HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

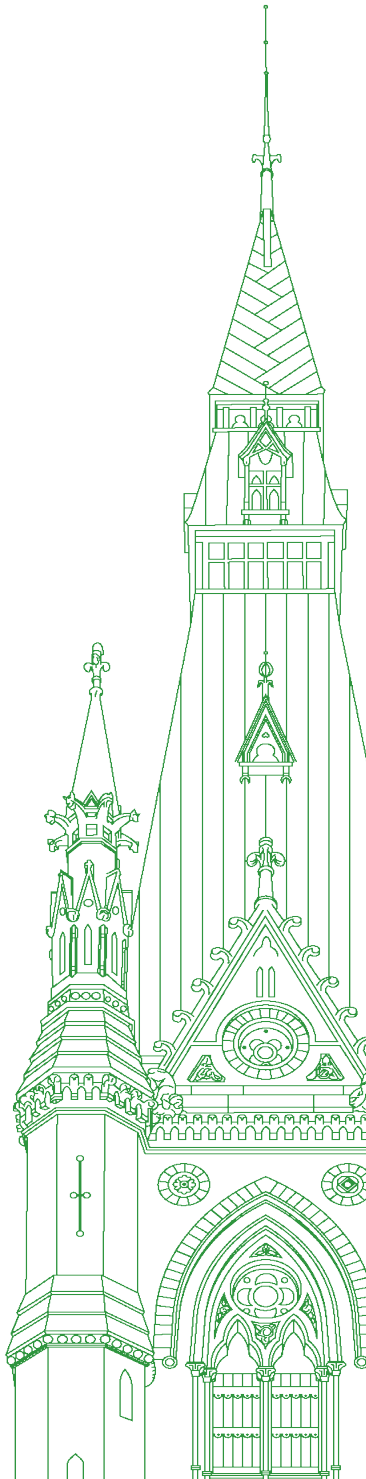
43rd PARLIAMENT, 2nd SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 038

Monday, June 7, 2021



Chair: Mr. Chris Warkentin

Standing Committee on Access to Information, Privacy and Ethics

Monday, June 7, 2021

● (1100)

[*English*]

The Chair (Mr. Chris Warkentin (Grande Prairie—Mackenzie, CPC)): Colleagues, I'm going to call this meeting to order.

This meeting is the 38th of the House of Commons Standing Committee on Access to Information, Privacy and Ethics. We are resuming our study today on the protection of privacy and reputation on platforms such as Pornhub. I would like to remind colleagues that today's meeting is televised and will be available on the House of Commons website.

I would like to welcome Minister Guilbeault, Minister of Canadian Heritage, for the first hour. Accompanying him from the Department of Canadian Heritage, we have Joëlle Montminy, senior assistant deputy minister, cultural affairs; and Pierre-Marc Perreault, acting director, digital citizen initiative.

Minister, I'm going to turn it over to you for your opening statement, after which we'll have some questions for you.

[*Translation*]

Hon. Steven Guilbeault (Minister of Canadian Heritage): Thank you, Mr. Chair.

Mr. Chair, members of the committee, good morning.

I would first like to acknowledge that I am joining you from Montreal, on the traditional territory of the Mohawk and other Haudenosaunee peoples.

Thank you for inviting me to speak to you today. With me, as you said, are Joëlle Montminy, senior assistant deputy minister, cultural affairs, and Pierre-Marc Perreault, acting director, digital citizen initiative.

Like you and many other Canadians, I am concerned by the disturbing rise and spread of hateful, violent and exploitive content online and on social media.

[*English*]

As a legislator and father of four children, I find some of the content of these platforms to be profoundly inhuman.

[*Translation*]

I am also deeply troubled by the consequences and the echoes of that content in the real world.

The overall benefits of the digital economy and social media are without question. In fact, I published a book, shortly before I took up politics, wherein I talked about the benefits of the digital economy, of artificial intelligence in particular, but also about some unintended negative consequences.

In Canada, more than 9 out of 10 adults use at least one online platform, and since the beginning of the pandemic, online platforms have played an even more important role in our lives.

[*English*]

We use social media platforms like Facebook, Twitter, Instagram and YouTube to stay connected to our families, friends and colleagues. We use them to work, to conduct business, to reach new markets and audiences, to make our voices and opinions heard, and to engage in necessary and vital democratic debate. However, we have also seen how social media can have negative and very harmful impacts.

[*Translation*]

On a daily basis, there are Internet users who share damaging content, either to spread hate speech, the sexual exploitation of children, terrorist propaganda, or words meant to incite violence.

[*English*]

This content has led and contributed to violent outbursts such as the attack on the Islamic Cultural Centre in Quebec City in 2017, and similar attacks in Christchurch, New Zealand, in 2019.

Canadians and people all over the world have watched these events and others unfold on the news with shock and fear. We all understand the connections between these events and hateful, harmful online discourse. We worry about our own safety and security online. We worry about what our children and our loved ones will be exposed to.

According to a recent poll by the Canadian Race Relations Foundation, an overwhelming 93% of Canadians believe that online hate and racism are a problem, and at least 60% believe that the government has an obligation to prevent the spread of hateful and racist content online.

In addition, the poll revealed that racialized groups in Canada are more than three times more likely to experience racism online than non-racialized Canadians.

[*Translation*]

Since the beginning of the COVID-19 pandemic, we have seen a rise in anti-Asian hate speech on the Internet and a steady increase in anti-Semitic rhetoric, further fuelled by recent events.

A June 2020 study by the Institute for Strategic Dialogue found that Canadians use more than 6,600 online services, pages and accounts hosted on various social media platforms to convey ideologies tinged with white supremacism, misogyny or extremism. This type of content wreaks havoc and destroys lives. It is intimidating and undermines constructive exchange. In doing so, it prevents us from having a true democratic debate and undermines free speech.

The facts speak for themselves. We must act, and we must act now. We believe that every person has the right to express themselves and participate in Internet exchanges to the fullest extent possible, without fear and without intimidation or concern for their safety. We believe that the Internet should be an inclusive place where we can safely express ourselves.

Our government is therefore committed to taking concrete steps to address harmful content online, particularly if the content advocates child sexual exploitation, terrorism, violence, hate speech, and non-consensual sharing of intimate images.

In fact, this is one of the priorities outlined in the mandate letter given to me by Prime Minister Justin Trudeau. So we have begun the process to develop legislation that will address the concerns of Canadians.

● (1105)

[*English*]

Over the past few months my office and I have engaged with over 140 stakeholders from both civil society organizations and the digital technology sector regarding this issue. This has included seven round-table discussions. We also spoke with indigenous groups, racialized Canadians, elected provincial officials, municipal officials and our international partners to assess our options and begin to develop a proposed approach.

In addition, given the global nature of the problem, I have hosted a virtual meeting with my counterparts from Australia, Finland, France and Germany—who were part of the multi-stakeholder working group on diversity of content online—to discuss the importance of a healthy digital ecosystem and how to work collectively.

[*Translation*]

I am also working closely with my colleagues the ministers of Justice, Public Safety, Women and Gender Equality,Diversity and Inclusion and Youthas well asInnovation, Science and Industry to find the best possible solution.

[*English*]

Our collaborative work aims to ensure that Canada's approach is focused on protecting Canadians and continued respect for their rights, including freedom of opinion and expression under the Charter of Rights and Freedoms. The goal is to develop a proposal that establishes an appropriate balance between protecting speech and preventing harm.

Let me be clear. Our objective is not to reduce freedom of expression but to increase it for all users, and to ensure that no voices are being suppressed because of harmful content.

[*Translation*]

We want to build a society where radicalization, hatred, and violence have no place, where everyone is free to express themselves, where exchanges are not divisive, but an opportunity to connect, understand, and help each other. We are continuing our work and hope to act as quickly and effectively as possible. I sincerely hope that I can count on the committee's support and move forward to build a more transparent, accountable and equitable digital world.

I thank you for your attention and will be happy to answer any questions you may have.

[*English*]

The Chair: Thank you, Minister.

We'll turn to Ms. Stubbs for the first question.

Mrs. Shannon Stubbs (Lakeland, CPC): Thank you, Chair.

Minister, thanks for being here.

Just to start, do you think Bill C-10 is adequate to combat child sexual abuse material and rape and non-consensual material online?

Hon. Steven Guilbeault: I was invited to talk about our upcoming legislation regarding online harms, which I'm happy to do. If this committee would like to invite me to talk about Bill C-10, I would be happy to appear at another time to do that.

Mrs. Shannon Stubbs: I'll take that as a “no” for Bill C-10.

Witnesses said previously that Canada's Criminal Code “child pornography” definition is among the world's broadest. It bans images, audio and written forms. Platforms are already liable for circulating illegal user-generated content. There are circumstances in which a company becomes liable for something that somebody else said or did if the company knew about it in advance and published it anyway, or if the company was notified about it after the fact and failed to take action. These situations are very well documented with MindGeek and Pornhub. It seems the real and disturbing issue is a lack of application of the law and its enforcement.

In January, you said that within a few weeks you were going to create a regulator to stop child sexual abuse material and sharing of non-consensual images online. I'm just wondering why there hasn't been any serious progress on that. I have a couple of questions about that for you from survivors. What's the delay?

Hon. Steven Guilbeault: I respectfully disagree with the premise of the question. What we see here in Canada, and frankly, all around the world, is that the tools we have to deal with these harms in the physical world just aren't adapted to deal with them in the virtual world.

Let me give you an example. In 2019, the RCMP saw a 1,106% increase from 2014 of reports regarding child sexual exploitation online. This exploitation disproportionately impacts girls. In 2019, the RCMP found that girls made up 62% of identified Canadian victims depicted in online child sexual exploitation material.

I did say I was hoping to introduce this legislation in January. Unfortunately, the systemic obstruction by the Conservative Party regarding Bill C-10 has prevented me from doing so. However, I am still hoping to table this bill as soon as possible.

● (1110)

Mrs. Shannon Stubbs: Wow, what a ridiculous and partisan evasion on your part. What I would suggest is that if you hadn't spent months and months figuring out how to regulate Canadians' freedom of expression in their Facebook, Twitter and social media posts, maybe you would have had time to do a little work on this crucial issue.

