



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

Standing Committee on Canadian Heritage

EVIDENCE

NUMBER 125

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Thursday, June 13, 2024

Chair: The Honourable Hedy Fry



Standing Committee on Canadian Heritage

Thursday, June 13, 2024

• (1545)

[*Translation*]

The Chair (Hon. Hedy Fry (Vancouver Centre, Lib.)): I call this meeting to order.

Welcome to meeting number 125 of the House of Commons Standing Committee on Canadian Heritage.

I'd like to acknowledge that this meeting is taking place on the traditional and unceded territory of the Algonquin Anishinabe people.

[*English*]

According to Standing Order 108(2) and the motion adopted by the committee on February 14, 2022, the committee is resuming its study on online harms.

Before we begin, I want to ask all members and other in-person participants to consult the cards on the table in front of them and to take note of the preventative measures in place to protect the health and safety of the participants, especially the interpreters. Only use the black, approved earpiece. Keep your earpiece away from all microphones. There's a little decal in front of you. When you're not using your earpiece, you can put it face down on that decal. Thank you for doing that because we do have problems with interpretation sometimes with feedback.

Today's meeting is taking place in a hybrid format. In accordance with the committee's routine motion concerning connection tests for witnesses, I want to let you know that all the witnesses have completed their connection tests in advance of the meeting.

I want to make a few comments for the benefit of members and witnesses. Please wait until I recognize you by your name before speaking. Put your hand up. If you're in a chat, you have a little hand icon that you can put up, and if you're in the room, put your actual hand up, and I will recognize you.

I will remind you that all comments should be addressed through the chair. Also, please do not take pictures of the meeting because it's going to be produced online later for you anyway.

Pursuant to the motion adopted by the committee on Tuesday, April 9, we have Claude Barraud, psychotherapist from Homewood Health, in the room with us today.

Claude, can you put your hand up or stand up so that people know where to go?

If you feel distressed or uncomfortable with some of what you're hearing and you feel you want to talk to him, he's here to help you out.

I want to welcome our witnesses. We have our witnesses set up in a particular order, but I just want to flag the two witnesses who must leave at 4:30 p.m. They are Heidi Tworek, associate professor, the University of British Columbia; and Monique St. Germain, general counsel for the Canadian Centre for Child Protection. They are both here by video conference and will be leaving at 4:30 p.m.

Then, from 3:30 to 5:20 p.m.—or if, because of the votes, we are starting later—we will have Shona Moreau from the faculty of law, McGill University; Chloe Rourke from the faculty of law, McGill University; Signa Daum Shanks, associate professor, faculty of law, University of Ottawa; and Keita Szemok-Uto, lawyer.

• (1550)

Before we begin, I want the witnesses to know that they have five minutes, but not each. If you represent a group, then that group has five minutes. I notice that we have two people from McGill, so they can decide who's going to be their speaker.

I will give you a 30-second shout-out—and I mean shout-out because I'll say “30 seconds”—so that you can wrap up what you're saying. You will have the opportunity later on, when you get to the question and answer period, to finish up some of the things you wanted to say.

Thank you very much.

We'll begin with Heidi Tworek from British Columbia for five minutes, please.

Dr. Heidi Tworek (Associate Professor, University of British Columbia, As an Individual): Thank you, Madam Chair, for the opportunity to appear virtually before you to discuss this important topic.

I'm a professor and Canada research chair at the University of British Columbia in Vancouver. I direct the centre for the study of democratic institutions, where we research platforms and media. Two years ago I served as a member of the expert advisory group to the heritage ministry about online safety.

Today, I will focus on three aspects of harms related to illegal sexually explicit material online, before discussing briefly how Bill C-63 may address some of these harms.

First, the issue of illegal sexually explicit material online overlaps significantly with the broader question of online harm and harassment, which disproportionately affects women. A survey in 2021 found that female journalists in Canada were nearly twice as likely to receive sexualized messages or images, and they were six times as likely to receive online threats of rape or sexual assault. Queer, racialized, Jewish, Muslim and indigenous female journalists received the most harassment.

Alongside provoking mental health issues or fears for physical safety, many are either looking to leave their roles or unwilling to accept more public-facing positions. Others have been discouraged from pursuing journalism at all. My work over the last five years on other professional groups, including political candidates or health communicators, suggests very similar dynamics. This online harassment is a form of chilling effect for society as a whole when professionals do not represent the diversity of Canadian society.

Second, generative AI is accelerating the problem of illegal sexually explicit material. Let's take the example of deepfakes, which means artificially generated images or videos that swap faces onto somebody else's naked body to depict acts that neither person committed. Recent high-profile targets include Taylor Swift and U.S. Congresswoman Alexandria Ocasio-Cortez. These are not isolated examples. As journalist Sam Cole has put it, "sexually explicit deepfakes meant to harass, blackmail, threaten, or simply disregard women's consent have always been the primary use of the technology".

Although deepfakes have existed for a few years, generative AI has significantly lowered the barrier to entry. The number of deepfake videos increased by 550% from 2019 to 2023. Such videos are easy to create, because about one-third of deepfake tools enable a user to create pornography, which comprises over 95% of all deepfake videos. One last statistic is that 99% of those featured in deepfake pornography are female.

Third, while it is mostly prima facie easy-to-define illegal sexually explicit material, we should be wary of online platforms offering solely automated solutions. For example, what if a lactation consultant is providing online guidance about breastfeeding? Wholly automated content moderation systems might delete such material, particularly if trained simply to search for certain body parts like nipples. Given that provincial human rights legislation protects breastfeeding in much of Canada, deletion of this type of content would actually raise questions about freedom of expression. If parents have the right to breastfeed in public in real life, why not to discuss it online? What this example suggests is that human content moderators remain necessary. It is also necessary that they are trained to understand Canadian law and cultural context and also to receive support for the very difficult kind of work they do.

Finally, let me explain how Bill C-63 might address some of these issues.

There are very legitimate questions about Bill C-63's proposed amendments to the Criminal Code and Canadian Human Rights Act, but as regards today's topic, I'll focus briefly on the online harms portion of the bill.

Bill C-63 draws inspiration from excellent legislation in the European Union, the United Kingdom and Australia. This makes Canada a fourth or fifth mover, if not increasingly an outlier in not regulating online safety.

However, Bill C-63 suggests three types of duties for platforms. The first two are a duty to protect children and a duty to act responsibly in mitigating the risks of seven types of harmful content. The third most stringent and relevant for today is a duty to make two types of content inaccessible—child sexual exploitation material and non-consensual sharing of intimate content, including deepfakes. This should theoretically protect the owners of both the face and the body used in a deepfake. A newly created digital safety commission would have the power to require removal of this content in 24 hours as well as impose fines and other measures for non-compliance.

• (1555)

Bill C-63 also foresees the creation of a digital safety ombudsperson to provide a forum for stakeholders and to hear user complaints if platforms are not upholding their legal duties. This ombudsperson might also enable users to complain about take-downs of legitimate content.

Now, Bill C-63 will certainly not resolve all issues around illegal sexually explicit material, for example, how to deal with copies of material stored on servers outside Canada—

The Chair: Thank you, Ms. Tworek.

I would advise you to wrap up. You can expand on this later on in the question and answer section. Thank you.

If you want to finish your sentence, go ahead.

Dr. Heidi Tworek: Bill C-63 is a step in the right direction to address a problem that, tragically, is swiftly worsening.

I'm looking forward to your questions.

The Chair: Now we go to the Canadian Centre for Child Protection and Monique St. Germain.

Ms. St. Germain, you have five minutes.

Ms. Monique St. Germain (General Counsel, Canadian Centre for Child Protection Inc.): Thank you for the opportunity today.

My name is Monique St. Germain, and I am general counsel for the Canadian Centre for Child Protection, which is a national charity with the goal of reducing the incidence of missing and sexually exploited children.

We operate cybertip.ca, Canada's national tip line for reporting the online sexual exploitation of children. Cybertip.ca receives and analyzes tips from the public and refers relevant information to police and child welfare as needed. Cybertip averages over 2,500 reports a month. Since inception, over 400,000 reports have been processed.

When cybertip.ca launched in 2002, the Internet was pretty basic, and the rise of social media was still to come. Over the years, technology has rapidly evolved without guardrails and without meaningful government intervention. The faulty construction of the Internet has enabled online predators to not only meet and abuse children online but to do so under the cover of anonymity. It has also enabled the proliferation of child sexual abuse material, CSAM, at a rate not seen before. Victims are caught in an endless cycle of abuse.

Things are getting worse. We have communities of offenders operating openly on the Tor network, also known as the dark web. They share tips and tricks about how to abuse children and how to avoid getting caught. They share deeply personal information about victims. CSAM is openly shared, not only in the dark recesses of the Internet but on websites, file-sharing platforms, forums and chats accessible to anyone with an Internet connection.

