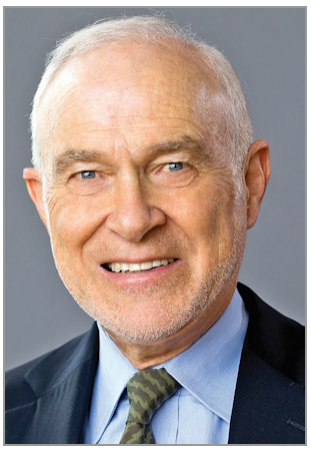
LAW360® Canada

Law360 Canada | 2 Sheppard Avenue East, Box 54 | Toronto, Ontario, M2N 5Y7 Canada | www.law360.ca
Phone: (800) 668-6481 | customerservice@lexisnexis.ca

OPC's Grok deepfake investigation points to the need for privacy and online harms reform

By **David Young**

Law360 Canada (June 19, 2026, 11:50 AM EDT) -- In an investigation report released on June 11, the federal Office of the Privacy Commissioner (OPC) found that the AI chatbot Grok, a feature offered to users of X, the social media platform (formerly Twitter), breached the current privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), by creating sexualized artificial images of real people, in particular women and children, without their consent.



David Young

Like all chatbots, Grok can create content, answer questions and generate images. The controversial feature that Grok provided was its ability to create deepfake sexualized images of individuals without their knowledge or consent and, potentially, post those images online.

Deagreez: ISTOCKPHOTO.COM

Grok had argued that it was the X user, not it, who was responsible for obtaining such consent and furthermore that the generation of such images was not a commercial activity and therefore outside the scope of PIPEDA. The OPC rejected these contentions, concluding that it was Grok, not the user, that collected the information and that this collection did constitute a commercial activity of Grok.

Grok argued that they are not responsible for obtaining consent from individuals that appear in sexualized deepfakes because users bear primary responsibility for the content they generate. Furthermore, it argued that where a user instructs Grok to generate images that are subsequently posted on the platform, any collection or use of personal information for the purpose of generating and sharing that content is determined solely by the user. In essence, Grok was arguing that it was an agent providing a service to the user, on their behalf, and that it was not responsible for the user's actions.

Grok further argued that the use of its image creation tool was for the personal or artistic purposes of the user — not for its, Grok's, commercial purposes — and Grok therefore was not required to obtain consent for the creation of such deepfakes.

The OPC disagreed with Grok's arguments. The OPC referred to Grok's privacy policy, which stated that, with a view to providing its service, Grok may collect personal information directly from users, whether it is the user's personal information or not, and that user content may include prompts and other inputted content such as images, audio, video and other materials as well as Grok's outputs. The OPC concluded therefore that in its own materials, Grok acknowledged its collection of such information. Furthermore, while users provide the prompts and images on the basis of which Grok generates sexualized deepfakes, it is ultimately Grok that collects this information and enables their use for the purpose of generating this content, via a tool that it developed and which it makes accessible to users of its platforms in the course of a commercial activity — all of which brings it within the purview of PIPEDA's application.

The conclusions in the OPC report, which are not exceptional, make clear that any personal information, whether available on a public medium like the internet or privately, is protected by privacy law unless consent to use it has been obtained, or it falls within the — to date — limited categories of publicly available information exempted from the law. However, they have particular significance in the context of government's tabling of two bills over the past week that address not only reform of the privacy law but also protection against online harms, including deepfakes.

In issuing the OPC's report, the privacy commissioner lamented his inability either to force Grok to comply with the platform governance recommendations contained in the report or impose any financial penalty on Grok. Under Bill C-36, tabled this past Monday — enacting the new reformed privacy law, the *Protecting Privacy and Consumer Data Act* — the proposed new regulator, the Digital Safety and Data Protection Commission of Canada, will have the power not only to issue mandatory compliance orders but also to impose significant fines — of up to $10 million or three per cent of an organization's worldwide gross revenues.

However, potentially even more significant are the proposed new rules for platform governance for social media platforms and chatbots under the government's proposed revised online harms law — Bill C-34, the *Safe Social Media Act*.

Notwithstanding its being touted as the vehicle for imposing a social media ban, significantly, Bill C-34 provides for the institution of platform governance rules for both social media sites and chatbots. This framework will require, for example, for all regulated platforms to have a "digital safety plan" addressing measures to mitigate risks of exposure to harmful content including deepfakes and the adoption of design features for protecting against such harms in particular for youth.

In responding to the OPC's investigation, Grok, notwithstanding acknowledging that it did not obtain consent of persons whose images were modified, submitted that it had in place platform governance procedures to protect against the generation and posting of non-consensual sexualized deepfake images. Its procedures included measures such as privacy impact assessments, policies addressing mitigation of risks associated with such posting, mechanisms for reporting and addressing incidents of potential harmful content, and a framework for the review and taking down harmful content. Grok also submitted that users must comply with its Acceptable Use Policy, which explicitly prohibits the sexualization and exploitation of children and stipulates that whenever violative content is detected, it is taken down and enforcement measures are taken, including potentially reporting the user to law enforcement. Grok also represented that it has implemented content filtering and moderation protocols that check for keywords such as "child," and refer to national databases of missing and exploited children.

However, the OPC determined that Grok's internal governance procedures clearly were insufficient to prevent the widespread generation of non-consensual sexualized deepfake images that were observed and which the OPC was now investigating. In sum, it found that Grok had developed and deployed the deepfake imaging feature without properly assessing the risks or implementing sufficient safeguards.

A key takeaway that can be drawn from the OPC's Grok investigation is not that Grok breached the privacy law — which is consistent with previous OPC findings under PIPEDA — but that this AI-generating platform failed to comply with appropriate community standards for safe platform governance. It may be surmised that if the government's proposed *Digital Safety Act* had been in place, Grok would have been required to institute protocols in compliance with such standards, which could have obviated the need, after the fact, to rely on privacy law for remedy.

David Young is principal at David Young Law, a privacy and regulatory counsel practice in Toronto.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the author's firm, its clients, LexisNexis Canada, Law360 Canada or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

Interested in writing for us? To learn more about how you can add your voice to Law360 Canada, contact Analysis Editor Richard Skinulis at Richard.Skinulis@lexisnexis.ca or call 437-828-6772.
