Transcript for Technology Facilitated Sexual Violence
BCcampus event held on February 23, 2022
Facilitators: Cynthia Khoo and Suzie Dunn

CYNTHIA KHOO:
Thank you so much and hello everyone. Thanks so much for participating in this webinar today. My name is Cynthia Khoo. My pronouns are she and her. I am currently a full time associate at the Center on Privacy and Technology at Georgetown Law in Washington DC, as well as a Canadian technology and human rights lawyer and a fellow ethicist at the University of Toronto. My co-facilitator and close today is Professor Suzie Dunn at Dalhousie University Schulich School of Law. Who also brings many years of working with community organizations and doing this kind of community training when it comes to responding to technology facilitated gender based and sexual violence. And these are examples of some of our work.

So, what will be going over today is to start off I'll be starting off the first half of the webinar, just introducing you to what is technology-facilitated sexual violence. Which is really a subset and has a lot of overlap with the general category of tech-facilitated gender-based violence. And then talk about the harms and impacts of such violence on an individual level but also on a collective systemic level. Then I'll be handing it over to Suzie to talk about if somebody comes to you saying that they're experiencing this type of violence or abuse, how to respond. And what are some resources that you can consult in figuring out whether it's planning a safety strategy, how to navigate social media platforms or how to just provide better support to the person experiencing the type of violence and abuse.

So, to start off with what is technology-facilitated gender-based and sexual violence. I thought instead of diving into a series of definitions, I would start off with some case studies just to see what this type of violence, abuse and harassment looks like on the ground level from the perspective of the person experiencing it. There's going to be a lot of terminology coming at you quickly, I'll say that upfront, but hopefully the way I've structured it will make of it easier to digest.

So, to start off with...These are composite profiles of activities that have happened to women in Canada and around the world and continue to happen. The composite profiles are drawn from examples in Canadian case law, media reports and academic literature. So, with that said I would like to introduce you to Imani. Imani as a non-binary engineering student at a college or university in DC. They are an active part of the LGBT community and they are extremely outspoken and vocal activist on social media.

So recently, they published an Op-ed talking about misogyny and racism that they experienced in the engineering faculty. And they are now experiencing a lot of backlash to that Op-ed from their classmates, some of the professors and the broader public. So, what are some of the things that Imani is experiencing in the realm of technology-facilitated, gender-based and sexualized violence? Well, they log on to the next day and their notifications are filled with violent, sexualized insults, rape and death threats, hate speech based on their gender identity, race and sexuality. This is known as the general umbrella term of online harassment, trolling and swarming when hundreds of people just decided to

target one person all at once. And further, they discover that someone's created nude photos of them and has manipulated videos to make them look unflattering or compromised.

This is a form of image-based abuse. Tweets and reddit post defending them are reported as violations of community standards and downvoted which tells the algorithm this is bad bury this post. While abusive posts and tweets are retweeted and upvoted which then changed the algorithm to say, Oh, this is getting a lot of engagement let's upload it. Let's show us more of this and push this to more people. At the same time their own Facebook page has been subjected to what's known as coordinated flagging. Which is when everybody decides to mass support a piece of content saying this is violating community standards. And because of faulty content moderation systems that Facebook is just now taking that with no due process or notice or anything. And so this additional resource that they are providing is now inaccessible. Similarly, their professional website is also being attacked through a coordinated attack by many people accessing their website all at the same time. Which means that overloads the website's servers and has now crashed and again is now inaccessible to anyone. So, this is what's known as a DDoS or DoS attack. Then, the next day they find out that somebody has published or gotten a hold of their home address and phone number and disseminated that all over the internet. This is known as doxing when someone's personal, private previously closely held information is now published online. And because technology-facilitated violence is cumulative and confounding and self amplified someone now takes that published information, makes a false call to the police and tells them that there's a bomb threat at our family home. Or a someone is holding a hostage there. And what that does is the police then takes that threat seriously and will send a SWAT team to that person's home. This started off as a type of prank, obviously a terrible prank, and people have gotten killed as a result of this activity. That's known as swatting because you're sending a SWAT team to somebody's home. So, this is just a sampling of types of technology-facilitated gender-based violence, abuse and harassment. Obviously, it can be sexualized or not sexualized. And oftentimes it is sexualized when it comes to women and girls members of marginalized gender identities. So, this is what happens though, some of the things that you can space if you're a public outspoken figure. So, taking it...But of course a lot of tech and non-tech abuse happens in a much more private space. So, what happens there?

