


# Technology-Facilitated Sexual Violence: What It Is and How To Help

**Suzie Dunn, JD, LLM**

Assistant Professor  
Dalhousie University  
Schulich School of Law  
suzie.dunn@dal.ca

 @suziemdunn

**Cynthia Khoo, JD, LLM**

Associate  
Center on Privacy & Technology  
Georgetown Law  
ckhoo@cynthiakhoo.ca

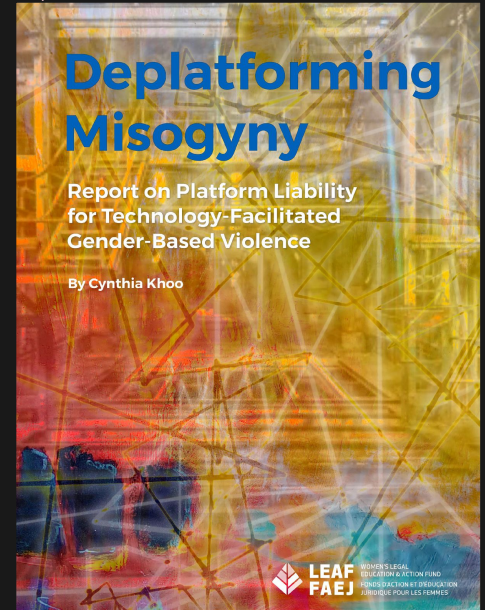
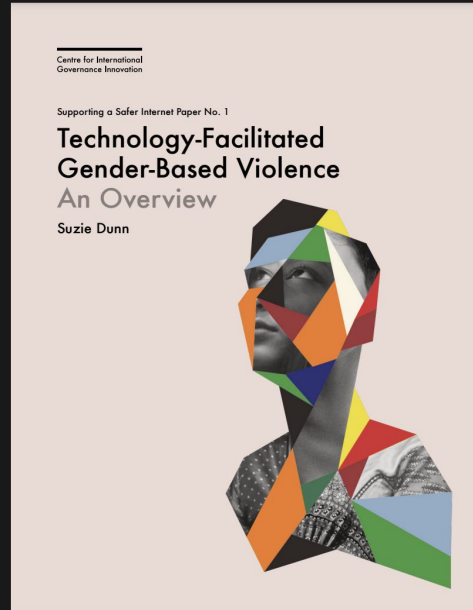
 @cyn\_k



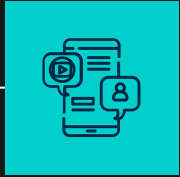
**Webinar (Part 1 of 2)**

**February 23, 2022**

**1:00pm - 2:00pm PST**

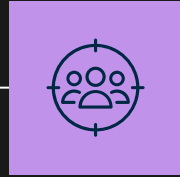


# TABLE OF CONTENTS



01

What is technology-facilitated gender-based and sexual violence?



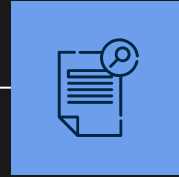
02

Harms and Impacts of TFGBV & TFSV



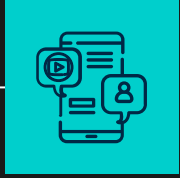
03

How to Respond: Supporting Targets of TFGBV & TFSV



04

Resources



01

WHAT IS  
TECHNOLOGY  
-FACILITATED  
GENDER-BASED  
& SEXUAL  
VIOLENCE?

# CASE STUDY: PUBLIC ADVOCACY /ACTIVISM



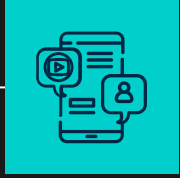
- Notifications are filled with violent & sexualized insults, rape & death threats, offensive memes, hate speech based on their gender, race & sexuality ([online \[sexual\] harassment/abuse, trolling, swarming](#))
- False nude photos of them and media of them manipulated to be unflattering or compromising flood platforms ([image-based abuse](#))
- Tweets & reddit posts defending them are reported & downvoted, while abusive tweets & posts are retweeted & upvoted ([brigading](#))
- Facebook page was mass reported for removal ([coordinated flagging](#))
- Their professional website has crashed due to being spammed with false requests ([\[distributed\] denial-of-service \[DoS /DDoS\] attack](#))
- Their home address and phone number have been disseminated all over multiple social media platforms to “teach her a lesson” ([doxing](#))
- Someone makes a false call to the police about their family, claiming dangerous activity is occurring at their home ([swatting](#))
- Someone creates a video game that involves battering their face

