Office of the
Saskatchewan Information
and Privacy Commissioner

AI AND CHILD DIGITAL PRIVACY – PART 2 (JAN 26, 2026)

Grace Hesson David, Information and Privacy Commissioner, Saskatchewan

Diane Aldridge, Deputy Commissioner

Grace: In this podcast our office hopes to shed more light on the increasing privacy dangers connected to children and the use of artificial intelligence chatbots. We are going to focus on children's privacy issues and how parents can intervene to ensure the safe use of AI chatbots. Some recent cases out of the United States disclose that the developing technology of AI chatbots have become quite dangerous for children and young people who have turned to the bots as a friendly source of information and company. Its when the inspiration and informational aspect of the chatbot turns into advice or direction – a deadly direction in some cases – that parents need to know and intervene. Diane – can you define "chatbot" for us?

Diane: In essence, Google is a chatbot – you can ask it questions, it will search the internet and it will give you a quick answer. You may wonder how some of the new AI chatbots differ from Mr. Google? The difference is the interface. Chatbots can interact with their user in various ways. Children can create a cartoon character or an adorable animal that interact with them in a cute voice or send them texts that answer their questions. Young adults will interact differently with a chatbot but the bottom line is that whatever chatbot that is used – it will offer a single synthesized conversational answer based on the large language model that it works from – usually the totality of the internet. But how can these developing new chatbots affect the privacy of children and young people?

Grace: There are cases coming out of the United States that show some chatbots start off as providing answers and company for lonely children or young adults who have issues that they do not feel comfortable addressing with an adult. Several lawsuits filed in the United States during the past year alleged that an AI chatbot platform called "Character AI" affected young people in a very similar and disturbing way. These lawsuits were joined and settled out of court on January 13th, 2026. As an example, 13 year old Juliana Peralta committed suicide in 2024. Her parents believed that they took an active role in monitoring their daughter's life online and off - but instead they discovered that her conversations with a Character AI chatbot had become more than just a comfortable friend. It had morphed into a romantic relationship that had begun to send her sexually explicit content in the weeks leading up to her death. Diane – how is this even possible?

Diane: Up to this point, most parents have not been concerned when their children download and engage with AI apps on their phones. Most chatbots guarantee that they are safe for kids 12 and up and they are desirable because they can be downloaded for free. These apps offer immersive and creative outlets for children to create characters that they enjoy interacting with and the characters that are offered for children to choose include historical figures, cartoon figures, celebrities, talking animals and anything you can imagine that a child might like to engage. These AI powered characters then begin a relationship with the child. The issue with these platforms is that there are no regulatory or ethical bodies to monitor the development and interactions of the chatbots with children and at the end of the day – this role must fall on the shoulders of the parents.

Grace: In young Juliana's case, her parents thought that she was texting her school friends but in fact, most of her interactions were with the chatbot. This was only learned after her death and when her phone was examined by a forensic expert. Juliana's parents alleged in the lawsuit that the chatbot became dangerously addictive to their daughter and as her interactions progressed with the bot, the conversations became more and more sexually explicit. Another lawsuit filed in the State of Florida alleged that a 14 year old boy was coached on how he could commit suicide after

lengthy conversations with an AI chatbot. This boy had created a "Game of Thrones" character that he related to and with whom he felt comfortable interacting. The real issue is two-fold: first parents are not armed with sufficient knowledge of the capabilities of AI technology and what it can and cannot do and secondly, the privacy rights of children who engage with this technology are being manifestly abused. We ask some relevant albeit rhetorical questions: Can children interact with this technology in the first place? Do children or even young adults possess the skills to deal with a technology that is so advanced that it cannot itself discern between right and wrong? Can children be left alone with this technology? And what about the parties that produce this technology – what role are they playing in the development of such dangerous interactive options that is marketed towards children and young people?

