

BIG BROTHER WATCH

**Response to “Growing Up in the
Online World: A National
Consultation” by the Department for
Science, Innovation and Technology**

May 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: 020 8075 8478

Email: silkie.carlo@bigbrotherwatch.org.uk

Maya Thomas

Legal and Policy Officer

Direct line: 07864733785

Email: maya.thomas@bigbrotherwatch.org.uk

Introduction

During the passing of the Children's Wellbeing and Schools Bill, the Government voted to introduce a social media ban for under-16s. To establish the scope of the ban and how it could be implemented, the Department for Science, Innovation and Technology published "Growing Up in the Online World". This consultation included both multiple choice and text-based questions. This document sets out our responses to the text-based questions most relevant to our expertise and, where necessary, includes our responses to multiple-choice questions where these are directly relevant to our written answers.

1. What are the benefits of social media use, and being online, for children?

As one of the most multifaceted technologies in history, social media's impact on children fundamentally depends on how it is used. Asking what the benefits of social media use are

is akin to asking about the benefits of 'media', or even just 'information' or 'talking'. In the vast majority of cases, they are context-dependent.

Academics and governments across the world have struggled to identify a clear definition of 'social media', which has often led to confused debate around what it means to restrict it. For the purposes of our response, we will assume that 'social media' refers to the list of ten services that were restricted for Australian children under-16, as well as platforms that operate in a similar way. However, we remain concerned that terms like 'user-to-user service', which appears in the Online Safety Act, or 'specified internet service', which is used in the Children's Wellbeing and Schools Bill, are extremely broad, and any restrictions designed around these terms could inadvertently also affect platforms or services that are overwhelmingly beneficial for children.

Social media networks and feeds provide access to a wealth of educational and creative information, including from children's organisations as well as different countries and cultures. They have allowed hundreds of millions of children and young people to connect and interact on a huge variety of topics and scales. As a free and easily accessible medium, social media can significantly empower children to shape their own learning by exploring interests, skills, hobbies, and languages not offered in a school context.

According to an Ofcom report on 'News Consumption in the UK', as of 2025, over half of 12-15-year-olds use social media platforms to access the news, including information from trusted, large-scale media outlets like the BBC. For children who may not otherwise actively try to access the news via more traditional means like broadcasts or websites, receiving news alerts via social media can be a helpful and easily accessible way of keeping up with current events. Social media helps children discover and engage with smaller, or more niche news outlets, as well as local journalists. Social media allows children to discover and engage with a diverse range of news stories in real time, and also allows them to follow the experiences of their peers across the world first hand.

In this way, social media provides children with an accessible way with which they can practise being civically and politically engaged. We are concerned that, particularly at a time where the government is considering giving 16-year-olds the vote by 2029, restricting social media for children would deprive young soon-to-be voters of opportunities to gain and strengthen political literacy skills. Additionally, the UNHCR explicitly grants children the right to organise politically, and young people have used social media to exercise this

right. This includes the organisation of, and participation in, mass protest movements like the Climate Marches, as well as creating and engaging with content exploring young people's perspectives on political events.

Social media provides children with access to political, social, and cultural perspectives that may be absent from their immediate environment. This is particularly important for children raised in restrictive or ideologically narrow household or school environments, as online platforms can expose them to alternative viewpoints and broaden their understanding of the world. For instance, a child growing up in a highly religious household may encounter secular perspectives for the first time online, while another from a more liberal background may use social media to explore different views on national identity or tradition. Social media also allows children with similar experiences, such as those questioning their upbringing or identity, to find support and community that may be absent in their immediate environment.

This ability to explore and connect with people outside of their immediate environment is particularly important for vulnerable children whose circumstances –including domestic abuse at home or low school attendance– can preclude them from seeking advice through more traditional routes. Many children's charities recognise this, and consequently have a prominent presence on social media. As of May 2026, Missing People launched a WhatsApp service that lets children and young people in crisis message for help instead of calling, as this is often less confrontational for this age group. Similarly, besides hosting their own moderated user-to-user service for children, Childline uses Instagram to share resources with children and teenagers in an accessible format. The NSPCC has expressed their opposition to a social media ban along with 41 other children's organisations (including the 5 Rights Foundation and Internet Matters) and bereaved parents (including the father of Molly Rose Russell).

