



By: Tomorrow's Affairs Staff

# The deepfake scandal that revealed the boundaries of the AI industry



In mid-January, New York's courts became the stage for an unexpected conflict that combined personal drama with profound questions about the future of artificial intelligence.

Ashley St. Clair, a conservative influencer and mother of Musk's son Romulus, filed a lawsuit against xAI (Elon Musk's artificial intelligence development company), accusing its product Grok (an AI chatbot capable of generating and processing images) of enabling the creation and distribution of sexually explicit deepfake photos without her consent.

The lawsuit was first filed on 15 January in New York State Court (New York County Supreme Court, Manhattan). xAI then exercised the legal right available to every defendant in the US to transfer the case from state to federal court, citing interstate jurisdiction and the nature of the dispute.

Thus, the proceedings are not suspended or weakened but are instead conducted before the federal court in New York.

In parallel, xAI filed a separate lawsuit against Ashley St. Clair in federal court in the Northern District of Texas on the same day, arguing that the platform use agreement required the dispute to be based in Texas. It is for the judges, not the company, to decide which court will ultimately have jurisdiction.

This case is not merely a personal dispute between former partners; it exposes systemic weaknesses in the approach Musk has advocated for years – maximum freedom in the development of AI technologies with minimal restrictions.

Although the allegations in the lawsuit are extremely serious, including claims that artificial intelligence was used to sexualise and humiliate a person when she was a minor, this case goes beyond a personal tragedy and the criminal dimension of the abuse.

It raises the question of the systemic responsibilities of technology companies and demonstrates how inadequate existing models

of self-regulation are at a time when generative AI can produce content on a massive scale that directly threatens the dignity, security, and rights of individuals.

## Lawsuit claims failure to stop AI-generated abuse

Ashley St. Clair is described in media reports as a 27-year-old author and political strategist, active on the X platform.

Her having a child with Musk did not become public knowledge until 2025, following posts on the X network and subsequent media confirmation of the child and the name Romulus.

However, the lawsuit does not address the personal relationship but directly claims that Grok enabled the generation of degrading images at the request of X platform users.

**St. Clair claims that she repeatedly requested content removal and protection, but instead of effective protection, she experienced "retribution" on the platform**

According to court filings, users took actual photos of St. Clair – including photographs from when she was a minor – and asked Grok to modify them into sexualised or degrading images.

It is claimed that the generated photos were convincing enough to appear authentic. One of the most controversial examples cited in media summaries of the lawsuit involves a display with offensive Nazi symbols, which the lawsuit describes as intentional humiliation, with the added element that St. Clair is Jewish.

St. Clair claims that she repeatedly requested content removal and protection, but instead of effective protection, she experienced "retribution" on the platform itself through the

cancellation of premium features and verification, which affected the monetisation of her account, while the content in question continued to appear.

## xAI faces growing regulatory pressure

Deepfake technology, which uses generative AI models to create fake but realistic images or videos, is not new.

However, Grok differs from its competitors in its publicly promoted philosophy: fewer "restrictions" and more provocative content, with the narrative that the user receives a "less filtered" version of the answer.

That freedom brought xAI rapid growth in attention and use but also a wave of criticism in late 2025 and early 2026, when regulatory bodies and the media increasingly recorded cases of non-consensual sexualised depictions of women and, in some reports, minors.

### Indonesia temporarily denied access to Grok, and Malaysia also restricted or blocked access

The xAI response was gradual and, by all accounts, externally pressured. At the beginning of January, the company limited the generation and editing of images so that some functions were linked to a subscription and then announced that additional restrictions were being introduced on the editing of images of real people.

In parallel, some countries responded with **blockades**: Indonesia temporarily denied access to Grok, and Malaysia also restricted or blocked access, with announcements of legal steps by regulators.

**California Attorney General** Rob Bonta opened an investigation on 14 January and on 16 January sent a cease-and-desist letter to xAI, demanding that it immediately cease the creation and distribution of illegal, non-

consensual intimate deepfake content.

This is a decisive moment because it does not come from tabloids or political commentary but from the institutional framework of a state where the technology industry is concentrated and where sensitive privacy and identity protection standards have been the subject of judicial practice for years.

## From free speech to liability

The media's focus on Elon Musk diverts attention from a key issue: institutional responsibility for the misuse of generative artificial intelligence.

At a time when the United States is striving to maintain its lead in the AI race against China, such scandals undermine confidence in American innovators and pave the way for stricter regulation.

Beijing can always claim that "control prevents chaos"—even when that control serves as oversight and political discipline.

Washington faces a paradox: too much freedom leads to chaos that necessitates regulation, but regulation, if imposed too harshly or broadly, can stifle innovation.

### "Freedom without brakes" is no longer just an internal American debate but becomes a security issue

The St. Clair lawsuit comes as the US Senate pushes for a legal response to the surge in sexual deepfake content.

In January, the Senate passed the **DEFIANCE Act**, a proposal that strengthens the basis for civil lawsuits by victims of non-consensual sexually explicit "digital fakes," making it easier to hold creators and distributors of such content accountable.

If the judicial trend moves towards broader

liability for platforms and producers of generative systems, it could trigger a wave of similar proceedings against more actors, not just xAI.

In the broader security context, deepfake technology is already transforming information operations: identity falsification, compromise, blackmail, and erosion of trust are becoming cheaper and faster.

In this context, "freedom without brakes" is no longer just an internal American debate but becomes a security issue.

A model defended as "anti-censorship" can be turned into infrastructure for attacking its own society, as the most harmful content crosses borders fastest and remains in circulation longest.

## A shift towards stricter AI oversight

The outlook is not optimistic for xAI. Even if the company wins procedural battles, such as disputes over jurisdiction, the reputational damage is already evident in regulatory backlash, access blocks, and institutional actions such as the California investigation and formal cease-and-desist order.



*The outlook is not optimistic for xAI - Elon Musk*

Investors who have committed large sums to xAI may become more cautious about the risk of escalating lawsuits and compliance costs. Grok may need to implement more rigorous safeguards, which could lead to a loss of its

original identity.

This creates opportunities for competitors who have invested in protection mechanisms from the outset, even at the cost of slower expansion.

In the long term, this case may accelerate transatlantic coordination. The **European Union** is already implementing the phased application of the **AI Act**: the act entered into force on 1 August 2024; prohibitions and obligations regarding AI literacy apply from 2 February 2025; rules and obligations for general-purpose models (GPAI) apply from 2 August 2025; and the law becomes fully applicable on 2 August 2026 (with longer transitional periods for certain categories of high-risk systems).

The United States, traditionally supportive of market freedom, may be pushed towards a more similar regime precisely because cases show that harm is occurring faster than platforms can respond.

As artificial intelligence becomes an integral part of daily life, the case of Ashley St. Clair is a reminder that technological progress cannot be separated from responsibility.

Without balance, freedom becomes chaos, and innovation turns into a tool for humiliation and abuse. For security and stability, the lesson is clear: control over AI will not emerge on its own – if systems and rules do not establish it, courts and regulatory bodies will, under pressure from scandals.