Countries have prioritized the arrest and conviction of individual offenders. While that absolutely has to happen, we've not tackled a crucial player: the companies themselves whose products facilitate and amplify the harm. For example, Canada has only one known conviction and sentencing of a company making CSAM available on the Internet. That prosecution took eight years and thousands of dollars to prosecute. Criminal law cannot be the only tool; the problem is just too big.

Recognizing how rapidly CSAM was proliferating on the Internet, in 2017, we launched Project Arachnid. This innovative tool detects where CSAM is being made available publicly on the Internet and then sends a notice to request its removal. Operating at scale, it issues roughly 10,000 requests for removal each day and some days over 20,000. To date, over 40 million notices have been issued to over 1,000 service providers.

Through operating Project Arachnid, we've learned a lot about CSAM distribution, and, through cybertip.ca, we know how children are being targeted, victimized and sextorted on the platforms they use every day. The scale of harm is enormous.

Over the years, the CSAM circulating online has become increasingly disturbing, including elements of sadism, bondage, torture and bestiality. Victims are getting younger, and the abuse is more graphic. CSAM of adolescents is ending up on pornography sites, where it is difficult to remove unless the child comes forward and proves their age. The barriers to removal are endless, yet the upload of this material can happen in a flash, and children are paying the price.

It's no surprise that sexually explicit content harms children. For years, our laws in the off-line world protected them, but we abandoned that with the Internet. We know that everyone is harmed when exposed to CSAM. It can normalize harmful sexual acts, lead to distorted beliefs about the sexual availability of children and increase aggressive behaviour. CSAM fuels fantasies and can result in harm to other children.

In our review of Canadian case law regarding the production of CSAM in this country, 61% of offenders who produced CSAM also collected it.

CSAM is also used to groom children. Nearly half of the victims who responded to our survivor survey of victims of CSAM identified this tactic. Children are unknowingly being recorded by predators during an online interaction, and many are being sextorted thereafter. More sexual violence is occurring among children, and more children are mimicking adult predatory behaviour, bringing them into the criminal justice system.

CSAM is a record of a crime against a child, and its continued availability is ruining lives. Survivors tell us time and time again that the endless trading in their CSAM is a barrier to moving forward. They are living in constant fear of recognition and harassment. This is not right.

The burden of managing Internet harms has fallen largely to parents. This is unrealistic and unfair. We are thrilled to see legislative proposals like Bill C-63 to finally hold industry to account.

● (1600)

Prioritizing the removal of CSAM and intimate imagery is critical to protecting citizens. We welcome measures to mandate safety by design and tools like age verification or assurance technology to keep pornography away from children. We would also like to see increased use of tools like Project Arachnid to enhance removal and prevent the reuploading of CSAM. Also, as others have said, public education is critical. We need all the tools in the tool box.

Thank you.

The Chair: Thank you very much.

I will now go to Ms. Moreau and Ms. Rourke.

Who is going to be the spokesperson? You will share it?

Ms. Shona Moreau (BCL/JD, Faculty of Law, McGill University, As an Individual): We will if possible, yes.

The Chair: You still have only five minutes. You know that. Okay.

Go ahead. Which one of you will begin?

Ms. Shona Moreau: I will begin, if possible. Thank you so much.

The Chair: Thank you, Ms. Moreau.

[Translation]

Ms. Shona Moreau: Madam Chair, members of the Standing Committee on Canadian Heritage, thank you for inviting me to testify before you today.

While this study covers a wide range of topics, we're here to highlight a very specific dimension: the need to address the growing threat of deepfake pornography and its effects on women and girls in Canada.

[English]

Our presentation will touch on three key aspects of deepfakes— one, what they are; two, who is affected; and three, what can be done about them.

Deepfake technology, as you know, is generated AI that creates fake audiovisual content by manipulating a person's appearance and likeness. As the technology has advanced, AI-generated content has become increasingly sophisticated and harder to distinguish from real-life footage. Lifelike deepfakes can now be generated using just a single photo of a person. As a result, it's not just celebrities and public figures who are vulnerable. Everyone is vulnerable to this technology, and though there are other applications for deepfakes, by far the most common use is for non-consensual porn.

The vast majority of deepfakes are pornographic, and these overwhelmingly feature female subjects. It's important for the committee to know that this gendered and sexualized use of the technology is not new. The term deepfake actually originated in 2017 and stemmed from the practice of using online tools to switch female celebrities' faces onto pornographic videos. In other words non-consensual porn has been central to the technology since its very beginning.

While the unauthorized use and creation of fake intimate images is not a new phenomenon—Photoshop, for example, has been around for decades—the advent of generative AI technology has taken this issue to a whole new level. Today, highly realistic and convincing fake pornographic content can be produced quickly and with minimal effort and skills. Even when fake, these types of images inflict real emotional, societal and reputational harm on victims.

Now even children are affected. In the past year, reports have exploded of schoolgirls who have found themselves the subject of pornographic deepfakes made and shared by their own classmates.

All this goes to show that deepfake porn is not a trivial matter. It's real. It poses a significant threat to people and to human dignity, and as such, it demands our attention and action.

The Chair: Thank you.

Ms. Rourke, you have two minutes and 16 seconds. Thank you.

Ms. Chloe Rourke (BCL/JD, Faculty of Law, McGill University, As an Individual): To effectively address this issue, it's crucial to understand how existing laws can be extended to cover deepfakes, but also why current regulatory frameworks are insufficient.

First, Canadian legislation prescribing the non-consensual distribution of pornography, such as section 162.1 of the Criminal Code, should be reviewed and extended to include altered images such as deepfakes. Doing that would send a clear message that it is wrong and must be denounced.

However, it is important to recognize that this is not enough. Unlike a real recording, deepfakes are not tied to a specific time, location or sexual partner. They can easily be produced and distributed anonymously. Therefore, in practice, it will often be difficult to identify perpetrators and hold them legally accountable, which will limit the deterrent effects of such provisions.

Additionally, even when an individual perpetrator is identified, criminal or civil penalties cannot restore a victim's privacy, dignity or sense of safety, particularly when the content continues to circulate in the public domain. To address these ongoing harms, we must consider the role and responsibility of digital platforms. Tech platforms such as Google and pornography websites have already created procedures that allow individuals to request that non-consensual pornographic images of themselves be removed and delisted from their websites. This is not a perfect solution. Once the content is distributed publicly, it can never be fully removed from the Internet, but it is possible to make it less visible and therefore less harmful.

Implementing such systems would mitigate the reputational harm caused by non-consensual porn, whether it be real or synthetic, and provide a more immediate and practical recourse for victims. Public regulatory bodies should work with major online platforms to require such procedures and to ensure they are effective, accessible and meaningfully enforced.

● (1605)

Lastly, this technology must be understood within the context of gender-based violence and societal attitudes toward women's sexuality.

The non-consensual sharing of porn is already weaponized against women and is further exacerbated by deepfakes because anyone is able to create and distribute such content. Women will have limited options to protect themselves. It's already being used to target, harass and silence female journalists and politicians. If unchecked, deepfakes threaten to rewrite the terms of participation in the public sphere for women.

This technology is rapidly evolving and harms have already materialized. While no one law can eliminate it, we can take action and legislatures have a role to lead these efforts.

Thank you.

The Chair: Thank you, Ms. Rourke.

I will now go to Ms. Shanks from the University of Ottawa's faculty of law.

You have five minutes, please.

Dr. Signa Daum Shanks (Associate Professor, University of Ottawa, Faculty of Law, As an Individual): Thank you.

I'm a law professor at the University of Ottawa and a law professor on leave at Osgoode Hall law school. I belong to the Law Society of Ontario.

I specialize in the history of laws, the impact of laws on marginalized peoples, law and economics, and tort law. I've taught at the university level for 26 years. Teaching has also included updating the judiciary about trends in law and professional development sessions for the legal profession.

Today, I'm going to focus on the influence of tort law upon legislation. Why? It's because it is directly responsible for responding to harm. Tort law is also a subject that has allowed courts to respond to matters that are not addressed in legislation yet. It has its benefits and shortcomings for making society better. It is considered part of private law and includes topics like personal injury, intentional infliction of mental distress, intimidation and breach of fiduciary duty, such as to children or the increasing topic involving indigenous peoples.

For me, two observations surface about legislation regarding harm.

First, I think about how private law interacts with legislation. Historically, many topics in private law have come across a judge's bench because parties, and ultimately the judge, have concluded that society would support the recognition of a certain harm. The harm, however, may not be articulated yet in legislation and may seem novel. However, those topics are constructed on jurisprudence, so while the name of a tort might be new, the details of the tort are familiar and already supported.

Tort law has helped create tools that have been and are integrated into legislation. Like other topics in law, there is often what is called a dialogue. Events in society impact arguments in court. Those arguments in court are learned about by those who create and implement legislation, like all of you. In this dialogue, sometimes the legislation introduces the idea first, and views about the legislation will then be brought up by parties in the courtroom.