For children rejected by families because of their sexual orientation, social media provides a space where they can seek help, resources, community and joy. There are hundreds of organisations like 'It Gets Better' who offer advice, resources and support to LGBTQ+ teens through social media, as well as a vast ecosystem of thousands of creators who do so by sharing their stories, but also create positive content exploring identity.

For children who are isolated from their offline peers, either because they are the victims of bullying at school, because they live in geographically remote areas, or due to physical

and/or mental disabilities, social media can offer a space to interact, make friendships and experience being part of a larger community of peers.

For economically disadvantaged children living in deprived areas, attending less well-resourced schools, or whose parents cannot afford or manage the logistics of extracurricular activities outside school, social media provides a huge range of opportunities for extracurricular enrichment. According to a 2024 report by the Education Policy Institute, children attending state schools were about 20% less likely to attend sports, arts, and hobby clubs than students at independent schools. Social media has democratised access to cultural and practical knowledge that was once reserved only for children from more advantaged social backgrounds and may ameliorate the gap. This also includes hard skills (like coding, video editing or learning a new language) and soft skills (like communication, researching, critical thinking) that can shape a child's choice of school subjects or career decisions.

2. What are the harms or risks of social media use, and being online, for children?

As with benefits, the possible harms and risks associated with social media are as diverse as the platforms and the content itself. Big Brother Watch supports this consultation's effort to better understand the harms and risks as reported by the general public, as this is not currently well understood.

Evidence submitted by the Digital Mental Health Group to the Science, Innovation and Technology Parliamentary Select Committee highlights the existing evidential gap. Specific harms to individual users have been identified, but harms at a population level, particularly harms which would be meaningfully ameliorated by blanket approaches such as age verification requirements or curfews, are not, at present, well established.

The Digital Mental Health Group notes "The question of whether to implement a social media ban is one of weighing up risks between adopting an intervention whose evidence base is still poor, or waiting to gain more evidence while the potential benefits of this intervention are not experienced (and individual-level harms can still accumulate)". Big Brother Watch agrees in part but notes that an age-gating policy also introduces a new set of harms for children.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the

wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information - earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents -even if this access is only momentary- would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those

with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfakes videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be

pushed towards more intrusive forms of age verification, like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

6. Would you support a legal requirement for social media services to have a minimum age of access lower than 16? If so, at what age would you set it?

a. Yes — 13

b. Yes — 14

c. Yes — 15

d. No — not lower than 16

e. Other (please specify)

This question did not offer respondents a clear option to voice their opposition to there being a minimum age of access at all. Big Brother Watch does not support legal minimum age requirements for social media services if this is enforced through invasive age verification technologies, including digital ID uploads or biometric face scans.

The Government and Ofcom have strongly advocated for the use of age-assurance technologies to enforce age-based restrictions to online spaces and/or features and functionalities. However, requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal

information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain

anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfake videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this

technology means that certain users are more likely to be pushed towards more intrusive forms of age verification, like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

7. What do you think the impacts would be of having a minimum age requirement higher than 13 for social media services? For example, impacts on the safety and wellbeing of children, or the impact for parents and carers, as well as other users. You could also comment on the impact on all users' privacy and data or on business costs, revenue and innovation.

Regardless of the specifics of minimum age requirements, Big Brother Watch does not support legal minimum age requirements for social media services if this is enforced through invasive age verification technologies, including digital ID uploads or biometric face scans.