This is another composite case study featuring a woman named Kendall who is a fine art student. Their significant partner is a police officer and they live together in an on off open relationship. And sometimes they will record sex videos of themselves for fun, and they've considered maybe even starting and only facts. So, technology-facilitated gender-based violence is a huge component of intimate partner violence. In fact, I believe a 2017 survey of Canadian women's shelters showed that among the respondents were 18 different forms of technology-facilitated violence and abuse that people seeking help from them had experienced. So, what are some examples of tech-facilitated gender-based intimate partner sexualized violence that someone might go through in this kind of scenario? Well, first off, her partner always seems to know where she is and has details about people and events that she's never mentioned. This may be due to the fact that he's installed software on her phone. Which is the type of consumer spyware that you can find in the Google Play Store or the Apple App Store that would lock your phone conversations, text messages, your private social media account, your GPS location at all times, your call histories. And then he can use

that information. Sometimes it's corporate spying but sometimes the abusive partner will be completely open about it, saying, I'm watching you. I know what you're doing. Don't try to do anything against me. And that ends up becoming what Molly Jane Lynch has called a technology-facilitated coercive control. He might also pretend to be her on her social media accounts. Of course, that impersonation. He's also secretly set up a hidden webcam in their bedroom as a form of voyeurism. These are, of course, crimes in Canadian law. Finally, she confronted him threatens to break up with him. And he threatens to email all of her private sexual photos, intimate photos and videos to her friends, family and co-workers unless she stays with him and does everything he says. And this is what's known as sextortion. When he threatens to abuse someone's intimate photos and videos unless you do what they tell you to. She refuses and changes her mind. He distributes the photos anyway. This is a crime in Canada. A nonconsensual distribution of intimate images. Known as a form of sexual violence. And again, going back to that amplification and building aspect, other people online who don't know either of them now take these circulated materials to create fake but very realistic looking pornographic videos of her. Cheapfakes are using commonly available video editing techniques that are available now. Deepfakes are what we're seeing this type of violence and increasingly trend towards, which is a type of technology where artificial intelligence uses pre-existing video footage, photos of people in order to create videos that makes it appear as if they've said or done things that they've never actually done but it looks like real video footage. And lastly, this does not have a pat name attached to it but it is something that's happened. There's a case involving two gay men in the United States where someone set up a fake personal ads, sending men to their ex's home and workplace to have sex with them without their knowledge claiming that they consented she said it was part of a rape fantasy. So, these are all different types of behaviors that all constitute a technology-facilitated gender-based and sexual violence. And I want to stress that hopefully it's clear you obviously do not have to be a public figure or an activist or someone who's dating or in a partnership for these to happen to you. This is just a way that I felt would make all of the terminology easier to digest. But as long as somebody has decided to target you for whatever reason whether they are a stranger or not, these are the types of behaviors that someone might be subjected to.

So, this brings us back to our question of what is a facilitated gender-based and sexual violence? You now have specific examples of types of behavior that this term covers. But just to draw some overarching common factors of what it means as a society wide phenomenon and at our schools, for example. So, first off, it is part of a continuum of gendered oppression. So, you can tell that there's a broad spectrum of activities. Whether it's just one random, mildly harassing tweet once a month all the way up to somebody setting up a fake website with all of your nude photos and videos lying about you sending it to all your co-workers and your friends and family. This type of behavior is rooted in a pre-internet, misogynistic beliefs, sexist norms, patriarchal rape culture and that's important to remember because a lot of times people end up saying, Oh, well, it's the internet's fault or this wouldn't happen at work or Facebook or TikTok. And all those things absolutely exacerbate the problem. Play a role. And that's why we're here. We have to remember that the problem did not start with the internet and it won't end with the internet. Of course, it is gender and intersectional. The problem disproportionately impacts women and girls. With statistics supporting that with both compelling and unique harms to those in multiple marginalized groups. So, for example, intersecting with race, disability or income, for

example. How this is done? I think pretty clear it's done through devices such as phones, social media platforms, private messages. But something that might be less clear is that as a result of the abuse coming through these particular channels lends it a form of intimacy that it might not otherwise have if someone was just grabbing you off the street, for example. Because you're at home, on your phone in your bed and you're reading this and then all of a sudden this really violent message comes in to what is generally your personal space. And so that can end up having a much deeper impact.

Next. Again, because of it's all technology-facilitated happens online some people will tend to underplay the impacts and the harm. But by this point in time, especially after two years of this pandemic, I think there should be clear to everyone if it wasn't already that online is offline. There is no online world and a real world it's all the same world. If you are silence online then that is you being shut out of the public sphere. And so we need to start abandoning if you haven't already this false dichotomy between online and offline because it's an artificial distinction. Doesn't make sense. Especially for students. People who are students now are probably digital natives so make even less sense to them. Tech-facilitated sexual violence, it is underreported for all the same reasons that other gender violence and sexual violence is underreported. But now even more so because you put on top of that a layer of technological illiteracy whether that's from the authorities, institutions or law enforcement. And so that contributes to further victim blaming and not understanding of, well, this is where you get, oh, well, it's just a Facebook post what's the big deal? Or, well, if you didn't want the photo shared then you shouldn't have posted it. Things like that. And as part of that misunderstanding there's two ideas I'd like to leave you with in terms of understanding what is tech-facilitated gender-based and sexual violence. The first one is that because it all happens online, on one level it is just speech or just expression, right? It occurs through text messages, through memes, through images and videos sent online. But just because it occurs through a medium of expression, that is expression, that doesn't mean it is just words or just speech. They actually constitute substantive actions with devastating tangible impacts on people's lives. The last thing is that if you...I was going to say you take one thing away from this webinar that's wrong but there's many things you can take from this webinar. But hopefully this is one among them which is to abandon the term cyber bullying. It is so outdated by this point. And it does not do justice to what this phenomenon actually is, what these behaviors are and that impact what they have both on an individual and on a systemic level. It minimizes and obscures the extent of the harm. It raises the systemic and structural nature of how this is a form of gendered-based hate. And it undermines what's actually happening and obscures our understanding because it's so much more than what this term evokes. Which is essentially children being mean to each other on a playground which is not what this is.

