The Rt Hon Ian Murray MP
Minister for Creative Industries, Media and Online Safety

Dame Melanie Dawes
Chief Executive, Ofcom

Via email

30th October 2026

Joint Letter on Age Checking and Children's Rights Online

Dear Minister for Online Safety, Dear Chief Executive, Ofcom,

We write as organisations and researchers with technical and policy interests in the area of children's rights and online safety, security, and the internet. Defend Digital Me has just published *Who is age-gating our life online?*,[1] which examines the age checking and verification systems behind Australia's social media ban and the proposals now emerging across Europe. We urge you to look hard at what these systems ask of children before the UK writes them into law.

Decisions due in the coming weeks will settle how every person going online in the UK must prove their age. Ofcom's 'Rapid assessment of highly effective age assurance at 16' was published yesterday.[21] Regulations under section 214A of the Online Safety Act 2023 are expected by the end of the year, while legislation on device-level protections is being drafted now.[2] The Government still has time to discuss and consider more expert evidence before it acts.

Recognise what age checks ask of adults and children.

Checking a child's age means checking everyone's. In August 2026, France's Constitutional Council struck down an under-15 ban partly because it required every adult to prove their age too, with no limits that met the tests of necessity and proportionality required in law.[3]

Most methods involve several steps. A person first proves a claimed age belongs to them, using an identity document, a bank record or another state-accepted source. The service or a third-party provider then checks that proof, often with a face scan and a liveness check, and may go on profiling the user's behaviour. Data that leaves the device can pass through sub-processors in several countries. Children have no relationship with most of these companies and rarely know who they are. When checks fail, appeals ask for more. Some 70,000 Discord users had their government ID photos exposed after appealing age assessment decisions, when a third-party customer service provider was breached.[4]

The Defend Digital Me report, maps these processes across the ten platforms covered by Australia's law and the third-party providers they rely on. These systems normalise the processing of children's facial and bodily data at scale. They teach children to perform for a camera whenever a system tells them to, and to hand over their facial and ID data on demand because it is the quickest way to get online. *That is a child protection risk in its own right.* A child who learns that a stranger-on-a-screen can tell them to perform on demand, to move their body or smile on camera, and that complying even if they would rather not is the price of being "safe" to take part, learns the opposite of what safeguarding requires. There is no Ofcom or other

impact assessment on these behavioural implications for interaction in the digital environment or what it means for children's development of identity, agency, and trust as they are encouraged to perform on screen. Ofcom has said it is for Parliament to consider the impacts of the potential new duties.

This also engages children's right to privacy (UNCRC Article 16) and the special protection data protection law gives biometric data, which cannot be reset once lost. This summer the Internet Watch Foundation warned UK schools and parents against posting images of their children online given the risks of facial image exposure to AI training models and loss of identity through distribution to any number of strangers online.[5] Mandatory age checks most often require children to do exactly that thing we are told is unsafe, sending images and videos to companies in countries they have never heard of.

Recognise that Age-gating does not create safety online but creates its own harms.

Safety is an outcome. Age-gating is a process without any evidence of delivery. The evidence from Australia shows around 70% of under-16s who had accounts have kept access.[6] Of those who lost it, half report no difference to their safety[6] and one in two say they now get less news.[7] Cutting young people off from news and public debate restricts their freedom of expression and access to information (UNCRC Articles 13 and 17). It also puts their democratic participation at risk, just as the Representation of the People Bill would give 16 and 17-year-olds the vote. Children pushed off mainstream services have moved to sites with no checks and fewer protections.[8] Security researchers find no scientific evidence that banning children from online services improves their mental health or development.[9]

To make checks enforceable, some states then try to close the routes children use to get around them, through VPN bans and platform blocking. These tools bring their own harms of censorship and surveillance. They strip away the anonymity that protects journalists, whistleblowers and people escaping domestic violence, along with children's own privacy, from the everyday to the child seeking confidential help or campaigning. VPN restrictions would also hamper schools and businesses that rely on them to secure remote access.[10]

Age-gating also reaches the games industry, which sits within the Department for Digital, Culture, Media and Sport (DCMS). Games sold through the major storefronts can rely on the platform's own age checks and guardian accounts. Studios outside them must buy checks of their own, which makes independent distribution expensive and more difficult.[11] Games are where many children exercise their right to play (UNCRC Article 31), and gating them by age restricts it.