This idea that private law and legislation have an ongoing relationship is vital to also realizing that almost all tort litigation does not result in a trial decision. As a result, any litigating, negotiating and resolving happens at earlier stages of litigation. In fact, those earlier stages are organized by the courts and involve many parties, including judges, to evaluate the nature and scope of the claimed harm. When a tortious subject is not guided by legislation, figuring these subjects out takes time and space in the court system.

All of us know stories in which people have felt less heard due to the slowness of the court process. That slowness is arguably magnified when legislation does not exist to quickly determine one part or all parts of a problem. Private law has helped get some harms more recognized, but when the private law's focus on harm does not have legislative guidance, addressing examples of harm and preventing that harm can take time and arguably increase the number of times that said harm occurs.

My second observation is about when legislation is proposed. I see any legislation about online harm, particularly when it impacts groups we consider more vulnerable, capable of paralleling the benefits of private law, plus avoiding some of private law's limitations. Demanding that a party act responsibly, for example, is mirror-like to negligence law. The concept is also prevalent in many intentional torts, such as intentional infliction of mental distress. It might be a word we are now integrating, but the word's presence is already evident.

Moreover, we can learn how other countries have found that it's possible to integrate acting responsibly into a rights-based system like Canada's. I believe we have the underpinnings of acting responsibly already in Canadian law.

Legislation has also an effect of dissuasion that private law might not have. Legislation hopefully stops most intentional harm before it happens. Introducing such subjects by a legislation influenced by tort law, especially when subjects are urgent due to their own form and growth, creates a type of social and judicial efficiency that trends in private law often lack.

Thank you for including the duty of acting responsibly, so that courts and society will have more guidance about how to evaluate it. It is my view this duty makes legislation stronger and the need for lawsuits less likely.

Thank you for this opportunity. I look forward to our discussion.

● (1610)

The Chair: Thank you, Ms. Shanks.

I now go to Mr. Szemok-Uto, please, for five minutes.

Mr. Keita Szemok-Uto (Lawyer, As an Individual): Madam Chair, committee members, thank you for the opportunity to speak before you this afternoon.

By way of brief background, my name is Keita Szemok-Uto. I'm from Vancouver. I was just called to the bar last month. I've been practising, primarily in family law, with also a mix of privacy and workplace law. I attended law school at Dalhousie in Halifax, and while there I took a privacy law course. I chose to write my term paper on the concept of deepfake videos, which we've been discussing today. I was interested in the way that a person could create a deepfake video, specifically a sexual or pornographic one, and how that could violate a person's privacy rights, and in writing that paper I discovered the clear gendered dynamic to the creation and dissemination of these kinds of deepfake videos.

As a case in point, around January this year somebody online made and publicly distributed sexually explicit AI deepfake images of Taylor Swift. They were quickly shared on Twitter, repeatedly viewed—I think one photo was seen as many as 50 million times. In an Associated Press article, a professor at George Washington University in the United States referenced women as “canaries in the coal mine” when it comes to the abuse of artificial intelligence. She is quoted, “It's not just going to be the 14-year-old girl or Taylor Swift. It's going to be politicians. It's going to be world leaders. It's going to be elections.”

Even back before this, in April 2022 it was striking to see the capacity for, essentially, anybody to take photos of somebody's social media, turn them into deepfakes and distribute them widely without, really, any regulation. Again, the targets of these deepfakes, while they can be celebrities or world leaders, oftentimes are people without the kinds of finances or protections of a well-known celebrity. Worst of all, I think, and in writing this paper, I discovered there is really no adequate system of law yet that protects victims from this kind of privacy invasion. I think that's something that really is only now being addressed somewhat with the online harms bill.

I did look at the Criminal Code, section 162, which prohibits the publication, distribution or sale of an intimate image, but the definition of “intimate image” in that section is a video or photo in which a person is nude and the person had a reasonable expectation of privacy when it was made or when the offence was committed. Again, I think the “reasonable expectation of privacy” element will come up a lot in legal conversations about deepfakes. When you take somebody's social media photo, which is taken and posted publicly, it's questionable whether they had a reasonable expectation of privacy when it was taken.

In the paper, I looked at a variety of torts. I thought that if the criminal law can't protect victims, perhaps there is a private course of action in which victims can sue and perhaps get damages or whatnot. I looked at public disclosure of private facts, intrusion upon seclusion and other torts as well, and I just didn't find anything really satisfied the circumstances of a pornographic deepfake scenario—again with the focus of reasonable expectation of privacy not really fitting the bill.

As I understand today, there have been recent proposals for legislation and legislation that are come into force. In British Columbia there's the Intimate Images Protection Act. That was from March 2023. The definition of “intimate image” in that act means a visual recording or visual simultaneous representation of an individual, whether or not they're identifiable and whether or not the image has been altered in any way, in which they're engaging in a sexual act.

The broadening of the definition of “intimate image”, as not just an image of someone who is engaged in a sexual act when the photo is taken but altered to make that representation, seems to be covered in the Intimate Images Protection Act. The drawback of that act is that, while it does provide a private right of action, the damages are limited to \$5,000, which seems negligible in the grand scheme of things.

I suppose we'll talk more about Bill C-63 in this discussion, and I do think that it goes in the right direction in some regard. It does put a duty on operators to police and regulate what kind of material is online. Another benefit is that it expands the definitions, again, of the kinds of material that should be taken down.

• (1615)

That act, once passed, will require the operator to take down material that sexually victimizes a child or revictimizes a survivor—

The Chair: Thank you, Mr. Szemok-Uto. Can you wind up, please?

Mr. Keita Szemok-Uto: Yes, I'll conclude there.

The Chair: I'm now going to the question and answer session.

Before I begin, though, I'd like the committee to know that we have until 5:45. I would like us to have in camera work for 15 minutes, so I'd like to end at 5:30. We're going to try to fit everybody and their questions into that space.

Now we'll go to the first round of questions. They're six-minute rounds of questions. I'll begin with the Conservatives.

Go ahead, Mrs. Thomas, for six minutes, please.

Mrs. Rachael Thomas (Lethbridge, CPC): Thank you.

Thank you, witnesses, for giving us your time here today and for sharing your expertise.

My first question goes to Ms. Moreau and Ms. Rourke.

In your opening statement, you said the Criminal Code should be expanded to include deepfakes. Then you went on to say that this isn't actually enough. We must also consider the role platforms play, and how government has a responsibility to ensure there are teeth in terms of holding those platforms accountable.

In an article you recently wrote in February, you said, "Updated telecom regulations can play a part. But Canada also needs urgent changes in its legal and regulatory frameworks to offer remedies for those already affected and protection against future abuses."

You seem to be outlining that both are needed. I'm wondering if you can expand on that.

Ms. Chloe Rourke: Our position is similar to what was discussed. The Criminal Code provision would need to be amended if it were to apply to altered images and deepfakes, in our interpretation.

While that's important, it's not going to provide a remedy in many cases, in part because deepfakes are so easy to produce anonymously that the person who produced them, in many cases, won't be identifiable. As we discussed, it won't necessarily provide the complete remedy that all victims are seeking in the sense that the content itself can continue to cause reputational harm and be circulated.

It's our position, also, that it would be important to work with platforms and have them be held accountable for the content distributed on their websites. They are the ones that have control over the algorithms listing the results, and they are the ones that can take the content down—at least make it less visible, if not remove it entirely.

I can defer to my colleague for further comments.

Ms. Shona Moreau: Yes, I echo everything my colleague Chloe said.

Also, we feel a bit desperate when we see this: If you search "deep AI", "nude AI" or anything like that, they are so easily accessible. It just pops up on Google. You put in a picture, pay three dollars and you're able to generate massive numbers of deepfakes of an individual—or many individuals, if you choose.

That accessibility is really what we're fighting against the most, because, as we know, litigation can take many years. Oftentimes, it doesn't make a victim whole. It's really about the ability to make sure these platforms don't make this technology as easily available for everyone. Also, as we've seen, children have an ability to use this. They might not know the consequences or realize how detrimental this is to the victims.

• (1620)

Mrs. Rachael Thomas: Thank you.

Bill C-63 does something very interesting. Rather than updating the Criminal Code to include deepfakes.... It doesn't do that at all. Deepfakes aren't mentioned in the bill, and folks are not protected from them—not in any criminal way. I believe that's an issue.

Secondly, platforms will be subject to perhaps an assessment and a ruling by an extrajudicial, bureaucratic arm that will be created, but again, there's nothing criminal attached to platforms allowing

for the perpetuation of things like deepfakes or other non-consensual images.

Does that not concern you?

Ms. Shona Moreau: I can take this one first.

As all the witnesses today talked about, it's a very good step in the right direction. We are here to showcase that this is a big issue and it needs to have further steps.

As you said, if there's more work we can do to protect, specifically—as we talked about—children, women and schoolgirls from this technology, it should be done. If there's a possibility for further legislation in the future, having a body that takes this on or more studies about this would be very beneficial, because this is not an issue that's going away.

