

# **BIG BROTHER WATCH**

**Big Brother Watch's Briefing  
on Government plans to  
enforce an under 16s social  
media ban through "hard" ID  
checks**

**October 2026**

## **About Big Brother Watch**

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous technological change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

## **Contact**

### **Silkie Carlo**

Director

**Direct line: 0208075 8478**

Email: [silkie.carlo@bigbrotherwatch.org.uk](mailto:silkie.carlo@bigbrotherwatch.org.uk)

### **Maya Thomas**

Legal and Policy Officer

**Direct line: 07864733785**

Email: [maya.thomas@bigbrotherwatch.org.uk](mailto:maya.thomas@bigbrotherwatch.org.uk)

## **Introduction**

Children deserve an online experience where they are safe, protected and can easily access adult help if something goes wrong. However, we are deeply concerned that the Government's social media ban would work against these goals. Requiring users to upload a digital ID document such as a passport or driving licence, or to undergo a credit check in order to access social media will not guarantee children's safety. Instead, it would introduce a host of serious unintended risks that will affect the safety, cybersecurity and human rights of children and adults alike.

For children, a social media ban enforced through mass ID checks would:

- Fail to reliably keep under-16s off social media.
- Cause social media platforms to abandon a raft of child safety measures and de-incentivise safety by design.
- Drive children to less regulated corners of the internet.
- Prevent children, who may soon be able to vote in elections, from reading and engaging with legitimate political discourse.
- Make it less likely for young voters aged 16 and 17 to access news and discourse through social media

For children and adults alike, hard ID checks for social media would:

- Introduce mandatory digital ID or credit checks for the entire UK population, locking millions of people out of social media who do not have or do not wish to use ID online, and creating serious cybersecurity risks for those who do
- Force millions of people to submit their most sensitive personal data to platforms or third-party age-verification services, putting them at serious risk of data breaches
- End anonymity on social media and introduce a serious chilling effect on freedom of expression. This will be felt particularly strongly by the many journalists, campaigners, domestic abuse victims, members of LGBTQ communities and others who rely on online anonymity for safety and free expression.
- Automatically exclude millions of Britons from social media entirely, simply because they do not have a valid ID document.

## Expert opposition

Far from keeping under-16s safer, a blanket ban on social media would cut children off from educational resources, community support groups, and children's safeguarding services.

**42 leading children's organisations, experts and bereaved families, including the NSPCC and Molly Rose Foundation** have said in a joint statement that they do not support a social media ban.<sup>1</sup>

**Human rights experts, including the Council of Europe's Commissioner for Human Rights<sup>2</sup> and Amnesty International<sup>3</sup>** oppose a social media ban for children.

Big Brother Watch is one of a large group of **20+ European digital rights organisations** joined in a coalition called Stop Killing the Internet, campaigning against social media bans for children and for more Big Tech accountability.

## Build a better internet

To effectively tackle the harms faced by children on social media, the Government should instead:

- Require companies to implement safety-by-design principles when creating their platforms.
- More effectively regulate data exploitation by Big Tech social media platforms.
- Support parents with accessible information about how to impose healthy, age-appropriate restrictions on their children's internet use (only one in three parents currently use any parental controls).
- Require platforms to engage in algorithmic transparency practices.

**Big Brother Watch urges MPs to oppose the Government's plans for a social media ban and to join the petition debate on Monday 2nd November at 4:30pm.**

<sup>1</sup> Joint statement from children's and online safety organisations, experts and bereaved families on a social media ban for under-16s – Molly Rose Foundation and others, January 2026: <https://mollyrosefoundation.org/wp-content/uploads/2026/01/Joint-statement-from-childrens-and-online-safety-organisations-experts-and-bereaved-families-on-a-social-media-ban-for-under-16s.pdf>

<sup>2</sup> Regulate online platforms, not children: Commissioner for Human Rights urges caution over social-media bans, 23 February 2026: <https://www.coe.int/en/web/portal/-/regulate-online-platforms-not-children>

<sup>3</sup> Australia: Government should strictly regulate social media platforms, not ban children and young people – Amnesty International, 10 December 2025: <https://www.amnesty.org.au/social-media-ban-for-children-and-young-people-an-ineffective-quick-fix-that-will-not-prevent-online-harms/>

## **Hard ID Checks for Social Media Make Children Less Safe**

Children deserve an online experience where they are safe, protected and can easily access adult help if something goes wrong. However, we are deeply concerned that the Government's social media ban, particularly if enforced through hard ID checks, would actively work against these goals.

