AI Explained · Deepfakes, Part 2

What to Do When Someone Uses Your Face or Voice

By Dr Peter Fields

THE 2-MINUTE SUMMARY

Call 999 if you're in immediate danger. If someone is using your voice to ask for money, warn the people they may contact. Anyone who has paid should call their bank straight away.

If it's safe, keep a record of where the fake appeared, who posted it and when. Save threatening messages and report the post or account.

If someone shares a fake intimate image of you, report it to the site that hosts it and to any search engine that shows it. Specialist services can help with removal.

"Have you seen what they're sending round?"

Imagine a friend sends you that message. An intimate image is doing the rounds and the person in it looks like you. Or a colleague has heard a recording in which your voice asks them to pay an invoice. Part 1 looked at why people believe these AI-made or altered images and recordings. If someone uses your likeness this way, you can act while you're still finding out what happened.

What to do straight away

• **Threats or blackmail.** Call 999 if you're in immediate danger. For other threats, blackmail or stalking, report to your local police online or on 101. If someone demands money or more images, stop contact and seek help. If you've already paid, call your bank and do not pay again.[1,2]

• **A scam in your name.** Warn the people likely to receive the message. If anyone has sent money, they should contact their bank immediately using a number they trust. Use Report Fraud (formerly Action Fraud) in England, Wales and Northern Ireland. In Scotland, contact Police Scotland on 101.[2]

• **Evidence you can keep safely.** Keep links, usernames, dates, threatening messages and report numbers. If the image is of you and you're sure everyone shown is an adult, a screenshot of the post with its web address and date can help if it's safe to take one. If anyone shown may be under 18, avoid downloading, screenshotting or forwarding the image. Note where it appeared and report it. You can contact the police without screenshots.[1]

What does the law say?

The law depends on what the person did and where. An intimate image, a fraudulent demand and a pattern of threats can each raise different issues.

Intimate images

Since 6 February 2026, it has been an offence in England and Wales to deliberately make, or ask for, a fake image that appears to show another adult in an intimate state, such as naked or engaged in a sexual act. The offence requires that the adult did not consent to the making of the image or to the request, as applicable, and that the person acting had no reasonable belief in consent. A reasonable excuse is a defence. A request can be an offence even if nobody makes the image.[3]

Sharing an intimate image without consent can also be an offence in England and Wales, including a fake image that appears to show the person. The basic offence requires no intent to cause distress. Threatening to share can be an offence even if the image does not exist. The test is whether they intend to make the person depicted, or someone who knows them, fear that the image will be shared, or are reckless about whether it causes that fear. Separate laws cover indecent images of children, including certain computer-generated images.[3,4]

In Scotland, the law against sharing or threatening to share intimate images can cover deepfakes. The Scottish Parliament is looking at whether the law goes far enough. In Northern Ireland, sharing or threatening to share private sexual images without consent and with intent to cause distress can be an offence. There are limits on which altered images the law covers. Specific offences for sexually explicit deepfakes have been proposed.[5,6]

Fraud, harassment and stalking

In England, Wales and Northern Ireland, using a fake voice or video to make a dishonest claim can be fraud. The person must know the claim is or could be false or misleading and intend to make a gain, cause a loss or expose someone to a risk of loss. Fraud can occur even if nobody pays. In England and Wales, repeated impersonation or threats can form part of harassment or stalking. Keep a timeline and ask a solicitor whether you can apply for an injunction, a court order to stop the harassment.[7]

What if it is a fake account or a clip sent to work?

If friends, clients or colleagues might receive the fake, tell those affected directly. You could send a short message. “Someone is using my name and voice. If you get an unusual request from me, call me on the number you already have.” A private correction can reach the right people without giving the fake a wider audience.