AI technology is rapidly expanding, more than we can even predict regarding its effects. You could argue that there needs to be a constant committee and study on the new and innovative issues coming through this technology.

I think my colleague Chloe wants to talk a bit, as well.

Mrs. Rachael Thomas: Sure. I am running out of time, so perhaps the comments could be brief.

Ms. Chloe Rourke: I was just going to add that I think the Criminal Code provisions that currently exist and apply to actual real recordings of intimate images, or so-called revenge porn, are an incomplete remedy as is. That's not even including the issue of deepfakes and how much more complicated it is to apply there. I think our bigger priority is about what accessible remedies there are that can be implemented in the vast majority of cases. Many revenge porn cases would never be litigated or criminally prosecuted, and the harm continues. That's why I think involving the platforms is really important in that respect.

Mrs. Rachael Thomas: Thank you very much.

The Chair: You have 35 seconds, Rachael.

Mrs. Rachael Thomas: Mr. Szemok-Uto, I'm sorry. I did intend to leave you more time. I'm not sure if you wish to comment.

Mr. Keita Szemok-Uto: Do you mind repeating the last part of the question?

Mrs. Rachael Thomas: We're probably out of time.

Maybe I'll conclude by saying this. I think at the end of the day, what's being made clear at the table is that it's not enough just to signal good intentions. Rather, what I'm hearing from folks is that we do need an updated Criminal Code in order to go after those who would create and propagate deepfakes. I think that's really important for all women across our country.

I think what the witnesses have certainly drawn attention to is the fact that this is a gendered issue. It is women and girls who are subjected to it far more than men, and it does ruin lives. I think the government has a responsibility to act on that.

The Chair: Mrs. Thomas, you're going over. Thank you.

I will now go to Michael Coteau for the Liberals.

You have six minutes, Michael.

Mr. Michael Coteau (Don Valley East, Lib.): Thank you very much, Chair.

Thank you to all of our witnesses here today. I appreciate the work you're doing to protect young people and all Canadians from online harm.

My first question will go to Ms. Tworek.

We heard from Professor Krishnamurthy from Colorado a few days ago. He said something interesting. He said that sometimes one of the big challenges is the “elephant and mice” in the room. The big platforms, obviously, are the ones that have a lot of control, but there are also the small entities online that come and go quickly. For regulators it's hard to keep up with these fly-by-night websites.

What are your thoughts on how we go about tackling that challenge that was presented at the last heritage meeting?

• (1625)

Dr. Heidi Tworek: Thank you very much.

I served with Mr. Krishnamurthy on the expert advisory group. This is something we grappled with quite a lot. Of course, major platforms like Facebook and so on have many employees and can easily staff up, but we often see these harms, particularly now with generative AI lowering the barrier to entry, that could be a couple of individuals who create complete havoc or very small firms.

I think there are two aspects to this question. One is the very important question of international co-operation on this. We've talked as if all of the individuals creating harm would be located in Canada, but the truth is that many of them may be located outside of Canada. I think we need to think about what international co-operation looks like. We have this for counterterrorism in the online space, and we need to think about this for deepfakes.

In the case of smaller companies, we can divide between those whom I think are being abused and then the question of how the new proposed online bill, Bill C-63, could have a digital safety commissioner who actually helps those smaller firms to ensure that these deepfakes are removed.

Finally, we have the question of the more nefarious smaller-firm actors and whether we need to have Bill C-63 expanded to be able to be nimble and shut down those kinds of nefarious actors more quickly—or, for example, tools that are only really being put up in order to create deepfakes of the terrible kinds that have been described by other witnesses.

I would just emphasize that the international co-operation, finally, is key. Taking things down in Canada only will potentially lead to revictimization, as something might be stored in a server in another country and then continually reuploaded.

Mr. Michael Coteau: You talked about a massive increase in deepfakes. I think you said it was 550% or something around there. Obviously, the technology is shifting quickly. Over the course of my lifetime, we've seen technology rapidly shift. You know, I've

gone from buying the same album as a record, cassette, disc and MP3, and that's just in the music sector. Technology is constantly shifting.

I was reading recently about AI agents who can be created and who have a mind of their own. They can be programmed to do things themselves. Was there any discussion around how a specific AI agent can be programmed to do stuff on their own, which relates to online harm?

Dr. Heidi Tworek: We didn't specifically discuss generative AI that much within our group, but I think that within Bill C-63 there's certainly at least an attention to the question of deepfakes. I think there's a concept of a duty to act responsibly that's certainly capacious enough to be able to deal with these kinds of updates. If we're thinking about generative AI companies, they too will have a duty to act responsibly and then I think the question becomes, what exactly should that duty to act responsibly look like in the case of generative AI? A lot of the things we've been talking about today would obviously be a very central part of that.

Mr. Michael Coteau: Thank you very much.

I have another question. This is for Monique St. Germain.

Thank you again for being here. Thank you for the work you're doing around the protection of children.

What happens when the AI technology is so good that it can create, without using a deepfake, images and videos of illegal sexual exploits and acts that may look real but are actually fake? There is no technical living victim, but it obviously has a harsh impact on a sector and on society as a whole. Is it becoming more of a problem, where you have a person who doesn't exist but the exploitation of that image is being used more and more? Can you talk about that?

Ms. Monique St. Germain: Yes, absolutely.

We've been talking a lot about adults and this is also happening in the space of child sexual abuse material. There is a lot of harm that is done in terms of the systems that detect this type of material, which rely on hash values of real material. The fake material doesn't have those hash values in the databases that are being relied on, so removal of them becomes an incredible challenge.

There are all sorts of new CSAM out there. There's already a lot of CSAM out there, so we're now talking about making it even more—

• (1630)

Mr. Michael Coteau: What do you call it...CSAM?

Ms. Monique St. Germain: It's child sexual abuse material. The Criminal Code still calls it child pornography, unfortunately.

Mr. Michael Coteau: That's interesting. That's a big definition change that's necessary.

Thank you so much for your time. I appreciate your being here.

Ms. Monique St. Germain: Thank you.

The Chair: Thank you, Michael.

I will now go to the Bloc Québécois with Martin Champoux.

Martin, you have six minutes.

[*Translation*]

Mr. Martin Champoux (Drummond, BQ): Thank you, Madam Chair.

Thank you to the witnesses for being here today.

We're dealing with a very sensitive topic that I think we all care about on this committee. Although we sometimes have different opinions on how to approach this issue, I think that all committee members, all parties represented here, share a single objective, which is to make web browsing safer. We all want to make sure that our children, our daughters, our women, our sisters can feel safe and that they can be spared from this kind of reprehensible behaviour.

Ms. Moreau, Ms. Rourke, you mentioned in your article, as well as in your opening remarks, that deepfakes don't just affect celebrities. However, that's really our perception, that it's generally used to provide us with images of Taylor Swift, say, in pornographic poses—as a witness told us a little earlier. However, anyone can be a victim of this, not just politicians in election campaigns, but also ordinary people.

Are there many examples of this?

Have you noted many cases where ordinary people who are not famous are victims of sexual deepfakes?

Ms. Shona Moreau: We talked a little bit about that in our article. There really are cases where people—as you say, ordinary people—have been victims since 2017. So this is not a new phenomenon.

There are also a lot of articles in the newspapers that show this is growing in schools. We read a report in December that at a school in Winnipeg, some 40 young girls had been victimized using these technologies. That's significant.

If there's one story like that, I'm sure there are more, everywhere. It is really becoming more popular as the technology gets more accessible.

Mr. Martin Champoux: This type of content is easy to produce. There are even applications for that. It's quite appalling.

People are talking a great deal about Bill C-63, which seeks to regulate hateful and inappropriate content online.

Beyond legislation, do you feel that the platforms could do more about this?

Do you think they are now able to do more technologically, contrary to what they claim?

[*English*]

Ms. Chloe Rourke: It's possible. Certainly, once the technology became open source, it's been impossible to completely remove the

technology and the capacity to create deepfakes from the Internet, that's for sure.

It could be less accessible. I think decreasing the accessibility would decrease the frequency of these types of attacks. Just as an example, while we were doing research for this article, if you type “deep nude” into Google, the first results will get 10 different websites you can access, and it can be done in minutes.

It's possible to make it less visible and less accessible than it is now. It's pretty unnerving just how easy and how accessible it is. I think that's why we're seeing teenagers use it, and that's why a criminal remedy or civil remedies would be inadequate, considering how accessible it is.

[*Translation*]

Mr. Martin Champoux: As you said, you type keywords into Google, and you end up with a bunch of content. Everyone knows this, but some claim that we can't force these large companies to control this content at the source. I can't believe that they are not able to put in place a mechanism to raise a red flag when this inappropriate content is requested.

If we made the platforms more accountable and required them to better control the inappropriate content that may be on them, do you think that would improve the situation?