DCMS has sought to boost innovation in age assurance since 2019.[12] So far the growth has gone to venture-capital and private-equity-backed verification firms, with Yoti reporting revenue up 62% in 2025 to £29 million,[13] despite its fine from the Spanish AEPD for legal compliance,[14] while costs land on the smaller UK studios and start-ups the Government wants to grow. Providers rarely publish their prices. One 2026 rate card seen by Defend Digital Me charges an organisation-wide fee of up to US$25,000 a month, then about US$500 to US$50,000 a month for each app, game or website. Integration, security and support add to that, and human review for people wrongly refused is sold as a premium extra from about US$9,000 a month. Per-check prices fall with volume, from US$0.10 to US$0.01 at 100 million checks a year, so the largest platforms pay least per user.[15] Smaller UK studios, forums and start-ups face the full cost from their first user, and some may withdraw services from UK users or from children altogether. Device-level checks

would give operating system makers, mostly large US firms, more control over what people in the UK can reach online, and could lock out anyone using open devices and software.[16]

Age-gating engages the rights of children and adults alike, including privacy, expression, access to media and information, association, play and the right to be heard (UNCRC Articles 16, 13, 17, 15, 31 and 12). It also engages children's protection from economic exploitation under Article 32, since age assurance turns their faces and behaviour into raw material for a growing market; as well as impeding the wider right of Article 31 to participate freely in cultural life and the arts.

Checks also shut out people without ID, a compatible device or the skills to use one, including many older people, visitors and minority communities.[18]

In June, 69% of adults supported a law using age verification to keep under-16s off social media, but support fell to 50% when people would have to upload ID or a credit card.[17] Ofcom has today said exactly this; “of the methods currently available at 16, photo ID is either required as part of the method itself, or as the likely backstop for other methods, such as facial age estimation.”

In March, 438 security and privacy researchers from 32 countries warned of these risks.[9]

The Council of Europe Commissioner for Human Rights and the UN High Commissioner for Human Rights have both raised them too.[19] [20]

Put children's rights first in the decisions ahead.

We ask the UK Government to:

- Commission and publish a full, independent, human and child rights impact assessment of the under-16 restrictions and any age assurance requirements before regulations are laid;
- Ensure Ofcom’s impact assessment in consultation on draft guidance on ‘highly effective age assurance at 16’ will cover users of all ages and assess wider effects on children's behaviour, identity and development (e.g. in liveness checks), and lifelong data security (i.e since “ageing up” accounts means keeping dates of birth or running a second check at 18)[21];
- Withdraw plans for wide age assurance mandates. In March, 438 researchers urged a pause while the evidence on their benefits, harms and feasibility remains unsettled;[9]
- End the routine processing of facial biometric and bodily data in age checks;
- Treat the normalisation of on-camera coercive compliance as a child protection risk in its own right; and Ofcom must do the same in its consultation on guidance and impact assessment;
- Rule out VPN restrictions and platform blocking, and do not respond to circumvention by escalating checks, which means collecting more data from everyone;
- Hear children under Article 12 of the UNCRC and organisations that are expert on the technology and children’s rights before final policy decisions and the drafting of regulations;
- Use the law that already exists. The children's safety duties of the Online Safety Act and the Age Appropriate Design Code already apply, and regulators should enforce them in full before any new access restriction is introduced;
- Require services to be safe by default for every user, with private accounts and no profiling-based recommendations, and limit the collection and use of personal data for

targeting content and features, for all users, and make child safety testing a pre-condition of launching high-risk features;
- Fund education for children, parents and teachers on what age and identity checks involve, the lasting risks of biometric data loss and identity fraud, and the rights people hold. This should form part of the comprehensive digital literacy long absent from England's national curriculum and from initial teacher training and CPD, beyond "stranger danger" messaging about online behaviour.

Children's safety online depends on how services are designed and how the law is enforced. Age-gating the internet would put the security of identity of the whole population at lasting risk, and those risks are predictable now.

We urge you to commission the full evidence of age-gating on human rights, and act on the evidence we set out, before these decisions are made, and to work with us on alternatives that achieve the aims we all share.

Sincerely,

Jen Persson, Director, Defend Digital Me (coordinator)

Professor Martin Albrecht, Chair of Cryptography, King’s College London

James Baker, Director, Gamers Voice

Big Brother Watch

Professor Rikke Bjerg Jensen, Professor of Information Security, Royal Holloway University of London

Professor Olivier Blazy, École Polytechnique

Professor Eerke Boiten, Head of School of Computer Science and Informatics and Professor of Cyber Security, De Montfort University

Phil Booth, National Coordinator, NO2ID

Mikaela Brough, Lecturer in Information Security, Royal Holloway University of London

Sofía Celi, Principal Researcher at Brave and Fellow at University of Bristol

Dr. Ben Collier, Senior Lecturer in Science Technology and Innovation Studies, University of Edinburgh, and Chair, the Foundation for Information Policy Research (FIPR, Cambridge)

Paige Collings, Senior Speech and Privacy Activist, Electronic Frontier Foundation

Dr. Olivier MJ Crépin-Leblond, Chair, Internet Society United Kingdom Chapter

Professor Jon Crowcroft, Professor of Communications Systems, University of Cambridge

Paul Diegel, Director, Stop Killing the Internet

Dr François Dupressoir, Associate Professor in Cryptography, University of Bristol

Professor Hamed Haddadi, Professor of Human-Centred Systems, University of Oxford

Stephen Karmeinsky, FBCS CITP, MIET, MIEEE, MACM; Executive Committee, Internet Society UK

Jim Killock, Executive Director, Open Rights Group

Matthew Lesh, Public Policy Fellow, Institute of Economic Affairs

Jesper Lund, Chairperson, IT-Pol Denmark

Dr Chloe Martindale, Senior Lecturer in Cryptography, University of Bristol

Professor Guido Noto La Diega, Professor of Law, Technology and Innovation & Co-Director of the Socially Progressive AI Lab, University of Strathclyde

John Pane, Chair, Electronic Frontiers Australia Inc.

