Six in Ten Britons Fear AI Image Misuse, Though Many May Have Already Consented

New research from Bridewell exposes a dangerous gap between public concern, legal reality and personal accountability in the age of AI

READING, UNITED KINGDOM, February 11, 2026 /EINPresswire.com/ -- Six in ten UK adults fear that artificial intelligence will misuse their photos for deepfake scams, impersonation or other harmful purposes, yet many will have already consented to such misuse by accepting platform terms and conditions they have not properly read or understood. This is according to new research from cyber security specialist Bridewell.

Over a third (36%) of adults also believe they retain legal rights over images uploaded to AI tools. The findings reveal a worrying gap between public anxiety about AI misuse and a lack of awareness about the legal agreements that govern how personal data, images and likenesses can be used.

Public fear rises while legal understanding falls away
Nearly six in ten UK adults (59%) believe images uploaded to AI platforms could be used for deepfake scams or impersonation. However, when asked about their legal rights, confidence quickly collapses.
Key findings include:

- 36% believe they have legal rights over images of their own face
- The same proportion (36%) say they are unsure what rights they have at all
- 24% think they retain rights over photos they upload publicly
- 21% believe they have rights over AI-generated content made to look like them
- 19% think they have rights over AI-generated content resembling their child

In reality, many of these rights are already defined, limited or waived within platform terms and privacy policies that users agree to without reading.

“People are right to be worried about AI misuse, but many do not realise they are agreeing to usage of their data by accepting terms and conditions when using publicly available AI products,” said Chris Linnell, Associate Director of Data Privacy at Bridewell. “There is a dangerous mismatch between public concern and legal reality. If people do not read the terms, they do not understand the risks or where responsibility truly lies.”

From deepfakes to courtrooms, fears over image misuse grow

Concerns extend far beyond simple data sharing. When asked how images uploaded to AI tools could be used, respondents highlighted a wide range of risks:

- 56% fear images could be used to create realistic fake images or videos
- 51% worry about their images being used to create sexual or pornographic content
- 45% believe images may be shared with third parties
- 38% think images could be used to train AI models
- 27% fear images could be used against them in a court of law

More than a quarter of respondents (27%) say real-world examples of these risks have already changed how they behave online.

Responsibility is pushed upwards, not inwards

Despite growing concern, personal accountability remains low. The majority of respondents believe responsibility for protection sits elsewhere:

- 56% say technology companies should be responsible
- 54% believe the government should take responsibility
- 50% point to regulators
- Only 19% believe individuals themselves should be accountable

At the same time, confidence in existing safeguards is weak. Over half of respondents (56%) believe protections currently in place to prevent AI misuse are ineffective, while just 4% describe them as very effective.

Free AI training is coming, but engagement looks uncertain

These findings emerge as the UK government announced it will provide free AI training for all adults. However, Bridewell's research suggests voluntary education alone may struggle to close the knowledge gap:

- Less than half of respondents (47%) say they are likely to take part
- More than a quarter (26%) say they are unlikely to engage at all

This raises questions about whether optional training can meaningfully address widespread misunderstanding around AI, consent and digital rights.

"Training matters, but it cannot compensate for unread terms, unclear legal frameworks and a culture that treats AI risk as someone else's problem," added Linnell. "If people will not engage with free training, then stronger safeguards, clearer (enforced) regulation and far greater transparency from platforms are essential."

A widening trust gap
As AI becomes embedded in everyday life, Bridewell warns that public trust is being undermined not by innovation itself, but by confusion over rights, responsibilities and consequences.

Without meaningful legal transparency and a clearer understanding of what users have already agreed to, the gap between AI capability and public confidence is set to grow.

METHODOLOGY:
The study of 2,000 UK adults was carried out by OnePoll in February 2026.

About Bridewell
Bridewell is the UK's leading cybersecurity services business, offering strategic cybersecurity consulting (including OT security, cloud security, security architecture, engineering and GRC), managed security services (including 24x7 MDR (IT & OT), threat intelligence and digital forensics), penetration testing, and data privacy services. Bridewell is one of the UK's most highly accredited cybersecurity services specialists and has strong relationships with industry leaders like Microsoft and Forescout. For more information on Bridewell please visit Bridewell.com

Bethany Smith
Eskenzi PR
beth@eskenzipr.com