It's all well and good to legislate, regulate and crack down on abuse, but if the technology exists, the least these companies that provide the content to whoever requests it should be held accountable for what they give us.

Isn't that right?

• (1635)

Ms. Shona Moreau: I can't speak for the platforms, and I'm not here to represent them. However, I think it would be beneficial for everyone to ensure that these types of technologies are not readily available.

To preserve their reputation, I think these platforms would want to work on that. We're already seeing them take steps to remove this type of content when they see that there's an issue.

Mr. Martin Champoux: We talk a lot about what we can do and the expectations you have of us as politicians and lawmakers. However, as a parent, what do I tell my daughters?

Ms. Shona Moreau: Tell them that over the next year, you're going to work to make sure that this will no longer be a problem and that they will not be victimized using these technologies.

Mr. Martin Champoux: What steps can they take to guard against that threat? Is there anything they can do? Of course, they share their photos with their friends. Photographs, information and data are all over the place.

Ms. Shona Moreau: That's why I'm so afraid of these technologies. You can no longer take photos of yourself to give to your boyfriend or a friend, for example. It's online and you're completely vulnerable, because you don't have the power to take it down.

We need to show leadership on this problem, and it's not just a matter of legislating. We need people to find solutions to quickly remove this type of content from the web.

Mr. Martin Champoux: Thank you very much.

[*English*]

The Chair: Thank you, Ms. Moreau.

I will now go to the New Democrats and Niki Ashton for six minutes.

Ms. Niki Ashton (Churchill—Keewatinook Aski, NDP): Thank you very much.

I just saw, Ms. Rourke, that you had your hand up. Do you want to add something? I have some questions, but you can add what you were going to say.

Ms. Chloe Rourke: That's very kind. I just going to add that you have to see that this technology exists within a societal context of gender-based violence and oppression.

Education and combatting that societal, cultural context is part of the solution. It's not going to fix the technology, but educating in schools to understand the harms so that teenage boys who have access to technology know why it's so harmful is part of the solution. No one single thing will fix it.

Ms. Niki Ashton: Thank you.

Speaking of education, I actually wanted to direct my first question to Ms. St. Germain. In part, it's because of the extent to which it's clear we are failing Canadian kids. Looking at the statistics, that's very clear.

We heard of the 15,630 incidents of online sexual offences against children and 45,816 incidents of online child pornography reported by police in Canada from 2014 to 2022. We know that the rate of police-reported online child pornography has almost quadrupled since 2014. You spoke of some of these trends.

Specific to the non-consensual distribution of intimate images, we also see a heartbreaking image emerge. Most people accused of this offence are of a similar age to their victim, and we know they were previously known to the victim. In these situations, it's clear it's kids victimizing kids without necessarily understanding all of the ramifications, both for the victim's future and their own, the perpetrator.

I want to get back to the topic of education that you talked about. How important is education around consent and sexual safety? When it comes to young people, what more can we be doing to teach them how to keep themselves and each other safe?

Ms. Monique St. Germain: Education is always a critical component of any policy or initiative that we have. We have lots of different tools in the tool box. We have our criminal law. We have potentially Bill C-63 coming forward to provide some regulatory... On the education side, obviously it's ensuring that young people are

educated about sexual consent and understand the ramifications of sharing intimate images or creating this type of material, etc.

We can't lose sight of the fact that the reason they can do these things is because of the platforms that facilitate this kind of harm. We should have education for parents and for kids, taught through schools and available in a lot of different mediums and the places that kids go. While we can have education, we also need to make sure that we don't lose sight of the fact that there are other actors in the ecosystem who are contributing to the harm that we're all seeing.

• (1640)

Ms. Niki Ashton: I believe you did refer to Project Arachnid in your presentation. I'd like to get back to that.

Can you describe the process and work it took to develop this, which I know you referred to? What other tools are you missing that we should be encouraging government to help you with?

Ms. Monique St. Germain: Our organization, as I have mentioned, has been operating cybertip.ca for a long time. We are very steeped in technology. Our technological team is very sophisticated in terms of ensuring that the work that we do is done in the most efficient way and that we're not overexposing our staff to things that they don't need to be exposed to.

We leverage technology in a lot of different ways through Project Arachnid. It took a lot of time to develop that system. It's been tweaked over the last several years. It's gotten better and better at doing what it's doing.

What we have now is a very robust source of data that can be relied upon not just by companies but also by governments and other actors. There's a lot of known material out there that human beings have already laid eyes on. It's already classified, and that material can come off of the Internet. However, we need to start using those tools in ways that make sense, instead of overexposing victims to having their imagery repeatedly looked at by different moderators in different countries that have fewer robust safeguards than we have in institutions like our own and in policing, which does this work on a daily basis.

Ms. Niki Ashton: I want to get to the big question around stigma that victims face in terms of coming forward. We know that the most recent data provided by Statistics Canada says that in 2022 there were over 2,500 police reports of non-consensual distribution of intimate images. We know, of course, when it comes to sexual assault, that there's a real issue of under-reporting, given victims' lack of trust in the justice system and the policing system, fearing the stigma that they will face.

I'm wondering how we fix this question of stigma in terms of the work that you're involved in and what you're seeing with young people.

The Chair: You have 45 seconds to do that.

Ms. Monique St. Germain: I'm sorry...?

The Chair: You have 45 seconds to do that.

Ms. Monique St. Germain: I've lost track of the question. I'm sorry.

Ms. Niki Ashton: No problem. It's on stigma and dealing with the stigma.

Ms. Monique St. Germain: Yes, victims are facing a real stigma. These are the victims of non-consensual distribution of intimate imagery and victims of CSAM.

The types of things that these victims will include in their victim impact statements, for example, are very similar. There is a fear of recognition. There is an unwillingness to participate publicly in different ways because they don't want to be identified or linked to sexually abusive material.

We do have a lot of stigma that is going on online. Part of it is that we are allowing all of this material to be up in public view and not doing a lot to get rid of it. We have the big companies doing the things that they do, but even they can't keep in front of it. Then we have all of the smaller websites that we were referring to earlier in this discussion.

There are a lot of issues going on.

The Chair: Thank you very much, Ms. St. Germain.

I will now go to the second round. It's a five-minute round for the Conservatives.

Kevin Waugh, you have five minutes, please.

Mr. Kevin Waugh (Saskatoon—Grasswood, CPC): Thank you, Madam Chair.

Welcome to everybody here this afternoon.

Mr. Szemok-Uto, you're recently a lawyer. Thank you for that.

As you know, Bill C-63 did not expand to include the Criminal Code. It's not been updated to include deepfakes. That seems to be a concern not only around this table, but everywhere.

I don't know why, when you introduce a bill, you would not... We've seen that since 2017 deepfakes are accelerating around the world, yet it's not in this bill. What good is the bill when you don't talk about deepfakes?

What are your thoughts?

Mr. Keita Szemok-Uto: I would echo your concerns.

I presume there's an issue with the international element that the Internet and deepfakes present. You could have a perpetrator who is in Russia or some small town in a country we don't have much familiarity with. It would be hard to potentially go after those perpetrators.

I did note in my paper that there is inherently a limitation in pursuing criminal prohibition of deepfakes. Again, the standard of beyond reasonable doubt perhaps would play into limiting who is convicted of these crimes, as well as the scope and the resources that would be required to actually provide and enforce criminal prohibitions of this kind of behaviour.

I think that with private law, civil remedies and things that are based on the balance of probabilities, potentially there is a wider scope for not criminal justice but justice of some kind and at least some kind of disincentivization for engaging in this kind of behaviour. That would be my answer.

• (1645)

Mr. Kevin Waugh: The problem with having an extrajudicial bureaucratic arm, which I think Bill C-63 is, is that it can actually perpetuate harm.

We can see that because victims—some have mentioned it here today—have to come bravely forward and share their stories with a commissioner or a body that they really don't know. That has actually led to no real power. I think the victim in this case is led to hope and then hope is deferred because there are no real teeth in the legislation.

What are your thoughts on that?

I do think Bill C-63 is a bureaucratic nightmare ready to explode if it does get through the House.

Mr. Keita Szemok-Uto: I would agree that potentially more could be done than what Bill C-63 presents.

I do note, at least, that there is the inclusion of the word “deepfake” in the legislation. If anything, I think it's a good step forward in trying to tackle and get up to date with the definitions that are being used.

I note that legislation that was recently passed in Pennsylvania is criminal legislation that prohibits the dissemination of an artificially generated sexual depictions of individuals. I won't read the definition out in full. It's quite broad.

Bill C-63 does refer to deepfakes, at least, though no definition is provided. I think in that respect, broadening the terminology... As I said, the privacy law torts are restricted by their definitions and terminology to not include this new problem that we're trying to deal with. To the extent that it gets the definitions more up to date, I think it is a step in the right direction.

