

OSINT BRIEF: RISKS, ABUSES, AND REGULATORY PRESSURE IN THE ADULT PORN INDUSTRY

Prepared for: Strategy & Policy Review **Author:** OSINT Team (Marie Landry Spy Shop) **Date:** 18 August 2025

1. Executive Summary

The global adult content ecosystem is undergoing a seismic shift driven by regulatory pressure, technological disruption, and financial chokepoints. Our analysis reveals a landscape where platforms face existential threats from fragmented, yet aggressive, legal frameworks concerning **age verification**, **consent**, and **platform liability**. The structural vulnerabilities that have long facilitated harms—including the proliferation of non-consensual content, producer coercion, and fraud—are now the primary targets of regulators in key Western markets.

Pivotal developments, such as the **U.S. Supreme Court's 2025 decision upholding state-level age verification laws** and the **EU's designation of major porn sites as Very Large Online Platforms (VLOPs) under the Digital Services Act (DSA)**, have moved compliance from a reputational concern to a legal and operational necessity. These actions, coupled with the **Canadian Privacy Commissioner's legal challenge against Aylo (Pornhub) over its consent model**, signal a new era of enforcement.

Simultaneously, the rapid evolution of **generative AI** presents a dual threat: it enables the mass production of non-consensual deepfake pornography while also offering potential tools for content moderation and verification. Financially, the industry remains at the mercy of major **payment processors like Visa and Mastercard**, whose de-risking policies function as a powerful, non-governmental regulatory force. This brief provides a comprehensive overview of this threat landscape and offers a playbook for navigating the significant governance, compliance, and operational risks ahead.

2. Scope, Methodology & Caveats

- **Scope:** This Open-Source Intelligence (OSINT) review provides a global assessment of the adult entertainment industry, focusing on systemic harms, legal and regulatory actions, platform governance failures, producer-level abuse, financial network pressures, AI/deepfake threats, and labor concerns through August 18, 2025.
- **Methodology:** The findings are derived from public records, major press reporting, regulatory publications (e.g., OPC Canada, UK's Ofcom), court filings, case law, industry standards (e.g., PASS), and reports from NGOs and academic institutions.
- **Caveats:** The legal status of content and platform obligations varies significantly by jurisdiction; this brief is not a substitute for jurisdiction-specific legal counsel. Commercial details for privately-held companies are based on press and regulatory findings. All OSINT data should be cross-verified with primary legal and financial advisors before operational action.

3. Timeline of Major Incidents & Regulatory Actions (2019–2025)

- **Oct 2019:** A seminal report by Deeptrace (now Sensity) reveals that 96% of all deepfake

videos online are non-consensual pornography, highlighting the scale of the emerging threat (1).

- **Dec 2020:** Following a *New York Times* exposé, **Mastercard and Visa halt payment processing for Pornhub's** parent company, MindGeek, citing allegations of unlawful content, including CSAM and non-consensual material (2, 3).
- **Aug 2022:** Visa and Mastercard suspend ties with TrafficJunky, the advertising arm of MindGeek, further tightening the financial squeeze on the company's revenue streams (4).
- **Aug 2023:** MindGeek rebrands to **Aylo** under new private equity ownership, a move aimed at distancing the company from its legacy of controversy (5, 6).
- **Oct 2023:** The **UK's Online Safety Act** receives Royal Assent, establishing a comprehensive regulatory framework with a duty of care for platforms to protect users, especially children, from harmful content (7).
- **Feb 2024:** The Office of the Privacy Commissioner of Canada (OPC) finds Aylo in contravention of federal privacy law (PIPEDA), ruling its consent model for user-generated content is inadequate (8, 9).
- **Jan 2025:** The UK Government announces its intention to create a new criminal offense for the creation of sexually explicit deepfakes without consent, regardless of the creator's intent (10).
- **Mar 2025:** The OPC announces it is **taking Aylo to Federal Court** to seek a mandatory order to force compliance with its recommendations on obtaining direct, express consent (11, 12).
- **Jun 2025:** The **U.S. Supreme Court upholds Texas's age-verification law (HB 1181)**, ruling that such laws are subject to intermediate scrutiny and setting a major precedent that validates similar laws in over a dozen other states (13, 14).