The Government and Ofcom have strongly advocated for the use of age-assurance technologies to enforce age-based restrictions to online spaces and/or features and functionalities. However, requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded

to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

We also note that any minimum age requirement enforced through parental consent mechanisms compounds rather than resolves these risks: linking verified adult identities to specific children creates new opportunities for predators and hostile actors that do not exist under the current system by creating a route to children through their parents.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those

with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfakes videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be

pushed towards more intrusive forms of age verification, like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

10. What should be considered to make raising the digital age of consent effective and workable? For example, suitable approaches to verify users' ages (including where parental consent is required) or suitable approaches to verify a parent or carer's identity, age and relationship to the child.

Requiring a parent or carer to prove their identity, age and relationship to a child will create a de facto mandatory digital ID scheme for parents, who would necessarily need to prove the connection between them, not just their age. Moreover, if implemented, such an approach introduces a new set of risks of harm to children and adults. Existing parental controls do not create these risks.

The only way to link a specific adult to a specific child is to collect the ID documents of both. Alternatives like biometric face scans will not suffice as they do not provide evidence of a relationship. Parents will therefore be required to have and give ID if they wish to give their children access to social media. Public support for, and confidence in, such schemes is low. More in Common polling identified a decline in support for a recent mandatory ID scheme from a net +35% support to a net negative -14% following its announcement, support remaining low even for a non-mandatory version. A Parliamentary petition on the subject raised nearly three million signatures.

Any leak, hack or future commercial use of data connecting specific children and adults would also expose children to a new risk from predators, and children and adults to risks relating to hostile regimes.

A database linking specific children to named adults would give those who seek to harm children a new avenue of approach. Any actor able to compromise a parent's account would gain a verified connection, enabling them to identify and locate the child. If such a system also gave parental access to see or exert control over the child's online activity, this power would also fall into the hands of anyone able to gain access and create a tool for grooming and coercion.

For children of political dissidents, particularly those who have escaped hostile regimes, a leak could be used by those regimes to target them and their parents for exercising their freedom of speech in Britain. For many activist parents, knowledge of this risk alone would be enough to chill their willingness to engage in legitimate political activity and the exercise of their Article 10 and 11 rights.

Parents unwilling to expose themselves and their children to these risks would face a binary choice between complying with a scheme they have good reason to distrust or effectively removing their children from social media entirely. This would not be a burden distributed evenly across society. The parents with the strongest reasons to protect their privacy, political dissidents, foreign nationals whose families remain under hostile regimes, survivors of domestic abuse, whistleblowers, and journalists would be acutely impacted.

11. To what extent do you agree or disagree with the following statement: "There is a case for changing the digital age of consent for some online services but not others"

C. neither agree nor disagree

It is important that extra care is taken when platforms, services or companies process children's data, and we are generally satisfied with the provisions made in the GDPR to ensure this.

However, due to its many risks, Big Brother Watch believes that the Government must find ways other than age verification technologies to enforce this.

The Government and Ofcom have strongly advocated for the use of age-assurance technologies to enforce age-based restrictions to online spaces and/or features and functionalities. However, requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfakes videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification like digital ID uploads. This is the very same group who the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

15. What do you think the impacts would be if some online services were required to introduce age restrictions on specific features and functionalities? For example, impacts on the safety and wellbeing of children, or the impacts for parents and carers, as well as other users. You could also comment on the impact on all users' privacy and data or on business costs, revenue, and innovation.

Any feature restriction that applies differently to users based on age necessarily requires a mechanism to establish that age, and consequently inherits all of the risks of such a system.

Differing functionalities do have different implications for potential harm, to children and adults. An approach focused on limiting access to functions, rather than regulating which functions are permitted at all, presupposes that the issue is the age of the user and not the product on offer. The solution to unsafe car manufacturing is not additional driving lessons tests. As the Joint Committee for the Draft Online Safety Bill recognised more broadly, 'The companies must be held liable for the systems they have created'.