Mr. Kevin Waugh: Ms. Moreau or Ms. Rourke, the biggest entertainer in the world, of course, is Taylor Swift. She got deepfaked twice this year. One was sexually explicit, and the other was the debacle that happened at the Grammys, where it wasn't her voice. It wasn't her.

How do you address this? There's no bigger entertainer in the world than Taylor Swift, yet this blew over with little or no news from it, actually. It died fairly quickly.

Go ahead, Ms. Rourke.

Ms. Chloe Rourke: I think the deepfakes of Taylor Swift are what prompted a lot of these conversations in recent months. I think it has actually brought this conversation more into the light.

I would also add, though, that Taylor Swift has many more resources than the average individual to combat this and to respond to issues, but it does show the difficulty of banning the technology and preventing its reusage and the reharmed of future individuals.

Mr. Kevin Waugh: Thank you.

The Chair: I now go to the Liberals' Taleeb Noormohamed, for five minutes, please.

Mr. Taleeb Noormohamed (Vancouver Granville, Lib.): Thank you so much to the witnesses for being here.

I'm going to split my time with my colleague, Ms. Lattanzio.

One of the things that we have sought to do in addressing some of the concerns related to online harms, and in particular some of the issues that have been raised during the course of the study, are making sure that our legislation, Bill C-63, the online harms bill, takes on some of these challenges head-on and works.... As we have said, we are willing to work with all parties to ensure that it's the best possible bill out there.

I don't know if you had a chance to follow the deliberations of our meeting on Tuesday, but our colleague, Mrs. Thomas, raised what I would argue is a very important concern in a number of her questions. It would appear, at least from my read of it, that she was advocating—I don't want to put words in her mouth, but this is the way that I understood what she was suggesting—that we take a risk-based approach in the legislating of regulations around social media platforms. Our belief is that this is exactly what Bill C-63 proposes to do.

Do you agree, first of all, with Bill C-63 and what we're trying to do, and that the right approach to legislating regulations around social media platforms is really to take a risk-based approach, as suggested by Mrs. Thomas and others?

I would refer that question to you, Professor.

• (1650)

Dr. Signa Daum Shanks: Thank you very much.

I want to be blunt. I don't have a horse in this race. I want to also say, in my attempt to make my words brief, I was also a member of the advisory panel. I also want to say that we didn't agree about everything. We were very congenial and, I think, very thankful for everyone's contributions, but we had mixed views on things.

I guess I do lean towards that idea of risk management. I guess where I would also like to put a little bit of faith in is that I'm more optimistic about that because, in this idea of concepts and wondering whether.... I think we've heard the term “teeth” being used. What's handy about not having specifics is that those concepts can be what they need to be at the time that some topic is brought up.

There's another idea in law that happens sometimes when things are too specific and we don't have a “moving forward” approach that might allow some moments where we try to improve things. There's a concept called “freezing rights”. Perhaps the most notable place we might have thought of that has been in the interpretation of fiduciary obligations, mainly to indigenous peoples.

What ends up happening is that case law has to come back to the courtroom to then redefine something, and then that case is com-

pared to previous cases that have a very specific definition. Then the legislation has to come back. It has to be redefined. If there are regulations, then the regulations have to be evaluated, so you end up coming to the place we are here, and that's what I'm very afraid of happening.

The way I see it, law is a work-in-progress. There's a very cliché, if not cliche idea that law is like a living tree. That idea is to have faith in people like you to evaluate things and, when it's important to contribute to the regulations, we can dive deeper to decrease potential risks we suddenly see. What actually can be very intimidating to other parties is that there isn't a specific, so they might be very nervous that what is potentially going to be done by them just might qualify even if it's not mentioned. Therefore, I'm very supportive of it.

Mr. Taleeb Noormohamed: Thank you.

With the minute that I have left, I'm going to give it to my colleague, Ms. Lattanzio.

Ms. Patricia Lattanzio (Saint-Léonard—Saint-Michel, Lib.): Thank you, Professor Daum Shanks.

In your presentation, you mentioned making the two observations. You just discussed the first one. I'm going to go with the responsibility.

How is Bill C-63 addressing the notion of responsibility?

Dr. Signa Daum Shanks: I'm going to tweak again. I see it as “responsibly” as compared to “responsibility”, because in law and legislation there can be that word as well. I see it as a way to prevent some problems that especially come up in civil actions. I see it as a very comparative idea to, for example, duty of care in negligence. I also see it as very similar to something that used to be called “nervous shock” but is now the idea of “mental distress”.

What I really like about it is that—and perhaps this is already connected to what I said before—it is going to help speed up some really important evaluations that I think could get really slowed down by thinking of things, for example, in a civil way.

Thank you.

• (1655)

The Chair: Thank you very much. We've gone well over time here.

I'm going to go now to Mr. Martin Champoux for two and a half minutes, please.

[*Translation*]

Mr. Martin Champoux: Thank you, Madam Chair.

Professor Shanks, I'm sorry, but I don't have much time. I'll try to keep my questions fairly brief.

You were part of the expert advisory group on online safety. The group was appointed by the government to advise the government.

Did the members of the group use foreign legislation as a basis for making recommendations to the government?

Is there anything being done elsewhere in the world from which we can draw inspiration to combat this content online?

[English]

Dr. Signa Daum Shanks: We very regularly were able to talk about the United Kingdom, the EU and Australia. I was not at all a person who could contribute in those specific moments, but I would say, particularly with the U.K., I found myself thinking that how we were being influenced by what we could have done was based on, perhaps, the imperfections, if not shifts of things, that we could learn from what was happening in the United Kingdom.

Sometimes the benefit of being a little bit slower—or, unfortunately, a lot slower—is that you can notice what's going on somewhere else, and you can do or not do what they've done or not done. What has also been handy, especially about those comparisons, is learning about stages that are very similar to what we've done here and thinking of that idea of input and how things could change over time with people learning more terms, like deepfake. How do you increase the knowledge of that?

[Translation]

Mr. Martin Champoux: Ms. Moreau, do you believe that until a very large majority of civilized nations around the world, including the ones we're talking about today, have come together to legislate on this, we will always be exposed to the dissemination of this type of content?

Ms. Shona Moreau: Yes, I do.

In addition, it's not that everyone needs legislation to counter this problem, but rather that the places where these companies are based need legislation to stop this.

Mr. Martin Champoux: Thank you, Ms. Moreau.

Madam Chair, I will answer that in a few seconds.

As I understand it, a simple amendment—

[English]

The Chair: Thank you, Martin. You have zero seconds left.

[Translation]

Mr. Martin Champoux: You're absolutely right, Madam Chair. However, given the time we have to allow for interpretation, we sometimes have a bit of leeway in terms of speaking time.

I'll just conclude by saying that, generally speaking, from what I'm hearing from the witnesses, if we were to add to the Criminal Code the definition of deepfake in relation to images, I think it would be an important step forward in this legislation. I just wanted to add that comment in closing.

[English]

The Chair: Thank you, Martin.

Ms. Ashton is next for two and a half minutes.

Please go ahead, Niki.

Ms. Niki Ashton: Thank you.

My questions are for Ms. Moreau and Ms. Rourke.

We know that digital platforms are not being held accountable for the harmful and illegal content they are hosting, and we in the NDP have been repeatedly calling for accountability. In your writing, which you referred to today, you've highlighted how somebody like Taylor Swift had a fan base that forced Twitter to eventually take down deepfakes of her, but we know that regular women simply don't have that option.

In your view, would something like a digital safety commissioner who could force the removal of these types of images be helpful?

Ms. Chloe Rourke: I think the role of a public regulatory body is necessary. To leave it up to individuals to police their own content or to constantly be on the search for, or vigilant about, their own likeness being used on the web is an unrealistic expectation. For individuals to have to maintain their own protection in that way, I think it underestimates the level of accessibility and widespread use of the technology and how difficult this is.

I know it's also happened to voice actors for video games. They have had their likeness used and manipulated. For people with these fan bases, like you said, if they're not Taylor Swift.... Individuals with a smaller following can be recognized, and it's difficult for them to locate all of the content and constantly notify different hosting platforms to have it removed.

I don't think this idea of self-policing is a practical solution.

● (1700)

Ms. Niki Ashton: This came up on Tuesday as well. We know the devastating impact that all of this, particularly the non-consensual distribution of intimate images, has on mental health, including long-lasting impacts. One of the witnesses on Tuesday, Ms. Lalonde, talked about how frontline groups specializing in helping people cope with the fallout of these situations don't have the support they need.

Do you agree with this statement? Do you think the federal government should be funding mental health supports with a particular focus on working with victims and survivors in this area?

Ms. Shona Moreau: I'm not looking to be extremely prescriptive, but I think that, yes, 100%, it would be beneficial for the victims to have that support, wherever it comes from. I think the House of Commons has the leadership to do something around that—coordinating, funding or finding ways to make it more accessible to the public.

The Chair: Thank you very much, Ms. Ashton.

I'll now go to Mr. Gourde for the Conservatives for five minutes.