# CASE STUDY: INTIMATE PARTNER VIOLENCE



- He seems to always know where she is and details about people and events she hasn't mentioned ([spying](#), [stalkerware](#), [Apple AirTags](#)), and uses that knowledge against her ([technology-facilitated coercive control](#))
- He pretends to be her on her social media accounts to pump her friends for information, trying to catch her in a lie ([impersonation](#))
- He has secretly set up a hidden webcam in their bedroom and records her engaging in sexual activity ([voyeurism](#))
- He threatens to email all of her private photos and videos to friends, family & coworkers unless she does what he says ([sextortion](#))
- He distributes the photos and videos of her as well as posts them online ([non-consensual distribution of intimate images \[NCDII\]](#))
- Others take the circulated materials to create fake but realistic pornographic videos of her ([cheapfakes](#) & [deepfakes](#))
- He sets up fake personals ads sending men to her home & to her workplace to have sex with her, claiming that she has a rape fantasy





01

# WHAT IS TECHNOLOGY -FACILITATED GENDER-BASED & SEXUAL VIOLENCE?

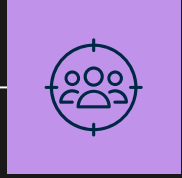
- **Continuum of Oppression:** Broad spectrum of harmful actions & behaviours targeting women, girls, and minoritized genders
- **Misogyny & Patriarchy:** Rooted in, fuelled by, & exacerbates pre-Internet misogynistic beliefs, sexist norms, rape culture
- **Gendered & Intersectional:** Disproportionately impacts women & girls, with unique harms to those in multiple marginalized groups
- **Devices & Platforms:** Phones, social media (facebook, twitter, instagram, youtube, tiktok), private messaging (sms, snapchat, whatsapp), streaming sites (twitch), gaming platforms
- **Online *Is* Real-World:** Collapses false dichotomy between “online” & “offline”; artificial distinction divorced from lived experience
- **Underreported:** Due to victim-blaming, technological illiteracy (of professionals & institutions), and re-traumatization by police
- **Not “Just Speech”:** TFGBV / TFSV occurs through online expression, but amount to substantive actions with devastating consequences
- **Not “Cyberbullying”:** minimizes and obscures extent of abuse and erases the systemic and structural nature of TFGBV & TFSV

# CAMPUS EXAMPLES

uOttawa:  
student  
leadership

Dalhousie:  
dentistry  
students

Western:  
orientation  
week



## 02 HARMS & IMPACTS OF TFGBV/TFSV

- **Psychological:** fear, anxiety, depression, self-harm, suicide, loss of self-worth, emotional and mental trauma
- **Physical/Geographical:** leads to violence and abuse “offline”, such as stalking or physical attacks; psychological stress can cause physical illness; moving homes or schools for safety
- **Social:** isolation, ostracization, shaming; social networks turned against them or cut away; withdraw from potential social support networks based around school, work, sports/hobbies
- **Professional:** lost opportunities for career advancement; impedes fulfilling work or academic responsibilities; reputation
- **Financial:** financial abuse, missed wages, costs of legal or other professional support, medical costs, costs of safety measures
- **Democratic:** TFV prevents women & girls from fully participating in (and influencing) society, politics, and culture (see e.g., legal & medical professions, technology industry)
- **Fundamental (Human Rights):** impedes ability to exercise or enjoy benefit of fundamental human rights: violates right to equality, privacy, and freedom of expression





# 03

## HOW TO RESPOND: SUPPORTING TARGETS OF TFGBV/TFSV

- Identifying
- Documenting
- Removal
- Safety Planning

- Remember: risk factors are different for people being targeted by partners, ex-partners, friends, roommates or family

# Victim-blaming

## Survivor-centric responses

- Nude photos are a normal form of sexual communication
- Don't blame people who have had their images shared
- Threats online are as serious as those offline
- Online harms have serious repercussions, mentally, physically, and financially
- Don't ask the victim/survivor to stop using social media, texting, email, or going to digital spaces