Alternative approaches, that avoid age-verification technologies, include but are not limited to:

- Strengthening the regulation of permissible services, potentially requiring platforms to assess and report on the harms of specific functions;**
- Limiting Big Tech companies' ability to exploit user data (for instance, by promoting algorithmic transparency and expanding user control over content and data); and**
- Equipping parents and teachers with clear, up-to-date resources on digital literacy to help children establish healthier screen habits.**

20. What do you think the impacts would be if online platforms were required to restrict specific features or functionalities, or to introduce time limits? For example, impacts on the safety and well-being of children, or the impact for parents and carers, as well as other users. You could also comment on the impact on all users' privacy and data, or on business costs, revenue and innovation.

This question does not specify whether the restrictions described above would be age-based. If these restrictions are intended to be general and optional, we would welcome the Government encouraging platforms to launch versions of accounts that do not include specific features. We always welcome options that give adults and children alike more control over their screen habits. However, if the question is intended to refer to age-based restrictions, we oppose these.

The Government and Ofcom have strongly advocated for the use of age-assurance technologies to enforce age-based restrictions to online spaces and/or features and functionalities. However, requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfake videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification, like digital ID uploads. This is the very same group that the Electoral Commission has already warned face issues when voting because

they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

21. What factors are important when determining which apps, sites or services to apply minimum age of access restrictions to? For example, user-to-user interaction, the ability to post material, persuasive design features, risky functionalities, the ability to generate non-text mediums such as video or images, the target age group, the size of the service.

Regardless of the type of apps, sites or services (or features and functionalities thereof) that restrictions are imposed upon, if these restrictions are enforced through age-verification technology as the Government has suggested, they will all pose severe risks to the privacy, cybersecurity and freedom of expression of all users.

Requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and

its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfakes videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification, like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

22. Are there any types of apps, sites or services that you would want to be captured by minimum age of access restrictions?

No. We oppose the imposition of minimum age of access restrictions on all apps, sites or services if these are enforced through invasive age verification technologies, including digital ID uploads or biometric face scans.

The Government and Ofcom have strongly advocated for the use of age-assurance technologies to enforce age-based restrictions to online spaces and/or features and

functionalities. However, requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will

remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfake videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification

requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

23. What factors are important when determining which apps, sites or services to apply age-restrictions on specific features and functionalities? For example, user-to-user interaction, the ability to post material, persuasive design features, risky functionalities, the ability to generate non-text mediums such as video or images, the target age group, the size of the service.

Regardless of the type of apps, sites or services (or features and functionalities thereof) that restrictions are imposed upon, if these restrictions are enforced through age-verification technology as the Government has suggested, they will all pose severe risks to the privacy, cybersecurity and freedom of expression of all users.

Requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and

its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfakes videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

24. Are there any types of apps, sites or services that you want to be captured by age-restrictions to features or functionalities?

Regardless of the type of apps, sites or services (or features and thereof) that restrictions are imposed upon, if these restrictions are enforced through age-verification technology as the Government has suggested, they will all pose severe risks to the privacy, cybersecurity and freedom of expression of all users.

Requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will

instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply

concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfake videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

25. Some services are already exempt from the Online Safety Act. Examples include internal business services, services with limited functionalities and services provided by persons providing education or childcare. Are there additional types of services which you think would be appropriate to exempt from age restrictions? These might include services whose primary purpose is to deliver educational content, services that offer specific child or teen accounts or versions, or services which offer parental controls.

We fundamentally oppose all services being subjected to minimum age requirements if these are enforced through invasive means like digital ID uploads or biometric face scans.

The Government and Ofcom have strongly advocated for the use of age-assurance technologies to enforce age-based restrictions to online spaces and/or features and functionalities. However, requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and

its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfake videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

26. What are the benefits to children of using AI chatbots? For example, this might include as a search function, for educational purposes, for creativity.

Big Brother Watch does not have subject matter expertise on AI chatbots and how they are used by children. However, we remain deeply concerned by the dangers posed by age-gating online services.