The facts you read out are correct, of course, and deeply disturbing. Let me see if you have any answers at all on the legislation that you say is necessary for regulating online harm.

In terms of this regulator, what rules is it actually going to enforce, will it be the CRTC and what enforcement mechanisms will be in place?

Hon. Steven Guilbeault: Obviously, I'm here to talk about the objective of the legislation. Since it hasn't been tabled, I can't go into detail about it. However, once the legislation has been tabled, I would be happy to come before this committee again and testify as to the details and mechanics of said legislation.

Mrs. Shannon Stubbs: I think you have spoken about the concept of having a 24-hour takedown rule, so that once it has been notified that material is there, there would be a provision for that. I think that's a good idea. Of course, the trouble is that when child sexual abuse material or non-consensual images have been up for even 24 hours, they can have hundreds or thousands of viewers—millions in the case of Pornhub and MindGeek. We've heard from victims that explicit images of them were online for three years before they found out. In the case of Serena Fleites, hers was shared and downloaded all over her school before she knew. Then she got into a never-ending back and forth to try to get the platforms to be accountable and to take down the materials.

Can you explain or enlighten us about what prevention mechanisms might actually be in place?

Hon. Steven Guilbeault: This is a very good question. My office and my department have spoken as well with victims and victims' organizations. What we want to do with this legislation is to really shift the challenge for victims of having to try to get these images taken down—if we're referring to images that we would find on Pornhub, for example. We're trying to shift the burden of doing this from the individual to the state. It would be up to the Government of Canada, through a regulator, to do that, as it is in other countries, such as Australia, with their e-safety commissioner.

That's the goal we're pursuing with the tabling of this legislation. You are correct; we are also working to ensure that not only are the images taken down but they are removed from websites or associate websites to prevent, for example, the download of such images. They're not going to be downloaded and uploaded and downloaded and uploaded, as we've seen in many cases.

Mrs. Shannon Stubbs: Do you also believe that companies must be more responsible for ensuring that the content they are publishing does not contain minors and has the express and explicit consent of the individuals depicted?

Hon. Steven Guilbeault: Companies should abide by Canadian laws. Whether they're online companies or physical companies, there should be no distinction. As I said earlier, the challenge we face now is that the tools we have to deal with these online harms just aren't adapted to the virtual world.

The Chair: Thank you, Ms. Stubbs.

We'll turn to Mr. Sorbara for the next six minutes.

● (1115)

Mr. Francesco Sorbara (Vaughan—Woodbridge, Lib.): Thank you, Chair, and good morning to everybody. It's nice to be here this Monday morning, and again, welcome, Minister. It's great to see you here today. Thank you for all the hard work that you and your team are undertaking for all Canadians.

Minister, the first thing I would like to inquire about is the following. In mid-January, the Canadian Race Relations Foundation conducted a survey on Canadians' perceptions and recommendations on the spread of hate speech and racism on social media platforms. The survey shows that racialized groups are three times more likely to be exposed to or targeted by violence on social media. The proliferation of such content can result in hate crimes, which have gone up seven per cent this year across the country. These numbers have resonated painfully with our own recent history. Just four years ago, six people were murdered as they gathered for the evening prayer at the Grand Mosque in Quebec City. Islamophobia and xenophobia motivated this act. We learned shortly after that the perpetrator was radicalized through social media.

People here in Canada are harmed and victimized by hateful, violent, extremist, terrorist and radicalizing content. The online environment amplifies and spreads hateful messages against minority communities and the disenfranchised in ways we have never seen before. It's actually quite terrifying, to be honest.

Given that creating new regulations for social media platforms is in your mandate letter, and you mentioned you would bring legislation forward soon, could you provide us with an update on the essential work you are doing to protect Canadians online?

Thank you, Minister.

Hon. Steven Guilbeault: As I said, we have been hard at work for more than a year to prepare this legislation. We've held consultations with, as I said, in my case, more than 140 organizations. The Parliamentary Secretary to the Minister of Justice also held some consultations on some of the more legal aspects of the legislation and issues pertaining to the Criminal Code.

It is a complex issue. There are only a handful of countries in the world that have introduced legislation to do that, namely France and Germany; I spoke earlier about Australia, and the United Kingdom tabled a white paper on this just this past December. I was on the phone recently with the heritage minister in the U.K. to discuss that.

It is a complex issue, but nonetheless an issue we want to tackle. You referred to the 24-hour takedown notion, which is, in fact, in the mandate letter the Prime Minister gave to me at the beginning of the mandate. It's a more novel element; very few countries are doing that. The Australians are just introducing this in their legislation. We want to ensure that we find this right balance, and that's what we're working towards. It is still my intention to introduce the legislation in the very near future, but let me give you, perhaps, one other example of how online hate affects Canadians, and more specifically, indigenous people in this country.

I want to give you two quick examples, if I may. In 2018, two women in Flin Flon, Manitoba were charged with uttering threats and inciting hatred after posting a photo of a vandalized car, saying that indigenous people would be killed and calling for a “shoot an Indian day”. In 2020, two known nationalist groups called the Proud Boys and the Sons of Odin used social media to threaten and attack members of the Wet'suwet'en community during the pipeline protest. In fact, data from Statistics Canada show that police-reported hate crimes against indigenous people are on the rise. Between 2016 and 2018, incidents targeting first nations, Métis and Inuit communities rose by 17% during those two years alone.

Mr. Francesco Sorbara: Thank you, Minister.

I have a follow-up question on what we are seeing in terms of some content that is being posted online and its negative impact on various communities.

With that, communities across Canada are extremely worried about the rise of Islamophobia, hate speech online, as you just mentioned, towards our indigenous communities, and other forms of prejudice that have only intensified during this pandemic. We've all seen that words can lead to violence.

As parliamentarians, we recognize that we all have a duty to lead by example; that is to say, to engage in respectful dialogues, to be open to debates of ideas and to hear the positions of Canadians in order to work for a society where everyone is free to flourish with dignity.

Minister, can you tell us more about what our government is doing to fight the promotion of hatred and violence online?

Thank you.

● (1120)

Hon. Steven Guilbeault: This is really an important point. There are some people out there—a minority, clearly—who would advocate that we shouldn't intervene and that there should be no laws whatsoever regarding the Internet in any way. What happens on the Internet stays on the Internet. Well, it's clearly not the case.

In June 2020, the Institute for Strategic Dialogue published a report on right-wing extremism in Canada, as I said earlier, identifying more than 6,000 right-wing extremist channels, pages, groups and accounts. Since 2014, Canadians—inspired in whole or in part by extreme views they've gathered online—have killed 21 people in this country and wounded 41. This idea that this stays on the Internet is simply false.

Notwithstanding that, we haven't waited until the introduction of this legislation. For two years now, we have been funding an initiative called the digital citizenship initiative, whereby we're working with victims groups and with academics around the country to increase the level of online literacy for Canadians, to help them detect false news and to help them recognize hate speech and extremist groups online.

The Chair: Thank you, Mr. Sorbara.

We're going to turn to Madame Gaudreau now.

Madame Gaudreau.

[*Translation*]

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Thank you, Mr. Chair.

Good morning, Minister. I hope you are well on this Monday, as we approach the end of the parliamentary session.

First of all, I congratulate you on all the work you have done on Bill C-10. Of course, I am very disappointed with what is happening right now. In December, the committee made a point of meeting with witnesses to get to the bottom of everything that was going on with child pornography. However, because we are on the Standing Committee on Access to Information, Privacy and Ethics, we had to address other issues.

Today, I would like to shed some light on all of the testimony that we have heard. Initially, our motion was to invite Pornhub executives. We've heard a lot of comments, and I'd like to express a concern that I have.

We talked about the Five Eyes group and how this is a global issue. That being said, our current position is unfortunately not at the forefront. As you said earlier, other countries have already introduced similar legislation or are in the process of doing so. Canada does not have any concrete bills in the works on this topic.

How is Canada positioning itself? How do we position ourselves internationally in terms of protecting our fundamental rights?

Hon. Steven Guilbeault: Thank you, Ms. Gaudreau. Good morning. I wish you a good Monday as well.

I am as disappointed as you are to see the lack of ambition of some of the other parties in the House with respect to the passage of Bill C-10. However, we are not here to talk about that.

Canada is among the lead countries in addressing this issue. The countries I named earlier, which can be counted on the fingers of one hand, are among the only ones that are currently taking action.

It was at Canada's initiative that a coalition of countries was created that are committed to working together, not only on the issue of hate speech and other online harm, but also on cultural issues. Several countries are very interested in what we are doing with Bill C-10 and with respect to media compensation. This sort of informal coalition of countries is working collaboratively at Canada's initiative. In a few weeks, an announcement will be made about this joint international work.

Of course, a country like ours needs to have legislation that addresses the issue of online harm. However, this is indeed a global problem, and it needs to be addressed on a global level. That's why we formed this coalition of countries. Right now, there are only five of us, but I suspect that before long, many more people will be around the table.

Ms. Marie-Hélène Gaudreau: It is reassuring to hear that. I hope that other countries will be on board, because this is a real problem. Every witness we've heard told us that. We are unable to legislate well with the tools we have, especially with regard to uploads and downloads.

There was another thing that really upset me. Witnesses told us that the more we legislate, the more there will be an increase in these misdeeds on the dark Web.

How are we going to do this? There are so many solutions, and I'm the first one to be overwhelmed by it all.

How will we get it right and sort things out to curtail these reprehensible activities insofar as possible and put an end to their proliferation on the dark web?

● (1125)

Hon. Steven Guilbeault: That's an excellent question.

I would like to clarify something first. Regarding online cultural content issues, which are addressed in Bill C-10, obviously some political parties have decided to join the big companies like Google and YouTube rather than support our artists. As for media compensation, Facebook reacted very strongly in Australia.