# Intimate images

- Make a list of images and videos that may exist
- Consider if abuser may have been able to record other images without consent
- Images may have been recorded on Zoom or Skype by third party app
- If images have been shared see the Cyber Civil Rights Initiative guide on how to get content taken down
- Facebook hashing system
- If sharing images consider what images are shared
  - Avoid images with their face or identifying marks (tatoos, birthmarks)
  - Avoid images in places that are identifiable (is the room recognizable?)
  - Use programs like Signal that allow for disappearing messages

# Finding content online

- Reverse image search
- Google alerts for their name

Google  
images





Suzie...o pic.jpeg ×

picture frame



🔍 All

Images

📍 Maps

🛒 Shopping

⋮ More

Settings

Tools

Page 2 of about 8 results (0.28 seconds)

www.suziedunn.com ▾

## Suzie Dunn



738 × 930 — Suzie Dunn. Suzie Dunn is PhD candidate and part time professor at the University of Ottawa, Faculty of Law. She currently teaches contracts law and the Law of ...

droittech.uottawa.ca ▸ personnes ▾ [Translate this page](#)

## Personnes - Centre de recherche en droit, technologie et société



1000 × 1000 · Oct 20, 2020 — Notre équipe. Toutes et tous · Direction · Chercheur(e)s · Chercheur(e)s associé(e)s · Chercheur(e)s invité(e)s · Chercheur(e)s post-doctoraux ...

# Alerts

Monitor the web for interesting new content

🔍 Create an alert about...

My alerts (7)



\*revenge porn\*



deepfake



inimate images



non-consensual distribution



sexbot



Suzanne Dunn



Suzie Dunn



# Reporting to social media companies

- Document before reporting as the content may get removed
- See HeartMob "Media Safety Guides" for tips on understanding social media companies' policies and reporting mechanisms



# Documenting/Logging Abuse

- Create a log of what has happened
  - Date, time
  - What happened
  - Which app used
  - Evidence
  - Who you think did it
  - Impact on you
  - Evidence still needed
  - See “Sample Digital Evidence Chart” Not Without My Consent resource, upcoming BC Society of Transition Houses

# Internet history

- If the abuser has access to the client's computer in the home
- Abuser may be able to access search history
- Abuser may see the client is looking for help or ways to leave
- Your client want to use a library computer or work computer to do searches for things like shelters, new places to live, helplines, etc
- Can delete selective internet history
- Some browsers off a “private” or “incognito” option for browsing that doesn't record the search history
- Domestic violence organizations often have a “Quick Exit” button that takes the user to an innocuous site

# Unwanted access to accounts

- Sign out of all accounts when done using them
- Don't share your password or automatically save passwords to devices
- Abusive partner may force their partner to share passwords
- Create alternate secret accounts that you only use at work or on a public computer and only with a secure group of people
- Use an email address or username that would not identify you or provide identifying information such as your year of birth
- ProtonMail is a secure service

# Location tracking

- Turn off location sharing and Bluetooth when not using those functions
- For example, have client look at Google Maps Timeline on their phone, shows everywhere they have been everyday
- Go into settings of devices to see what apps are tracking location
- Look at all apps on the phone
- Delete unknown or unnecessary apps
- Turn off “Find my phone” feature if partner has access to iCloud or similar features
- Family Sharing
- Find My Friends



# Geotagging in photos

- Photos posted on the internet may contain metadata that records the GPS location of where the photo was taken
- This can allow the abuser to find your client's location
- Can turn this function off on your phone, remove the data from a single picture or change the geolocation data on a photo posted on the internet

# Hidden cameras and trackers

- Audio or visual recording devices can be hidden in many items
- Look at gifts given from abuser
- Especially with children's items
- Some may allow for photos to be taken, recordings to be made or to wipe the device
- Apps and devices can scan for hidden cameras (Network scanners, port scanners, RF signal detector)

# Phone plans and shared accounts

- Shared phone plans can allow the owner of the plan to access the call records of everyone on the plan
- Shared calendars and accounts can give access to a person's schedule and files
- Consider whose emails are on these accounts and who has access to them
- Automatic backup to cloud storage
- Photos, contact, texts
- May want to turn this off