Experts including Nicola Killean, Scotland's Children and Young People's Commissioner and Chris Sherwood, CEO of the NSPCC have warned that a social media ban risks driving children towards darker corners of the internet as they will migrate to unregulated platforms.<sup>4</sup>

We are deeply concerned that the existence of a social media ban would allow platforms to assume that children are no longer using their services, thereby removing the incentive to design them in a way that is safe.<sup>5</sup> However, evidence from Australia shows that three months after a government social media ban was implemented there, a staggering 81.5% of teenagers were still accessing age-restricted social media platforms. In the same period, parental awareness of children's social media use declined by 10%.<sup>6</sup>

This is a concerning trend. Internet Matters notes that parents are often who children turn to when something goes wrong online, and that when children choose report an online harm they have experienced to a social media to a platform, parents and guardians play an essential role in supporting them.<sup>7</sup> However, if a child has circumvented a Government-imposed ban, particularly without their parents knowing, they may be even less likely to speak to a trusted adult if they experience any online harms. Polling conducted by the Molly Rose Foundation, FlippGen and the Breck Foundation shows that children's confidence in speaking to a parent about online safety drops by 12% in such a scenario.<sup>8</sup> Similarly, a child who has circumvented a ban may also be reluctant to report harm to the platform itself, for fear that doing so would reveal their age and lead to their account being removed.

---

4 BBC News, 'Social media ban 'won't keep children safe', commissioner warns', 29 May 2026; <https://www.bbc.co.uk/news/articles/c1721n4klp2o>

5 Plan International, 'Social media ban would sideline action on the addictive algorithms that drive misogyny, charity warns', 8 June 2026; <https://plan-uk.org/press/social-media-ban-would-sideline-action-addictive-algorithms-drive-misogyny-charity-warns>

6 esafety Commissioner, 'Early days early insights: Understanding experiences of social media age restrictions at the three-month follow-up'; July 2026; <https://www.esafety.gov.au/sites/default/files/2026-08/Early-days-Early-Insights-SMMA-Evaluation-Understanding-experiences-of-social-media-age-restrictions-August2026.pdf?v=1787148433841>

7 Internet Matters, 'Understanding and improving how children report online harm: Data briefing', May 2025

8 Molly Rose Foundation, 'Some teens could feel less confident speaking to safe adults about online safety worries once the social media ban comes into effect'; <https://mollyrosefoundation.org/some-teens-could-feel-less-confident-speaking-to-safe-adults-about-online-safety-worries-once-the-social-media-ban-comes-into-effect/#:~:text=confidence%20in%20speaking,despite%20a%20ban.>

We are deeply concerned that a social media ban enforced through hard ID checks would lead to online harms such as grooming and sextortion going unreported for longer, or not at all, while children are left to deal with the consequences alone.

A ban that pushes children's online lives out of sight leaves them less safe, not more.

### ***State of New Mexico v Meta Platforms, Inc.***

The landmark judgment against Meta in New Mexico in August 2026 marks a significant shift in the legal treatment of child safety online and required an overhaul of Meta's platforms.

The court ordered Meta to implement a five-year set of court-supervised safety and structural reforms to Facebook and Instagram, and to pay a \$375 million civil penalty alongside \$567 million into a New Mexico state abatement fund for teen mental health bringing its total financial liability in the state to \$942 million. The measures include stronger age verification, mandatory time limits for under-18s, restrictions on overnight notifications, default privacy protections and enhanced safeguards against child sexual exploitation.

Whilst Meta must now plan to redesign its products in the US, UK Government threats of an outright ban on children accessing their platforms creates a completely different incentive in the UK. In the UK, platforms are being threatened with legislation that would make them explicitly *adult* platforms, creating no incentive at all for them to implement the child safety measures being developed for other parts of the world. Given the high likelihood that millions of children will continue to access these platforms, as per Australia, this diversion from the US approach could have serious negative consequences.

## **Privacy and Cybersecurity**

### **A Trojan Horse for Digital ID**

Hard ID checks would force the UK's 68 million internet users to hand over copies of their passports, driving licences and financial records to foreign companies simply to use social media. This would constitute a de facto mandatory digital ID system – which millions of people opposed last year by signing petitions and joining Big Brother Watch's No2DigitalID campaign,<sup>9</sup> resulting in Prime Minister Andy Burnham rightly scrapping the scheme in one of his first major policy announcements.