So, in terms of bringing these slightly closer to home I thought I would go over some concrete examples that have actually happened on Canadian campuses. So, the first one...And actually I will give a content warning at this point just because these all involve things happening on social media and potentially graphic and definitely violent and misogynistic language. So, to start off with at the University of Ottawa recently. There was a Facebook chat leaked where five men were essentially talking about committing sexual violence against the president of the Student Union at University of Ottawa at that time

essentially saying that she should be punished sexually. At the University of Dalhousie Faculty of Dentistry there was a 15 men who started a Facebook group called The Gentlemen's Club or something like that. They voted on which female classmates they would commit sexual violence to. They joked about drugging women with chloroform and nitrous oxide before sex. And as both Schulich professor Jane Bailey has mentioned. We'll talk. These are future medical professionals who are going to be rendering patients unconscious in the future during surgical procedures. And they're talking about rendering women unconscious before sex. Up then at Western University recently. This is actually an example that I put up here that slightly flipped the script because the sexual violence wasn't happening through social media and technology. What happened is that there was a series of TikTok videos published during Orientation Week during a week at Western that alleged up to 30 female students were drugged sexually assaulted allegedly at a first year residence. And for an entire evening if not day this was this information was only available on TikTok. And none of the allegations were investigated until people were making enough noise about it on TikTok and on Twitter saying this is happening, why is no one investigating? Finally, Western start investigating and then mainstream media started covering it one or two days later. But all of the point of that is just to say that it's really easy, I think, to get out of touch and not quite understand what's happening if you don't have firsthand experience of being on these platforms yourself. And so that might be something as a way of helping to support students. It's just doing that self-education to know, OK, How do these platforms...? What are the dynamics of it? That's kind of hard to get across unless you're actually on it. So, to wrap up the section I will just briefly go over what are some of the harms and impacts of tech-facilitated gender-based violence and sexual violence? I am completing to two just because we thought as an introductory webinar it would be helpful for you to have the full context of all of that activity in the sphere of which sexual violence is a subset. And often perpetrated through the same channels and in the same ways. So, the harms and impacts occur again on an individual and on a collective systemic level. First, of course, you have psychological impacts, fear, anxiety, depression that can lead people to self-harm and death by suicide as well as long lasting emotional and mental trauma that extends far beyond the timeline of the abuse itself if it does end. This of course can lead to physical illness as well as violent attacks. We know, for example, that online misogynistic rhetoric and hate speech has led to offline violence such as the Toronto van attack, for example, that was committed by someone who had spent a lot of time in cell forums. In addition, people have been threatening to the point of needing to move homes and schools for their safety. Then you have the social impacts such as isolation, ostracization. Something that the internet and social media allows in particular is for the person who's the abuser can actually start weaponizing the victim or survivors social networks against them. Because if in physical space, work, school, dating, family are all in separate spheres and might be separated. Now online they're all in the same space. And so the abuser can work that to their advantage and start turning their networks against the person who's been subjected to abuse, cut them away and just further isolate them or embarrass or shame them. Which then leads to

further ostracization and isolation. Particularly, when it comes to students who are at an extremely vulnerable stages of their careers. They're just starting out. This type of abuse can lead to lost opportunities for career advancement. It can prohibit them from fulfilling their work or academic responsibilities. So, that's probably important to note from a support perspective and potentially impact the reputation as well. So, for example, Justice Laurie Douglas several years ago was penalized professionally due to being subjected to her nude images being distributed without her consent. So, she was professionally punished for somebody else committing sexual violence against her. Of course, there's potential financial abused involved but even if there's no financial abuse, again, tech-facilitate violence if you being persecuted everywhere you go online that could lead to miss wages the cost of legal support or professional support and medical costs of health care or cost of having some sort of backup or extra plan. So, those are a lot of things that someone might experience on the ground who is subjected to these types of behaviors and activities. But again, I think it's really important to stress that this is not just an individual harm that can be solved from a person by person basis. Although it obviously has to be addressed on that level. It is also a societal problem. This leads to women and girls as a class being unable to be full members of society and to participate in the public sphere on an equal basis to people who are not systematically targeted for this kind of abuse and harassment and violence. So, you can see this for example, because it is women who are journalists and politicians and feminists and activists who tend to be the most targeted. And I don't think it's a coincidence that is to be women who are in the public sphere try to influence society and politics and culture. And that of course leads to where I generally started which is all these amounts to a violation of their fundamental human rights. Whether that is the right to privacy, the right to equality or the right to freedom of expression because there are signs online. You can just see how all of these behaviors together wherever you go just results in essentially just a web of silencing and persecution surrounding the person who is subjected to this. So on that note, I'm going to pass it over to Suzie.

