Written evidence submitted by Yoti (OSB0130)

Table of contents

Will the proposed legislation effectively deliver the policy aim of making the UK the safest place to be online?

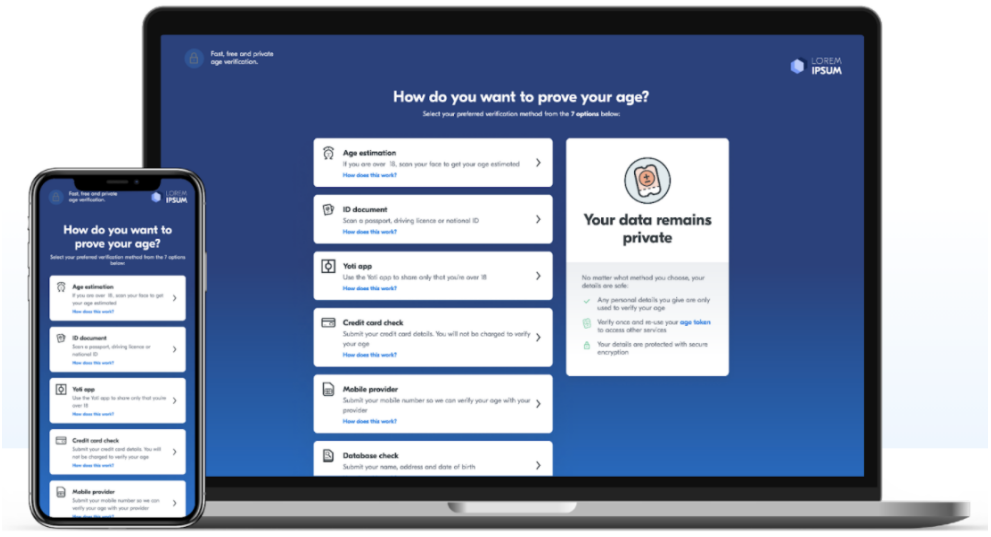
Yoti owns and operates a free digital identity app and wider online identity platform that allows organisations to verify their age online and in person. There are two areas where our approaches could support these policy aims - via standards based and independently accredited approaches to age verification and identity verification for social media registration.

Age verification

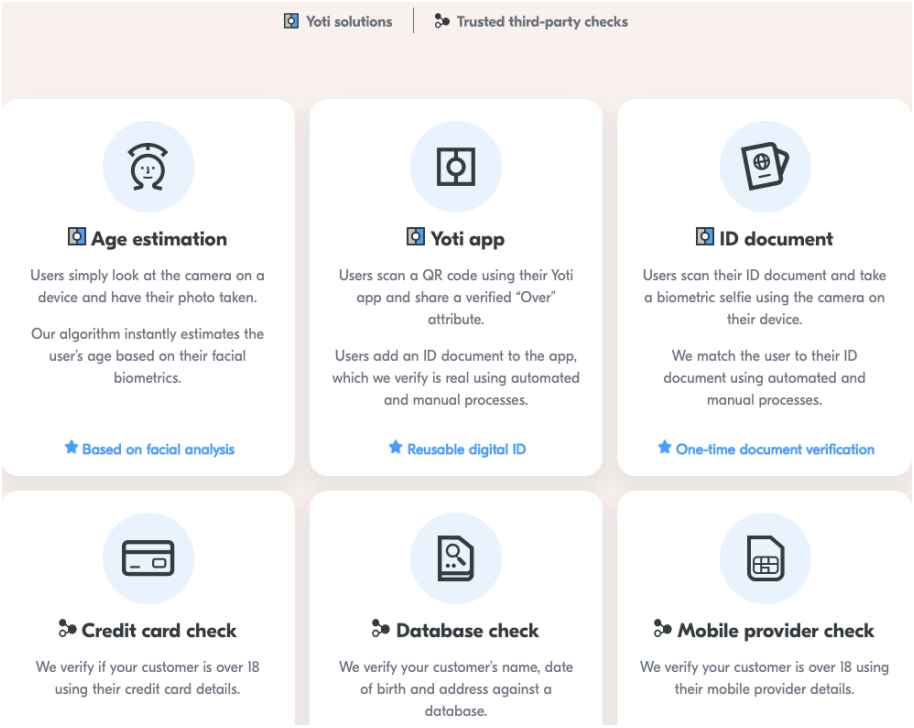
Yoti supports the premise of standards based age verification.