Diane: In Canada the Federal Privacy Commissioner has taken a momentous stand in an effort to monitor and control this technology. On January 15th the Privacy Commissioner of Canada, Philippe Dufresne, announced that he was expanding his current investigation into X Corp which operates the social media platform X. The focus of this investigation will reflect directly on the privacy rights of children and adults online. Our federal Commissioner will especially examine the AI version of X which is known as "Grok". A complaint was recently filed with the federal Commissioner that Grok has spontaneously created and shared explicit sexual images of individuals without their consent. The federal Commissioner noted that personal information has been used to create deepfakes including explicit content. The concern is that this information may be disseminated online in violation of the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). Deepfakes can use the images of children and can possibly aid in the production of child pornography when the technology is in the wrong hands. Grace, can you explain what a deepfake is?

Grace: I do not need to define this term because our Canadian courts have already done so. In *R v Larouche,* 2023 QCCQ 1853, Justice Gagnon of the Quebec Superior Court found that the 60 year old accused had created sexual deepfakes of children using

AI and included them in his collection of real child pornography. This individual was convicted of making, possessing and distributing child pornography. Justice Gagnon explained the process behind making a deepfake and in so doing, he explained what a deepfake is in paragraphs 62 to 66 of that ruling:

> [62] When the police searched the offender's home, they noted that some files appeared different from a series of photographs they had seen in the past. They noticed some anomalies in the quality of the image. They decided to analyze this series further at the laboratory to verify their theory that these files had been modified or altered.
>
> [63] After analyzing it, the investigators discovered software to create deepfakes and a user manual among the computer equipment seized at the offender's home. The investigators decided to download the software to better understand its features. The everyday person clearly cannot use this software's features. Using it requires computer skills and a significant investment in time.
>
> [64] To create a successful deepfake, a user must have source material and destination material. This can be done using a bank of photographs or video clips. For example, it takes between 3,000 and 8,000 photographs of the same face to create a sufficient source file to export a face onto the body of another person. The software sequences a video excerpt image by image to obtain a bank sufficient to create a minimally realistic deepfake.
>
> [65] Once the database is sufficiently complete, the software tries to teach the artificial intelligence to take into account the different facial features on each photograph: angle of the face, position of the eyes, lips, ears, etc. to mimic the source face's movements. Teaching requires considerable technological means and a number of hours of work that is difficult to quantify other than to say it is particularly long. The longer it takes, the better the result because the artificial intelligence has learned that much more. Note that deepfakes can be created using the same medium (video to video) or different media (photograph to video and vice versa).
>
> [66] The offender created several deepfake photographs and videos. While it is clear that there was an evolution in the offender's ability to create deepfake images, some results are of an exceptional visual quality. It is impossible to separate the real from the fake. Had the investigators not been familiar with the known child pornography, the "media library", it would have been impossible to know whether a photograph was a deepfake or the real thing. The police have clearly entered a new era of cybercrime.

Diane: Justice Gagnon was talking about creating a deepfake AI video in that excerpt you read above Grace – and clearly an offender needs thousands of photographs in order

to completely transform the image of a person onto a video of another individual. But when it comes to photographs – it is a much simpler matter. In her October 2024 article for the McGill Law Journal, Professor Dunn of the Schulich School of Law at Dalhousie University noted that non-consensual synthetic intimate images (i.e. intimate photographs) often are produced by means of AI technology or even Photoshop.[1] For this kind of image manipulation, only one photograph of a child is needed. Face-swapping technology is a very simple form of abuse and when children are online and interacting with others on a chat group, photographs can be traded either on a chat group or on Snapchat. Children may think that just because a photograph disappears quickly on Snapchat that it is gone forever. But it is not. And if the person they are interacting with is not a child of the same age but an adult offender who has spent months grooming the child and speaking with the child and now knows the child's friends – the scenario can lead to very disturbing results. Sextortion is now a new crime but still prosecuted under the Criminal Code section of extortion, section 346(1) in the Criminal Code. Sextortion occurs when a child has voluntarily provided a photograph of themselves to someone they think is a friend and the friend is an offender who has cropped the child's head off the photograph and swapped it onto the photo of a nude child or a child in a sexually explicit pose. The offender then bullies the victim and demands money or other favours in exchange for a promise that the photograph will not be sent to the child's parents or circle of friends or even published on the internet for all to see. In situations such as this, the emotional trauma to the child can be enormous and can involve the child isolating, becoming withdrawn and depressed and losing the ability to trust.[2]