# Trusted devices and check-ins

- A client may have signed into their accounts on their partner's devices and checked them as "trusted devices"
- Only have the client's personal devices be trusted devices
- Check for "Last Account Activity" to see where the account has been accessed
- Sign out of all devices

<u>Access Type [ ? ]</u>		Date/Time
(Browser, mobile, POP3, etc.)	<u>Location (IP address) [ ? ]</u>	(Displayed in your time zone)
Browser (Firefox) Show details	* Canada (154.212.33.385)	11:51 am (0 minutes ago)
Browser (Firefox) Show details	* Canada (154.212.33.385)	11:16 am (35 minutes ago)
Mobile	* Canada (154.212.33.385)	11:03 am (48 minutes ago)
Mobile	* Canada (154.212.33.385)	10:39 am (1 hour ago)
<b>Mobile</b>	<b>* Canada (154.657.43.212)</b>	<b>9:06 am (2.5 hours ago)</b>
Browser (Firefox) Show details	* Canada (154.212.33.385)	Oct 28 (12 hours ago)
Mobile	* Canada (154.212.33.385)	Oct 28 (19 hours ago)
Browser (Firefox) Show details	* Canada (154.212.33.385)	Oct 28 (22 hours ago)
Browser (Firefox) Show details	* Canada (154.212.33.385)	Oct 28 (22 hours ago)
Browser (Firefox) Show details	* Canada (154.212.33.385)	Oct 28 (22 hours ago)

# Stalkerware

- Be careful about looking for spyware on device, this can alert the abuser that you know it may be on the phone
- Use public computer to look information about stalkerware up
- May need to get a new device
- May need to wipe phone (Don't back up from previous phone, may redownload stalkerware)
- See resources from Clinic to End Tech Abuse
  - Technology Assessment Questionnaire
  - Privacy Checkup Guides
  - IPV Spyware Discovery Tool
  - Technographs
  - App Classification Guide

# Passwords

- Make a list of all accounts a person has online (social media, banking, shopping, cloud storage, school, email, food delivery, car services)
- Change the name of and password to their WiFi
- Change all passwords to unique passphrases (a sentence that is easy to remember)
- Do not use the same password for multiple accounts
- Use a sentence rather than a word
- Change letters to symbols or numbers (instead of “a” use “@”, instead of “E” use “3”)
- Example: MyC@tT1g3rLov3sTun@
- Do not use children’s names, old addresses, old phone numbers, important dates or anything a person who knows them well can guess
- Use a password manager
- Use two-factor authentication

# Social Media

- Turn off location services
- Go through each notification setting (See HackBlossom resource for detailed information)
- Get alerts that may be useful, such as when someone tags your client or comments on posts
- Get alerts whenever anyone logs into the account
- Avoid “checking in” to locations
- Don’t allow for app to access contact list to connect with other people
- Do not link social media accounts with other accounts (i.e. don’t use Facebook to sign in to other accounts)
- Talk to friends who may provide access or information to abusive partner, intentionally or or not

# Zoombombing

- Waiting room
- Limit who can comment
- Limit who can share
- Do a Webinar rather than a group
- Don't share public links
- Require registration
- Consider privacy issues when recording
- See NNEDV's "Using Zoom: Safety, Privacy, and Confidentiality Considerations"



# 04

## RESOURCES

- **Privacy and cybersecurity**, passwords, privacy settings, digital hygiene
- **Documentation and removal**, how to detect and collect evidence of the abuse, how to get content taken down
- **Education**, learning more about technology facilitated violence
- **Law and direct supports**, legal rights, anti-violence organizations