How age verification is delivered and ensuring the relevant safeguards are in place is crucial. As such, Yoti supports the Private Member's Bill - Age Assurance Minimum Standards[1]. It would be constructive if this Bill progresses at a faster pace than the Online Safety Bill, so that this area is tackled head on and in advance. The UK has developed an age checking standard - PAS 1296:2018 Age Checking, to which Yoti is accredited. Yoti also serves on the UK drafting group for the next ISO standard on age checking.

The Yoti platform has been designed to enable relying parties to meet requirements such as to ensure under 18s do not normally access age inappropriate content. We have developed an age portal so that organisations large and small can integrate and access a wide range of age checking approaches, through one simple integration, in just a couple of hours. This enables organisations which operate globally to assign the appropriate methods to each jurisdiction and undertake A/B testing with users.



[1] https://bills.parliament.uk/publications/41683/documents/325



Yoti has been live since November 2017 and has already surpassed 10 million installs globally. Yoti has undertaken over 500 million age checks using the Yoti age estimation algorithm since February 2019. Yoti has organised and participated in a number of roundtables for regulators and NGOs to understand its age checking approaches.

Yoti provides age verification services to global social media platforms, adult content websites, online gaming sites, e-commerce sites and physical retailers.

Yoti was the first organisation certified to the BBFC's Age Verification Certificate scheme, which was put in place to regulate the provision of age verification services under the Digital Economy Act 2017, part 3. This required Yoti's age verification services to adhere to very high standards for privacy and data security. Yoti has also been awarded the seal of approval from the German Association for Voluntary Self-Regulation of Digital Media Service Providers (FSM)[2] to provide age verification services in Germany. Yoti age services have also been reviewed by the KJM[3]. Yoti's Age Estimation has been reviewed by the Age Check Certification Scheme[4].

Users can perform age verification using the Yoti Digital ID app, which allows individuals to share verified information about themselves on a granular basis or it could be using Yoti's 'embedded' services which allow organisations to add a fully integrated identity verification flow into their website or app. It could also be using Yoti's age estimation algorithm. These verification options can be integrated as standalone solutions, or via the Yoti age verification portal offering more choice to the end users and configuration options to organisations. In all verification scenarios, Yoti calculates if the user meets the minimum age requirement to access the website.

[2] https://www.fsm.de/de/fsm.de/yoti
[3] https://www.kjm-online.de/service/pressemitteilungen/meldung?tx_news_pi1%5Bnews%5D=4890&cHash=e45ae6dfeee26fcd23d10c6994b7a9ef
[4] https://www.accscheme.com/media/2ntishhf/age-estimation-results-executive-summary.pdf

If the Yoti Digital ID app is used, an individual will scan a Yoti QR code with the Yoti app to share their age attribute. Then Yoti generates a hashed age token, which tells the website that the user is over the required age. The token and Yoti's record of the individual's age, or characteristic as over an age threshold, only last for the browsing session and do not identify the individual personally. Further, no personal information is shared with the site beyond the age attribute, making this a private and secure solution. The user's interaction with the website itself remains entirely anonymous.

Yoti generates a share receipt that only shows a date, timestamp, and that an age attribute was shared. Yoti stores this receipt securely in Yoti's data centre and the individual can view it in the Activity tab of the Yoti Digital ID app. These receipts can be archived by a user. Yoti cannot undertake tracking of users through the receipting mechanism.