The Government and Ofcom have strongly advocated for the use of age-assurance technologies to enforce age-based restrictions to online spaces and/or features and functionalities. However, requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at

keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply

concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfake videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

30. What do you think the impact would be of introducing age restrictions on AI chatbots or certain features and functions? For example, impacts on the safety and wellbeing of children, or the impact for parents and carers, as well as other users. You could also comment on the impact on all users' privacy and data or on business costs, revenue and innovation.

Regardless of the type of apps, sites or services (or features thereof) that restrictions are imposed upon, if these restrictions are enforced through age-verification technology as the Government has suggested, they will all pose severe risks to the privacy, cybersecurity and freedom of expression of all users. This also goes for AI technologies.

Requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions

of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfake videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for

online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification, like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

31. To what extent do you agree with this statement: "Adults should complete age checks more often, if it means children are safer online"?

It is a false dichotomy to present children's safety as being in conflict with adults' privacy. Both can exist simultaneously; online privacy for users of all ages actively contributes to children's online safety. Expanding age checks and surveillance does not inherently make children safer online and instead creates new risks of online harm to children and adults alike.

A more heavily monitored digital environment that normalises the routine surrender of personal data sets a concerning example for children, who will grow up with low expectations surrounding their right to privacy, cybersecurity and freedom of expression. These values are fundamental to living in a democratic society, and the steady erosion of them through routine age checks presents serious risks to the long-term freedoms of future generations.

The Government and Ofcom have strongly advocated for the use of age-assurance technologies to enforce age-based restrictions to online spaces and/or features and functionalities. However, requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images, including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfake videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because

they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

32. What should be considered to make minimum age restrictions effective and workable? This could mean either age restrictions for access to whole services, or for specific risky or 'addictive' features or functionalities.

By presenting age restrictions to whole services in opposition to age restrictions for specific features or functionalities, this question presents a dichotomy that does not exist. The societal impact of an age gate does not depend on what is restricted, but on the technology used to enact the restriction.

The Government and Ofcom have strongly advocated for the use of age-assurance technologies to enforce age-based restrictions to online spaces and/or features and functionalities. However, requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age checks, such as

those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents –even if this access is only momentary– would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age

verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfake videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification, like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

33. What do you think the impacts might be from requiring age assurance across a greater number of online platforms? For example, impacts on the safety and wellbeing of children, or the impact of parents and carers, as well as other users. You could also

comment on the impact on all users' privacy and data or on business costs, revenue and innovation.

Expanding the use of age-gating across platforms increases the number of users exposed to the risks associated with age-verification technologies.

The Government and Ofcom have strongly advocated for the use of age-assurance technologies to enforce age-based restrictions to online spaces and/or features and functionalities. However, requiring users to part with deeply sensitive personal information through digital ID uploads or biometric face scans will not be effective at keeping children safe and will instead create significant risks to the cybersecurity and freedom of expression of all users of all ages.

The mass collection of sensitive ID and/or biometric information creates a wealth of targets for criminals, abusers and hostile states. The more platforms that require users to undergo these checks, the greater the risk that ordinary people's IDs and biometrics will eventually fall into the wrong hands. There have been numerous examples of personal information used for age-verification purposes being leaked. In 2025, the ID information used to verify the ages of over 70,000 Discord users was leaked. There was a similar breach in 2025 on a women's dating app called Tea, leading to over 70,000 images including IDs and verification selfies, which users were told would be 'deleted immediately', being uploaded to 4chan. There is a global market for (large volumes of) personal information – earlier this year, the medical details of over 500,000 volunteer participants of UK Biobank were found listed on the Chinese market site Alibaba. The mass rollout of age verification technologies would significantly increase the risks of similar breaches of our most sensitive data, and expose all of the UK's 68 million internet users to unnecessary cybersecurity risks.

