Proposal for the inclusion, in the Illegal Harms Codes of Practice, of a measure requiring platforms to offer their users options to verify their identity

1. Background

This document forms part of Clean Up The Internet's response to Ofcom's "Protecting people from illegal harms online" consultation.

Clean Up The Internet has long recommended requiring platforms to offer users optional identity verification as a proportionate solution to the risks associated with anonymous and fake accounts. Our work on this has highlighted the role of anonymous and fake accounts in a range of harms, including harms named as "priority offences" under the Online Safety Act such as harassment and hate offences, fraud, and foreign interference.

Ofcom's current proposals under the OSA's illegal safety duties include an exploration of recommending a measure of mandatory user verification. Having identified that such a measure could help address a wide range of harms, but that it would also entail fairly significant implications for users' privacy and right to freedom of expression, Ofcom concludes that it is unable to assess the proportionality of such a recommendation.[1]

However, Ofcom has yet to consider recommending a measure along the lines proposed by Clean Up The Internet, of offering users optional identity verification. This is despite such a measure having potential to address a similarly wide range of illegal harms, and with far less significant trade-offs for users' rights. Ofcom has suggested that such a recommendation has not yet been considered under its illegal harms duties because a similar measure will eventually be required of "Category 1" platforms, under their additional "User Empowerment" and "User Identity Verification" duties.

However, this approach is not consistent with Ofcom's duties under Section 41 of the Act. As Ofcom notes, the "user identity verification" and "user empowerment duties" for Category 1, platforms will "require designated services to provide features specifically for adult users around *legal* content" [Ofcom's emphasis][2]. Section 41(1), (2), and (3) require Ofcom to recommend measures to reduce *illegal* content, for any relevant user-to-user service and not

[1] Ofcom: Protecting people from illegal harms online, Volume 4. p334

[2] Ofcom: Protecting people from illegal harms online, Volume 4. p281

just Category 1 platforms, to comply with the illegal content safety duties in section 10 of the Act.

It clearly was not the intention of legislators, in introducing specific extra “user empowerment” duties for “Category 1” platforms in relation to legal content, to preclude Ofcom from considering on its merits a measure which is relevant to the illegal content safety duties. On the contrary, the fact that parliament has already accepted the potential effectiveness of such a measure, for a different but related purpose, should surely be taken by Ofcom as an indication that it is precisely the kind of measure which legislators expected Ofcom to be considering under section 41. Put simply, if a measure is appropriate and proportionate to reduce harm from legal content it is not at all obvious why it should not be considered in relation to illegal content.

This document therefore sets out the case for recommending that platforms offer their users optional user verification, along with labelling of verification status and options to filter non-verified accounts, as a measure to tackle illegal harms. We trust that Ofcom will give this potential measure due consideration.

2. Summary of proposed measure

We propose that Ofcom recommend to platforms a measure which:

- offers their users options to verify their identity
- clearly labels which accounts are and are not verified, so that the verification status of each user is visible to all users of the platform
- offers their users enhanced controls to manage their interaction with non-verified accounts, up to and including an option to block all interaction from non-verified accounts

We suggest that this measure is recommended for all large services which offer user accounts, and for any other service that is medium or high risk for any of the following harms where fake or anonymous accounts are a risk factor: Terrorism; Grooming; CSAM; Suicide and Self-Harm; Harassment, stalking, threats and abuse; Hate offences; Drugs offences; Firearms offences; Extreme pornography; Intimate image abuse; Fraud; Foreign Interference offence; False communications offence; Epilepsy trolling; Cyberflashing

3. Harms this measure could address

Ofcom’s draft register of risks notes that anonymous user profiles are a risk factor for the following offences: Terrorism; Grooming; CSAM; Suicide and Self-Harm; Harassment, stalking, threats and abuse; Hate offences; Drugs offences; Firearms offences; Extreme pornography; Intimate image abuse; Fraud; Foreign Interference offence; False communications offence; Epilepsy trolling; Cyberflashing

Ofcom’s draft register of risks notes that fake user profiles are a risk factor for the following offences: Grooming; CSAM; Suicide and Self-Harm; Harassment, stalking, threats and abuse; Hate offences; Drugs offences; Firearms offences; Extreme pornography; Intimate image abuse; Fraud; Foreign Interference offence; False communications offence; Cyberflashing

An optional verification scheme would reduce the number and the potential impact of fake and anonymous accounts, and improve other users’ ability to identify and avoid such accounts. It would therefore contribute to addressing the full range of harms associated with anonymous and fake accounts.

