


Technology-Facilitated Sexual Violence: What Rights Do Students Have?

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 2 of 2)

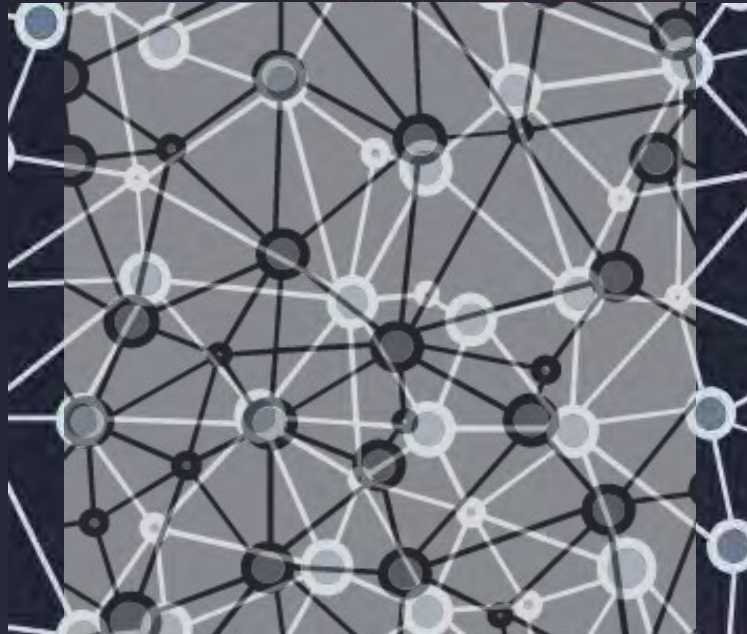
March 16, 2022

1:00pm - 2:00pm PST

APPLYING THE LAW TO TFGBV & TFSV

Forms of Technology-Facilitated Gender-Based and Sexual Violence, Abuse, & Harassment (TFGBV & TFSV):

- Online abuse and harassment (often sexualized)
- Rape threats & death threats
- Image-based abuse
- Stalking
- Non-consensual distribution of intimate images (NCDII)
- Impersonation
- Deep fakes
- Sextortion
- Covert surveillance (stalkerware)
- Smart-home device manipulation
- Trolling, Swarming, Brigading
- Coordinated attack campaigns
- Denial-of-service attacks
- Doxing
- Swatting



OVERVIEW

01

Civil Law (Private Lawsuits)

02

Digital Platform Liability

03

Criminal Law: Tech-Specific and Non-Tech Offences

04

Collecting Evidence

CIVIL LAW (PRIVATE LAWSUITS) [1/2]



Intentional Torts

- Tort of Defamation
- Tort of Intentional Infliction of Mental Suffering (IIMS)
- Tort of Intimidation (ON)
- Tort of Internet Harassment (ON)



Invasion of Privacy

- *BC Privacy Act*
- Breach of confidence
- Common law privacy torts in other provinces:
 - Intrusion upon seclusion (ON)
 - Public disclosure of private facts (ON, AB)
 - False light (ON)



Non-Consensual Distribution of Intimate Images

- Laws in force: PEI, NFLD, Alberta, Manitoba, Nova Scotia, Saskatchewan
- In progress: New Brunswick, BC
- *Uniform Non-Consensual Disclosure of Intimate Images Act (2021)* (Laidlaw & Young)

Sexual privacy protects “the behaviors, expectations, and choices that manage access to and information about the human body, sex, sexuality, gender, and intimate activities.”

Sexual privacy is “a distinct privacy interest that warrants recognition and protection. It serves as a **cornerstone for sexual autonomy and consent**. It is **foundational to human dignity and intimacy, and its denial results in the subordination of marginalized communities.**”

— Danielle Keats Citron, “Sexual Privacy” (2019) 128:7 Yale LJ 1870

CIVIL LAW (PRIVATE LAWSUITS) [2/2]



Family Law

- Protection orders through family court
- Tort of Family Violence (ON only)



Liability of Higher-Education Institutions

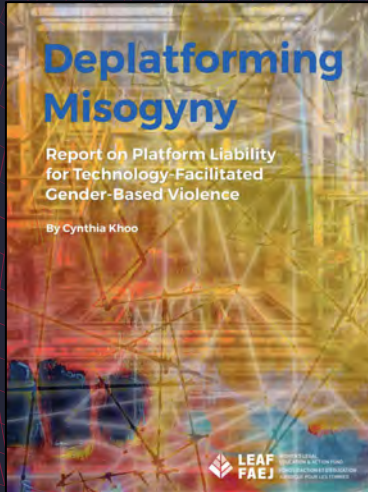
- Do post-secondary education institutions have any duties or legal obligations in the event of their student(s) being targeted by TFGBV or TFSV?



Considerations in Pursuing a Civil Lawsuit

- Control over the case
- Monetary compensation
- Financial costs (lawyers' fees, lost wages)
- Physical & mental health costs (stress, depression, re-traumatization)
- Potential class action; dignity; justice

DIGITAL PLATFORM LIABILITY FOR TFGBV/TFSV



- 1. What is digital platform liability?**
 - Holding a digital platform company (e.g., a social media company) legally responsible for the words or actions of its users
 - A type of intermediary liability
- 2. What kind of TFGBV or TFSV might current Canadian laws hold social media platforms liable for addressing?**
 - NCDII & Generally: subject to court orders to assist
 - *Copyright Act*: notice-&-notice; “enabling”
 - Defamation + Quebec: notice-&-takedown
 - *Criminal Code*: direct liability if platform involved
 - Under consideration: “Online Harms” legislation
- 3. No statutes address platform liability for TFGBV / TFSV specifically. However, broader laws may apply:**
 - human rights statutes
 - corporate negligence
 - commercial host liability

CRIMINAL LAW



Fear-Based Crimes

e.g., Threats of
Violence, Intimidation,
Criminal Harassment



Sexual Privacy

e.g., Non-consensual
distribution of
intimate images



“Computer Crimes”

e.g., Interception
of Private
Communications

“[This case] involves the use of electronics and with the capacity to strike to the heart of a person’s well-being in our community..