As for online harm and hate speech, several social media platforms have publicly called for government intervention, perhaps because they feel they are losing control of the situation. I'm not saying that they all have. I've personally met with most of these large platforms that have a presence in Canada. They obviously won't agree with everything that's going to be in the legislation—I've never seen a company agree with all of it. They do agree that more and more governments need to step in on this issue to help them.

Let me come back to the argument about the dark web. It's somewhat like saying that we should not put criminal sanctions in the laws, and eliminate them all instead, otherwise people will hide to commit their crimes. It may happen, but that's no reason to do nothing.

Honestly, the percentage of people who have the technical skills to access the dark web is very small. So we need to put the necessary laws in place. We won't solve everything, but with these laws we will solve a lot of the problem.

Ms. Marie-Hélène Gaudreau: If I have a few seconds left, Mr. Chair, I'd like to ask one last question.

I am still a new member of the House, and when I came in, I found that our approach to privacy was identity-based. Earlier, you mentioned countries like France and Germany. In the previous session, we apprised ourselves of a lot of reports, including on Estonia, which has taken the lead.

My concern is about hacking and traceability of content on the web. I am worried about that. Do you think it is indeed urgent for Canada to prepare for this? Right now, there are a lot of international companies that are laughing at us a little because we don't protect our basic rights enough.

What do you think about that?

Hon. Steven Guilbeault: If I understood your question correctly, I think you're referring to the issue of personal data online, a topic that I'm very interested in and which was actually part of the last book I wrote.

Of course, I am not sponsoring this bill, but I would be happy to discuss it with you at other times, Ms. Gaudreau.

Ms. Marie-Hélène Gaudreau: Excellent.

Do I have any time left, Mr. Chair?

[*English*]

The Chair: You are out of time. Thank you for asking.

[*Translation*]

Ms. Marie-Hélène Gaudreau: Thank you very much, Minister.

[*English*]

The Chair: Mr. Angus, we'll turn to you.

Mr. Charlie Angus (Timmins—James Bay, NDP): Thank you, Minister, for coming today.

I'd like to ask you right off the top, on what date did the cabinet begin to discuss the issues of the allegations of sexual violence against young people on Pornhub?

When did cabinet start to talk about the Pornhub issue?

Hon. Steven Guilbeault: As you know, there is confidentiality around cabinet discussions, so I'm not at liberty to disclose this information.

Mr. Charlie Angus: Okay.

Minister Bill Blair told us the government was creating this new regulator. Is this new regulator going to be the CRTC?

Hon. Steven Guilbeault: Again, as I said to your colleague earlier, I am here to discuss the objectives of the legislation. In terms of the details of the legislation, that's not possible until the bill is tabled, but I would be happy to come back and testify at the committee.

Mr. Charlie Angus: Are you saying that Bill C-10 is not covering Pornhub?

Hon. Steven Guilbeault: Bill C-10, as I've said a number of times, is about cultural content. It's about ensuring that the web giants pay their fair share, and that our artists are fairly compensated for their—

● (1130)

Mr. Charlie Angus: I understand that. I'm just wondering whether, on the use of generated content, it's not going to apply to Pornhub.

Hon. Steven Guilbeault: It's not about content. BillC-10 is not about content moderation, which is also something I've said a number of times in the past.

Mr. Charlie Angus: I just need you to say yes or no. Bill C-10 is not going to be the means by which you regulate Pornhub. You'll have something else—another regulator or some other process?

Hon. Steven Guilbeault: It will not be done through Bill C-10, yes, that is correct.

Mr. Charlie Angus: Rose Kalemba contacted our committee and asked us to fight for her. At age 14, she was kidnapped, brutally tortured and sexually assaulted, and her videos were posted on Pornhub, downloaded and promoted.

In your view—and I just have to be blunt here because we've talked about some really difficult stuff at our committee so I hope you don't find me being too blunt—would you believe that the posting of those videos represents criminal acts?

Hon. Steven Guilbeault: As you are well aware, they are criminal acts according to the Canadian Criminal Code, yes.

Mr. Charlie Angus: Good, because it has sections 162, 163 and 164, and yet those laws are not being applied.

I need to know why we need a regulator to oversee something that's already under the Criminal Code. The promotion of these videos, according to law, is a criminal act, so why don't we just apply the law?

Hon. Steven Guilbeault: As I said earlier, the challenge that we in Canada, and countries all around the world, are facing is that the tools that we have to deal with these issues in the physical world just aren't adapted to the virtual world. This is why Australia created a new regulatory body to deal with that, and it is why a number of countries either have created or are in the process of creating new regulations, new regulators, or both, to deal with this. It's because the tools we have just aren't adaptable.

Mr. Charlie Angus: Are you saying we simply don't need to use the Criminal Code? What surprises me is that internal documents from the RCMP's December 12 briefing note on Pornhub pointed out that your office is going to be taking the lead.

According to those documents, they are not going after Pornhub, so did cabinet tell the RCMP to stand down while you developed this regulator? Why is it that the RCMP are under the impression that you're the lead on this, and that the Canadian laws that exist are not going to be applied?

Hon. Steven Guilbeault: I respectfully disagree with the premise of your question. As I stated earlier, the legislation will address five categories of online harms, which are already criminal according to Canadian law, and which are already criminal activities under the Canadian Criminal Code.

Mr. Charlie Angus: I get that. I guess my concern is that you haven't actually come up with legislation. You don't know when this regulator's going to appear, and the RCMP internal notes say your office is taking the lead.

We have survivors who suffered serious crimes and abuse. We have the Criminal Code. I'm wanting to know why your government is saying that it will be the regulator that handles that, as opposed to telling the RCMP and the justice minister to do their job.

Hon. Steven Guilbeault: I think you're misunderstanding what we're trying to do.

There are many reasons we need to create a regulator. One—

Mr. Charlie Angus: I don't have a problem with the regulator. What I have a problem with is the fact that we actually have criminal laws in place, and it seems that the RCMP has decided that Pornhub doesn't have to actually follow the law—there's voluntary compliance; your Attorney General says he's not even sure if they're a Montreal company; you're telling us there's going to be some kind of regulator, but you don't have one....

I just have to be honest. Having the minister of culture and communications handle a file about horrific sexual assault videos to me is like asking the minister of transportation to look after human trafficking.

Why is it that the laws of the land are just not being applied? You can go and get a regulator, but why are the laws not being applied?

Hon. Steven Guilbeault: Your analogy would be correct if I were the only one doing this. I'm not.

As I stated in my remarks initially, I am working with the Minister of Public Safety, with the Minister of Justice and with a number of other colleagues. This is a whole-of-government approach. It's not—

Mr. Charlie Angus: I know, and they say you're the lead on this. They defer to you.

Hon. Steven Guilbeault: That doesn't—

Mr. Charlie Angus: We don't have a regulator. We don't have any action. Again, what do I tell the survivors who are being told, sorry, not much is going to happen but maybe a regulator, and maybe there will be a new CRTC for porn? How long are they going to have to wait before they actually see something?

● (1135)

Hon. Steven Guilbeault: This was in my mandate letter when I was nominated as the Minister of Canadian Heritage. We started right away, despite the most important pandemic we've seen in the last 100 years, doing public consultations, doing the work. Some people may like—

Mr. Charlie Angus: Have you spoken with survivors?

Hon. Steven Guilbeault: Of course we've met with survivors.

Mr. Charlie Angus: Have you met with survivors of Pornhub?

Hon. Steven Guilbeault: I have not personally, but the department and people on my team have, so yes, we have, but it's not something that can be solved overnight. It's a complex issue. As we're seeing all around the world, countries are struggling with this.

The Chair: Thank you, Mr. Angus.

We're going to turn to Mr. Viersen for the next round of questions.

Mr. Viersen.

Mr. Arnold Viersen (Peace River—Westlock, CPC): Thank you, Mr. Chair.

To the minister, have you, your staff or your office ever had a meeting with Chuck Rifici or any of his associates or employees?

Hon. Steven Guilbeault: I would be happy to provide the committee with....

I can't see the image of the member, but maybe I should proceed anyway, Mr. Chair.

The Chair: Please proceed.

Hon. Steven Guilbeault: I'd be happy to provide the committee with the list of organizations and people we've met—we being the government—on this issue over the last year and some months.

Mr. Arnold Viersen: All right.

I'd like to hand the rest of my time over to Mr. Gourde.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Minister, would it have been possible to include a provision in Bill C-10 to regulate platforms like Pornhub so as to finally protect our children, who are going through unspeakable things right now?

Hon. Steven Guilbeault: Thank you for the question.

I find your question very cynical, as your party consistently opposes the passage of Bill C-10, which is not about content moderation, but rather about web giants contributing to our cultural sector's artists and musicians.

Mr. Jacques Gourde: Forgive me, Minister, but you are changing the subject.

Hon. Steven Guilbeault: No, not at all...

Mr. Jacques Gourde: It is our duty to protect our children.

Hon. Steven Guilbeault: What you are talking about...

[*English*]

The Chair: Minister, Monsieur Gourde, it's difficult when you're talking over each other.

Monsieur Gourde, I'll turn the floor back to you.

[*Translation*]

Mr. Jacques Gourde: Thank you, Mr. Chair.

[*English*]

Hon. Steven Guilbeault: I'm sorry. Are you turning it back to Mr. Gourde or to me, Mr. Chair?

The Chair: Thank you, Minister.

The time is Monsieur Gourde's.

Monsieur Gourde, we'll turn it back to you.

[*Translation*]

Mr. Jacques Gourde: Thank you, Mr. Chair.

We have had some very disturbing testimony about underage children being exploited by platforms, and we need to take action. You told us you would put in place a new provision, new legislation, which probably won't come into effect for a year, a year and a half. We need to move much, much faster than that. We live in a society where our children are not protected, currently, from web giants.

How are you going to speed up the process? Why couldn't C-10 close the loophole for now?

Hon. Steven Guilbeault: Once again, your party opposes the passage of Bill C-10, which has nothing to do with content moderation, while the hate speech and online harm bill specifically addresses the issue of content moderation.

Yet you say you oppose content moderation. You and many of your colleagues say that the government wants to take away your freedom of expression. The exploitation of persons bill will ensure...