If Yoti's fully integrated identity verification solution is used, the end user scans or uploads their ID document straight from their web browser or mobile app. An age is computed from the date of birth included in their ID document, and used to establish whether the person is old enough to pass the age verification test.

If the user uses Yoti's age estimation algorithm, users simply look into their phone's camera or their computer's webcam, and Yoti Age Scan will estimate their age. The image is captured and securely transmitted to Yoti's server using 256-bit encryption. Then, Yoti's algorithm gives a result in approximately 1.5 seconds. The image is immediately deleted from Yoti's servers and no record of the user is retained. The only output is an anonymous, hashed age token, used to determine if they are old enough to access the age-restricted content material. No user is personally identified or recognised.

Yoti Age Scan does have a margin of error. For initial rollout, after consultation with the nominated UK regulator, the BBFC, Yoti agreed to implement a three to five year safety buffer in its off-the-shelf solution. The accuracy continues to improve and now some organisations are looking at lowering this buffer, depending on their risk profile. For 13-24 year olds the MAE (Mean absolute error) is under 1.5 years of accuracy. The safety buffer can be configured accordingly in the Yoti solution. More on Yoti's approach to privacy, ethical oversight and accuracy can be found in Yoti's white paper on age estimation. Yoti has developed a method of detecting masks and images presented to a camera in an attempt to fool Yoti's age estimation solution.

Yoti has an ongoing programme of R&D reviewing spoofing techniques and challenges, such as make-up, masks, facial hair pieces. Yoti is alive to the fact that young people may try to 'game the system'. As a result Yoti has established a threshold for image quality, and an uncertainty value for the age estimation prediction. These two thresholds enable Yoti to create a bar of what is an acceptable image.

Yoti is also part of the EU Consent project devising pan-European interoperable infrastructure for age verification and parental consent.

Yoti welcomes the Draft Online Safety Bill's focus on encouraging platforms to introduce more robust ways of protecting their users online such as age verification measures. Yoti agrees that

the Bill will help make the UK a much safer place online, providing that clear standards are in place for age verification.

Identity verification

To date there seems to have been quite a polarised debate in terms of identity verification for users of social media - at the one extreme requiring full anonymity and at the other full verification. We would recommend that a deeper review be undertaken to assess the nuances and art of the possible in terms of pseudonymous and anonymous verification for 'upstream' social media verification, as in verification when a person sets up a social media profile. We would recommend that a workshop be convened with technical experts and would be happy to participate. Inclusion is a key consideration to be tackled.

I link below to a discussion on this topic by the Institute for Global Change[5],

Before the internet, 'identity' meant driving licences, passports or ID cards: physical documents with lots of sensitive personal information on them collected in one place. When you bought alcohol, you'd not only reveal your full date of birth (instead of just proving you were over 18) but also your home address or even your passport number. Applying this model of identity to the internet would be a mistake. It would undermine important rights while also forcing unnecessary and intrusive sharing of personal data. Digital identity, however, can be different. Usually stored in a secure, privacy-protecting mobile app that only you can access and control, this information can be split up into individual credentials. This means you can demonstrate you're 'over 18', your citizenship, or that you've passed a criminal record check, without also revealing other sensitive data. With this digital identity infrastructure in place, social media services could verify specific pieces of information – like "are you a real person?" or "are you old enough to use the service?" – without forcing users to reveal any identifying information. In turn, as identity expert Dave Birch has argued, this could enable several different tiers of 'verified' accounts, rather than today's confusing status quo.

Figure 1: Proposed tiers of verification for social media accounts

As a suggestion, a workshop of experts could review what could be achieved in terms of selective sharing of data minimised credentials e.g. a 13+ or 18+ attribute with a verified name, however allowing a pseudonym to be used. Another option could be to consider accepting solely a liveness check and biometric template (not face photo) where someone does not have or does not wish to use a form of identification - to ensure that a unique individual is signing up. That biometric template could have a deletion window provided the account does not demonstrate hate speech or non permitted behaviours.