Privacy and  
digital  
hygiene



# SURVEILLANCE SELF-DEFENSE

**TIPS, TOOLS AND HOW-TOS FOR SAFER ONLINE  
COMMUNICATIONS**

A PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION





## WITHOUT MY CONSENT SAMPLE COMPLETED EVIDENCE CHART

Date	What Happened	Evidence It Happened	Who You Think Did It	Evidence They Did It	Evidence Still Needed & Who Has It
Jan 1-2, 2015	Ex-romantic partner sent 7 texts between 10:00 p.m. and 4:00 a.m.	Texts saved on phone. Screen shots of texts saved to computer and printed to binder (Exhibit A).	Ex-romantic partner	Texts display sender's ID by name and number.	Expect that ex-partner's phone will show these texts were sent.
Jan 2, 2015	At 4:11 a.m., sexually explicit photos of me were posted to [insert website URLs] without my consent.	Webpages saved to computer as PDFs and printed to binder (Exhibit B).	Ex-romantic partner	Ex-partner took these photos and is the only person I have ever given the photos to.  Ex-partner has threatened me with the photos in the past. For example, [insert specific].  The 4:00 a.m. text message states, "You'll be sorry." Screen shot of text saved to computer and printed to binder.  The event happened the day after ex-partner found out. [insert specific].	My friend [insert name] has a text on her phone about the event ex-partner found out about. I need to ask her to preserve the evidence and provide me with a PDF copy for my files.
Apr 1, 2015	A friend googled my name and alerted me that there were sexually explicit images of me online. The pictures are live at the following links: [insert URLs].	Webpages saved to computer as PDFs and printed to binder (Exhibit C).	Ex-romantic partner	Ex partner took these photos and is the only person I have ever given the photos to.  He has violated court orders before. [insert specific].  The photos were posted to a webpage along with comments about me for our relationship or him that only he could know. [insert specific].	This may be enough to prove contempt, but I might want to ask the court. I can ask the court by filing a Request for a Court Order Enforcing Petitioner's Restraining Order By Contempt, Or, in the Alternative, Permission To Serve Limited Discovery (i.e., subpoenas on the websites and ISPs) To Prove Contempt.



### Social Media Safety Guides

Staying safe on social media- We've got your back!

Introducing our new Social Media Safety Guides for Facebook, Twitter, Reddit, Tumblr, and Youtube! We have worked hard alongside each of these platforms to make it easier for you to stay safer online. Every guide gives user-friendly information on how use different platforms' reporting and privacy tools - and for the very first time all of this information is gathered in one location.



Facebook



Instagram



Reddit



Tik Tok



Tumblr



Twitter




YouTube



Zoom

# Documentation and removal

# Safety Planning



The cover features the BC Society of Transition Houses logo in the top left. The background is dark grey with a grid of small white dots. A stylized illustration of a woman and a child walking is shown in the lower right, with pink signal waves emanating from the woman's head. The text is in white and pink.

BC Society of  
Transition Houses

A guide for Canadian women experiencing  
technology-facilitated violence:  
**Strategies for Enhancing Safety**



The screenshot shows the website's navigation menu at the top: 'Get Help Now', 'Donate', 'Members', 'Resources', and 'News'. Below the menu are links for 'Who we are', 'Who we support', 'How we support', 'Projects', and 'Training'. The main content area is titled 'PROJECTS' and features an illustration of a woman and child with signal waves. The page title is 'Technology Safety'. The text below discusses the increasing trend of technology-facilitated violence and provides information on resources and training.

BC Society of  
Transition Houses

Get Help Now Donate Members Resources News

Who we are Who we support How we support Projects Training

PROJECTS



## Technology Safety

There has been an increasing trend reported by Canadian anti-violence workers where technology use and violence overlap. Technology can be used both to keep women<sup>1</sup> and children safe and misused by perpetrators to commit crimes of domestic violence, stalking, sexual assault, impersonation and harassment.

BCSTH's **technology safety resources** and training assist anti-violence workers to learn more about how to support women and young people experiencing technology-facilitated violence including strategic methods to use technology safely and incorporate them into safety plans. Our resources and training also assist anti-violence workers to consider how their program's use of technology in operational and administrative practices impact women and children's safety and suggest ways to implement best practices.