[T]he trauma, the fear, the intimidation that goes with the course of harassment is harm itself. [...]

The accused’s act of putting the [keylogger] on the computer gave him complete access to codes and pass words [sic] and thereby the entire contents of the victim’s computer and all of the plans that she had within that realm. He used it aggressively and badly. He disrupted her life with a specific plan of making her pay.”

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

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	

<https://www.equalityproject.ca>

@eQuality_ca

Tech-Facilitated Violence – Criminal Case Law – Extortion

home / resources / tech-facilitated violence – criminal case law / tech-facilitated violence: criminal case law – criminal offences / tech-facilitated violence – criminal case law – extortion

OFFENCE ELEMENTS - EXTORTION OFFENCES

§ 346 (1) Every one commits extortion who, without reasonable justification or excuse and with intent to obtain anything, by threats, accusations, menaces or violence induces or attempts to induce any person, whether or not he is the person threatened, accused or menaced or to whom violence is shown, to do anything or cause anything to be done.

(1.1) Every person who commits extortion is guilty of an indictable offence and liable

(a) if a restricted firearm or prohibited firearm is used in the commission of the offence or if any firearm is used in the commission of the offence and the offence is committed for the benefit of, at the direction of, or in association with, a criminal organization, to imprisonment for life and to a minimum punishment of imprisonment for a term of

(i) in the case of a first offence, five years, and

(ii) in the case of a second or subsequent offence, seven years;

(a.1) in any other case where a firearm is used in the commission of the offence, to imprisonment for life and to a minimum punishment of imprisonment for a term of four years; and

(b) in any other case, to imprisonment for life.^[1]

[1] Criminal Code, RSC 1985, c. C-46, s. 346.

<https://www.equalityproject.ca>

@eQuality_ca

TECHNOLOGY-FACILITATED VIOLENCE: PRESERVING DIGITAL EVIDENCE TOOLKIT

The Technology-Facilitated Violence: Preserving Digital Evidence Toolkit is a guide to help women and anti-violence workers preserve digital evidence in circumstances involving technology-facilitated violence against women. Technology misuse is just one more abusive behavior that occurs in violence against women cases. Technology is not the problem; it is the underlying pattern of violent and sexist behavior that presents itself in digital forms. Because of the prevalence of technological devices today, their use can extend the reach of the abuse by the perpetrator, but it can also leave a trail of digital evidence that can be used strategically in safety planning and evidence collection by women targeted by this type of violence.

Technology-facilitated violence is when technology is misused by perpetrators to commit violent abusive acts including acts such as domestic violence, harassment (stalking), sexual assault, impersonation, extortion, and the non-consensual filming and sharing of intimate images.

Digital evidence is the overarching term that includes evidence from digital devices including the devices themselves, as well as emails, texts, pictures, videos, voice recordings, direct messages (DMs), screenshots, account logs or billing statements, apps, GPS and location information, and "metadata" or the information embedded in emails and other electronic documents. It is worthwhile to note that in the Canada Evidence Act, digital evidence is referred to as "electronic documents." Within this report, we will use the term "digital evidence" as it is more commonly used when describing evidence of technology-facilitated violence.

<https://bcsth.ca/digitalevidencetoolkit/>
@BCSTH

DIGITAL EVIDENCE

Create a document log

Collect evidence (screenshot, record)

Collect contact information

Back-up your evidence and print copies, store somewhere safe

Report and remove

TECHNOLOGY SPECIFIC EVIDENCE PRESERVATION GUIDES

- [Preserving Evidence for Civil Court Using Video Recording IOS and Android 2020](#) – PDF ONLY
- [BCSTH's Apple IOS Video Screen Recording Tutorial](#) – VIDEO
- [How to Save and Print Screen Shots for Evidence Preservation](#) – PDF ONLY
- [How to Preserve Videos as Evidence](#)
- [How to Preserve an Audio Recording as Evidence](#)
- [How to Save a Website Page as a PDF or HTML](#)
- [How to Preserve Emails as Evidence](#)
- [How to Back Up and Store Evidence of Technology-Facilitated Violence](#)

DIGITAL EVIDENCE

Evidence Law

Authenticate - showing that the document is what you say it is

Testimony - who actually took the screenshot

Authorship - who wrote the messages/made the post (email, phone number, IP address)

Best evidence rule - try to make a direct copy

Circumstantial evidence - helps prove event happened

RECOMMENDATIONS

1. **Train, educate, and raise awareness** among police, educators, frontline support workers, lawyers, judges, and actors in the education, criminal justice, and family law systems to recognize signs of technology-facilitated gender-based violence and respond in a victim/survivor-centric way.
2. 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.**
3. **Tech industry must adhere to human rights obligations** and seriously consider **impacts** of their products and business practices on **vulnerable or marginalized individuals.**
4. Recognize that **the root problem is not technological** and requires societal reform.

THANK YOU

Questions or Comments?

ckhoo@cynthiakhoo.ca
TekhnosLaw.ca
[@cyn_k](https://www.instagram.com/cyn_k)

suzie.dunn@dal.ca
www.suziedunn.com
[@SuzieMDunn](https://www.instagram.com/SuzieMDunn)