[5] https://institute.global/policy/social-media-futures-anonymity-abuse-and-identity-online

Sanctions could be considered if the account owner does then commit hate speech, e.g. then a new liveness and biometric face template could be captured. The person could be warned, for instance with a yellow card and support provided to explain why they have been presented with a yellow card. Any further hate speech and the next stage of sanction could be imposed - supported by re education. The platform and the regulator could consider where other sanctions or re-education would be appropriate and monitor their effectiveness. If deemed appropriate, it could be possible to review new account face templates against records of prior activity, education and sanctions. In this way anonymity could be retained but hate authors could be prevented from rejoining platforms which would have a deterrent effect and this would reduce the risk of repeat-offending. Hate authors would also understand that there are alternative ways to express themselves and clear sanctions for illegal acts - as deemed appropriate by the regulators and platforms.

Will the proposed legislation help to deliver the policy aim of using digital technologies and services to support the UK's economic growth? Will it support a more inclusive, competitive, and innovative future digital economy?

Yes. The Draft Bill will help further develop a crucial segment of the UK's digital and tech economy, driving job creation and further research.

To deliver an inclusive future, it is important that the standards and audit frameworks being developed for technologies in this area, such as the proposed Age Assurance Bill, require solutions to be inclusive and understandable by their users, of all ages.

As an organisation in that sector, Yoti continues to focus on transparency, inclusivity and innovation as non-mutually exclusive concepts through continued investment in research and partnerships. As a case in point, we aim to explain clearly how our AI age estimation technology is built and publish a white paper transparently detailing its efficacy across skin tone, ages and gender and the fact that it does not uniquely recognise any individual.

Are children effectively protected from harmful activity and content under the measures proposed in the draft Bill?

Yoti believes that the Draft Bill will help better protect children from harmful activity and content online, but that the regulator also needs to assess on an ongoing basis the ease with which minors are able to bypass age and identity checks to access harmful content online.

Yoti has studied and developed thinking on the various possible attack vectors that minors or others can exploit to bypass current age verification measures.

In our opinion, the Draft Bill should specifically mandate platforms with high risk use cases to implement age verification measures which have a high level of assurance. This could be done by referring to methods and documents which are designated in the Good Practice Guide 45 as offering a 'High' level of age assurance and looking to define an equivalent 'High' level of assurance for non document based approaches.

Yoti would be delighted to collaborate with the Committee and parliamentarians on further developing this guidance.

What role do you see for e.g. safety by design, algorithmic recommendations, minimum standards, default settings?

Safety by design and the inclusion of age verification measures at entry or before accessing potentially harmful content must be a cornerstone of the upcoming Online Safety regime. This dovetails with the principles of the Age Appropriate Design Code.

Yoti believes that platforms must be required to prioritise safety and privacy by design when developing new products, features or services which users can access and exchange user-generated content on or through.

There has clearly been success in the gambling world of age gating at the age of 18 and this is no longer seen as controversial. In accordance with current requirements for video-sharing platforms and on-demand service providers, we would recommend that the Bill should similarly mandate the use of age verification measures, so that harmful content is 'not normally accessible' to minors, and that minors are protected from grooming.

How does the draft Bill differ to online safety legislation in other countries (e.g. Australia, Canada, Germany, Ireland, and the EU Digital Services Act) and what lessons can be learnt?

In Germany there is a clear process for age verification methods to be reviewed, audited and deemed acceptable approaches. This is offered both by the FSM [6]and the KJM[7]. This both encourages innovative companies to invest in R&D to devise solutions and aids relying parties in their due diligence, particularly smaller companies who may not have the resources to engage in protracted due diligence.

In contrast the UK regulation is currently not looking to give any indications as to what are acceptable approaches.

