

Your Face Is Not a Free Asset

Image-based rights, deepfakes and safety by design



Uloaku (Ula) Ojiaku

Founder & CEO, Mezahab Group • AI governance strategist

info@mezahab.co.uk

45-minute interactive talk • 15-minute Q&A

Opening pulse: where does the risk begin?

In one or two words, add to chat:

When you hear “AI-generated image abuse”, what is the first harm that comes to mind?

Look for patterns...

AI has separated capability from permission

CAN

≠

MAY

The ability to generate a convincing version of someone does not create a right to use their identity.

What should law, product design and governance each prevent?

Where would you draw the red line?

A

A flattering filter changes facial features

B

A realistic fake shows a politician taking a bribe

C

An app digitally removes a woman's clothing

D

A labelled parody puts words into a CEO's mouth

Put A, B, C or D in the chat — which is hardest to classify?

One case exposed a wider structural gap

A person may be recognisable, harmed and stripped of autonomy—yet still fall between existing legal categories.

CATALYST

Jess Asato MP v X.AI LLC

The claim concerns alleged sexualised images generated through Grok. The outcome is not yet determined.

THE PROBLEM

Image-based abuse is wider than “deepfake porn”

INTIMATE

Nudification, sexualisation, fabricated sexual conduct

DECEPTIVE

False speech, conduct, attendance or endorsement

DEGRADING

Humiliating, violent or discriminatory depictions

EXPLOITATIVE

Commercial use, impersonation, extortion or coercive control

Sexualised deepfakes target women at extraordinary rates

98%

of deepfake videos identified in a widely cited 2023 analysis were pornographic

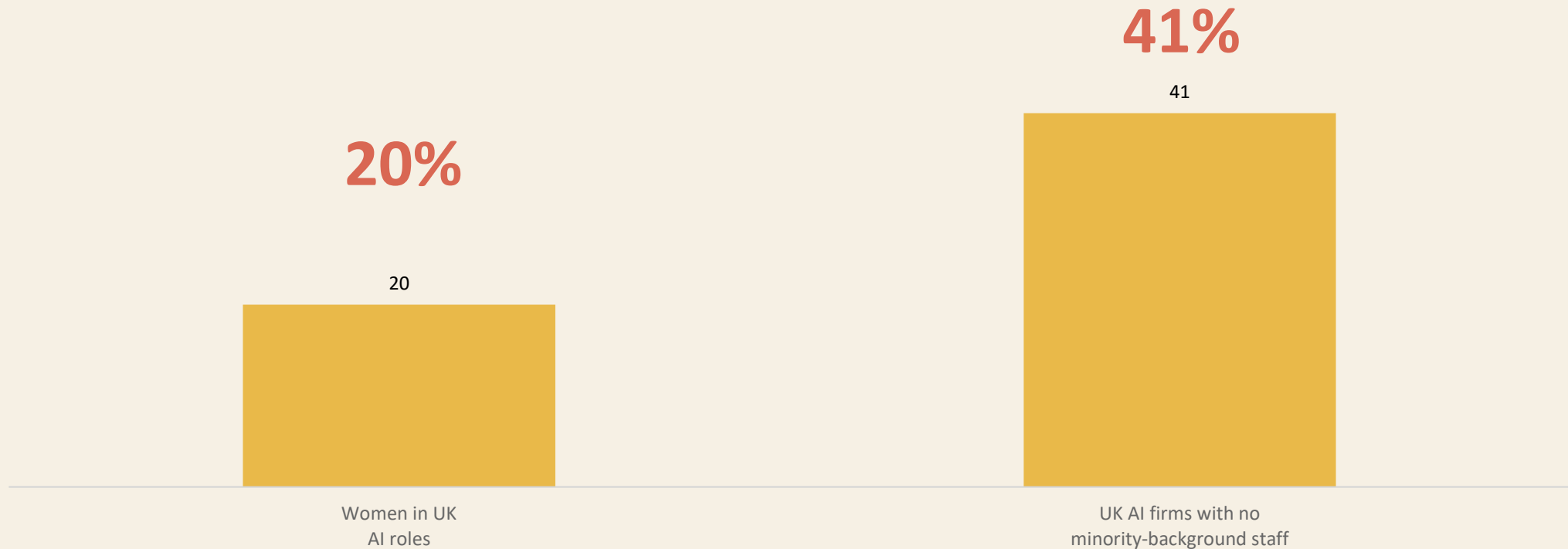
99%

of the people depicted in those pornographic deepfakes were women

These figures describe an observed online dataset, not every deepfake ever created. The direction of harm is nevertheless unmistakable.

Source: UN Women (2025–26), citing the 2023 State of Deepfakes analysis

Those most exposed to harm remain underrepresented in AI teams



Women's share of UK AI roles fell four percentage points between 2020 and 2025.

Source: UK Government, AI Labour Market Survey 2025 (published January 2026)

The imbalance narrows further in technical authority

12%

of AI-specific research positions
are held by women

18%

of authors at leading AI
conferences are women

>80%

of AI professors are men

Participation matters most where technical choices, research agendas and product safeguards are set.

Source: UNESCO Women4Ethical AI and UNESCO's 2024 generative-AI gender study

Representation affects what teams notice, test and prioritise

NOTICE

Whose misuse scenarios are treated as foreseeable?

TEST

Which bodies, skin tones, accents and contexts appear in evaluations?

DECIDE

Who can delay launch when safeguards fail?

LEARN

Whose reports become product evidence rather than “edge cases”?

Diversity is a governance input. Accountability still requires standards, evidence and authority.