4. Key Findings — The Evolved Threat Landscape

- **A. Non-Consensual Content & Flawed Consent Models:** The historical "safe harbor" model for User-Generated Content (UGC) is collapsing under regulatory scrutiny. The OPC's action against Aylo demonstrates that relying on an uploader's attestation of consent is no longer a defensible position for high-risk, intimate content.
- **B. Producer Coercion and Fraud:** The **GirlsDoPorn** case, which resulted in convictions for sex trafficking by fraud and coercion, remains a stark example of how production entities can systematically abuse performers. This case highlights the need for due diligence not just on content, but on the producers who supply it.
- **C. Financial De-Risking as De-Facto Regulation:** Major payment networks (Visa, Mastercard) and their acquiring banks act as the industry's most powerful regulators. Their decisions to suspend services, often driven by reputational risk and media pressure, can cripple a platform's ability to operate commercially, irrespective of the platform's legality.
- **D. The Age-Verification Mandate:** The SCOTUS ruling has solidified age verification as a legal requirement in a significant portion of the U.S. market. This creates immense technical, operational, and privacy challenges, forcing platforms to handle sensitive user data and navigate a patchwork of state-specific laws.
- **E. The Industrialization of AI/Deepfake Abuse:** Generative AI tools have made it trivially easy to create high-quality, non-consensual sexual imagery. This has shifted the threat from a niche problem to a widespread form of digital abuse that is technically

challenging to detect and moderate at scale.

- **F. SESTA/FOSTA Externalities:** The 2018 U.S. laws, intended to curb online sex trafficking, have had the documented side effect of pushing sex workers off mainstream platforms and onto more clandestine, higher-risk channels, impeding their ability to screen clients and access support networks.

5. Case Studies in Platform Failure & Forced Evolution

- **A. GirlsDoPorn:** This San Diego-based production company deceived and coerced hundreds of women into appearing in videos under false pretenses. The subsequent federal prosecution and multi-million dollar civil judgments against the owners and MindGeek (for distributing the content) established a clear precedent for platform liability in distributing content from fraudulent producers.
- **B. Pornhub / MindGeek → Aylo:** This entity provides a masterclass in reactive governance. For years, its business model relied on a largely unverified UGC firehose. It was only after immense public pressure and the withdrawal of payment services that the company implemented significant changes, such as deleting all unverified content and launching a verification system for uploaders. The ongoing legal battle with the OPC in Canada shows that even these reforms may not be sufficient to meet evolving legal standards for consent.

6. Red-Flag Indicators for Operational Due Diligence

An assessment of any platform, partner, or investment target in this space should screen for the following red flags:

- **Content Moderation:** Absence of a robust, pre-publication verification system for performer identity, age, and consent for every scene. Slow or non-existent takedown processes for reported content.
- **Financials:** High revenue concentration with a single payment processor or acquiring bank. Lack of transparency in payment flows.
- **Producer Management:** No formal onboarding, vetting, or oversight process for content producers.
- **Technology:** Lack of automated scanning for CSAM (e.g., PhotoDNA) and Non-Consensual Intimate Imagery (NCII). No stated policy or technical review process for synthetic/AI-generated content.
- **Governance:** No public transparency reporting on content moderation actions, law enforcement requests, and safety measures.

7. Governance & Compliance Playbook: Practical Controls

To operate defensively in the current environment, platforms must adopt a proactive, trust-and-safety-centric model.

- **Content Safety & Consent:**
 - **Mandate Pre-Publication Verification:** Require government-issued ID verification for all performers.
 - **Digital Consent Artifacts:** Implement a system to collect and store verifiable, scene-level consent records for all participants.
- **CSAM/NCII Defenses:**

- **Automated Scanning:** Integrate industry-standard hash-matching technologies (e.g., PhotoDNA, Semasio) for all uploads.
 - **Human Moderation:** Maintain a 24/7 trust and safety team with clear SLAs for reviewing flagged content.
- **Age Assurance:**
 - **Privacy-Preserving Solutions:** Deploy robust, privacy-preserving age verification technologies that attest to age without retaining underlying personal data.
- **Financial Resilience:**
 - **Processor Diversification:** Establish relationships with multiple payment acquirers and processors to mitigate de-risking from a single source.
 - **Proactive Audits:** Conduct quarterly compliance audits to provide assurance to financial partners.
- **AI/Deepfake Safeguards:**
 - **Explicit Policy:** Enact a clear and strict policy banning all non-consensual synthetic sexual content.
 - **Detection Technology:** Invest in or partner with providers of AI detection tools to scan for manipulated media.
- **Transparency & Accountability:**
 - **Publish Annual Reports:** Release public transparency reports detailing content takedowns, policy enforcement actions, and safety initiatives.
 - **Independent Oversight:** Consider establishing an independent advisory board or submitting to third-party audits of trust and safety practices.
- **Labor & Health Standards:**
 - **Adopt PASS:** Mandate adherence to the PASS (Performer Availability Scheduling Services) standard for all producers, which includes regular STI testing.
 - **Provide Resources:** Offer performers access to mental health support and legal resources.