Mr. Lawrence and Mr. Gourde, Mr. Gourde is up now for five minutes.

Thank you.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Madam Chair.

I'd like to thank all the witnesses who are with us today.

My question is for two of the representatives of the Faculty of Law at McGill University, Ms. Moreau and Ms. Rourke.

Earlier, you talked about awareness and prevention. It might be important to undertake that process.

Should awareness be raised in schools, or should the problem be publicized more broadly, on television or on social networks, for example, since people are always on those networks?

However, we would have to put that material in place.

Would that be an option?

Ms. Shona Moreau: That would certainly be an option.

In fact, I believe that all the options you've given are good.

Schools have a role to play, since it's the physical location where there's a lot of social interaction. They know the students and the youth who socialize.

In my opinion, platforms also have a role to play in educating the people who use them to distribute or even create material. I think a lot of platforms allow for the creation of material, such as the Deep Nude app, and things like that. The platforms say that you have to make sure you get the consent of the people concerned when you are creating all this content. However, they know very well that no one is doing it.

I think people need to know what's going on. Users need more protection from these platforms, particularly if they're creating content for the public and they want to try to make money from it.

Mr. Jacques Gourde: I'm a grandfather and I have seven grandchildren. I get the chills when I realize that we can't control artificial intelligence and that producers are using artificial intelligence applications to create content that can truly destroy the lives of the most precious thing we have. I'm talking about our youth, who represent our future.

Can we create tools using the same weapon, artificial intelligence, to tackle this problem? People can't keep watch 24 hours a day. We'll have to find a solution.

It might be a good idea to pass legislation to punish people who promote all this.

That said, when a person realizes that their children or grandchildren are on one of these sites, it takes so long to have the content removed that it might remain accessible for quite some time.

Can we come up with tools to wipe it off the face of the earth?

[*English*]

Ms. Chloe Rourke: We're not AI programmers, but I think it's definitely possible to have that, and I think that's one of the reasons that public regulatory bodies ought to work with platforms. They would understand how these systems work and how they could be used to help regulate content. Platforms already do content moderation, any of the major tech platforms like YouTube, Google, Facebook, etc.

It's a new wave of content that they'll have to account for in their current systems.

• (1705)

[*Translation*]

Mr. Jacques Gourde: If you had a magic wand to help us with this study so we could really change things, what would you tell us to do?

[*English*]

Ms. Chloe Rourke: I keep going back to this, but I really do think that there needs to be a relationship built with platforms and an accountability for the platforms.

What's so shocking to me is really just how accessible this technology is. As long as it remains that accessible, it's inevitable that there will be more people harmed.

One thing that I really felt frustrated about when I was looking at it was the way in which the technology is presented. It's in a very neutral and a gender-neutral way, almost as if it's not deliberately intended to do harm and to create non-consensual pornography. Here's one example of the way these platforms describe themselves: "sophisticated AI algorithms to transform images of clothed individuals". They have a disclaimer that the AI should comply with the law and be consensual, when clearly that's not how they're designed to work, and there are no control mechanisms on there to ensure that any of the images being used are being used in a consensual manner.

I think that, as long as it is that accessible and not challenged, we're going to continue to see these harms. I would start there.

The Chair: Thank you very much, Mr. Gourde.

I now go to Rachel Bendayan for the Liberals for five minutes.

[*Translation*]

Ms. Rachel Bendayan (Outremont, Lib.): Thank you very much, Madam Chair, and thank you to my colleagues for having me. I don't usually sit on this committee, but I'm pleased to be with you today.

I'd like to begin by saying that I quite agree with the spirit of the amendment moved by Mr. Champoux. I hope the committee will look at that.

Ms. Moreau, I believe you said that trials are long and costly. I used to be a litigator, and I quite agree with you on that.

That said, I just want to make sure I understand your comments.

You say that the time it takes to get a judgment is a little too long.

Is that correct?

Ms. Shona Moreau: That's correct.

First, I'd like to make a small clarification. I don't have the title "master" yet. I have six months to go before I can get it.

With respect to your question, I think that's correct, yes. It's not really realistic to think that every single person who has a deepfake photo circulating somewhere on the Internet is going to go through the whole process of challenging it in court. So much content causes problems and that really has an impact on people, so we need to find solutions that are a little more practical.

Ms. Rachel Bendayan: To follow up on Mr. Gourde's comments, I'd like to ask you the following question.

I know you're not a technician, but wouldn't it be interesting, if not preferable, if platforms could quickly recognize deepfakes, even after they've been posted online?

I don't know if that technology exists yet. If not, I hope it will be developed soon.

Ms. Shona Moreau: If that's possible, then platforms should do it. Platforms are already testing AI systems to perform content moderation. I think they are already looking at nudity.

Ms. Rachel Bendayan: Thank you.

[*English*]

Professor Daum Shanks, allow me—taking off my lawyer hat and maybe putting on my mother hat—to ask you how the online harms legislation that we put forward will empower users to flag harmful content.

I am worried that we are literally asking parents to police the Internet, and I would like to hear from you on the tools in the legislation that might help in that regard.

Dr. Signa Daum Shanks: I think that's a great question. I'm going to keep the lawyer's hat on, though, in answering it.

Ms. Rachel Bendayan: Yes, please.

Dr. Signa Daum Shanks: One of the things I would like to be put forward in whatever happens...and that's the way I'm going to put it: "whatever happens".

I might say this too because of your professional work cap, but I really appreciate the idea of having some functions that are very similar to what have been trends in administrative law. The thing I'm the most concerned with is that people feel like they can be themselves—people who have less access to legal counsel and people who are working with whatever commissioner ombuds office is functioning—and that they can also have the space that administrative law has often had to think of some spontaneous adjustments to procedure, which means everything from having translators who

only speak English and French, for example, to having things like literally a comfortable chair.

I think Cindy Blackstock has brought up many topics in what she has done on thinking of the long list of little things that can make people feel more safe. That's probably my biggest bailiwick—to think of however there is a moment when we think someone can call an official space, whether it's a toll-free number or filing a written report or something, that they feel like the support system is right there.

I think in criminal law functions, as someone who's worked a lot for the Crown in the past and then connected with law firms, that first stage of getting things going is incredibly intimidating to people not trained in law. I want to find as many ways to avoid that as possible, and I think we have every obligation to provide that. I did mention earlier that idea of fiduciary obligations, which I think is one of the best ways to help us imagine those ways, because—

• (1710)

The Chair: Thank you, Professor Daum Shanks. I think we're well over that time.

Dr. Signa Daum Shanks: Okay.

The Chair: Thank you very much.

I'm going to go now to the next round, but I don't think we can finish a full round, guys. I'm going to do two five-minute rounds, and then the Bloc and the NDP get two and a half minutes each. We have 15 minutes left, and this will bring us to exactly 5:30. Thank you.

I start with Philip Lawrence for the Conservatives.

You have five minutes, Philip.

Mr. Philip Lawrence (Northumberland—Peterborough South, CPC): Thank you, Madam Chair.

I want to go to you first, Ms. St. Germain. I just wanted to, first of all, confirm that I heard what I thought I heard in earlier testimony. You said your organization currently has flagged, I don't think you said "the quantum" but, I would assume, a large amount of material that you've already classified as non-consensual or otherwise inappropriate. Did I get that correctly?

Is she still there? No, she's gone. Okay, I apologize.

I'll go with that line of questioning to you, Ms. Rourke, and you, Ms. Moreau.

My challenge with the legislation is that, while directionally I agree with it, I don't think it's going to help enough people quickly enough. We already have the Internet awash with non-consensual pornography and child pornography. With this legislation, someone has to complain about it, they have to go to a commissioner and it has to get removed.

I see opportunities to improve this legislation by including automatic removal of deepfakes or non-consensual pornography that's already been flagged and tagged. Do you think there's an opportunity there or no?

Ms. Shona Moreau: I think I wouldn't be prescriptive on an amendment for this specific bill, but I do think there should be work done around that. If it's a future bill, a report or even just working with regulators in order to be able to do something like that, I think that would be really great. Yes.

Thank you.

Mr. Philip Lawrence: Continuing along that line, there are a number of different levels that we could put enforcement on. One is the creator of illegal pornography or illegal deepfakes. There are also the platforms, and then there are also the devices, the computers, the laptops and the phones.

The bill doesn't capture a lot of that. I don't think, just because we can't necessarily enforce all the mice, we should then not enforce the elephants. I believe that we should consider going after the platforms directly.

Would you agree with that?

• (1715)

Ms. Shona Moreau: There's an expression in French that says, *le mieux est l'ennemi du bien*.

I think that having work done on this issue currently is great. Technology is not going away. AI is not going away, and more work is going to be coming down the pipeline. Hopefully, you as legislators will be able to do that work quickly enough to catch up.

I think it also makes us understand that, when we're making legislation now, we have to be looking five to 10 years or even sometimes 25 years out. We can't just be legislating and working on current issues. We almost have to be working on future issues.