In England and Wales, civil claims depend on what the fake does and how it is used. If it seriously harms your reputation or intrudes on your private life, ask a solicitor whether defamation, misuse of private information or data protection law can help.[7]

Getting it taken down

Report the post to the site or app that hosts it. If the account is also pretending to be you, report the profile for impersonation. For an intimate image, use the service's intimate-image reporting form if it has one. Say who is depicted, that the image was shared without consent and whether you are reporting for yourself or on someone's behalf. Give a direct link or enough detail to find the post. If the image also appears in search results, ask the search engine to remove the result. The copy on the original site needs its own report.[8,9]

Will it come down within 48 hours?

The 48-hour provisions came into force on 29 June 2026. They require regulated services to have systems designed to act within 48 hours of a valid report about an unlawfully shared intimate image, including a fake. The person shown or someone acting for them must make the report. The duty also covers copies the service identifies as the same or substantially the same. Ofcom is preparing changes to its codes and guidance. Its October 2026 bulletin says it plans to consult by the end of 2026, with a view to implementation in 2027. For now, use the service's existing reporting route.[8]

If the material stays up or the service rejects your report, use its complaints or appeals process. You can tell Ofcom how the service handled it. Ofcom uses these reports to check compliance. For help getting a specific image removed, contact one of the services below.[8,10]

Who can help with an intimate image?

The Revenge Porn Helpline helps adults in the UK with removal requests. If the person depicted is under 18, Childline and the Internet Watch Foundation run Report Remove. It can help with eligible images made or altered with AI. Parents and carers can ask for help without asking the child to show them the image.[4,11]

If you can, ask someone you trust to keep track of reports and replies. Some services also accept reports from someone acting on your behalf.

Geek Box · Can you stop a copy being posted again?

StopNCII.org can help eligible adults who have access to a fake nude or semi-nude image of themselves. Your device makes a digital fingerprint, called a hash. The service sends the fingerprint to participating platforms to check for matches. The file stays on your device. Report the posts you already know about as well.[12]

Sources and notes

Law and reporting routes checked on 18 November 2026.

1. Metropolitan Police, reporting intimate-image abuse and preserving evidence. National Crime Agency, Sextortion. Police guidance · NCA advice

2. Report Fraud, where to report and what to tell your bank. Stop Scams UK, safe callback advice. Report Fraud · Stop Scams UK · Change from Action Fraud

3. Sexual Offences Act 2003, s 66B (sharing and threats) and ss 66E–66G (creation, requests and definitions). Data (Use and Access) Act 2025, s 138 and SI 2026/31. CPS, Communications Offences. 2025 Act · Commencement · CPS guidance

4. Internet Watch Foundation and National Crime Agency, Stopping AI Child Sexual Abuse Imagery, advice for parents and carers. Childline and IWF, Report Remove. Parent guide · Report Remove

5. Abusive Behaviour and Sexual Harm (Scotland) Act 2016, s 2. Scottish Government consultation, online harm. Scottish Parliament, October 2026 inquiry. Scottish Government · Inquiry

6. Justice Act (Northern Ireland) 2016, ss 51–53, as amended by the Justice (Sexual Offences and Trafficking Victims) Act (Northern Ireland) 2022, s 6. Northern Ireland Assembly, Committee for Justice, 8 October 2026. Act · Committee minutes · 2022 amendment

7. Fraud Act 2006, ss 2, 5 and 15. Protection from Harassment Act 1997, ss 1, 2A, 3 and 7. Abbasi and Haastrup [2025] UKSC 15, paras 95–97. Fraud Act · Harassment Act · Supreme Court judgment

8. Crime and Policing Act 2026, ss 100–101, amending the Online Safety Act 2023. SI 2026/689, reg 2(1)(j). 2026 Act, ss 100–101 · Commencement · Ofcom, October 2026 bulletin · Online Safety Act, s 51 · Government factsheet

9. Google Search Help, requesting removal of personal sexual content, including fabricated images. Google removal form

10. Ofcom, complaints about the safety measures of an online service. Ofcom complaints

11. Revenge Porn Helpline, advice and takedown support for adults in the UK. Helpline

12. StopNCII.org, eligibility, synthetic images and how the matching service works. StopNCII.org FAQ