SUZIE DUNN:
Great. Thanks Cynthia. I'll just take a minute to share my screen. While I get this going. Yeah. So, I'm a professor at Dalhousie and I work a lot of these issues. And I just want to acknowledge that Dalhousie sits on Mi'kmaq the traditional territory of the the Mi'kmaq people and that we're all treaty people.

One thing that Cynthia and I both wanted to point out as is that we will be sharing the slides. This is a really complex issue and trying to fit even an introduction to technology-facilitated sexual violence. Let alone other issues of technology-facilitated gender-based violence. It's is difficult to do in an hour. I think we probably could have spent a whole day on this. But we will share our slides and we will share our resource list. And then, of course, we have an upcoming webinar in about a month or so that will get a bit into the law and what legal protections people have when they experience technology-facilitated violence. But for now, what will be speaking about is really how to respond to people who've been

targeted by tech-facilitated violence. And we've heard this quite a lot from anti-violence organizations, transition houses, different support workers that they're starting to hear more about how technology is influencing abusive relationships. Is coming in to the organizations that they're working for and people are asking for help and sometimes they don't know what it is or what to do. And so this portion of the presentation is gonna be focused a bit on what to do. Some helpful tips and tricks. We'll talk a bit about how to identify the harms, how to document them. With many forms of tech-facilitated violence. Particularly with nude images, people want the content taken down. We'll talk a bit about getting content removed. And then safety planning around tech-facilitated violence which is a different experience. And then safety planning around intimate partner and violence that involves a physical violence. But one thing I think is important to remember is that when we're talking about safety planning it's really gonna depend on whether someone's in a relationship where their partner might have access to their device. So, this can include family members, friends, roommates or family. Because often in those circumstances they may be able to put content on their devices such as Stalker where they might be able to get around two factor authentication because they've got the device on their hands. And then in some cases they're being monitored in a way that's different then if it's a stranger or an acquaintance who's perpetrating the violence. And it's important to be aware that because technology always leaves a digital footprints. That whenever you're working with someone who's experiencing some sort of technological based harm then you consider how this content might be redistributed. Whether someone might be monitoring a phone or monitoring their computer. Because even when looking at ways to help them it might trigger more abuse that the person who's monitoring their device can actually see what's happening. And also some tricks like asking someone to change their password that might not be effective if they're, for example, in an intimate partner relationship where they're forced to give up their passwords by their controlling partner.

One thing that Cynthia was speaking to that I think is important is really to avoid victim-blaming and focusing on a survivor-centric response. You know, for example, when we think about nude photos I think the new form of victim blaming in the way that often women who are dressed with short skirts were told that they were provoking sexual violence. Now, when people take nude photos or even post fun cute photos of themselves online and then they experience sexual harassment or have those images released without consent they're often blamed for taking those images themselves. And what we know is that taking nude photos and sharing sexual content is a normal part of many healthy relationships. People shouldn't be blamed for expressing themselves sexually in digital spaces. It's also important to remember that online harms should be taken as seriously as offline harms. We've heard repeatedly that when women go to police and when people go to their schools or report to official organizations they're often told it's just happening online. They shouldn't worry about it. No one's being serious. Even one of the things is as harmful as death threats and rape threats. So, it's important to take those issues seriously. And stalking is something that

occurs very easily through technology and so, often someone will come in and they'll say things that might sound paranoid to some people. They say, I think I'm being tracked. I think that someone knows where I am. Is listening to my calls. But with technology this is possible. And so it's important to take those things seriously. And it's especially important to make sure that you're not asking other victim or survivor to stop using social media, to stop texting, to stop emailing or to stop going through digital spaces, for example, don't go to the classroom another person sending the messages or stop using their Instagram. I think it's an unrealistic response especially during COVID. We all know our lives are online these days. And also it's putting the responsibility on survivors when really the responsibility should be on the abuser to stop their behavior.

