

COMPLIANCE WEEK

FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE

U.K. regulators move to curb AI nudification tools as scrutiny of Grok grows



By Neil Hodge | Wed, Jan 14, 2026 11:26 PM

The U.K. government's spat with Big Tech owner Elon Musk over the more risque capabilities of X's AI assistant Grok has exposed more cracks than the chatbot was ever meant to.

The political furor caused by Grok's ability to transform fully-clothed people into realistic, naked renditions of themselves has raised serious questions about what steps tech firms should take to remove such content, as well as prevent it from ever happening in the first place: after all, wasn't AI meant to be more than this?

Following widespread concerns over Grok's capabilities and use of personal data, as well as Musk's reluctance to act, the U.K. government has said it will quickly introduce further legislation that will make it illegal to create non-consensual intimate images, as well as make it illegal to supply online tools used to create such images. British Prime Minister Sir Keir Starmer has also warned X that it could lose the "right to self-regulate", adding that "if X cannot control Grok, we will."

The government has said it will add provisions to the Crime and Policing Bill—which is currently going through the House of Lords for review—to criminalize nudification apps.

Currently, X's Grok service has not been suspended in the U.K.: only Malaysia and Indonesia have so far done so, though many other countries have criticized it, including Australia, which in December banned under 16-year olds from having social media accounts.

The U.K.'s media regulator Ofcom, which oversees compliance with the U.K.'s Online Safety Act, announced on January 12 it was launching an investigation into X over "deeply

concerning reports" that Grok was being used to create and share non-consensual sexualized images of people—including children—which could constitute pornography or child sexual abuse material.

Under the Online Safety Act, sharing images—or even threatening to share them—is a criminal offense, both for individuals and for social media platforms. The Data (Use and Access) Act, passed last year, made it a criminal offense to create, or request the creation of, non-consensual intimate images.

Ofcom first contacted X with its concerns on January 5, and by January 9 (the deadline), the regulator decided to launch a full investigation. No timeline has been set, but Liz Kendall, Secretary of State for Science, Innovation and Technology, has said it "must not take months and months."

Meanwhile, X has been slammed by U.K. lawmakers for failing to take action quickly or to recognize and follow best practice compliance. The tech platform's initial response was simply to warn that "anyone using or prompting Grok to make illegal content will suffer the same consequences as if they upload illegal content." It then tried to offset any concerns by limiting Grok's image creation function to paid subscribers only—a move Kendall slammed as "monetizing abuse" and "insulting to victims."

Musk, in turn, criticized U.K. moves to ban the service as "any excuse for censorship" and later posted an image of Starmer in a bikini. In a statement to Parliament on January 14, the Prime Minister said that he had been "informed that X is acting to ensure full compliance with U.K. law." X followed that announcement by saying it has "implemented technological measures to prevent Grok from allowing the editing of images of real people in revealing clothing such as bikinis." The ban applies to all users, though only "in those jurisdictions where it's illegal."

But Ofcom's investigation continues, and if the regulator finds that X has broken the law, it can fine the tech firm up to £18 million (\$24 million) or 10% of its global revenues (whichever is greater). The regulator can also require it to take specific steps to ensure compliance or to remedy harm caused by its breach of the rules. In the most serious cases of ongoing non-compliance, Ofcom can seek "business disruption measures" through which a U.K. court could impose an order on an interim or full-time basis to require payment providers or advertisers to withdraw their services from X, or force

internet service providers to block U.K. access to the site altogether.

However, there are concerns that Ofcom might be unable to use these powers in this case. Dame Chi Onwurah, chairwoman of Parliament's innovation and technology committee, has written to Kendal for clarification, citing concerns that the Online Safety Act does not explicitly cover generative AI and online harm in the same way as it does with internet platforms directly. She has also questioned how enforcement would work in practice, especially since the legislation only requires platforms to remove harmful content, but does not make it an offense to create non-consensual intimate images using an AI platform (providing they are not shared). While the Data Act—which came into effect last year—will do this, “the relevant section of the Act does not appear to have been fully implemented yet,” she added.

The government has said that it will now expedite those relevant provisions of the Act.

Caroline Dinenage, chairwoman of Parliament's culture, media and sport committee, likewise told the BBC she had a “real fear that there is a gap in the regulation”, adding that “there are doubts as to whether the Online Safety Act actually has the power to regulate functionality—that means generative AI’s ability to nudify someone’s image.”

Lawyers also believe U.K. regulation has its limits. Emma Wright, partner, privacy and cybersecurity, at law firm Crowell & Moring, said the U.K.’s online safety legislation does not specifically mention “AI products” which “is arguably what Grok would fall into,” meaning it is “probably the best example of how even our current and recent legislation may not be fit for purpose when dealing with AI and emerging technology.”

Nicola Finnerty, criminal litigation partner at law firm Kingsley Napley, said that the U.K. Data Act “was never designed to police harmful or illegal AI-generated content, so the fact that much of it has yet to come into force is ultimately irrelevant”. Its purpose, she said, is to modernize data governance, “but it doesn’t give regulators the tools to stop platforms generating or circulating abusive imagery.”

Even the Online Safety Act, which Finnerty said provides clear and immediate powers to tackle illegal content (including intimate-image abuse and child sexual exploitation), may not be specific enough as AI-generated imagery increasingly becomes more sophisticated. She believes “there is a real case for targeted legislation which goes

beyond the Online Safety Act to explicitly regulate the AI systems which produce the content."

James Clark, data protection, AI, and digital regulation partner at law firm Spencer West, believes U.K. legislation may be targeting the wrong people. "While the Data Act criminalizes the individual creator, there is a growing consensus that the law needs to target the source—namely, tools such as Grok. The Online Safety Act places a duty of care on the platform, such as X, to monitor for and take down unlawful content, but there is a growing feeling that additional rules might be required to criminalize the supply of nudification tools."

However, Clark warned that rushing legislation into force could stifle future AI innovation, while the fact that many developers are based overseas could make enforcement tricky. He added that creating more legislation could put the U.K.'s principles-based approach to regulation at risk.

The sorry episode has revealed many weaknesses around AI regulation, enforcement, and compliance. Chiefly, U.K. regulations brought in only last year to provide adults and children alike with better protection from potential harm do not appear to specifically address AI-generated "deepfake" images (or at least not yet). As a result, potential loopholes in the legislation also make it hard for regulators to act tough—even if, on paper at least, they have the powers to do so.

Perhaps more dispiritingly, despite nearly eight years of the General Data Protection Regulation (GDPR), the launch of Europe's landmark AI Act that prioritizes risk of harm, and widespread concerns globally about safeguarding children on the internet, one of the biggest tech firms in the world has not only given the greenlight to an AI tool that can create fake naked images of minors, but has also defended the practice as free speech.

RATE THIS RESOURCE

Select your rating



MORE FROM NEIL HODGE



Experts outline core skills compliance teams need to develop in 2026



U.K. sets out strategy to combat bribery and corruption



FCA indicates path for future crypto regulation