---

<sup>9</sup> See for instance: Parliamentary Petition, 'Do Not Introduce Digital ID Cards', closed on 9 January 2026; <https://petition.parliament.uk/petitions/730194>; Big Brother Watch, No2DigitalID; <https://bigbrotherwatch.org.uk/campaigns/no2digitalid/>

Recent Ipsos polling shows that public support for an under-16 social media ban drops significantly when nationwide ID or credit card verification is required.<sup>10</sup>

Due to concerns about privacy and accessibility, Australia's social media ban explicitly prohibits platforms from collecting government-issued ID unless a reasonable alternative is offered.<sup>11</sup> It is deeply concerning that the Government is planning to introduce such a controversial policy via secondary legislation, without full parliamentary scrutiny.

### **Offline Age Checks Cannot Be Compared to Online Age Checks**

In debates about social media restrictions, parallels are often drawn between offline ID checks, such as those required to buy alcohol, and online ID checks. However, the two raise very distinct data protection and rights issues. Firstly, offline ID checks are not universal but rather are applied with discretion in relation to controlled substances. Secondly, unlike offline ID checks, online checks necessarily electronically collect, process and store highly sensitive personal information. This means that any time ID information is uploaded to the internet, it is put at risk of being hacked, leaked or sold. This risk persists even if the personal information is stored or processed only briefly.

### **The Myth of 'Instantly Deleted Data'**

There is no guarantee that a platform's promise to delete ID information immediately will be kept. An October 2026 report by Defend Digital Me about age verification systems used under Australia's social media ban shows that data retention practices vary widely. For instance, while the third-party age-verification service used by Facebook and Instagram deletes ID documents after the check is done, Meta itself retains its own copy for up to 30 days. Exposed code from Persona, a verifier used by Discord, Reddit and Roblox, showed its software was capable of retaining names and government ID numbers for up to three years. The Australian Government's Age Assurance Technology Trial found that some providers even retained personal data in anticipation of future requests from regulators and law enforcement – in other words "just in case".<sup>12</sup>

<sup>10</sup> Bogdan, A., '2 in 3 support social media ban for under-16s, though support softens if it requires nationwide ID verification', Ipsos, 6 July 2026, <https://www.ipsos.com/en-uk/2-3-support-social-media-ban-under-16s-though-support-softens-if-it-requires-nationwide-id>

<sup>11</sup> Australian Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Social Media Minimum Age – Fact Sheet', December 2025; <https://www.infrastructure.gov.au/sites/default/files/documents/social-media-minimum-age-and-age-assurance-trial-fact-sheet-july-2025.pdf>

<sup>12</sup> Persson, J. and Stone, M., Defend Digital Me, *Analysis of the technology used in the Australian Social Media Ban, emerging proposals in Europe, and the outcomes for privacy and data protection rights*, 20 October 2026; <https://defenddigitalme.org/wp-content/uploads/2026/10/Who-is-Age-Gating-our-Life-Online-v3.pdf>

## A Honeypot for Hackers

The mass collection of highly sensitive passport, driving licence and credit check information used for age-verification purposes creates a honeypot for hackers, criminals, abusers and hostile states. ID information is valuable, and can be abused in a wide variety of ways, including for fraud, identity theft, stalking, harassment, and surveillance. The personal information on an ID document cannot be changed. This means that, unlike a password, once it falls into the wrong hands, that damage is permanent.

At a time when cybersecurity risks are the most serious and numerous they have ever been, and in a context of growing autonomous AI and hostile foreign state threats, this policy's profound implications for the architecture of the internet and our safety in it do not appear to have been appropriately assessed. It is not clear that the Government has assessed the serious cybersecurity risks or planned to mitigate them. It is not enough to simply defer such fundamental national security risks to foreign, profit-seeking companies.

### Case study 1: Discord<sup>13</sup>

In 2025, ID photos used to verify the ages of over 70,000 users of the social media platform Discord were leaked in a data breach after hackers targeted the third-party company it used to conduct the age verification tests. A year later in October 2026, Double Counter, a third-party service used by Discord to verify so-called 'alt-accounts' faced a data breach exposing usernames, email addresses and other personal information of its 28 million users.<sup>14</sup> While luckily this leak did not include ID information, it is a chilling example of the frequency at which social media users' information is targeted by criminal actors.