With intimate images one of the things that you may want to ask is you have images been captured because they've been taken by a person and shared or are there possibility of there being images that are recorded on computers or phones? One thing that we've heard and seen data on, and I think is common on university campuses, is that people will leave their computer up and it will look like the computer's off but it's actually on and they'll film someone sexually and people can do this with their phones as well. Often this will happen during oral sex where someone will use their phone to record that without the other person noticing. And so sometimes sexual images are captured without consent. So, thinking about the different ways that images could be captured. And if someone has a copy of the image there's certain ways that you can look to see whether that image exists elsewhere online. For example, if it's been posted on pornography websites. So, you can do reverse image searches on the internet using Google. And you can also put Google alerts for a person's name. Often, when someone's experiencing online harassment or abuse people are putting their name with the content because it's part of the reputational harm. So, if someone's sexual image is posted and their name and their university or their workplace it amplifies the harm. And so by having a Google alert it can help show when content is coming up about a particular person. It's not perfect. It's not going to show every time someone tweets someone's name or if they spell their name slightly off, but it can be helpful. So, for Google Images, you can just actually drag and drop an image into Google Images. So, for example, this is a head shot of mine. If you drag and drop it into Google Images it'll show where it shows up on the internet. So, for me it showed up on my website. It showed up on uOttawa website where I used to teach. And so that way you can find out other spots where that image might be on the internet to help figure out where it might need to be taken down.

This is a Google alert system you can just put in your own name and then it will pop up alert. So, if you have someone who's harassing you and posting content about you online this might be a helpful way to find out if more content is being shared.

A lot of people wanna report to social media to get the content taken down. And this seems like a simple process but it's not always very simple especially if you're a support worker. So, there's a lot of media safety guides that help explain what social media companies policies

are and what the reporting mechanisms are. And what we're sharing that in the resource document that we'll be giving you and so those are helpful things to become familiar with when you're helping someone. But it's important to document the contents before you take it down. This is especially important if you may need this for a report at the university for misconduct or if you want to report it for legal reasons.

So, documenting and logging abuse. You can keep track of this in various different ways. So, what time when it happened? what app was used? This information can be very important as well, too. If you're not sure who is the person who might be sharing sexual images or sexually harassing you on the internet. Because you might need to keep track of what accounts that's coming from even though it might not have a person's name on so that later on that might be able to be investigated differently. And there's many organizations who provide helpful kits. I'll be mentioning the BC Society of Transition Houses many times in this presentation because they're doing some of the leading work in Canada on tech safety. And if you go to their websites and look for their safety web page they have many resources on how to document evidence, on how to support victims and how to get content taken down. And really practical tips on how to document content and then also how to get it taken down. So, I really recommend that you look to that website in particular. Often, abusive partners will be tracking someone's whereabouts, tracking what they're looking at, tracking what they're doing. So for example, if someone's experiencing sexual violence through digital means or harassment through digital means they might be searching for where to get help. It's important that they know that their internet history might be tracked by their abuser. And so it's important to either recommend they use a computer that's not their computer or find ways to visit using a private or incognito mode. And if they're not able to do that, to learn how to selectively delete their search history so their partner won't know that they're looking for help and the ways that they are looking for help. Even looking up something like the campus sexual violence support people that might show up on their internet history and their abusive partner might find that. Which can lead to additional abuse. Particularly after someone's left an abusive relationship or is getting away from someone often there will be shared accounts or for example, someone will use their partner's computer to sign in to their email. And so you want to make sure that this person that you're helping has signed out of all of their accounts when they're done using them. And there's ways to look into your accounts to see if someone else is getting access to them. So, going in and making sure that other people don't have access. And if they do you can actually delete and remove. And again, we're not going into too much detail today. There's a lot of videos out there that show you how to do this including some on BC Society of Transition Houses as I mentioned before.

Location tracking is a new form of abuse that we see in intimate partner relationships. And so, we'll see things that Apple AirTags have come into media attention recently for causing issues. Because if you pop this little tag into someone's bag they can find out where you're going. So, helping someone who might feel as though they're being stalked or tracked by

learning how to identify where these tags are helping them turn off location tracking on their devices. And there's certain features like Find My Phone that abusive partners can use to track where someone is. And so, learning how to turn those features off and helping people turn those features off is an important skill set to gain. And so this is just an example you can see on this phone. This person's turned it off so the location is not happening on the App Store and only on Bumble or the BusBuddy when they're using it. And so you can go down through all the different apps and change location setting on them.

When people take photos of themselves and photos actually include quite a lot of metadata. And so what that means is there will be metadata it's just kind of code or information in the back of the photo that if someone has a copy of it they can look up the metadata and it'll often show the location of where someone is. So, especially if someone's trying to avoid another person and they're posting photos of themselves on the internet they're gonna wanna make sure that they remove that GPS location. Otherwise, someone will be able to take that photo. Look at the metadata and figure out where that person is located. And so, if someone's trying to avoid an abusive partner and this is an important thing to learn how to do to make sure that your information isn't on your photos. Social media companies strip that information when photos are posted but just an important one to have if someone's got a website.

Again, hidden cameras and trackers or something that we're seeing more commonly among younger people especially secretly filming sexual activities. And so having conversations around being more cognizant of where there might be hidden cameras and the risks that come along with that. Of course, you should never victim blame anyone who might be in a position where they're being filmed without their consent. But there are some different devices that can scan for hidden cameras especially if there's a camera hidden in a person's, for example, in their dorm. And if someone might have given them a radio or given them a gift or some sort of device that has a hidden camera in it there is technology that can help you detect that. Especially if it's Wi-Fi enabled. Often, these hidden cameras are Wi-Fi enabled so that the person can then download the content.