The UK protects categories of harm—not the digital self

CRIMINAL LAW

Intimate-image
and harassment
offences

DATA & PRIVACY

Personal data and
misuse of private
information

REPUTATION

Defamation and
passing off

COPYRIGHT

Usually protects
the image-maker,
not the person
shown

No single, accessible right governs materially harmful replication of face, body, voice or likeness.

The hardest cases live between the legal boxes

- False but non-intimate depictions
- Fabricated speech, conduct or political activity
- Degrading, violent or discriminatory representations
- False commercial endorsement
- Distress or loss of autonomy without an obvious civil claim

Other countries solve different parts of the problem

No single jurisdiction provides a complete model for prevention, removal and redress.

Borrow functions—not entire foreign laws

AUSTRALIA

Specialist regulator-led removal

UNITED STATES

Federal 48-hour process for intimate imagery

FRANCE / GERMANY

Stronger image and personality protections

DENMARK

Proposed digital-replica right; legally contested

The UK opportunity: combine clear rights, practical enforcement and prevention.

Takedown alone arrives after the harm

01

PREVENT

Reduce foreseeable misuse
before release

02

REMOVE

Stop distribution and repeat
uploads quickly

03

REDRESS

Give victims accessible
remedies and support

Safety by design lowers both human harm and the enforcement burden.

Can we make the red line more determinable?

You will test a proposed scale—not endorse a finished legal answer.

A decision framework can make the red line more concrete

0–2	Routine edits, clearly signalled art, parody or satire
3–4	Material alteration or realistic fabrication
5	Degrading, violent or discriminatory depiction
6	Nudification, sexualisation or fabricated sexual conduct
7	Sexual imagery involving children

Assessment factors: consent, identifiability, realism, deception, intimacy, degradation, purpose, disclosure, audience, vulnerability and likely harm.

* Note: this is a **proposed** consultation framework, **not** a statement of current law

Levels 0–2: ordinary and expressive uses

0	No modification; use within valid consent	Acceptable
1	Cropping, resizing, lighting or accessibility changes	Usually acceptable within the agreed purpose
2	Recognisable parody, satire, art or non-deceptive meme	Generally permissible, subject to existing law

Levels 3–5: consent and harm become decisive

3

Material alteration of body, clothing, age or characteristics

Consent normally required

4

Realistic fabrication of speech, conduct or endorsement

Presumptively unacceptable without consent or public interest

5

Degrading, violent, discriminatory or humiliating depiction

Strong civil protection and rapid removal

Levels 6–7: the prohibition line

6

**Nudification, sexualisation or
fabricated sexual conduct**

Prohibited without explicit consent

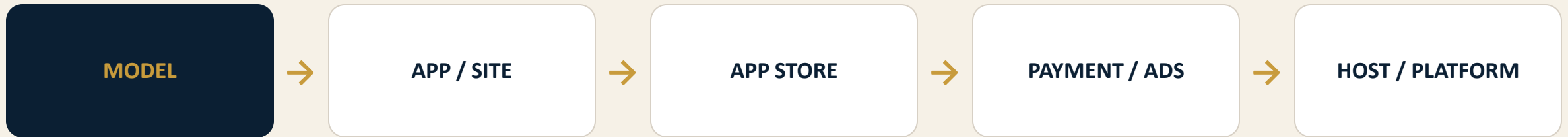
7

**Sexual imagery involving children—or
adults made to look like children**

Absolute prohibition and immediate safeguarding

Labelling may reduce deception. It does not make sexual or exploitative use acceptable.

The final post is only one link in the chain



Who develops, distributes, promotes, monetises, hosts—or knowingly enables—the abusive capability?

Overseas services and open repositories complicate enforcement; they do not remove the need to allocate responsibility.

Safety by design must reduce the opportunity for abuse

1

TEST

Sexual, violent, identity-based and intersectional misuse

2

GUARD

Prompts and uploads involving identifiable people

3

MONITOR

Recurring abuse patterns, workarounds and repeat offenders

4

RESPOND

Rapid escalation, evidence preservation and corrective action

A provider should be able to show what it tested, what failed, what changed and who accepted the remaining risk.

Seven practical moves for UK policy

- 1 **Statutory decision framework for image modification**
- 2 **Limited, accessible digital-likeness right**
- 3 **Safety-by-design duties backed by evidence**
- 4 **Rapid removal, re-upload controls and evidence preservation**
- 5 **Proportionate responsibility across the supply chain**
- 6 **Affordable enforcement and specialist victim support**
- 7 **Transparent reporting on incidents, response and outcomes**

Which intervention would you prioritise?

A

A limited digital-likeness right

B

Mandatory pre-deployment misuse testing

C

A regulator-led 48-hour removal route

D

Duties for app stores and payment providers

Vote A, B, C or D in the chat—and add one sentence if you disagree with the choices.

THE PRINCIPLE

Technological capability does not remove personal autonomy.

Safe AI protects people before harm, responds quickly when safeguards fail, and makes accountability real.

COMMITMENT

What can we change from where we sit?

BUILDERS

**Add gendered misuse cases to pre-release testing.
Track evasions and repeat abuse.**

GOVERNANCE LEADERS

Ask for evidence, named accountability and escalation thresholds before launch.

POLICY + CIVIL SOCIETY

Design remedies with victims. Test whether routes work without wealth or specialist knowledge.

FUNDERS + BOARDS

Treat representation, user safety and incident response as governance signals.

Write one action you can take in the next 30 days.

CONTINUE THE CONVERSATION

Give feedback and help shape the paper

YOUR FACE IS NOT A FREE ASSET

Register your interest to:

01

Receive the paper and practical governance check

02

Contribute evidence or comment on the decision framework

03

Join the Mezahab mailing list and be notified of relevant updates and events (e.g. expert roundtables, AI governance sessions)



<https://forms.gle/ahXdGiSDApgTS137>

Thank you