Mr. Jacques Gourde: Could Bill C-10 have helped, yes or no?

Hon. Steven Guilbeault: No, it's a bill that...

Mr. Jacques Gourde: Well, then, let's talk about something else, Minister. We're not talking about culture, we're talking about protecting our children.

When will your next bill be introduced?

Hon. Steven Guilbeault: As quickly as possible. I can already tell you that your party will oppose that bill as well. Your party...

Mr. Jacques Gourde: That is speculation, Minister.

We want to protect our children. Table your bill as soon as possible, before an election is called. If there is an election this fall, absolutely nothing will happen for the next two years.

There are children in Canada who are thinking about suicide. They are not being protected right now, Minister. Why is this coming back into your court? It should have been the responsibility of the Department of Justice. You may not be in the best position to help our children right now.

Hon. Steven Guilbeault: I want to start by saying that the Internet and the sexual exploitation of children on the Internet existed before 2015. Your party was in power for 10 years. On the one hand, you did nothing about this issue, despite the existence of this phenomenon.

On the other hand, the sooner your party stops its systematic obstruction of Bill C-10, the sooner...

● (1140)

Mr. Jacques Gourde: Minister, you are electioneering.

Hon. Steven Guilbeault: ...I can quickly table my bill.

Mr. Jacques Gourde: Your arguments are being made from an electoral perspective, Minister. You don't want to help children. Right now they need help and we want to help them. You are not helping us.

You are already in an election campaign. You are making election-minded comments and it's really sad. I'm really disappointed in your attitude, because we are all elected to improve the lives of Canadians. Please stop your electioneering and tell us how you are going to help our children.

Hon. Steven Guilbeault: We want to do several things. As stated in my mandate letter, the bill will make it possible to remove all illegal content within 24 hours, thereby forcing companies to do so. Companies currently aren't doing this. The bill will also help implement an effective and user-friendly content moderation system. Platforms will be subject to greater transparency obligations with respect to reporting online harms, such as child sexual exploitation, to law enforcement.

Mr. Jacques Gourde: Rest assured, Minister Guilbeault, that we'll be there to help you. Don't speculate. This bill hasn't been tabled.

Thank you, Mr. Chair.

[*English*]

The Chair: Thank you, Monsieur Gourde.

We're going to turn to Mr. Dong for the next round of questions.

Mr. Dong.

Mr. Han Dong (Don Valley North, Lib.): Thank you very much, Chair.

I want to thank you, Minister Guilbeault, for coming to the committee today and talking about a very important topic.

First of all, I want to go back to your opening statement. You cited an increase of xenophobia and Islamophobia in behaviours or speeches online over the recent months. As a member of the Asian-Canadian community, I observe and witness first-hand some of these intolerable behaviours online.

I have to say that the pandemic is changing people's socialized behaviour. More and more, people are spending time on social media. Then we have some of these bad actors using various platforms, seeing them as tools of disguise, seeing them as a protection, and also utilizing bots and trolls and saying all kinds of things they otherwise wouldn't say in public.

You mentioned that children in the country are being victimized, and the platforms are not doing anything. That's precisely what we are talking about today.

We know that social media companies, including the one we are doing a study on, have been acting unilaterally and opaquely. Sometimes they introduce half measures after public pressure, but they haven't been serious about consulting with industry experts and listening to the recommendations of the audience and the groups of victims.

In your opinion, what can the giants do to respect Canadians' will and Canadian law in terms of protecting the general public? It's in their best interest as well, because that's their audience and their client base. A very few bad actors are contaminating the online environment.

Can you talk a little about that?

Hon. Steven Guilbeault: There are many elements in what you said.

First, I think one of the purposes of the legislation is to ensure more transparency on the part of the platforms in terms of their guidelines and practices regarding content moderation, because right now it's very uneven. Some companies have better content moderation practices than others, and some have very little. You're right—they are not transparent.

Some may have rejoiced in the decision of this platform or that platform to ban this user or another user, but under which criteria? Why them and not someone else? This is clearly something we want to tackle. Frankly, there is an issue where we see the very business model of some of the platforms being about creating controversy and nourishing hate speech and intolerance, because it creates more traffic on their platform. Therefore, they can sell more publicity and make more money.

As part of the legislation that will be tabled, this is also something that we as a legislator will need to address.

● (1145)

Mr. Han Dong: Minister, thank you very much for that.

We heard opposition colleagues talk about.... We're dealing with content online; therefore, they suggested that it's your sole responsibility, but at the committee here we heard from the witnesses that the makeup and structure of these companies is designed to get around government regulations. We have a company that is operating out of Quebec but registered in another country, so I understand what you mean when you say it's going to be a joint effort between different ministries and different ministers.

I'll go back to what my colleague, MP Angus, asked about earlier, which I thought was interesting. In your opinion, is Canadian law, as is it currently, inadequate to police what's going on online, to the point that they are committing crimes according to our Canadian values and the Canadian law?

Are our laws adequate at all? If not, what will be the direction? What kinds of changes can we introduce to protect victims?

Hon. Steven Guilbeault: The first part of your question is a very interesting one, because what we are, in fact, seeing is that these companies—many of these companies, perhaps not all of them—are using different loopholes around the world to try to get away from having to obey national laws, whether it's in Canada, Australia, Germany, Finland, France or the United Kingdom. What we want to do with the legislation will ensure that whether or not a company is Canadian, or based in Canada, or registered in Canada, or its websites are housed in Canada, if it broadcasts images and videos in Canada then the law will apply to it.

The Chair: Thank you, Minister. I gave some extra time to allow you to answer some of that question.

Mr. Han Dong: Thank you, Chair.

The Chair: Hopefully we can get back to that if there are additional opportunities.

Madam Gaudreau, we'll turn to you for the next two and a half minutes.

[*Translation*]

Ms. Marie-Hélène Gaudreau: Thank you, Mr. Chair.

My remarks will be a little different. I want to talk to you. What just happened is a concrete example. I think, or rather I know, that I'm the only one who can make this type of comment.

Our conscience is telling us that we must protect our children, our youth. We need to legislate and move quickly to do so as well. We're in the committee making the case that this is important and necessary. We're trying to speed things up, but we've lost a tremendous amount of time. You'll argue that I'm a new member of Parliament. However, the fact remains that people are watching us.

Despite our willingness to help our constituents, the political scene ensures that the pursuit of power takes precedence. We're seeing this right now. We're seeing pre-campaigning, filibustering and so on. It's all about drawing things out. Minister Guilbeault, I believe that, in order to help our people, we should have had a meeting and a specific bill already in hand. However, we didn't even pass Bill C-10, which I find extremely disappointing.

People back home are telling me things. If you ask the people back home, they'll tell you to stop carrying on the political games and the pursuit of power. We need to help our people. I'm ashamed of that part. I won't give up. Why won't I? Because my party is the only one that can claim that it promotes and protects the interests of Quebeckers. We aren't looking for power. On the contrary, we don't want it anymore.

That said, Minister Guilbeault, you spoke about five categories of illegal activities included in your bill. I don't know what they are and I would like you to identify them.

● (1150)

[*English*]

The Chair: Minister, I just want to let you know that you have just 15 seconds left to respond, as the member took most of that short round. Minister, I'll give you a chance to answer with a short answer.

Hon. Steven Guilbeault: Thank you, Mr. Chair.

If I may specify, it is 11:50 and I must remind you and all members that I have a hard stop a few minutes before 12, as I must be present in the House of Commons at 12 o'clock sharp for a debate. Thank you for your understanding.

[*Translation*]

I'll respond in 15 seconds.

These are the five categories of harms that we want to address in this bill: child sexual exploitation, incitement to violence, incitement to terrorism, non-consensual sharing of intimate content and hate speech.

Ms. Marie-Hélène Gaudreau: Thank you, Minister Guilbeault.

Thank you, Mr. Chair.

[*English*]

The Chair: Mr. Angus, we'll turn to you.

Mr. Charlie Angus: Thank you so much, Minister.

In the examples we've had some really hard meetings with survivors sharing their stores. I look at Canada's Criminal Code. Section 162, filming people without their consent and then promoting it, is a five-year prison sentence. Section 163, selling and promoting non-consensual sexual assault videos, is a 14-year prison sentence.

I would ask you, how do you tell the survivors that it's okay for the Justice Department of Canada and the RCMP not to apply the laws to a company when they know it exists in Montreal, because some day there will be a regulator that will deal with this?

We have laws that are very clear. We're talking about very obvious issues of a breach of law. Why is it that your government has not acted?

Hon. Steven Guilbeault: As I said earlier, the body of tools that we have to deal with this issue.... In the physical world, it's very simple. I think you and I can agree on that. It's not so simple to deal with these criminal offences in the virtual world—

Mr. Charlie Angus: I guess I just have to interrupt you because—

Hon. Steven Guilbeault: It's like that all around the world, Mr. Angus.

Mr. Charlie Angus: I know, but we're not talking about buddy in his basement doing revenge porn on his girlfriend. We're talking about a well-known company that's established in Montreal and that the RCMP says is one of its voluntary partners. We're talking about a company that is established. We're not talking about idiots making online hate comments.

If we have a law in the land and your government is not willing to use it against a company that breaks that law, I don't see how we tell survivors, "Don't worry, a regulator is going to make those guys come to heel." How do we tell them that, if the laws of the land aren't going to be applied?

Hon. Steven Guilbeault: I think I understand your point, and I would like to respond that it's not just about the regulator. It's going to be about an entire new ecosystem to help us deal with these harms online in a way that we can't right now. The regulator is but one component of that. It's not the entirety of the system we want to propose.

Mr. Charlie Angus: Thank you.

The Chair: Thank you, Mr. Angus.

We'll turn to Mr. Viersen now for the next round.

Mr. Arnold Viersen: Thank you, Minister.

Have you watched any of the testimony that we heard from the victims before this committee?

Hon. Steven Guilbeault: Not in front of this committee.

Mr. Arnold Viersen: All right. Many of them talked about how non-consensual videos of them were put up and, overnight, had millions of views. How do you intend to combat that with a 24-hour takedown notice?