Mr. Philip Lawrence: I completely agree.

What I haven't heard much testimony on—and I would be curious if any of the witnesses have something to say—is the device level, because the manufacturer, almost by definition, has to be an elephant. There are a limited number of companies that manufacture smart phones and manufacture computers.

Is that something that anyone's come across in their research as a possible way of reducing online harms?

Ms. Chloe Rourke: The difference between manufacturing a computer or a phone versus AI technology is that, even if the initial software is developed by a larger company, it's now being made open source. Once it's open source, that code can be modified or appropriated, and there's really no way to take it back out of the public domain once it exists there.

It's a difficult question whenever you're talking about innovation in the context of innovating technologies, and there are multiple different applications. What are the ethics of that and how do you balance that with what is essentially a huge economic incentive to invest in AI technology and its development and to have the ability to experiment with that technology and see where it grows, but still

acknowledge that a technology like this has a lot of harmful applications?

As far as we can see, it's a fairly limited commercial application like in film, media and these kinds of areas, but it can clearly be manipulated, not just for sexually explicit material but for many other purposes as well.

Mr. Philip Lawrence: I believe that's my time.

I'm just going to thank you for all your great work. I appreciate it.

The Chair: Thank you. That's it.

I now go to Ms. Lattanzio for the Liberals.

Patricia, you have five minutes.

Ms. Patricia Lattanzio: Thank you, Madam Chair.

My question will be for Professor Daum Shanks.

Professor, are you familiar with the proposed changes in Bill C-63 with regard to the mandatory reporting act?

Dr. Signa Daum Shanks: I have it open here right now.

Are there some specific sections you'd like me to go to?

Ms. Patricia Lattanzio: I want to know if you can outline to the committee what you understand those changes to be.

I don't want to put you on the spot.

Dr. Signa Daum Shanks: I must confess that, just because of the short amount of time I had to get prepared for this, I don't want to say I'll pass on that, but if I don't have enough time right now, I'd love to pass on that.

Ms. Patricia Lattanzio: Okay.

Let me go back with regard to the consultation process with which you were involved in 2020.

Can you tell me a bit more about the consultations that were held and what, in your opinion, the advancements were that you would think have been made ever since then?

Dr. Signa Daum Shanks: That's a great question.

At least what I found was really good about the process was the sense that everyone had a different type of expertise and everyone could be on the same page of all wanting something to happen. I found that keeping to our confidentiality and keeping to our goals meant that the impact on me, at least, was that there's not just going to be this bill that takes care of this issue. In the brainstorming that we did together and in the brainstorming that's been done for whatever bill somebody's interested in here, that's not going to be the end of it.

One of the most important takeaways we need is to plant that seed with everyone: There will be other pieces of legislation that can be tweaked to match the purposes of what we're talking about right now. For example, I was inspired to think that, in particular, consumer protection law has been one of the greatest ways to have ideas of harm in one area be then even more refined in another piece of legislation.

In the spirit of realizing that something may not be in the perfect form that anybody and everybody wants in that group, the idea of slowing down is unthinkable. From my experience, it's given me at least way more recharge and hopeful creativity to see other pieces of legislation where this topic, which the purpose of this bill is to address, can be subsequently brought up. I'll give you one example: online harm that happens to children in some very distressful situations. Whether it's separating parents or brothers and sisters who are especially mean, there are things that can be done in family law in the future.

That idea of it is so cliché—that this is just the beginning—but one of the hopes I have is that everyone realizes that this is just the beginning, and this bill is not the end of it.

• (1720)

Ms. Patricia Lattanzio: In your introduction, Professor Daum Shanks, you spoke about the difficulty for victims to get specific harms recognized as such, as they're not covered by the existing jurisprudence. I'm curious to know how the digital safety commission and the digital safety ombudsperson proposed in Bill C-63 would help us better support victims and make sure they have their voices heard.

Dr. Signa Daum Shanks: One of the most familiar ways to think of that is as a place that I see as very similar to the idea of duty of care: having a place where individuals have a way to talk about what their harm is in a way that perhaps has never been heard before. In how duty of care has been thought of in the past, in some of its other imaginings, it is that we have to be prepared to learn about a new type of relationship. That might be students in the same classroom. It might be a supervisor at a job or it might be a former partner or girlfriend or boyfriend. We have to be prepared—

The Chair: We need to wrap up, please. We have to finish this. I still have Mr. Champoux and Ms. Ashton.

Thank you very much.

[*Translation*]

Mr. Martin Champoux: Thank you, Madam Chair.

What I understand, what we all understand, is that one organization or level of government won't find solutions to this problem. This is a whole-of-society issue, and everybody has to contribute. Obviously, the legislative branch has to do its duty, as do the technology platforms, in my opinion. However, as individuals and as a society, we must also do our part.

I realize that, despite the threat you're describing today, not a lot of awareness is being raised about this in primary and secondary schools or CEGEPs. People don't know much about deepfakes, and that concerns me. I wasn't born at a time when it was common to have cellphones with Internet access. I don't want to assume your

age, Ms. Moreau, but I get the impression that you probably grew up with this technology, unlike me.

Do you think we would be able to educate the younger generations enough if we started very early to give them the tools to protect themselves against this kind of danger? I'm sure you believe that. Seven-year-olds are given cellphones with Internet access. There are children, very young children, who can access this content and, as a result, they are susceptible to being victimized by this.

In your opinion, why are young people not being aggressively educated in primary school about the risks they are taking when they share their content and simply browse the Internet? Why isn't that being done yet?

• (1725)

Ms. Shona Moreau: We really need to embark on a societal project about this issue. Perhaps we should intervene at schools in all the provinces. I don't know the answer to your question, but it's important to point out two things.

First, we have to look at how we teach children to use new technologies. They often adopt these new technologies even faster than we, the older generation, do.

Second, it's important to understand why deepfake pornography is so harmful and why it constitutes a significant infringement. That's why we're so focused on this issue. We need to educate young people so that they understand that what happens on the Internet really affects them in the physical world. They need to know that when they talk to a classmate, for example, that once that same person is at home, they can use their image and make deepfake pornography. I think it's sometimes a little hard to picture yourself on a screen after a deepfake.

Mr. Martin Champoux: Thank you very much.

[*English*]

The Chair: Thank you very much.

I'm going to Ms. Ashton.

Niki, you have two and a half minutes.

Ms. Niki Ashton: Thank you.

I want to go back to a point, Ms. Moreau, that you mentioned in French: a social project.

Obviously, the whole point of our being here and hearing from you is to put together recommendations for government. All of the witnesses have spoken specifically about this very troubling reality with respect to the misuse of AI, the use of deepfakes and the victimization of, particularly, women.

I'm wondering if you have any thoughts to share on how this ought to also reinforce education and, more importantly, action around equality and ending violence against women. It seems to me that we can't be talking about the use of deepfakes and victimizing women online if we're not talking about it off-line as well. I'm wondering if, in the spirit of making recommendations, you have any suggestions on that front.

Perhaps Professor Daum Shanks could briefly share some thoughts on that too.

Thank you.

Ms. Chloe Rourke: The first thing you have to ask is why a nude image of a woman is so damaging. Why is there a reputational harm from that being shared? What kind of cultural response do we have to women's sexuality so that it's specifically women who are targeted with this—so that 99% of pornographic deepfakes are of women? There is a huge gender skew to that. I think you have to look at that fact in context with our treatment of women more broadly.

Also, look at it specifically in the context of physical, as you said, real-world violence against women, which is often taking place in conjunction with online violence against women. Many of the revenge porn cases we've seen litigated and that have gone to court have been in the context of intimate partner violence. Revenge porn is often used to threaten partners: "If you leave, I will release this of you." I think those things aren't separable. I think you need to have education to combat both and see them as fundamentally linked.

Dr. Signa Daum Shanks: I was just going to quickly pipe up, to make sure I don't take up all the time.

The Chair: You have seven seconds.

Dr. Signa Daum Shanks: Ombuds offices can do lots.

Thank you.

The Chair: Very well done. Thank you.

I want to thank the witnesses for coming and presenting to us, and for all of your vast knowledge on the very complex issue and the questions.

I also want to thank Monsieur Barraud for sitting here so patiently during these meetings, ready to help us if we needed him. Thank you, Monsieur Barraud.

I also want to make one point as a chair.

I think you heard that we now have seven-year-olds exposed to this kind of information. I was talking to one of our witnesses last week, and she said that means we're going to have a whole lot of new young generations that are going to become involved in this at a very early age. We have to think about that down the road. It isn't just that they're going to be victims; they may be perpetrators. I think it's an interesting question to ask. We have these two meetings. Would that we could have had longer, because it's a very important and interesting subject.

Thank you again very much for coming.

I'm going to suspend so we can go in camera. Thank you.

[Proceedings continue in camera]

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <https://www.ourcommons.ca>

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante :
<https://www.noscommunes.ca>