Lucy Roberts, co-founder of Youth Action Group

Professor Carmela Troncoso, Max Planck Institute for Security and Privacy and EPFL

References

1. Defend Digital Me (2026). *Who is age-gating our life online?* https://defenddigitalme.org/who-is-age-gating-our-life-online-full-report/
2. Woodhouse, J. (2026). *Proposals to ban social media for children* (Research Briefing CBP-10468). House of Commons Library. https://commonslibrary.parliament.uk/research-briefings/cbp-10468/
3. Conseil constitutionnel, Décision n° 2026-911 DC du 14 août 2026; reported in Franceinfo (2026). « Ne rien lâcher » : le gouvernement soumet une nouvelle version de l'interdiction des réseaux sociaux aux moins de 15 ans à la Commission européenne. https://www.franceinfo.fr/internet/reseaux-sociaux/le-gouvernement-soumet-une-nouvelle-version-de-l-interdiction-des-reseaux-sociaux-aux-moins-de-15-ans-a-la-commission-europeenne-apres-la-censure-d-un-precedent-texte-par-le-conseil-constitutionnel_8191493.html
4. Discord (2025). Update on a security incident involving third-party customer service. https://discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service
5. Milmo, D. (2026, July 3). UK parents warned over posting images of children amid AI sexual abuse fears. *The Guardian*. https://www.theguardian.com/society/2026/jul/03/ai-prey-watchdogs-telling-parents-protect-children-nudification-apps
6. Molly Rose Foundation (2026). *Australia's social media ban: is it working?* https://mollyrosefoundation.org/wp-content/uploads/2026/04/MRF_Australia-Social-Media-Ban-Research_Briefing-April-26.pdf
7. Notley, T., Chambers, S., Dezuanni, M., Park, S. and Lee, J. Y. (2026). *Social media ban: The impact on young people's news engagement.* https://apo.org.au/node/334363
8. Ofcom (2026). *Report on the use of age assurance: Report prepared under s157 of the Online Safety Act 2023*, para. 4.37. https://assets.publishing.service.gov.uk/media/6a5770ae6d6d5c7e2845c9d0/Web-_accessible_Report_on_the_use_of_age_assurance_1.pdf
9. Joint statement of security and privacy scientists and researchers on age assurance (March 2026). https://csa-scientist-open-letter.org/ageverif-Feb2026
10. Defend Digital Me (2026), *Who is age-gating our life online?* section 8, VPN bans and content blocking.
11. Gamers Voice (2026, 4 October). *Briefing: How the proposed EU KIDS Act could impact video games and the Stop Killing Games campaign.* Gamers Voice Ltd.
12. DCMS (2020). *VoCO (Verification of Children Online) Phase 2 report.* DCMS, GCHQ and the Home Office. https://assets.publishing.service.gov.uk/media/5faa9cffd3bf7f03a841cfc2/November_VoCO_report_V4__pdf.pdf
13. Yoti (2026). Thoughts from our CEO (January 2026). https://www.yoti.com/blog/thoughts-from-our-ceo-january-2026/
14. Burt, C. (2026, March 11). Spain's AEPD fines Yoti $1.1M for biometric data handling violations. *Biometric Update*. https://www.biometricupdate.com/202603/spains-aepd-fines-yoti-1-1m-for-biometric-data-handling-violations
15. Defend Digital Me (2026), *Who is age-gating our life online?* section 6.5, Pricing the check.
16. ibid, section 6.6, Proposed alternatives: credit reference checks and operating-system age signals.
17. Ipsos (2026). 2 in 3 support social media ban for under-16s, though support softens if it requires nationwide ID verification. https://www.ipsos.com/en-uk/2-3-support-social-media-ban-under-16s-though-support-softens-if-it-requires-nationwide-id
18. Defend Digital Me (2026), *Who is age-gating our life online?* section 7.6, Children's rights implications of social media minimum age restrictions and AV.
19. O'Flaherty, M. (2026). Regulate online platforms, not children. Council of Europe Commissioner for Human Rights. https://www.coe.int/en/web/portal/-/regulate-online-platforms-not-children
20. OHCHR (2026). Protection of children online needs to be done right: UN Human Rights Office issues guidelines for child safety online. https://www.ohchr.org/en/press-releases/2026/05/protection-children-online-needs-be-done-right-un-human-rights-office-issues
21. Ofcom (2026, 29 October). Rapid assessment of highly effective age assurance at 16. Overview and para. 3.43. https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/protecting-children/rapid-assessment-of-highly-effective-age-assurance-at-16.pdf