Hon. Steven Guilbeault: Well, as stated in my mandate letter, once an illegal publication is flagged, companies will have 24 hours to take it down. Instead of the victims having to try to deal with these companies, it's going to be the Government of Canada that's going to work to ensure that they remove that. If they don't, then there will be consequences for these companies.

Mr. Arnold Viersen: What's the prevention piece of this plan, though? How are we going to prevent these images from ending up on the Internet in the first place?

Hon. Steven Guilbeault: I think you're asking me if we have a magic wand to prevent crime. We don't, and I believe no government—

● (1155)

Mr. Arnold Viersen: We take steps in all other areas of life to prevent crime.

Hon. Steven Guilbeault: We will as well, by investing in more education so Canadians better understand these issues regarding the harms that these publications can have online. We will work to ensure that once posted they're removed as quickly as possible.

Mr. Arnold Viersen: There's no prevention piece. It's not going to be forthcoming in that bill that we—

Hon. Steven Guilbeault: That's not what I said. Earlier, I spoke about the digital citizen initiative, which our government has been funding for the last two years to work with victims' organizations, academic groups and non-governmental organizations on these very issues.

Mr. Arnold Viersen: All right. What steps would be taken to ensure that a regulator would be able to access the folks most affected by this problem—teenage girls and young adult women—seeing as they're not likely to be able to navigate complex bureaucracy?

Hon. Steven Guilbeault: It won't be complex.

Mr. Arnold Viersen: What enforcement mechanisms is this supposed regulator going to use?

Hon. Steven Guilbeault: Again, I'm happy to discuss the objectives of the legislation with you. I would be happy to come back to discuss the details of the legislation once it is tabled.

Mr. Arnold Viersen: What about cases in which the victim is Canadian but the site isn't necessarily Canadian?

Hon. Steven Guilbeault: I'm happy to repeat, but that's the answer I gave to your colleague, Madame Gaudreau.

The purpose of the legislation is that whether the company is Canadian, its servers are in Canada, its headquarters are in Canada or it's registered in Canada or elsewhere, if it's broadcasting images or videos in Canada, then the legislation will apply to that company.

Mr. Chair and Madam Clerk, I am being told that I must connect to the House of Commons debate five minutes before noon, which would have been a minute ago, I suppose. I'm in your hands, but I must get ready for another debate in the House of Commons.

The Chair: Okay, Minister. We thought we had you till noon, but we appreciate that we're all in the same boat, so we'll bid you goodbye. Thank you so much for joining us this morning.

Hon. Steven Guilbeault: Thank you very much, Mr. Chair.

The Chair: Colleagues, we will suspend our meeting just for a moment until we get the next witnesses lined up, then we will call this meeting back to order.

The meeting is suspended.

● (1155)

(Pause)

● (1200)

The Chair: [*Technical difficulty—Editor*] We have a number of witnesses. We have Charles DeBarber, who is a senior privacy analyst.

We have Arash Habibi Lashkari, who is an assistant professor in the Faculty of Computer Science at the University of New Brunswick and a research coordinator at the Canadian Institute for Cybersecurity.

I'd like to welcome back Melissa Lukings, as well, who is a juris doctor candidate and an advocate for cybersecurity research.

I know you'll have some opening statements, so we'll turn to Mr. DeBarber to begin.

Mr. Charles DeBarber (Senior Privacy Analyst, As an Individual): Hello. Good afternoon. My name is Charles DeBarber and I'm a senior privacy analyst with Phoenix Advocates and Consultants. My background is U.S. Army cyber-intelligence and cybersecurity.

I began my work with victims of non-consensual pornography, or NCP, in 2015, when I worked for the elite firm Fortalice. As the program manager for open source intelligence, I assisted victims of NCP through our reputation services. Since departing Fortalice in 2018, I have done freelance work on behalf of victims of revenge porn, extortion schemes and cyberstalking, and on purging content for victims of human trafficking. I've written bespoke information guides for clients to help protect their digital privacy and to reduce the chances of their being a target of successful doxing.

My background gives me deep insight into the sources of content on the Internet, and today I want to share with you guys some knowledge about the surface web, deep web and dark web. In addition, I'd like to share some research about the sources of adult NCP on these three layers.

As a disclaimer, I want to be clear that my data regarding NCP is limited in a few ways. First, my data is limited to the 90-plus cases that I've undertaken since 2019. You'll see these are sourced as "PAC Research 2016 to 2021". I recognize there's a selection bias to that data due to it being from only our casework. Second, much of my information on NCP involving children is largely anecdotal, as I've never produced statistics on it. In addition, the bulk of my work has been with adult victims. Third, I am discussing the concepts of surface web, deep web and dark web and how they relate to the volumes and types of NCP often found on them. This is not to paint any of these layers as good or bad. The dark web has an especially heinous reputation, but remember that there are people who use the dark web to subvert censorship or express their free speech in countries where freedom of speech is very limited.

You'll see in the handout the beautiful iceberg graph that is commonly used to explain the three layers. You have surface web, deep web and dark web. We'll start with the surface web.

The surface web is basically the Internet content indexed by search engines themselves and things you can directly jump to from search engines. It's aggregated web content that can be found with web crawlers, also known as spider bots or spiders. Make note of that, because it is very important for one of the points I'll make later. The surface web is the minority of online content, around 4% to 5%.

What's the deep web? That's the majority of the web, more than 90% of it. It's Internet content that's not part of the surface web and is not indexed in search engines. It's mostly content that is not readily accessible through standard means, such as search engines. As I said, it's the majority of content on the Internet.

Then there's the dark web. It's part of the deep web, but what makes it different is that you have to use encryption software and special software to access it—things like Tor Browser or Freenet or Freegate. It's also used interchangeably with dark net. It can be called both.

NCP comes in many forms. Some of the key forms for adult victims include revenge porn, non-consensual surveillance, human trafficking and data or device breaches. We have the following statistics from our casework. The majority of adult NCP, 73.5% of our cases, was found on the surface web. We believe that the reason for this is that adult NCP pornography easily blends in with amateur pornography. The ease of use and popularity of video- and image-sharing sites on the surface web is the main cause of this.

On top of that, the deep web accounts for about 23.2%. These are often private forums for pirated content, BitTorrent sites, and VoIP and messaging apps like Discord communities. The more compartmented nature of the deep web leads to a lower volume of content that is also less viral.

The dark web accounts for little of our content. Content there, in our experience, includes things that we consider highly illegal, things you would find only on the dark web because they are highly illegal. This could be things like hidden bathroom cam footage, extremely violent content, child pornography and bestiality. NCP blends in with amateur pornography and is readily available on upper layers. There's no reason to go to the dark web for it. Only a minority of Internet users have enough expertise and knowledge of the dark web to use it anyway. The even more compartmentalized nature of the dark web just keeps people off it. This results in more extreme and illegal content being relegated to the dark web.

● (1205)

In our casework, only about 3.3% is dark web content.

There are a few observations I would like to share with the committee. I've removed over 100,000 pieces of NCP content in the last five years. My average client has between 400 to 1,200 pieces of content, and that could be the same picture, video or handful of pictures, but it's shared on many different sites. Viral content itself can be upwards of 6,000 pieces of content and above. Very rarely do I utilize the NCP removal processes created by search engines such as Google or Bing or social media like Facebook, Twitter or Reddit.

I normally use the copyright removal process here in the United States, known as the Digital Millennium Copyright Act. The NCP process often is more complicated and takes longer for victims who have to follow it for every piece of content. Imagine, if you have 400 pieces of content out there, that might be 400 different applications you have to put out. These companies, frankly, respect intellectual property more than victims, because the copyright process is so much easier.

The removal process is costly in both time and resources. I utilize automation, which is not cheap. For a client with more than 400 pieces of content, it would usually cost $2,000 for automated removal and $5,000 for bespoke removal services, and that just mitigates the problem. Victims using it manually require a certain level of understanding of information systems, search engines and web caching, and that is if the victim can find most of the content without using automated aggregators. My junior analysts, some of them with information systems and computer science backgrounds, take up to a month of hands-on work to learn how to effectively purge content. The average victim is expected to have this expertise if they cannot afford professional services. The tools for victims to effectively mitigate their digital footprint of content aren't readily available.

Great strides have been made to get Silicon Valley to recognize the issue, and I don't wish to demean those efforts or that recognition. Laws in my home country are now in 48 states and two territories to protect victims of NCP. However, picking up the pieces after NCP floods surface web sites is still an uphill battle. We've worked tirelessly so clients can google their name without NCP coming up. One of our clients lives in fear of her 10-year-old using the computer and googling her name. Others have lost job opportunities, housing opportunities and relationships. Many of our clients have contemplated or attempted suicide.

Finally, video upload sites that allow pornography, such as Pornhub or Xvideos, have exacerbated the problem. This is one of the big points I want to make. Content goes viral a lot faster with these sites, and these sites use what is called search engine optimization to flood Google with their content. Even if the content is deleted within 72 hours, it often takes days, frankly, for a victim to even find out that they're a victim. Smaller video upload sites then aggregate this material from search engines and repost it, making this a feedback loop that keeps feeding the search engines and makes it a viral issue.

The issue has become so significant that when a victim's name is posted in a video title that they're aggregated in and it's then used in search engine keywords for porn sites that don't even have their content, it just becomes a random keyword—their name—and God forbid you have a unique name. Imagine googling your name, and hundreds of porn sites coming up because your name is a keyword empowered by SEO techniques.

We need to find a balance between verification and privacy. That's very easy for me to say, but sites having a reasonable policy for age verification is required. I compliment Pornhub in adopting a verified content policy in late 2020. I'm very angry [*Technical difficulty—Editor*] and I badly want them held accountable for that, but I want to make sure it's also not so cumbersome that sex workers who are free agents can't operate without reasonable privacy.

Search engines—and this is a key one, and I would recommend you put this forward, or at least encourage them to change their policies—shouldn't allow indexing from adult video image upload sites that do not come from verified accounts. This means that, with verified accounts, the spiders can be turned on so that they can feed into Google, Bing and so on. However, spiders should be turned off on any website where any Joe Schmo can come and upload content, whether it be videos or images. They should be turned off on that content until it is verified. That keeps it from hitting search engines in 72 hours.