Are there any types of content omitted from the scope of the Bill that you consider significant e.g. commercial pornography or the promotion of financial scams?

Yoti would welcome the inclusion of platforms which offer adult, pornographic and/or restricted content in the scope of the Draft Bill. We also believe that fraud and financial scams, which are also serious causes of harm, should be included in the Draft Bill.

Should fraud and financial scams be included, we see that identity verification measures and secure document signing can support the deterrence of fraud and scams.

Yoti is currently pioneering its eSignatures technology, Yoti Sign, which offers the convenience and simplicity of e-signing platforms with the added security of biometric verification and cryptographic signatures in accordance with privacy regulations. This would help reduce the huge cost and trauma which scams cause to UK internet users, numbered at over £1bn every year since 2019 according to UK Finance[8].

[6] https://www.fsm.de/de/fsm.de/yoti

[7] https://www.kjm-online.de/service/pressemitteilungen/meldung?tx_news_pi1%5Bnews%5D=4890&cHash=e45ae6dfeee26fcd23d10c6994b7a9ef

The draft Bill applies to providers of user-to-user services and search services. Will this achieve the Government's policy aims? Should other types of services be included in the scope of the Bill?

Yoti would welcome the expansion of the Draft Bill's scope to platforms which offer adult, pornographic and/or restricted content. This should be the case regardless of whether users have the capacity to exchange or access user-generated content or user-to-user services.

The Bill will only achieve the Government's policy aims, if enforcement powers are amended to enable them to be applied at scale to the 1.3 million adult websites. The enforcement regime would not be feasible if an individual application to the Court is required each time.

There is no benefit for young people for existing age verification measures, under the VSP and ODPS regimes, to be reversed. Even the prospect that this Bill may not require age verification for certain platforms and may potentially reverse prior legislation, is a disincentive for platforms to comply.

What role might algorithms play in reducing the presence of illegal and/or harmful content?

We believe that algorithms could play a key role in reducing the presence of illegal and/or harmful content online. However, to function properly they should include a number of safeguards through required design principles. The additional requirements should span:

- Transparency clearly showing the accuracy of algorithm (MAE - mean absolute error) - in the case of age algorithms this would span age, skin tone and gender as well as false positives and false negatives;
- Ethical sourcing of consented data set;
- Independent bias review;
- Understandability or use of plain English, so the demographic using the technology can understand the approach used, the terms and the privacy policy, following the Unicef Policy Guidance on AI for Children[9] and meeting the AADC;
- Participation in benchmarking, where this service is available.

Are there any foreseeable problems that could arise if service providers increased their use of algorithms to fulfil their safety duties? How might the draft Bill address them?

As stated in our answer to the previous question, Yoti believes that the Draft Bill and Ofcom should enforce strict rules for the use of algorithms such as ethical sourcing of data sets and independent bias reviews.

Is Ofcom suitable for and capable of undertaking the role proposed for it in the draft Bill?

[8] Fraud - The Facts 2020 | UK Finance

[9] https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf

Yoti engages with the regulator through frequent touchpoints and at events, industry and trade body meetings. We provide expertise and opinions where necessary and always are keen to input and support Ofcom's work.

We welcome Ofcom's inclusive and open attitude towards its stakeholders, and its eagerness to take into account leading industry members' views before making decisions and drafting guidance.

We also think that the regulator's approach of seeking expertise and input from academic, civil society and private sector experts is the right one. On that basis, we believe that Ofcom is indeed suitable and capable of undertaking the role.

How much influence will a) Parliament and b) The Secretary of State have on Ofcom, and is this appropriate?

Yoti believes that a healthy balance between branches of government with a strong focus on parliamentary scrutiny, the use of consultations and public fora will guarantee public confidence in the Draft Bill's aims and objectives.

Yoti would also welcome an enhanced role for civil society groups, age and identity verification industry members in discussions and the delivery of the Bill to create a more inclusive and more efficient Online Safety regime.

27 September 2021