Grace: Parental and legal intervention is crucial. In *R v Legault*, 2024 BCPC 29, Judge Patterson of the British Columbia Provincial Court sentenced an offender to a two

[1] Dunn, S. "Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI", (2024) 69:4 McGill Law Journal, 395 to 416

[2] Final Report to the AI Strategy Task Force, Professor Taylor Owen, January 22, 2026.

years less a day conditional sentence and two years probation for catfishing victims online, making child pornography (i.e. using technology to make deepfake images), possessing child pornography and internet stalking. "Catfishing" means the online trolling by a predatory adult, usually for sexual purposes, of vulnerable children and victims.[3] Judge Patterson noted that such crimes involve a breach of trust and the intentional infliction of emotional and psychological harm. The offender in this case was a 30 year old Baptist pastor who used his position to catfish his victims online after having gained their trust. In one photograph the offender had "nudified" the image of one of his victims, a teenaged girl, by using an app called "DeepNude". We further note the observations of Justice Fitzpatrick of the Ontario Superior Court in *R v Joaquim*, 2025 ONSC 6643, who sentenced an adult to 18 months of custodial time followed by three years' probation for possessing child pornography and accessing child pornography. At paragraph 18 of his reasons, Justice Fitzpatrick conveyed that the use of deepfake imagery involves an absolute violation of privacy and breach of trust. He said:

> [18] The case here is possessing and accessing child pornography. In my view, there has been a tendency in the past to see this as kind of a victimless crime, because the victims are never "live" before the Court and the material, appearing on a screen, makes it feel like no real person is involved. Today, at a time of internet deepfakes and AI generated porn, I can see a kind of numbness setting in to this kind of activity. I have no expert evidence on this application concerning the societal wide impact of child pornography. However, I have my experience as a community member, as a member of the judiciary who has attended continuing legal education concerning the issue and a consumer of news and other broadly disseminated information which over a broad expanse of time gives me a sense of community opinion about this issue. In my view, what Mr. Joaquim did was very very serious.

So while legal intervention is critical what else can we be doing to protect the privacy of our children Diane?

---

[3] See also the definition of "catfishing" in *R v Collinge,* 2025 ONCJ 99 at paragraph [31].

Diane: The Canadian Centre for Child Protection has many resources for concerned parents and children alike on the issue of deepfakes, sextortion and the online catfishing of children. We have included a link to this organization in the transcript of this podcast that follows. This wonderful group has many options for concerned parents to educate them and to facilitate the education of their children with respect to the dangers that are prevalent online. They offer proactive training models for parents to help parents and guardians educate children and to increase their awareness with respect to the violations of privacy that may occur online. There are also portals that can be accessed that will teach parents and guardians how to keep kids safe in this internet and online world. We encourage our patrons to visit this site and learn about the dangers of online luring, sextortion and AI deepfakes further.

That is it for today and we thank you for attendance at this podcast and we hope it assists in your efforts to keep our children safe from privacy violations.

References:

Privacy Commissioner of Canada New Release, Investigation of "Grok": https://www.priv.gc.ca/en/opc-news/news-and-announcements/2025/nr-c_250227/

"Mom thought her daughter was texting friends before suicide: It was an AI chatbot" CBS news (January 8, 2026): https://www.cbsnews.com/news/parents-allege-harmful-character-ai-chatbot-content-60-minutes/

Canadian Centre for Child Protection: https://www.protectchildren.ca/en/

Dunn, S. "Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI", (2024) 69:4 McGill Law Journal, 395 to 416

Report submitted to the federal Minister of AI and Digital Innovation: Final Report to the AI Strategy Task Force, Professor Taylor Owen, January 22, 2026.