEY KNOW

Consider the devices that you use daily:



- Cellular phones
- Laptops and desktop computers
- Tablets
- Smart TVs
- Smart toys (including drones and interactive children's toys)
- Wearable tech (including FitBits/fitness gadgets with location capabilities, location-enabled apps, and smart watches)
- In-home assistants (including Amazon Echo, Google Home, and similar devices)
- In-home smart cameras
- Public transit cards
- Pet tracking devices
- Passwords and usernames stored in these devices, including for social media accounts
- Spyware/stalkerware that may be stored in these devices without you knowing

DRCC
DURHAM RAPE CRISIS CENTRE

Adapted from Raine Liliefeldt,
YWCA Canada

PROTECT YOUR DIGITAL LIFE

Before Leaving an Abuser:

- Create a new email address unknown to an abuser
- Consider getting a new phone number, or a pay-as-you-go phone for privacy
- Do not link or use an existing account for confirmation/ backup to avoid sending notifications to an abuser that would alert them of the new account's existence
- Change passwords to complex passphrases an abuser would not guess
- Use a virtual private network (VPN) to remain anonymous and hide your IP address
- Do not close accounts that an abuser has access to; this could alert them that you are planning an escape
- Be aware of location tracking in apps and set privacy settings on devices and social media accounts to the most secure option
- Avoid networks shared with an abuser, when possible

DRCC
DURHAM RAPE CRISIS CENTRE

Adapted from DomesticShelters.org

PROTECT YOUR DIGITAL LIFE

After Leaving an Abuser:

Protect Your Devices

- Restore to factory settings or replace all computing/mobile devices
- Turn off all location-tracking services
- Keep your security software up to date
- Use a VPN to hide your IP address and keep your browsing history hidden, and consider using a library computer or other public Wi-Fi network with the VPN for added anonymity

Protect Your Home Network

- Use a router with network-level protection including automatic updates
- Protect your Wi-Fi network with a hard-to-guess passphrase containing upper and lower case letters, numbers and special characters
- Use a VPN at all times, but especially when browsing on your home network

Other Steps to Take

- Create new email addresses and contact information, being careful not to connect new accounts to old accounts for backup or password recovery purposes
- Consider deleting social media accounts, and not sharing personal information
- Update your security software regularly or turn on automatic updates
- Change all of your passwords to complex passphrases that include a mix of uppercase and lowercase letters, numbers, and special characters
- It is now safe to close any joint accounts
- Turn off any location-tracking services
- Block the abuser on phone, email, and social media

DRCC
DURHAM RAPE CRISIS CENTRE

Adapted from DomesticShelters.org

NEXT STEPS

RECOMMENDATIONS:

Train, educate, and raise awareness among police, frontline support workers, lawyers, judges, and members in the criminal justice and family law systems to **recognize signs of technology-facilitated gender-based violence**, and **know what laws apply**.

Understand that women and girls should not have to give up technology or stay off the Internet to have physical and psychological safety. They are not the problem. Effective responses must **focus on regulating and restricting abusers and enablers, not victims/survivors**.

The **tech industry must adhere to human rights obligations** and **seriously consider impacts** of their products and business practices on **vulnerable and marginalized individuals**.

Recognize that **the root problem is not technological** and **requires social reform**.

DRCC
DURHAM RAPE CRISIS CENTRE

Adapted from Cynthia Khoo, JD, LLM
Technology and Human Rights Lawyer at Tekhnos Law

SOURCES AND RESOURCES

- Canadian Women's Foundation
- DomesticShelters.org: Protect Your Digital Life When Leaving an Abuser
- Ontario Coalition of Rape Crisis Centres
- University of Ottawa
- University of Western Ontario VAW Learning Network

Resources for Fostering Healthy Security PRactices:

- DIY Cybersecurity for Domestic Violence
- DIY Feminist Cybersecurity
- Crash Override Network
- Remove Personal Information from Data Brokers

DRCC
DURHAM RAPE CRISIS CENTRE