

Why Generative AI's imitation game should worry enterprise leaders

Recent controversies around AI-generated art and content aren't just creative debates — they signal deeper, enterprise-level risks.

Generative AI models are trained on massive, often opaque datasets scraped from the web, including code libraries, corporate communications, brand voice, UX/UI patterns, and proprietary frameworks.



Businesses may face legal, reputational, operational, and cyber security threats when they deploy Gen AI tools trained on unlicensed or opaque data.

The Ghibli-style AI backlash¹



The "AI Ghibli" trend went viral but soon sparked controversy. While many used the tool for personal portraits and memes, others have generated unsettling and violent content, including disturbing depictions of historical tragedies.

While the backlash may seem aimed at individual creators, it's a reputational minefield for brands, platforms, and artists, as misused artistic styles can spark ethical concerns and public criticism by association.

Getty Images vs. Stability AI²

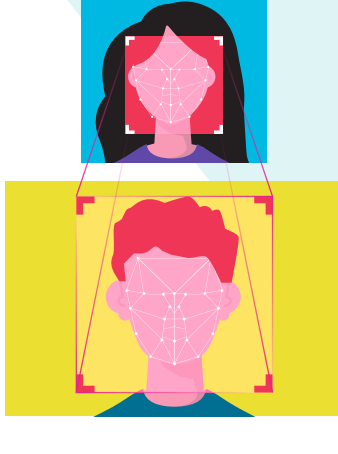
This case marks a watershed moment in enterprise AI, highlighting how training Gen AI on copyrighted data, without transparency or consent, can expose businesses to mass IP litigation, reputational risk, and legal uncertainty.



Deepfakes and Gen AI³

In January 2024, a Hong Kong-based employee transferred **US\$25 million** to fraudsters after being convinced during a video call with her CFO and colleagues.³

It turns out, the CFO and colleagues weren't on the call at all — the criminals used deepfake technology to manipulate the employee, highlighting the terrifying potential of deepfakes and generative AI to manipulate and deceive at scale.



By 2027, generative AI could drive fraud losses in the U.S. to a staggering **US\$40 billion**, up from US\$12.3 billion in 2023 — a **32% compound annual growth rate**.³

6 hidden risks of using unethical Gen AI

Enterprises adopting Gen AI tools built on unlicensed or opaque data sources face more than innovation challenges⁴:

 Legal exposure	 Brand integrity risk	 Reputational fallout
 Privacy violations	 Cyber security vulnerabilities	 Operational disruptions

Top enterprise use cases for Gen AI⁵

Gen AI is powering innovation across industries, but not all use cases carry the same risks.

- **Customer experience & chatbots**
Businesses use AI chatbots for customer onboarding, technical support, and product troubleshooting.
- **Predictive analytics & fraud detection**
Manufacturers use predictive analytics to forecast equipment failures, optimise maintenance schedules, and detect anomalies in supply chain operations.
- **Marketing automation & content generation**
Retailers automate product descriptions, promotions, and targeted ad campaigns.
- **Internal knowledge bases**
Healthcare organisations build internal AI knowledge bases for clinical research, compliance, and operational efficiency.

Where style theft creeps in: marketing and content generation

Unlike other use cases, marketing-related Gen AI outputs can unintentionally copy the tone, style, or creative identity of others. When trained on broad, unvetted datasets, these systems may cross ethical or legal boundaries.

**Brand mimicry in campaigns**

A retail brand uses Gen AI to generate visuals and taglines for a new launch. The output mirrors the visual style and messaging tone of a competing brand.

Risk: Brand confusion, legal exposure

**Influencer voice & persona cloning**

Social media team tasked with boosting engagement uses Gen AI for their campaign. The output mimics the voice of a well-known industry figure.

Risk: Reputation damage, potential lawsuits

**Thought leadership with a familiar voice**

A B2B marketing team uses Gen AI to produce blog posts and reports, but the tone, structure, and metaphors closely align with those of a competitor's published work.

Risk: Loss of authenticity and credibility; potential plagiarism accusations

Strategic moves for enterprise leaders

Modern enterprises need to shift from "Can we use Gen AI?" to "Can we use it responsibly?" That's why responsible Gen AI usage must be anchored in operational governance and clear accountability mechanisms.

**1 Data provenance**

Ensure training data is licensed, transparent, and compliant. Verify vendors to avoid IP infringement.

**2 Explainability and auditability**

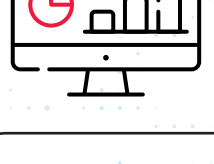
Mandate that AI outputs must be traceable and decisions explainable. Implement audit trails for compliance and accountability.

**3 Role-based access and model control**

Restrict who can prompt, modify, or retrain AI models to prevent shadow AI, data leaks, and rogue activities.

**4 Model risk scoring and vendor assessment**

Evaluate Gen AI models for legal, business, and security risks. Build a vendor framework focused on data transparency, bias control, and resilience.

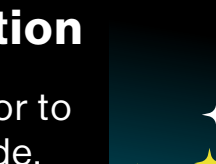
**5 Continuous monitoring and incident response**

Monitor in real time for output drift, style mimicry, and policy breaches. Set up clear escalation protocols for suspected infringement or compliance breaches.

**6 Governance alignment**

Adopt global standards like ISO/IEC 42001 (AI Management Systems) and the NIST AI Risk Management Framework⁶ into your corporate risk, legal, and cyber security governance.

AI in action at Singtel

**Ethical collaboration**

As a founding contributor to the GSMA AI Ethics Code, Singtel is helping set the global standard for responsible network-level AI governance.⁷

**Trusted infrastructure**

Singtel powers responsible AI through platforms like RE:AI and Singtel Paragon. **RE:AI** provides a turnkey AI Cloud service that simplifies development and deployment without the need for in-house infrastructure. **Singtel Paragon** enables real-time AI at the edge by bringing data processing closer to the source, reducing reliance on external cloud environments.

**Equity by design**

Through **Nxera**, Singtel is democratising AI access across Southeast Asia, ensuring innovation isn't locked behind economic divides.

Ready to innovate with AI safely and responsibly?

Contact us

References

¹ ABC News, Why the AI-generated 'Studio Ghibli' trend is so controversial, 2025

² Herbert Smith Freehills, Navigating representative actions: takeaways from Getty Images v Stability AI, 2025

³ Deloitte, Generative AI is expected to magnify the risk of deepfakes and other fraud in banking, 2024

⁴ Content Science Review, 6 Areas of Generative AI Risk for Enterprises, 2025

⁵ BCG, Gen AI, NA

⁶ ZenGRC, Navigating the Future of AI Governance: A Guide to NIST AI RMF, ISO/IEC 42001, and the EU AI Act, 2024

⁷ TelecomReview, Singtel Collaborates with GSMA and Global Telcos for Responsible AI Maturity Roadmap, 2024