Online age checks for access to information and everyday websites cannot be compared to offline age-checks, such as those required for the purchase of knives or alcohol. Such age checks throttle access to speech and information, engaging millions of people's right to freedom of expression protected by Article 10 of the ECHR, not weapons or intoxicants. Further, offline age-checks do not collect or store any personal information. However, online age checks through digital ID uploads or biometric face scan technologies necessarily collect, process and store sensitive data. Even if on some platforms this storage is only for a brief moment, anytime information is collected digitally, there is a risk that it will be leaked, sold or abused.

The collection of such information for the purposes of allowing a user access to social media platforms also introduces the additional risk that it will be tied to their online activity, as social media platforms are almost always accessed via a personal account. Where such a link between a user's ID and/or biometric information is created, it could easily be used by Big Tech companies 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. As more companies pivot towards using AI to help increase advertising revenue, access to details as sensitive and permanent as our faces and/or ID documents -even if this access is only momentary- would only result in further escalation of the granular targeting of users across platforms.

The risk of data breaches and surveillance linked to age verification requirements creates a chilling effect on freedom of expression. By removing trust that a user will remain anonymous, age verification requirements make it so that those with legitimate reasons to want to avoid identification will feel less able to. We are deeply concerned that this will have serious implications for civil liberties and (online) safety. Journalists, dissidents, campaigners and activists wishing to engage in criticism of the British government, foreign repressive regimes, religious institutions or their places of employment would no longer be able to do so in the certainty that their online activities would remain anonymous. These same risks apply to victims of domestic abuse or control, for whom the additional friction of having to pass an age-gate will mean that many will be unable to, or deterred from using social media to reach out for help or access resources.

The only way for a remote third party to reliably establish an individual's age online is by requiring all users, adults and children alike, to upload a digital copy of an ID document, or by using a digital ID system. Naturally, ID information cannot be collected or processed anonymously, and this form of age verification consequently carries the highest risks for the user.

Age-assurance technologies designed to estimate a user's age anonymously also come with serious risks. Currently, the most popular of these methods is the biometric face scan. However, like ID information, biometric facial data is deeply sensitive, and its abuse after a data breach would have significant negative impacts on the user. Data from biometric face scans can easily be used to create deepfake videos and images, which fraudsters or abusers can use to bypass facial recognition systems used for online banking or produce

fabricated videos of a person making political or incriminating statements, and even to create convincing deepfake pornography of their victims.

Biometric face scans also come with serious accuracy flaws. No algorithm can accurately distinguish whether someone is one day over or one day under a specified minimum age, meaning that an ID requirement is inevitable for a whole generation of internet users. There are examples of children bypassing biometric age checks by drawing on fake moustaches, asking an older-looking friend or sibling to do the face scan for them, or simply being estimated as older because they went through puberty a few months earlier than their peers. The reality of biometric face scans is therefore that users will only be required to 'look' over a specified minimum age according to the (often) biased perception of an algorithm.

Furthermore, the rate of flawed age estimations increases for non-white faces, users wearing heavy or alternative makeup, and those with facial disabilities. Inaccuracy of this technology means that certain users are more likely to be pushed towards more intrusive forms of age verification, like digital ID uploads. This is the very same group that the Electoral Commission has warned already face issues when voting because they are less likely to have access to ID documents. Widespread age verification requirements would represent a public policy step with foreseen disproportionate impacts on marginalised communities.

Big Brother Watch is therefore deeply concerned that the widespread rollout of age-verification technology would not keep children safe, but would actively endanger the (online) safety, privacy, data protection and freedom of expression rights of the UK's 68 million internet users.

34. How, if at all, could age assurance be made more effective?

We believe that the most effective way of keeping children safe online is through the empowerment of parents to control their children's access to devices, as well as digital literacy education aimed at children, parents and teachers alike.

Age assurance through existing forms of age verification technology, like digital ID uploads or biometric face scans, already relies on the collection of disproportionately large amounts of sensitive personal information. Despite this, these methods remain deeply flawed, with Internet Matters' fifth annual 'Children's Wellbeing in a Digital World' report

suggesting that 46% of children find them easy to circumvent.