### Case study 2: Tea app<sup>15</sup>

In 2025, over 72,000 images including scans of passports and driving licenses used for age verification purposes on the women's dating safety app Tea, were leaked and posted onto the notorious messaging board 4chan. This was despite users being told that these images would be 'deleted immediately'. The metadata attached to images the users had taken of themselves was then reportedly paired with data collected from their ID documents by a 4chan user to create an interactive map on which the women's

<sup>13</sup> Chia, O., 'ID photos of 70,000 users may have been leaked, Discord says', BBC News, 9 October 2025 <https://www.bbc.co.uk/news/articles/c8jmzd972leo>

<sup>14</sup> P. Okunyte, 'Hackers take over Discord security bot, spam groups, and steal from credit cards', 8 October 2026; <https://cybernews.com/security/discord-user-data-breach/>

<sup>15</sup> Wakefield, J. 'My ex stalked me, so I joined a dating safety app. Then my address was leaked', BBC News, 23 August 2025, <https://www.bbc.co.uk/news/articles/ce87rer52k3o>

addresses, names and photos could be found, and women could be ranked by attractiveness.<sup>16</sup>

Big Brother Watch is deeply concerned that mandatory hard ID checks for social media would severely increase the scale and likelihood of similar data breaches.

## **An End to Online Anonymity**

Social media use is typically tied to an individual account. Consequently, ID information used to verify the age of a user is necessarily connected to this account as well. This introduces the serious risk that a user's ID document may be tied to their online activity, and once this link exists, users can no longer trust that what they say and do online will not be traced back to them. Without that trust, meaningful online anonymity ceases to exist. A user may still post under a pseudonym, but their identity is only ever one breach, leak or data request away.

## **Freedom of Expression**

This has serious consequences for freedom of expression. There are many legitimate reasons why law-abiding people may want to access social media anonymously, including for the purposes of seeking advice on financial, relationship or health matters, or to participate in civic life by engaging in discourse, organising protests or expressing critique against the government or an employer.

For vulnerable people, including victims of domestic and/or sexual assault, members of the LGBTQ community, people belonging to (or distancing themselves from) religious minorities, or people struggling with stigmatised issues like addiction, anonymity is a matter of immediate safety as well as free expression.<sup>17</sup> In many cases, members of these groups already struggle to seek help or advice, and we are deeply concerned that mandatory age verification would put up yet another barrier preventing them from doing so.

Especially for vulnerable people without access to a passport or driving licence (for instance because an abuser has confiscated it), or those not willing to take the risk that their ID information will be leaked in a data breach or sold to be used for advertising or surveillance, social media access enforced through hard ID checks would be devastating.

<sup>16</sup> Madan, S., 'Tea App Map Goes Viral After 4chan Leak. Are Users Now Being Tracked?', 26 July 2025; <https://www.timesnownews.com/world/us/us-buzz/tea-app-map-goes-viral-after-4chan-leak-are-users-now-being-tracked-article-152347670>; Williams, A. 'Tea app fallout worsens as leaked selfies used in rating site, online map', 28 July 2025.

<sup>17</sup> See for instance: Floreani, S. 'Anonymity online is important', Digital Rights Watch, 30 April 2021; <https://digitalrightswatch.org.au/2021/04/30/explainer-anonymity-online-is-important/>

## Targeted Advertising

We are deeply concerned that where a link between a user's ID or credit check information is created, it could easily be used by Big Tech companies or third party services to deepen personal data collection. Companies like Meta have a long history of using sensitive information to target advertisements, allegedly even directing advertisements for beauty products to teenagers who had recently deleted selfies.<sup>18</sup> As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our ID documents – even if this access is only momentary – would only result in further escalation of the granular targeting of users across platforms. Importantly, even if an ID document is deleted immediately, the platform keeps information from the user's ID document linked to their account. At best, this is a signal that the user is over 16. At worst, it includes all personal information from an ID document. Combined with the vast behavioural data already collected by Big Tech platforms, from viewing habits and interactions to location and time spent on content, this makes every other data point more valuable for profiling and targeted advertising.<sup>19</sup>

## Exclusion and Discrimination

Millions of Britons do not hold the identity documents on which hard ID checks rely, and under this proposal risk being locked out of social media entirely. Census 2021 data from the Office for National Statistics shows that 13.2% of residents in England and 18.8% of residents in Wales do not hold a passport.<sup>1</sup> These figures were particularly high amongst economically disadvantaged communities.<sup>3</sup>

Since 16 year olds can't drive or undergo a credit check, this authoritarian policy essentially requires passports for the internet.<sup>20</sup> Over 530,000 16-24 year olds in England and Wales alone do not hold either a British or foreign passport,<sup>21</sup> meaning this Labour policy could lock out thousands of young, disproportionately poorer, people from the internet.