Our phone plans and shared accounts. If someone has a shared phone plan and then they break up with their partner their partner can still see who they're calling and what their records are. And so making sure that people who are leaving abusive relationships get removed from phone plans and shared accounts. And there's some things that you just don't think about, sometimes people will have their fitness tracker linked to their partners devices that can show where they are. You'll have cloud storage. You forgot that you shared or gave your partner access to. And especially if your photos are automatically loading up onto your cloud storage that may give them access to intimate information such as nude images or if you're in a new relationship with someone and you're texting and those texts might show up in cloud storage. So, making sure that those are disconnected and learning

how to help people disconnect those accounts is an important skill set to have as a support worker.

Again, trusted devices and check ins going in and making sure that you disconnected any trusted devices so that they can't access your email on their computers or their phones anymore. You can check things like last account activity that'll show where the account's been accessed. Even look for unusual IP devices or IP accounts that have access to it or other devices that aren't that person's computer or cell phone.

And so here's an example of what it looks like. This is an example from a Gmail account. So, you can see it's the same IP address whether someone's at home using their mobile phone and their computer same IP address. And also there's a funny one here. And so the mobile phone that might mean that they're at someone else's house. But if they remember where they were at 9:30 a.m. And they were at home and someone else's IP address is showing up on their email it means that someone else is accessing their email and might be able to gain access to their private information. Stalkerware is one of the trickier ones. It can be really difficult to know whether it's on a device or not. We've added a link to the clinic to end tech abuse which is a fantastic group out of the United States that works and can help people show whether stalkers on someone's phone. Someone is concerned that Stalkerware on their phone or their device you've got to be very careful on how to look for it. Because essentially what stalker does is it shows people chose the person who has the information being sent to them what's happening on the phone. So, if you start fishing around on the phone trying to find means to take the stalker off it'll alert the person that you're aware of the Stalkerware is there. Which can lead to additional abuse if the person overreacts thinking that they've been caught. Have encouraging people to have strong passwords. Again, this will depend on whether they're in a relationship where they might be forced to share their passwords. But if not there's all sorts of tips and tricks which I won't read them all out here. But using long sentences rather than words to create passphrases using password manager accounts are good safety tips for people.

On social media, it's important to turn off location services if someone is dealing with someone who is sexually harassing them or stalking them. For example, I'm asking their friends not to tag them in photos not to tag their location in photos. Not to allow random people to friend them so that they might be able to get secondary information about a person.

And Zoombombing is something that we've seen quite a bit since the beginning of the pandemic. And so this will often happen for groups that are in equality deserving group. So women, racialized folks, LGBT folks and we've all seen, by the way it's commonly happened where those groups have been targeted and often violent or offensive pornography is posted or racist slurs or yells or sexist slurs or yelled. And so having good zoom hygiene for places where people are organizing and NNEDV's is an organization of the United States.

And they've got a great toolkit called using Zoom safety, privacy and confidentiality considerations. That's worth checking out if you're someone who organizes a lot on Zoom.

And finally, we'll all go through four quick sections of resources in my last few minutes. But again, we're sharing a resource sheet where a lot of this information is and it links to a lot of groups that will provide more step by step tricks that you can look to. So, for privacy and digital hygiene, this is really helpful if someone's experiencing privacy attacks or harassment from strangers. It's not always as helpful with intimate partner relationships, but it's quite helpful. So, organizations such as the Electronic Frontier Foundation or here in Canada there's organizations that provide these surveillance self-defense tests and you can just go through here and it'll show you different ways to help protect your device or your accounts.

Documentation. Again, as we were saying, it's helpful to have documentation. This is a sample from another organization as well not without or without my consent. It helps to show people how to collect evidence. And then for removal guidelines many harassment organizations, heartmob it's an organization that helps people who've been harassed. They'll have really helpful guides on what the social media, safety guides and content removal guides are. That might be helpful for people who are doing frontline service work. And might be a bit more clear than what you see on the actual website themselves such as Facebook or Instagram.

Safety planning. I highly recommend going to the BC Society of Transition Houses. Over the last few years they are producing a lot of extraordinary work and often speaks to Canadian laws but has very practical safety guidelines. And some that are easy to use checkboxes if you're working with someone on how to do safety planning. Because doing safety planning for how to avoid sexual violence and how to avoid intimate partner violence or other forms of gender-based violence there's some good tips and tricks on those websites. And they've got really handy videos to watch as well. So, if you've got time make sure you don't miss out on that resource. And there's laws and direct supports. So, depending on the province that you're in, Nova Scotia has an organization called CyberScan. But people who've been targeted with intimate image distribution can call and get direct support. It's one of the things that Cynthia and I have been advocating for for a long time is to see more of these organizations across Canada where people can get direct supports. But if you're interested in learning about some of the criminal laws that apply to tech-facilitated violence the Equality Project is a fabulous project that has a criminal law database and shows all of these these legal issues. We'll also be doing a presentation in about a month. That will go more into detail on what laws apply here in Canada to this type of harm. And finally, education. A lot of people don't know what these harms are. What the terminology means. And how common it is. And what all the harms are. And these are a few reports that I think summarize the issues quite well. Installing fear as a recurrent stalker where technology-facilitated gender-based violence is an overview that I wrote generally on these these issues. It's good how to talk to Twitter and free to be online are ones that show statistics of