● (1210)

Remember, with all NCP, you're really fighting time, and that keeps it from going viral a lot more quickly, quite frankly. It makes the clean-up process significantly better, and it can mitigate it. Furthermore, it would probably protect the intellectual property of other sex workers. As I said, Pornhub and other major tube sites have more or less put NCP into the express lane via SEO techniques.

Finally, the doxing of victims and sex workers is a very serious issue. Despite many of my clients being Jane Does, I can't get Google to delist web pages that post the real names of victims. I wish there was a policy that allowed the delisting of the real names of Jane Does, of sex workers, that exist on sites such as the defunct Porn Wikileaks, which were very dangerous for them and were made for doxing victims.

I'm very open to questions you may have and appreciate your welcoming me today. I'm honoured to be here.

Thank you.

The Chair: Thank you, Mr. DeBarber.

Professor Lashkari, we'll turn to you for your opening statement.

● (1215)

Dr. Arash Habibi Lashkari (Assistant Professor, Faculty of Computer Science, University of New Brunswick and Research Coordinator, Canadian Institute for Cybersecurity, As an Individual): Thank you so much.

Good afternoon, everyone. I think Mr. DeBarber mentioned most of the content that I wanted to share with you, but maybe I'm talking from another perspective, as a researcher. I'm also going share some of my latest findings, which I have already published.

As a short bio, I am Arash Habibi Lashkari, assistant professor in the faculty of computer science at UNB, research coordinator at the Canadian Institute for Cybersecurity and also a senior member of the IEEE.

In the past two and a half decades, I have been involved in different projects related to designing, developing and implementing the next generation of detecting and preventing disruptive technologies in academia and industry.

Actually, on the academic side, I can share with you that I have over 20 years of teaching experience spanning several international universities. On the research side, I have published 10 books and around 90 research articles on a variety of cybersecurity-related topics. I have also received 15 awards in international computer security competitions, including three gold medals. In 2017, I was recognized as one of the top 100 Canadian researchers who will shape the future of Canada. My main research areas are Internet and Internet traffic analysis, malware detection and also threat hunting.

As has been requested here, today I am talking about the dark and deep web and also the dark and deep net, but I'm trying to make it simpler so that it's possible to easily visualize and so that everybody can imagine it.

We have three layers, and the first one, which is the common layer, we call the “surface web”. This is everything that is available and open, everything that can be found as you search the different search engines such as Google, Bing, Baidu and others. We call this the “indexed web”, which means the websites that have been indexed by the search engines.

The second one is the deep web, which is the portion of the Internet that is hidden from the search engines, and we call this “unindexed web”. It includes mainly personal information, such as payment information, medical records and corporate private data, or when, for example, we are using a VPN, a virtual private network, to connect to these contents.

The third one is the dark web, and this portion is certainly hidden from search engines and actually includes the www content that exists on darknets. These websites can be accessible to special software and browsers that allow the users and also the website operators to remain anonymous and untraceable. There are several projects going on here to support the dark net, such as Tor, The Onion Router; I2P, the Invisible Internet Project; and also Riffle, which is the collaborative project between MIT and EPFL in response to the problems we have with the Tor network.

What is the source of the basic darknet? In 1971 and 1972, two Stanford students, using an ARPANET account at the AI laboratory, tried to engage in a commercial transaction with their counterparts at MIT. This means that before Amazon and before eBay, the seminal act of e-commerce was a drug deal, and the students used this network to quietly arrange for the sale of an undetermined amount of marijuana through the precursor to the Internet we know today.

What is the new version of the darknet, or the modern darknet? In 1990 the lack of security on the Internet—and its ability to be useful in tracking and surveillance—became clear, and in 1995 three guys from NRL, which is the U.S. Naval Research Lab, asked themselves if there was any way to create Internet connections that didn't reveal who was talking to whom, even to someone, for example, monitoring the network. The answer was onion routing.

The goal of onion routing was to have a way to use the Internet with as much privacy as possible, and the idea was to route traffic through multiple servers and encrypt it each step of the way, making it completely anonymized.

● (1220)

In 2000, one student from MIT—Roger—had already started to work with one of these guys at the NRL and created a new project named Tor, or The Onion Router. After that, in 2006, another student or classmate joined this team. They received funds from the EFF, and officially in 2006 they opened this non-profit organization.

My latest research results—all of them have been published in 2016, 2017 and 2020—show that it is possible to actually detect users who are connecting to the dark or deep web in a short period of time—around 10 to 15 seconds. Also, we can detect the type of software or application they are using, but from their machine, not from the Internet. From the Internet, everything is completely anonymized, but from the actual user's machine it is possible to detect their activity somehow.

I am completely ready for any question if the committee asks.

Thank you.

The Chair: Thank you, Professor.

We're going to turn to you, Ms. Lukings. Thanks so much for joining us again this morning.

Ms. Melissa Lukings (Juris Doctor Candidate and Advocate and Cybersecurity Researcher, As an Individual): Hello, friends. I feel like most of us have met before, but in case we haven't, I'll quickly introduce myself.

My name is Melissa Lukings. I'm a juris doctor candidate in the University of New Brunswick's faculty of law. I'm also a cybersecurity law and legal researcher, an alumnus of Memorial University of Newfoundland with a B.A. in linguistics, and a social justice and legal reform advocate. I have intersectional lived experience as related to previous testimonial evidence, which was invited to be heard by this committee before. I sent in some handouts. Everyone can read about my background there. I don't really want to waste time on that. I just want to go right into what I wanted to say.

My message to you today, basically, is one of concern at the overbroad and ambiguous nature of some of the proposed legislation that has been put forward.

Here are the issues.

We're being told that the rationale behind the proposed regulations and the push for digital content censorship is to prevent the prevalence and dissemination of non-consensual pornographic material, child pornography and other abusive material, which tends to pop up mostly on the surface web, as we heard earlier. We also want to deter and detect illegal material, prevent it from being uploaded and, optimistically, reduce the instances of human trafficking done via a connection in Canada, and/or with some ties to Canada.

The last time I was here, I expressed my concern that creating more intensive regulations of any sort on surface web content will inevitably push fringe traffic onto dark forums, which are much more difficult to detect and where an influx of user access would saturate an already challenging area for law enforcement. As Dr. Lashkari pointed out, whereas you can detect dark web traffic from the user source computer, it cannot be detected in the Net, from inside, which presents a challenge.

We have some graphics that we've created. They're all in your handouts. They explain how all the different aspects of the dark web work, so if you have any questions, we have illustrations for that.

When I was last here, the response was that it's not the intention of the federal government to push human trafficking, sexual exploitation, illegal content, violence, child porn and all of that onto the dark web. That's great.

Also, as a side note, I really enjoyed being a professor for, like, a minute in your last meeting. Thanks. That was super fun. I made a GIF.

True, we don't want to push these things onto the dark web, and that's great. You wouldn't want to sweep these under the metaphorical rug that is the hidden Internet, yet we're continuing to discuss the creation of additional regulations as if there's not a direct consequence of doing so, even though there is. It's not just a matter of NIMBY or not in my backyard when it comes to illegal content. Hiding it doesn't make it go away. It just hides it from sight, which isn't really a way to address these issues.

On point number four on my notes, when I was last here, I found it really frustrating that the adult entertainment issue and sex work in general had been conflated with sexual exploitation, abuse and trafficking within discussions at this very committee.

Indeed, MP Arnold Viersen was so taken by the emailed testimony of people with common experiences in commercialized sexual activity that he felt it was appropriate to waste his speaking time reading out victim porn-type emails from unknown persons, rather than engaging with the spoken testimony of people who also had common experiences in commercialized sexual activity and who had been invited to be heard at the committee hearing.

That's not okay. Hearings are usually for being heard. You're supposed to be hearing from the people who you invite and who are to be heard at your hearing. That's why it's called a “hearing”. Anyway, that's that.

Through highly inaccurate media portrayals, the dark web has become nearly synonymous with illegal activities. However, it is also used....

An hon. member: [*Inaudible—Editor*]

Ms. Melissa Lukings: Chris, are you okay? Do you want me to stop?

● (1225)

The Chair: We were just.... Pardon me. I apologize.

Ms. Melissa Lukings: No worries.

The committee is dealing with a Canadian-controlled private corporation, a CCPC, which is a private commercial organization based in and operating with headquarters located in Canada. It is a Canadian company. We know this, and that's fine. Commercial organizations in Canada are bound by the Personal Information Protection and Electronic Documents Act. PIPEDA outlines the rules and remedies, including the fines and other penalties, for corporations that fail to abide by the provisions specified in the act.

Beyond the corporate level, we also have the Criminal Code of Canada, which outlines the criminal offences and punishments for committing such offences. We have these. We need to apply them. Everyone is bound by the Criminal Code of Canada.

Why, then, do we need additional regulations? Why do we need more oversight when we have not yet tried to simply apply the law we already have? We have these laws. We can use them, so let's use them. That's what they're for. What's the point in even having these statutes if you're not going to apply them when they're needed? What are we doing here?

We're here because a portion of those involved have decided to conflate the issue of corporate negligence with highly sexualized and emotive criminal activity—read again, child rape porn testimony. It elicits an emotional response—the sympathetic nervous system and all of that. It doesn't matter. This is about a corporation and user-generated content. It does not matter what is depicted in the content as much as it matters that the content, whatever it may be, should not have gotten past the corporation's screening system before being made live on the site. When the issue was brought to its attention, the corporation responded inadequately at first, so we need corporate law. We need to look at liability and feasibility standards.

Why has this become a forum for grandstanding religious ideologies? I'm sure you've all heard about Exodus Cry in the news, if you've been following it. Exodus Cry is a fundamental Christian organization founded on religious ideologies stemming from the United States. Why is it relevant to a question of corporate liability in Canada? It isn't. It doesn't make any sense.