8. Policy & Legal Watchlist by Jurisdiction (Detailed Analysis)

- **United States:** The legal landscape is now defined by the Supreme Court's decision in *Free Speech Coalition, Inc. v. Paxton*. This ruling validated the "intermediate scrutiny" standard for state-level age-verification laws, effectively green-lighting enforcement in Texas and over a dozen other states with similar legislation ([13](#), [14](#), [15](#)). Platforms now face a choice: implement costly and complex verification systems on a state-by-state basis or block access to a significant portion of the U.S. market.
- **United Kingdom:** The **Online Safety Act** is in full effect, with regulator Ofcom actively enforcing its provisions ([7](#)). The Act mandates "highly effective" age assurance for pornographic sites and imposes a duty of care to protect users from illegal content. Separately, new offenses under the Crime and Policing Bill now criminalize the *creation* of sexually explicit deepfakes without consent, a significant expansion of liability that targets the source of the abusive content ([10](#), [16](#)).
- **European Union:** The **Digital Services Act (DSA)** has classified major adult platforms like Pornhub and XVideos as VLOPs, subjecting them to the highest level of scrutiny ([17](#), [18](#)). The European Commission has opened formal proceedings to investigate their compliance with obligations related to risk mitigation, child protection, and age verification. Non-compliance carries the risk of fines up to 6% of global annual revenue.
- **Canada:** The OPC's Federal Court application against Aylo is a critical test case for digital

privacy and consent ([11](#), [12](#)). A ruling in the OPC's favor would likely force a complete overhaul of UGC consent models for any platform operating in Canada, mandating direct and explicit consent from all depicted individuals.

9. Labor, Safety, Health & Economic Risks

The precarious nature of work in the adult industry is exacerbated by platform instability and regulatory side effects.

- **Decreased Safety Post-SESTA/FOSTA:** Research continues to show that the de-platforming of sex workers has pushed many to less safe, unvetted channels, increasing their vulnerability to violence and exploitation.
- **Inconsistent Health & Safety Standards:** While standards like PASS exist, their adoption is inconsistent. Performers often lack access to employer-sponsored health insurance, mental health care, and retirement plans.
- **Economic Precarity:** Performers are highly vulnerable to the economic shocks that affect platforms. When a platform is de-platformed by a payment processor or blocked in a major market, performers who rely on that platform for income can lose their livelihood overnight. Piracy remains a constant drain on potential earnings.

10. AI / Deepfake Threat Matrix & Mitigation

The threat from generative AI is acute, pervasive, and rapidly evolving.

- **Threats:**
 - **Non-Consensual Deepfake Pornography:** Using a few source images to create realistic, explicit videos of individuals without their consent.
 - **"Nudifier" & "Stripper" Apps:** Automated tools that digitally alter images of clothed individuals to create synthetic nude images.
 - **Voice Cloning:** Using audio samples to create synthetic audio for use in deepfake videos, increasing their realism and potential for harm.
- **Likelihood:** Very High. The technology is widely available and becoming easier to use.
- **Impact:** Severe. Causes extreme emotional distress, reputational damage, and can be used for harassment, blackmail, and extortion.
- **Mitigation Strategy:**
 - **Zero-Tolerance Policy:** A publicly stated, strictly enforced ban on non-consensual synthetic sexual content.
 - **Proactive Detection:** Deploy AI-based tools that can detect digital artifacts and inconsistencies common in synthetic media.
 - **Industry Collaboration:** Participate in industry standards for content provenance and authenticity (e.g., C2PA - Coalition for Content Provenance and Authenticity) to help identify manipulated media.
 - **Rapid Takedown:** Establish a dedicated, expedited channel for victims of deepfake abuse to report content for immediate review and removal.

11. Payments & Ad/Monetization Chokepoints

Financial networks are the industry's most critical and volatile single point of failure.

- **The Power of Card Networks:** Visa and Mastercard's brand rules and risk appetite dictate the commercial viability of most platforms. Their decisions are often opaque and

can be triggered by negative press, making them an unpredictable operational risk.

- **Alternative Payments Are Not a Panacea:** While some platforms have turned to cryptocurrency or other alternative payment systems, these often come with higher transaction fees, increased regulatory scrutiny (anti-money laundering), and a smaller user base, limiting their effectiveness as a primary solution.
- **Resilience Strategy:** The only viable strategy is **diversification**. Building relationships with multiple acquiring banks and payment processors across different jurisdictions can provide a buffer if one partner withdraws services. This requires maintaining impeccable compliance documentation and undergoing voluntary audits to demonstrate low risk.