We do not believe that age assurance through age verification technologies (which is what the Government has most often referred to) can be made more effective without requiring users to upload even more amounts of even more sensitive personal information. Increasing the volume of sensitive information that users are required to upload also increases the risk that such information is leaked, sold or abused.

36. What methods to circumvent online safety rules do you think children in the UK use, beyond Virtual Private Networks (VPNs), or similar technologies.

A 2026 report from Internet Matters demonstrated that 26% of parents have helped their children circumvent bans, and many children ask friends or siblings to help them pass restrictions. Given the many accuracy flaws in age-verification technology, these friends and siblings do not even need to be older, but merely look older according to the algorithm used by biometric age estimation technologies.

Evidence from Australia's social media ban obtained by the Molly Rose Foundation shows that 60% of children still have access to social media after the introduction of age restrictions. Given the severely flawed and biased nature of age-verification technology, this is unsurprising. No algorithm can distinguish the biometric face scan of a 16-year-old on the day of their birthday from one taken the day before. With such a flawed system, many children do not need to use any distinct methods to circumvent age-verification technology - they simply rely on luck and coincidence.

39. What do you think the impact would be if VPNs were age-restricted? For example, impacts on the safety and wellbeing of children, or the impact for parents and carers, as well as other users. You could also comment on the impact of all users' privacy and data or on business costs, revenue and innovation.

Big Brother Watch very strongly opposes government-imposed restrictions on VPNs as these would represent a draconian crackdown on the cybersecurity and freedom of expression of users of all ages. The enhanced layer of privacy offered by VPNs means they are a vital tool that help keep individuals and their sensitive personal information safe online.

The only way presented so far by the government to enforce restrictions on VPNs would be for VPN providers to require all users to submit to invasive age verification technology. VPNs form the cornerstone of the digital infrastructure that helps citizens protect their privacy from a multitude of threats

online - including authoritarian governments. The ability to receive and share information absent unwanted commercial and state snooping is a vital part of living in a free democracy, and there is a reason why authoritarian governments in countries such as China, North Korea, Iran and Belarus ban or restrict VPNs.

The anonymity and enhanced privacy offered by VPNs allow journalists, whistleblowers, campaigners, and dissidents to communicate and access information securely. Requiring users to verify their ages through ID uploads or biometric face scans could seriously chill the activities of adults belonging to these groups, and would preclude children from safely participating in these activities online entirely.

For children wanting to use VPNs to access legitimate information without their parents' knowledge (e.g. information about sexuality, domestic, sexual or substance abuse, or political or religious beliefs that differ from their parents') the ability to access the internet privately and safely is particularly important, as not every child has a trusted adult they can speak openly with about these issues. Requiring age or identity verification would add significant friction between these children and their access to the internet, particularly given the accuracy flaws and cybersecurity risks of age-verification technology.

The same is true for adult victims of domestic abuse or control, for whom VPNs are one of the best ways to safely access online help without their abusers finding out. Many such users will not have easy access to a form of ID, and will be deterred from undergoing a biometric face scan for fear of data leaks or that their browsing activity will be tied to their personal identity.

Because age-verification requirements are fundamentally incompatible with online privacy, high quality VPN services may choose to withdraw from the UK completely. This would likely drive users towards unregulated, free or homemade VPN services, which may not offer the same protection and in some cases even collect and sell sensitive user data.

40. What should be considered to make age restricting VPNs effective and workable? For example, public trust and engagement with increased age assurance requirements, accessibility of age assurance methods and variations of age assurance approaches across services, interactions with legitimate uses of VPNs.

Big Brother Watch does not believe there are methods to make age restricting VPNs effective or workable which do not unduly impact the rights of UK citizens. See our response to Question 39

42. What impacts would there be if this guidance [no mobile phones in schools] was made statutory and why?

A statutory ban on smartphones in schools has already been brought into law through the Children's Wellbeing and Schools Bill. Big Brother Watch has no particular stance on the implications of such a ban.