Given plans to give 16 and 17-year-olds the vote, their heightened likelihood of being unable to provide an appropriate ID to access social media is all the more concerning. Ofcom has found that three quarters of young people aged 16 to 24 use social media as their primary method for accessing news. The reality of this policy would therefore be that a huge number of young people would no longer be able to access news in the

<sup>18</sup> Wynn-Williams, S. *Careless People: A Cautionary Tale of Power, Greed, and Lost Idealism*, Flatiron Books, 2025

<sup>19</sup> Persson, J. and Stone, M., *Defend Digital Me, Analysis of the technology used in the Australian Social Media Ban, emerging proposals in Europe, and the outcomes for privacy and data protection rights*, 20 October 2026; <https://defenddigitalme.org/wp-content/uploads/2026/10/Who-is-Age-Gating-our-Life-Online-v3.pdf>

<sup>20</sup> Ofcom, 'Report on the use of age assurance', 15 July 2026; <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/age-assurance-report-2026/report-on-the-use-of-age-assurance.pdf?v=423162>

<sup>21</sup> ONS 2021 data: [https://www.ons.gov.uk/datasets/RM109/editions/2021/versions/1?showAll=passports\\_all\\_18a#passports\\_all\\_18a](https://www.ons.gov.uk/datasets/RM109/editions/2021/versions/1?showAll=passports_all_18a#passports_all_18a)

way they are used to. Hard ID checks would therefore cut many of the UK's newest voters off from the platforms where they are most likely to encounter news and political debate, at the very moment they are entering democratic life.

A policy that makes access to political information conditional on holding a passport risks entrenching existing inequalities in democratic participation. Because young people typically rely on their parents to navigate the process of obtaining an adult passport, those from households without ID are less likely to hold any themselves, and less likely to have support with the application. An adult passport currently costs £102,<sup>22</sup> more than most 16 year olds have independent access to. As a result, young people from lower-income, non-passport-holding households would either be more reliant on their parents paying the upfront cost of a passport, or be forced to gain access to social media later than their more affluent peers after they have saved up the money themselves.

Freedom of expression is a universal right, but requiring ID to access social media would prevent millions from exercising it in the spaces where, in practice, most of our civic debate takes place. We are therefore concerned that a ban enforced through a mechanism that prevents a significant portion of eligible users from accessing a service cannot be considered proportionate, democratic or fair.

### **Legal action against social media bans**

Across the world, governments trying to implement social media bans are facing robust criticism from children's safeguarding groups, civil society organisations, cybersecurity experts as well as individual children and adults. For instance:

#### *France*

In July 2026, the French Parliament voted to block under-15s from accessing major social media platforms. Just a month later, this proposal was blocked by the French Constitutional Council, the country's top court, on the grounds that it was not consistent with human rights. In particular, the Council held that the proposed ban would infringe on the free expression of minors, and that its age-verification requirements contained insufficient safeguards for the privacy of all users. Additionally, the Council criticised the proposal for not including provisions allowing parents to make independent decisions regarding what amount of social media access is appropriate for their child.<sup>23</sup>

<sup>22</sup> HM Passport Office, 'Renew or replace your adult passport' (GOV.UK) <https://www.gov.uk/renew-adult-passport>. Standard online application fee from 8 April 2026.

<sup>23</sup> Gkritsi, E., Marzolf, E. and Durand, K., 'French court blocks social media ban for under-15s', 14 August 2026 ;<https://www.politico.eu/article/french-constitutional-court-shoots-down-social-media-ban-for-minors/>

## *Australia*

Immediately after Australia introduced its social media ban on 10 December 2025, two teenagers, backed by the Digital Freedom Project launched a legal challenge against it on the grounds that it goes contrary to Australia's constitution.<sup>24</sup> Specifically, they are concerned that Australia's ban is not proportional given the many other methods parents and platforms can employ to make sure children have a safe online experience, including parental controls, safety-by-design and digital literacy programs.<sup>25</sup>

## *India*

In October 2026, India's Supreme Court rejected the case for a social media ban, arguing that a blanket social media ban would infringe on the freedom of expression of children, and arguing that a ban would risk driving children towards less regulated corners of the internet. In their decision, the justices argued that "No jurisdiction has, so far, been able to demonstrate that children are any safer on account of such measures [social media bans]."<sup>26</sup>

---

<sup>24</sup> Turnbull, T. 'Teens launch High Court challenge to Australia's social media ban', 26 November 2025; <https://www.bbc.co.uk/news/articles/c9d9l7w1g8yo>.

<sup>25</sup> See Digital Freedom Project, 'Our High Court Case'; <https://www.bbc.co.uk/news/articles/c9d9l7w1g8yo>

<sup>26</sup> 'India's Supreme Court takes action on child internet harms', 20 October 2026; <https://iclg.com/news/indias-supreme-court-takes-action-on-child-internet-harms/>