Why are we arguing about exploitation? Why are we discussing mass censorship? Is that not a massive overreaction to a simple corporate negligence question? It seems glaringly obvious to me, so why are we not discussing reasonable options for encouraging corporations to better serve their users?

Also, I have some opinions about the genderedness of this. You can read about it in my notes.

When it comes down to it, you can't eliminate sex. We're humans, and there is always going to be a demand for sex. You can't eliminate sex work because the demand exists. You can't eliminate extramarital sex or porn or masturbation or demand for sexual services, but sexual assault is illegal, even when that person is your spouse. We need it to be that way. We want to protect people. If you're saying you can do certain things only within the context of marriage, you're setting yourself up for failure. It's true.

Yes, I said “masturbation” in a hearing. Oh my God.

You cannot eliminate base human desires, so you can't eliminate sex. That would be silly. It's okay to not like these things, and just because you don't like a thing or you feel that a thing is not for you, it doesn't mean it's inherently evil and should be eliminated. It doesn't work that way. It's not about and should not be about pornography or the actual content of online material here. This is about creating reasonable laws that work for Canada, Canadian corporations and everyone residing within Canada. We don't need new regulations; we don't need a new regulator, and we don't need online censorship. We need to use the tools we already have, which were designed for a reason. Why be redundant?

That is my diatribe.

Thank you for having me. I will take any questions you throw at me.

The Chair: Thank you.

Colleagues, we will begin with rounds of questions.

I want to highlight that I am getting notice that there is a possibility there will be a vote in the House of Commons. I will proceed with questions through the bells if there is consent from committee members. As we get closer to the vote, we'll suspend if need be, but I am hopeful that will not be the case.

Mrs. Stubbs, we'll begin with you for the first round.

● (1230)

Mrs. Shannon Stubbs: Thanks, Chair.

Melissa, thanks for your testimony and for being here today.

I share your perspective that it is crucial to distinguish between the hosting and distribution of child sexual abuse material and of material and images that don't have the explicit consent of the people depicted in them.

I think you'd agree—or let me know if you do—that people have a right to own their own images and content that include them, and also the right to withdraw that if they so choose. This is the thing that I think all of us are grappling with—your very strong point about the Criminal Code already being in place and the laws and the regulations that already exist to provide these protections for children and for others who do not give their consent.

What do you make of what the actual problem is, then? What is the enforcement issue, the lack of enforcement and the lack of application of the existing law?

Ms. Melissa Lukings: I think the current issue is that perhaps the penalties that currently exist in PIPEDA are not strong enough to deter corporations. I'm not saying to put in new regulations—I'm not saying that—but when you're going to do the digital charter implementation act and you're discussing things like Bill C-10 and Bill C-11, it's important to remember that.

I think there is room for improvement. Because we've found that financial penalties don't really seem to impact companies that make a lot of money, fines could instead be based on percentages. The key here is that we need to not have increased regulation. If what we're trying to do is in fact what we say we're trying to do, which is to reduce human trafficking and harm to young people, additional regulations are not going to help that.

Did I answer your question?

Mrs. Shannon Stubbs: Yes.

On April 19 you mentioned a couple of possibilities related to the digital charter implementation act. You touched on the possibility of fines for companies that host and distribute already illegal content. The Minister of Heritage was just here, as you know, so I just wonder if there is.... I understand that you got cut off in your testimony last time, so I just want to see if there are any other details or recommendations you wanted to add in terms of that work.

Ms. Melissa Lukings: In terms of the digital charter implementation act?

Mrs. Shannon Stubbs: Yes.

Ms. Melissa Lukings: For corporations the question here is, how much responsibility do they have to have in order to cover their own selves from liability for negligence? That needs to be specified. It needs to be put in words.

Other than that, we really need to work on applying the laws that we have, so if there's something standing in the way of that and that can be remedied through the new digital charter implementation act, that should be discussed, absolutely. That is my recommendation.

Mrs. Shannon Stubbs: Thank you.

I wonder if, from your work experience and your lived experience, you might want to expand on the importance of verification and consent. If platforms ever do that without your consent or your agreement, what are the commercial consequences, or the personal consequences in the case of adults who are choosing freely to engage in this work?

Ms. Melissa Lukings: We're talking about what are the consequences if someone consensually uploads their own material?

Mrs. Shannon Stubbs: If an online platform were to host your material without an agreement with you or—

Ms. Melissa Lukings: That's intellectual property. That's a copyright issue right there. As a photographer, when you take photos, you have a model release form. These are all contractual issues that would arise. If someone doesn't have your permission to use the material, then that is a digital copyright infringement. That's an artistic thing. It's exactly the same as if someone were to host any artistic content anywhere without the permission of the artist. It's very similar to that.

Again, we have the Copyright Act for that.

● (1235)

Mrs. Shannon Stubbs: I think this is probably what's mind-boggling to many of us on this committee and probably many Canadians listening. A colleague said to me recently that, somehow, organizations like ag societies and school fundraisers and Legions are put through mountains of paperwork and administration to, say, play certain songs or use certain visual material. Then there are also online sites, say, that sell cannabis or alcohol, or host gambling, and in those two cases the country seems fairly effective at having a set of laws and bylaws and policies and regulations for these organizations [*Technical difficulty—Editor*] seem to manage to enforce and crack down on all of that being done illegally.

Ms. Melissa Lukings: Yes. It's magic.

Mrs. Shannon Stubbs: I would just give you the opportunity to expand on any other specific recommendations in terms of both the enforcement and protections to combat the proliferation of child sexual abuse material and other illegal content, while also maintaining free expression, privacy and the right of individuals to have ownership and choice over their own images.

The Chair: Thank you, Ms. Stubbs.

You are out of time. You're over time, but we will allow Ms. Lukings the opportunity to respond to that. I just wanted to note that we're moving into other folk's time.

Ms. Lukings.

Ms. Melissa Lukings: Thank you.

Privacy is very important, and it's also a safety issue in a lot of these situations. I can't provide any specific solutions. I'm not [*Technical difficulty—Editor*]. I definitely recommend asking Dr. Lashkari about that.

In terms of law, we need to remember the foundations of law, so what is the Privacy Act based on? What are the rights and freedoms that Canadians hold as important? Our rights to freedom of expression, freedom of association and all these things need to be considered when we're implementing new technology and new standards for technology.

As for specifics, that wouldn't be my area. I would be more like poking holes in why those things aren't private enough.

The Chair: Thank you.

Ms. Shanahan, we will turn to you.

Mrs. Brenda Shanahan (Châteauguay—Lacolle, Lib.): Thank you, Chair.

I am thankful that Ms. Lukings agreed to appear in front of us again today. It's very refreshing to hear you, and you will be a professor one day. Of that I have no doubt.

Ms. Lukings, your work is so important to help us have a better understanding—and your comments certainly attest to that—of all the issues that are arising from what was a very disturbing, and I think you and other witnesses said this, unfortunately very sensationalist article, which brought concern to people because, of course, no one wants to see child sexual abuse material on the web or non-consensual intimate images on the web.

However, there are perhaps unintended harmful consequences that can arise, particularly to adult professional sex workers, if we're not thoughtful about how we legislate in this area.

I believe I still have about five minutes remaining. Please use my remaining time to share those concerns with us, and if you want to bring in Professor Lashkari.... By the way, congratulations on the great series of articles the two of you are working on. They're very interesting.

Please, go ahead.

Ms. Melissa Lukings: To have meaningful consultations with people is really important. I would encourage the committee to review the submissions made by the Canadian Alliance for Sex Work Law Reform. They have done a lot of research in the area, and I'm really supportive of their efforts right now to challenge federally the criminal offences related to sex work, third parties and clients, material benefiting, advertising and all of these things.

They are an amazing resource. What makes them unique is that they are an umbrella organization that connects...I think it's over 20 or 30 different sex worker-led organizations all across the country. Everything is done through voting and from hearings with actual people who have lived experience in that area, so when you get data from this organization, it's solid data. I would really recommend consulting them.

Other than that, I would love to pass over the torch to Professor Lashkari.

● (1240)

The Chair: Professor, I just want to remind you to lift your mike when you're speaking. We found it a bit difficult to catch your words earlier with the translation, but if you would lift your mike I'm sure we will be able to hear you well.

Dr. Arash Habibi Lashkari: Thank you so much, and thank you, Ms. Lukings.

Actually, I can highlight this point. When we are looking to detect a person who is using this part of the network, from the Internet side it's completely impossible. Based on the three layers of encryption that we have, rolling up and backwarding to find a source is impossible. If we have access to the machines, from the user side we can monitor the behaviour of the user. We can detect who is using, for example, Tor connections, and with which software application for which purpose—for example, for audio, for a video call, for a chat or for uploading or downloading.

This is the key point that I think we need to consider. It is not possible, even if you have rules or regulations here in the law, to follow from the Internet to detect those guys. It's not possible, except, for example, for ISPs that are delivering Internet service in different cities or provinces. They can do some monitoring of the system that shows who is actually using this type of secure connection.

There is another concern, which is that we are not actually able to detect if they are going to work on the child pornography side. Maybe they are journalists who want to use this ability of anonymization and then deliver the voice or the sound; maybe they want to talk about something that maybe some governments have not given them permission for. This is the key point. We need to be careful [*Technical difficulty—Editor*] become law here, it should be clear. Can we recognize who is using this part of the super-secure or anonymized connection, for which purposes?

The key point is that, unfortunately, we cannot realize and detect it easily. It would need a huge amount of research. Maybe after five or, I don't know, 10 years, there will be some solutions we can use. At this moment, as I'm talking to you, there is no clear solution. We can detect the type of activity, but we just can't determine who is connecting to this network, for how many hours or which application they are going to use.

This is just an additional part that I would like to add to the point Ms. Lukings already highlighted.

Thank you, Mr. Chair.

The Chair: Thank you.

Mrs. Shanahan, do you have a follow-up question? You have 20 seconds.

Mrs. Brenda Shanahan: No. I'm happy to give the time to the next member. Thank you.

The Chair: Thanks so much.

Madame Gaudreau, we'll turn to you.

[*Translation*]

Ms. Marie-Hélène Gaudreau: Thank you, Mr. Chair.