12. Recommendations (Short, Medium, Long Term)

- **Short Term (0–90 Days):**
 - **Conduct Urgent Gap Analysis:** Audit current practices against the requirements of the UK Online Safety Act, EU DSA, and U.S. state age-verification laws.
 - **Establish 24/7 Abuse Triage:** Implement a clearly accessible, 24/7 human-staffed line for urgent abuse reports (especially for non-consensual content).
 - **Publish a Trust & Safety Statement:** Issue a public statement outlining the platform's commitment to safety, consent, and its policies on AI-generated content.
- **Medium Term (3–9 Months):**
 - **Deploy Pre-Publication Verification:** Fully implement a system for mandatory ID, age, and consent verification before any content goes live.
 - **Secure Multi-Processor Payments:** Onboard at least one additional, independent payment processing partner.
 - **Launch Transparency Reporting:** Publish the first quarterly or biannual transparency report.
- **Long Term (9–24 Months):**
 - **Invest in AI/Deepfake Detection:** Deploy a robust technical solution for detecting synthetic media at the point of upload.
 - **Conduct Formal Audits:** Engage a reputable third-party firm to audit trust and safety practices and share the findings with key partners (e.g., payment processors).
 - **Establish Independent Oversight:** Form an external safety advisory board composed of experts in online safety, victim advocacy, and digital rights to provide guidance and accountability.

13. One-Page Audit Checklist for Investors & Auditors

Control Area	Question	Yes / No / Partial
Consent & Verification	Is there mandatory, pre-publication ID & age verification for all performers?	
	Are there verifiable, scene-level consent artifacts for all participants?	
Content Moderation	Is there automated CSAM/NCII hash-matching on all uploads?	

Control Area	Question	Yes / No / Partial
	Is there a 24/7 human-staffed abuse triage with a <24h SLA?	
Financial	Are payments processed through at least two independent acquirers?	
AI / Deepfakes	Is there a formal policy and technical review process for synthetic content?	
Governance	Is an annual T&S transparency report published?	
Labor Standards	Is there compliance with PASS or a similar health/safety standard?	
Legal / Regulatory	Is there a deployed, privacy-preserving age assurance system for relevant jurisdictions (UK, EU, US states)?	

14. Sources & Appendix

1. https://regmedia.co.uk/2019/10/08/deepfake_report.pdf
2. <https://www.reuters.com/business/mastercard-visa-halt-payments-pornhub-over-allegations-child-sex-abuse-content-2020-12-11/>
3. <https://www.theverge.com/2020/12/10/22168240/mastercard-ending-pornhub-payment-processing-unlawful-videos>
4. <https://www.reuters.com/business/finance/mastercard-visa-suspend-ties-with-ad-arm-pornhub-owner-mindgeek-2022-08-04/>
5. <https://www.aylo.com/newsroom/mindgeek-rebrands/>
6. <https://www.theverge.com/2023/8/18/23837670/pornhub-parent-company-mindgeek-rebrand-aylo>
7. <https://www.legislation.gov.uk/ukpga/2023/50>
8. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2024/nr-c_240229/
9. <https://www.reuters.com/world/americas/canada-says-pornhub-owner-broke-privacy-laws-by-sharing-explicit-images-2024-02-29/>
10. <https://www.gov.uk/government/news/government-crackdown-on-explicit-deepfakes>
11. <https://www.dentonsdata.com/federal-court-to-determine-whether-third-party-consents-violate-pipeda/>
12. <https://www.dww.com/articles/privacy-commissioner-seeks-federal-court-order-for-pornhub-operator-to-comply-canadian>
13. <https://www.keranews.org/government/2025-06-27/texas-can-require-porn-websites-to-verify-users-ages-supreme-court-rules>
14. <https://datamatters.sidley.com/2025/07/08/texas-age-verification-law-upheld-u-s-supreme-court-balances-free-speech-and-child-protection-in-the-digital-age/>
15. <https://www.techpolicy.press/supreme-court-ruling-shifts-ground-on-online-age-verification-and-free-speech/>
16. <https://corkerbinning.com/deepfakes-and-the-criminal-law/>

17. <https://eucrim.eu/news/overview-of-the-latest-developments-regarding-the-digital-services-act/>

18. https://en.wikipedia.org/wiki/Digital_Services_Act

Additional Reading:

- **Ofcom - Online Safety:** Official guidance and reports from the UK's regulator.
- **Electronic Frontier Foundation (EFF):** Analysis of age verification laws and their impact on privacy and free speech.
- **European Commission - The Digital Services Act:** The official resource page for the EU's landmark platform regulation.