what these harms look like and how equality seeking groups are deeply impacted by it. This image-based sexual abuse study is one of the most comprehensive studies that's been done globally by some of the world leaders Nicole Henry, Clare MacLean, Asher Flynn, Kelly Johnson, Anastasia Powell. These are these are real heavy hitters in this area. So, I recommend reading that study if you're really interested. And then Cynthia wrote this report deplatforming misogyny. That is a great explainer on many of the laws and especially how social media companies should be held responsible as well for some of their role in the harms that are experienced on their on their platforms. But thank you so much. I think we still have about 20 minutes for your questions and we're happy to take questions and answer what we can. So, I'll just stop sharing the screen here and bring it back to the group.

ROBYNNE DEVINE:
Awesome. Thank you. And just an invitation for anybody who wants to either put a question in the chat or if you want to ask your question about just maybe raise your hand so that we can manage that.

SUZIE DUNN:
I think we've got a hand up.

CHELSEA CORSI:
Hi, is that me?
(CROSSTALK) Hi Robynne, it's Chelsea Corsi not sure if you remember me? Nice to see you again.

ROBYNNE DEVINE:
I do. It's great to see you.

CHELSEA CORSI:
Thank you so much for your presentation. I'm Chelsea. My pronouns are she and her. And I'm joining from the Tkemlups te Secwepemc within Kamloops today. My role is I coordinate the Wellness Center at Thompson Rivers University. And I'm also here with a partner of mine. We were working on a consent cafe project for high school students that were partnered with our community on. But I really want to thank you this is there's so much information here. But it's quite fascinating because what I'm finding and I'm taking my role as wellness coordinator, especially during COVID last year, a lot of our student leaders were working from home virtually. And we tried to get involved in Instagram lives to connect with our followers and it was quite fascinating. And one of my colleagues was doing it from student life and we started noticing like the sexual harassment just starting on the chat. And my colleague was interviewing someone for a live about something and was just continually but in that moment she didn't know what to do. She thought I should just keep going. Her response was kind of like this let me keep going. But it prompted some conversations from our campus about, Well, what do we do it for having students in these spaces and places?

They're representing our university. And it primarily happened to female identified students. And so we actually had a situation on our end with my team and we had a plan. So, we had a plan. We had an extra student on. We had the two students reading the live. And so, it happened. These students started being sexually harassed. So, our quick plan was we documented. We stopped the chat immediately. We stopped the live immediately. We had...The show must not go on, right? We don't have to keep going because we think we need to. But something I also did was I did contact the RCMP. Which none of the my colleagues had done. And what they were saying to, and you may have seen this I was curious about this, is that they said that there's often algorithms. It might not necessarily be like a person behind it but there's some sort of set algorithm that starts sending these messages so it can't be traced back to a certain person. So, I guess that's just my quick story. But my my what kind of questions around do you have any kind of evidence informed practices around in those types of situations? What should be done? And then secondly, if it is some sort of manipulated computer system like how do you actually stop it? Or find the culprits? Or like is there a process for that? Thank you.

SUZIE DUNN:
Yeah. No problem. And I think what they were getting at they're probably suggesting they're bots. And so like bots or these kind of pre-programmed sexual harassment things. So number one, I think it's too bad that that you were brushed off and told that this was probably bots because they very likely could have been people. And ultimately, it can be difficult to identify who is the person who's attacking because it might not, you know, unless it's associated with their student number or their student account you might just end it. It might just be like hot guy 37 says this. And so in those moments it can be difficult. But if a crime has been committed it is the job of the police to investigate and to determine who this person is. And they can do that through tracking their IP address or making requests to Instagram and finding a way to link the account to the IP address that's probably affiliated with the person. So, it is the job of law enforcement to assist in those circumstances. But we do hear this that often people are brushed off. Unfortunately, a lot of the strategies around making these spaces safe is limiting who can talk. And it's unfortunate, right? Because here we wanna talk about whatever it is. We wanna engage with people. We wanna have women speak. We wanna have racialized people speak. What we see is that often we'll get racist or sexist commentary coming in. And so some of the strategies that you can do around that Instagram Live is more difficult. But for Zoom, you can have it's only people from the university can come and they have to sign in using their official accounts. Or you can make the decision not to have chats. Sometimes in the work that we've done we've had some presentations where we don't allow recording so that people can speak freely and that there's not concerns around that. But there's there's a variety of safety strategies that you need to take into consideration when doing this type of work. And it's really unfortunate that these spaces that are supposed to help build community can be turned into spaces of harassment. And I'm sure Cynthia probably has some excellent advice to share as well.