Thank you, Ms. Shanahan.

I listened very carefully to our witnesses. My questions will be more geared towards Mr. DeBarber.

I gather that we must correct and improve a response and ensure that it's done properly. However, there are many challenges.

I was surprised to learn that, for 400 images, there can be 400 applications to purge, and that it may cost $2,000 for an automated removal and about $5,000 for a custom removal. So we're talking about money.

In terms of access to the individual, service providers must provide some modulation. However, we've just completely switched gears, since there must be access to the machine. I heard that very clearly.

Obviously, this is about consent, but it's also about identity. As committee members, our job is to protect people's identity. With respect to the surface web and the dark web, I was wondering whether the notion of consent and identification was straightforward. I can give myself another name or I can use a keyword, as Ms. Lukings said earlier. I'm concerned about this. That's my first question. I'd like to hear your thoughts on this, Mr. DeBarber.

I respect the notion of consent. We won't take away what people like. However, we want to make sure that non-consenting individuals, including minors, can't become victims. I'd like to hear your comments on this as well.

● (1245)

[*English*]

Mr. Charles DeBarber: I believe the first thing to say is a little about what I do.

I use the current technologies that automate copyright technology. I use these technologies to go out and help my victims get NCP that was put out there, whether it's revenge porn or something involved with human trafficking. I've been working very closely on the GirlsDoPorn situation over the years. More or less, I'm using some of the technologies there. I don't get 100% of it, but I can probably kill about 95% of it and probably get their name and content out of search engines. That's when some of it is archived in the deep web. Even then, every few years you have to go in to touch it up.

When a person tries to get a job, their name will get googled and that content will come up. I'm trying to liberate them from that. I'm trying to protect that social media, that digital footprint.

The other part of your question—

[*Translation*]

Ms. Marie-Hélène Gaudreau: Sorry to interrupt you, but I'm running out of time and I have two more questions.

Why do the RCMP's responses make the process cumbersome?

You said that non-consensual content can be removed. It's expensive and complicated, but it's possible.

As legislators, what do we need to fulfill our role?

[*English*]

Mr. Charles DeBarber: The process of doing this is costly, and it's really just stacked against victims. On top of that, it's stacked against free agent sex workers who are trying to protect their intellectual property.

There's a great Vice article that talks about a lot of OnlyFans folks. They can't do the same services studios can, so it pushes them towards a more exploitive studio structure.

We need to make those things more available. One thing we need to change, once again, is SEO and search engines in unverified content, specifically for upload sites. What I mean by an upload site is any site like Imgur, Pornhub or Xvideos, where I can go in, make an account and post anything I want. Those are not moderated the way—

[*Translation*]

Ms. Marie-Hélène Gaudreau: As you said, once the damage is done, the process of removing the content is extremely difficult. There are delays and uploads involved.

What do you think of the right to be forgotten that several countries use?

[*English*]

Mr. Charles DeBarber: I might be a little biased there, because I'm an intelligence analyst by trade.

You're asking somebody who goes and subversively finds information about privacy. Honestly, I'm for it. I like the EU's stance on it, to be honest. I'm very biased on that question.

What I would like to see, especially, is that this content doesn't get SEO unless it's verified, because that keeps it from going viral to the point where it costs thousands of dollars to go out there and find the thousands of websites it's on and try to get rid of it. If I can kill it in the crib or at least get it to where.... Your average victim, from my calculation, at least for revenge porn, doesn't know for seven to 90 days. If unverified accounts can post anything they want, then it becomes part of that feedback loop, and that's a big deal. It's as easy as making them turn web spiders off that web page. That's something Pornhub can do. It's something that they really should just be—

● (1250)

[*Translation*]

Ms. Marie-Hélène Gaudreau: At the end of the day, the entire international community must be aware of this new way of operating online. People, both young and old, must be informed. They must be warned. Certain measures must be implemented, including the process for accessing service providers and the web.

[*English*]

The Chair: You are out of time, Madam Gaudreau.

Thank you so much.

[*Translation*]

Ms. Marie-Hélène Gaudreau: Thank you.

[*English*]

The Chair: We're going to turn to Mr. Angus now for the next round of questions.

Mr. Angus.

Mr. Charlie Angus: Thank you so much to the witnesses. It's wonderful to have Madam Lukings back.

This committee does not have a mandate to look into sex work. We are the privacy committee. There's the women's committee, the justice committee. There are many, many important issues. We've heard many important issues here.

Our focus started out from that article that Madam Shanahan called “sensationalist”. It was a New York Times article with Serena Fleites.

She came to our committee, and she stated that she tried time and time again, as a 13-year-old, to take it down. Pornhub's executives told us they had no record and they weren't sure of when she contacted them.

Mr. DeBarber, in your experience, is that a credible answer, that Pornhub wouldn't have known about this video or known about efforts to have it taken down? Is it the dark net inside corporate headquarters?

Mr. Charles DeBarber: My honest answer is that I believe your victim, first off.

To share something just as seedy that happened, there is right now a criminal conviction for human sex trafficking surrounding the defunct site, GirlsDoPorn. It's infamous. There are a lot of great articles about it. I had clients who were even raped during the entire time. It's a horrifying situation.

They were a content partner for Pornhub. As early as 2016, at least from my records, they were already seeing statements from more than one Jane Doe about the process and what went down there, and they kept them as a partner, literally almost to the day of the civil judgment in 2019, where 40 Jane Does stood up.

I completely believe them.

Mr. Charlie Angus: They just didn't bother to track it.

Mr. Charles DeBarber: Well, I'll put it this way. That is a lot of data to track, in fairness, if I'm looking at it from the cybersecurity point of view. I can't tell you if they had the data or not; it all depends on how much they archive.

To be plain, I fully believe your victim. This is a company that I strongly believe has some heavy liability out there and should face consequences for it.

Mr. Charlie Angus: I want to ask you a question.

I've spoken off the record with many people who worked at Pornhub, former executives and that, who are concerned. They told me that the traffic in these child-abuse and sex-assault videos was actually fairly small, but said that their business model was copyright evasion. They work in the legal content from the producers, running it right up to the very day they have to do takedown, changing tags and putting it up again.

Is that a credible claim, do you think?

Mr. Charles DeBarber: I think much of their business model has been built on pirated information.

Once again, Samanatha Cole did a great article that talked about many OnlyFans folks getting ripped off and having their content spread out there, which once again pushes sex workers toward a very exploitative studio system and just eliminates free agency. On top of it, you have people who were paid for their content having it ripped and remixed and put on there. I would argue that the bulk of their content was pirated. They even forced folks to the table, and these studios to the table, to become content partners.

It's the same way that iTunes kind of forced the music industry to the table. They said, “People are going to take it anyway, so come here and we'll bring down the prices and drive down the wages in your industries. You'll get something out of it, at the very least. It's going to be pirated anyway, so what are you going to do about it?”

● (1255)

Mr. Charlie Angus: That's a very helpful perspective on this.

I'm running out of time.

Ms. Lukings, I was really struck by your referring to the Privacy Commissioner.

Our Privacy Commissioner put the run on Facebook. He chased Clearview.ai out. He is investigating Pornhub. We have a regulator that does this.

The Liberals want to put in another regulator, not the regulator they're going to have to have for Pornhub, but the regulator who is going to oversee the Privacy Commissioner's work—who actually does excellent work.

I just want to get your perspective on this. If we have the Privacy Commissioner, who's not afraid to take on the giants, dealing with this as an issue of corporate liability, and if we already have laws, do you think we need to have this other set of regulations and regulators to do the job that right now we believe the Privacy Commissioner is probably doing quite well?

Ms. Melissa Lukings: We don't need more regulations of surface web content. We don't. We just need to use the laws we have. We have a Privacy Commissioner, so let's have that person do their privacy commissioning and apply the laws we have. I don't think we need to add anything, and I absolutely do believe that adding in new regulations will put people at risk of exploitation and other types of harm and will push traffic onto anonymized networks.

We don't need more regulation. That's the opposite of what we need.

Mr. Charlie Angus: Thank you.

Mr. DeBarber, I'd like to go back to the issue of how these images are promoted and exploited and can be found in search engines. One of our survivors said that she has tried again and again and again to deal with police, to deal with anyone, to get her thumbnails and all that information. Even though the video has been taken down, it's still out there. It's still available.

Are there not simple tools we can apply so that when something is taken down, it's actually removed, so that we have the right of survivors not to be harassed by what's still there?

Mr. Charles DeBarber: Yes and no. It all depends on where it's hosted. It also depends on where you're getting it through. One, there's live content on other websites and other platforms, but then there's the stuff that's right in Google cache. Those are two different animals in terms of getting them purged. You actually have to purge both. Caching is more or less backing the information up. When you click on Google Images, for example, you're usually seeing the cache. When you get rid of the live content, you have to get rid of the cache too—fun fact.

Now, with some companies, like Google, lawyer Carrie Goldberg helped Google write its policy to remove NCP back in 2016, I believe. I'm glad that the rest of the big tech giants, including social media like Reddit and Twitter, emulated that process. The copyright process is still easier, unfortunately. Once again, if that image is repeated 100 times, let's say, then often 100 different notices have to get sent out. You have to do it in both the search engine and on there, but here's the rub—you can get it un-cached on Google, and delisted, but that doesn't get rid of the live content.

Here's one short answer: Give my contact information, please, and I'll help your client pro bono.

Mr. Charlie Angus: Okay. Thank you so much. I will make that contact. She deserved better.

Mr. Charles DeBarber: Was there a part of the question that I forgot, sir?

Mr. Charlie Angus: Our chair is going to get the hook and pull me off the line. I can keep asking more if he's not going to do that....

Mr. Charles DeBarber: Play me off, Sam.

The Chair: I hate to interrupt. I know there are always some good discussions and some good questions that could be answered.

To the witnesses, I certainly want to convey to you that we very much appreciate the fact that you took the time out of your day to bring compelling and informative testimony. Thanks so much.

Colleagues, we will now move to adjourn.

Thank you again to our witnesses.

The meeting is adjourned.