British Columbia Society of  
Transition HUses

Tech-safety Tool Kit  
<https://bcsth.ca/techsafetytoolkit/>

## Tech-Facilitated Violence: Criminal Case Law – Criminal Offences

[home](#) / [resources](#) / [tech-facilitated violence – criminal case law](#) / [tech-facilitated violence: criminal case law – criminal offences](#)

### OFFENCES AGAINST MINORS

### OFFENCES AGAINST ADULTS

CHILD PORNOGRAPHY OFFENCES	CRIMES RELATED TO SEXUAL SERVICES	CRIMINAL HARASSMENT
DEFAMATORY LIBEL	EXTORTION	HARASSING COMMUNICATIONS
HATE PROPAGANDA	HUMAN TRAFFICKING	HUMAN TRAFFICKING, ADVERTISING SEXUAL SERVICES
IDENTITY FRAUD	INVITATION TO SEXUAL TOUCHING	INTIMIDATION
LURING A CHILD	MAKING SEXUAL MATERIAL AVAILABLE TO A CHILD	MISCHIEF IN RELATION TO DATA
NON-CONSENSUAL DISTRIBUTION OF INTIMATE IMAGES	SEXUAL ASSAULT	SEXUAL EXPLOITATION
SEXUAL EXPLOITATION OF A PERSON WITH A DISABILITY	SEXUAL INTERFERENCE	UNLAWFUL USE OF A COMPUTER
UTTERING THREATS	VOYEURISM	

## CyberScan

### Intimate images and cyber-protection: support for victims

If you've been bullied online or had intimate pictures of you shared without your consent, you're protected under the law.

The Intimate Images and Cyber-Protection Act aims to discourage people from bullying others online or by text or email, and from sharing intimate images of someone without their consent. The act also gives victims a way to respond when these things happen.

If you believe you are the victim of cyberbullying or that an intimate image of you was shared without your consent, CyberScan can help.



call CyberScan:

[902-424-6990](tel:902-424-6990) (within HRM)

[855-702-8324](tel:855-702-8324) (toll-free)

Law and  
direct  
supports



# Education

Centre for International  
Governance Innovation

Supporting a Safer Internet Paper No. 1

## Technology-Facilitated Gender-Based Violence An Overview

Suzie Dunn



## Deplatforming Misogyny

Report on Platform Liability  
for Technology-Facilitated  
Gender-Based Violence

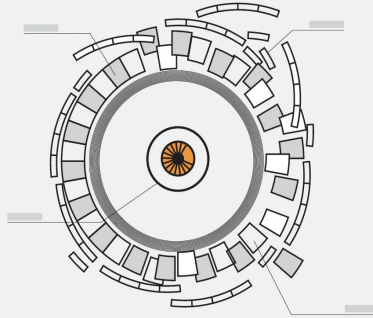
By Cynthia Khoo



PLAN FOR EQUAL

FREE TO BE  
ONLINE?

Girls' and young women's experiences  
of online harassment



## INSTALLING FEAR

A Canadian Legal and Policy Analysis of Using,  
Developing, and Selling Smartphone Spyware and  
Stalkerware Applications

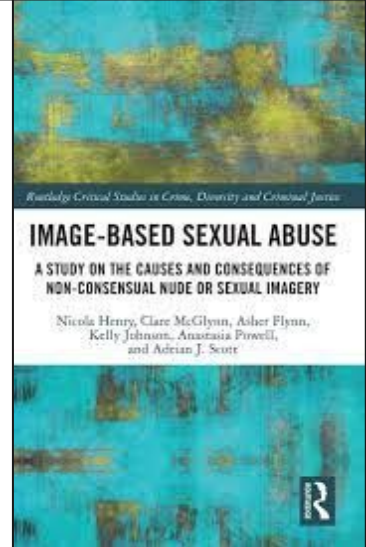
By Cynthia Khoo, Kate Robertson, and  
Ronald Dalbert

Research report #120  
June 2019



## #TOXICTWITTER

VIOLENCE AND ABUSE AGAINST WOMEN ONLINE



*Knowledge Critical Studies in Crime, Diversity and Criminal Justice*

## IMAGE-BASED SEXUAL ABUSE

A STUDY ON THE CAUSES AND CONSEQUENCES OF  
NON-CONSENSUAL NUDE OR SEXUAL IMAGERY

Nicola Henry, Clare McGlynn, Asher Flynn,  
Kelly Johnson, Anousha Pirovelli,  
and Adrian J. Scott

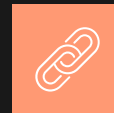


Questions / Comments?

**@suziendunn**

**@cyn\_k**

# THANK YOU



Please keep this slide for attribution