CYNTHIA KHOO:
Well, I was just thinking it is a sign of how unfortunate things are. As much as we emphasize not telling people just go off the platform. My first thought was, unfortunately, it doesn't seem like Instagram gives you the level of control needed to prevent selectively harassing comments while still adding other comments go through. On a practical level. I know YouTube does have a similar feature where you can have live conversations with people commenting. And I've never used it myself but it would be worth looking into to see if there's a way to moderate it more than Instagram one. It might actually be called YouTube Live. But it's very similar feature with maybe more content moderation features. And then what you said about... So, where they said it was algorithms. I tend to be a bit careful when it comes to attributing technological causes depending on how much of technical expert the person is. Especially because technology uses so much these days that you get people to think like nothing as the algorithms and you get other people thinking everything is the algorithms, And this tends to be a lot more work needed just to make the single distinctions between what is actually happening. So, for example, like Facebook is not literally listening to our phones. They just have such an extensive advertising and tracking system that they may as well be listening to your phone. So, I mean neither is good but only one of them is true. And so in this case, when it comes...I mean, if they just set the the algorithms that could affect any number of things. One, it could have been standards that have been set up to troll people. Although, I actually am not familiar with that condition Instagram Live. They are definitely rampant on Twitter with like disinformation botnets adding there.

Which other researchers, one of the disinformation states have been tracking. They also could have just meant algorithms in the sense of all of the social media platforms. Facebook and Instagram which is now owned by Facebook and TikTok based on algorithms that are optimized for engagement, right? And so, maybe they meant something like, well, sexual harassment is this "engaging" from the statistical platform's growth perspective. And so the platform algorithm could have trained to promote this type of content. But algorithms doesn't know what kind of content it is. It only matters to humans. And so, they could have also meant it that way. So, on Twitter for example, if you see a lot of people retweeting something because it's a network of abusers. Users who have decided to target a particular person that will tell the algorithm to show it to more people purely by virtue of all the engagement that it's getting.

SUZIE DUNN:
Well, thank you very much. And the one thing with Instagram you mentioned the one thing that we did learn is, someone said I'm not sure how many slang words you can use because you can go through Instagram and put a bunch of words in that I think will block. And so that was quite an interesting meeting having to sit down and decide, Well, what words are we going to block off our Instagram instead, right?

CYNTHIA KHOO:
Instagram gives you the power to block specific words. OK. That's very interesting. Cause Instagram itself has been criticized for blocking words but generally to do with sexual content with consensual adult sexual content or with LGBT content, for example. And the other thing I was going to speak to something you mentioned is when you said, kind of what can we do? Cause at some point it's under control the companies. That's actually why the majority of my research in this space has actually been focused more on the social media companies themselves rather than the actual perpetrators. So, this will come up more in our part two when we're focusing on laws. But the Deplatforming Misogyny report is all about how to hold...I basically skipped over the actual abusers altogether and went straight to what can the companies do? Because they're profiting off of this abuse. They've purposely designed they're not dumb pipes like internet service providers are. They actually designed the platforms and have control over the algorithms in terms of what kind of content succeeds and what doesn't. And what kind of online environments are cultivating.

SUZIE DUNN:
Thank you so much.

CYNTHIA KHOO:
Thank you.

ROBYNNE DEVINE:
Awesome. And we have another question in the chat. Maybe I'll read it out. We ask if in your research experience have you ever found for the post-secondary institution in Canada have taken steps to address technology-facilitated sexual violence in terms of policies, strategies and training?

SUZIE DUNN:
So, there's not a lot of work being done in this area now. We're starting to see more and more of an interest in it. Even this presentation here today is a sign that institutions are taking some interest into it. There's a researcher, I believe, at a Western University named Sean Bell Goss, who's been looking at policies also within the faculty level because it's been interesting as academics were also expected to tweet and exist in digital spaces where a faculty member might actually experience harassment. So, we're starting to see some research in the area and in some movement in the area. Some universities like the University of Ottawa, includes technology-facilitated sexual violence in some of their training on bystander intervention or on general digital etiquette. But right now it seems most universities are acting fairly ad hoc as far as we're aware of. But if anyone in the group does know more about that we'd love to hear any other information that you know of. And something I'm not sure if you've heard of much or. And you're also in the States you might have some interesting examples out of the United States.

CYNTHIA KHOO:
Yeah, I think you would probably be more tapped into that. I'm not familiar.

Thanks for your question.

ROBYNNE DEVINE:
Are there any other questions before we wrap up today's session?

Well, I just want to thank Cynthia and Suzie for this webinar and I really look forward to the next one. As a mom, I'm taking notes too because these are all things that impact a lot of us personally too. So, yeah. Thanks so much again for the great session. Well, thanks to everybody who came out today. It's great to see everybody.

SUZIE DUNN:
Thanks so much for inviting us.

CYNTHIA KHOO:
Thank you.