4. Effectiveness

Expected impact on illegal content

The ability to create anonymous, pseudonymous, and fake user profiles increases the risk of harmful behaviour via a number of routes, including:

- Enabling users to conceal their identity, reducing traceability and impeding action by law enforcement
- Enabling the creation of “phoenix accounts” to circumvent blocks by other users, and/or suspensions or bans from platforms
- Increasing users’ subjective feelings of disinhibition and a lack of accountability
- Enabling the creation of false, deceptive identities, including both impersonations of real people and fictional identities
- Enabling the creation of multiple fake accounts which can be operated as a network

Our proposal would reduce the potency of all these routes, albeit to varying degrees:

- The use of “phoenix accounts” to circumvent platform bans or blocks from other users would be significantly impeded. Whilst a user who has been blocked or banned would still be able to create new, non-verified “phoenix accounts”, other users would be able to prevent interaction with such accounts by applying the filter to non-verified accounts. Victims of online abuse often describe the process of attempting to block abusers as a game of “whack-a-mole”, so an option to filter all non-verified accounts would greatly reduce the burden placed on victims. Similarly whilst a user banned or suspended from the platform might still be able to create a new account to circumvent that measure, the new profile would be labelled non-verified, and subject to the optional filter on non-verified accounts, significantly reducing its ability to harm other users.
- The ability to deceive other users through the creation of false, deceptive identities, would be significantly impeded. Whilst a user would still be able to

create such profiles, all other users would be able to see that the profile was not verified. This would make deception for the purposes of false communications, fraud, or foreign interference more challenging to perpetrate - for example "check whether the account is verified" could become a simple, standard piece of fraud prevention advice. In addition, users would have the option to filter out non-verified accounts entirely, providing the option of an even higher level of protection from being deceived by fake accounts.

- A voluntary option for identity verification, would not prevent users from creating non-verified, anonymous or pseudonymous accounts, with the reduction in traceability and increased feelings of disinhibition such accounts can entail. However, other users would have the option of filtering such accounts out. This would reduce the reach of these anonymous accounts and any illegal content they attempt to disseminate, and give individual users the option of applying the filter to gain higher levels of protection from offences such as harassment and hate.
- A voluntary option for identity verification would not prevent the creation of multiple accounts to be operated as a network, including for illegal purposes such as attempting harassment and hate, fraud, false communications, or foreign interference. However, other users would be able to see that the accounts in the network were non-verified, reducing their potency for offences which rely on deception such as false communications, foreign interference, or fraud. Users would have the option of blocking interaction with such a network via the filter on non-verified accounts, making such networks much less able to perpetrate harassment or hate via a sustained "pile on".

Given that anonymous and fake accounts are a risk factor for so many kinds of illegal harm, and that this measure would mitigate some of the key routes by which anonymous and fake accounts are associated with harm, there is a very strong case for expecting a voluntary verification measure to make a significant contribution to preventing a range of illegal harms.

Clean Up The Internet has been in contact with several senior police figures who have confirmed to us that in their view this measure would be expected to limit the use of anonymous or inauthentic non-verified accounts to commit offences including threats, harassment, and fraud - thus 'designing out' an opportunity for criminals, and reducing the burden on law enforcement. Additionally they have suggested that it could improve rates of detection and prosecution, as any criminal who chose to use a verified account would be easier for law enforcement to detect.

Impact on effectiveness of other proposed measures

In addition, a voluntary verification measure would improve the effectiveness of several other measures already proposed by Ofcom:

- **Measure 9A User blocking and muting:** Ofcom notes of this recommendation that “the effectiveness of individual blocking tools may be limited in circumstances where the blocked user creates new accounts through which to continue targeting the blocking user”. A voluntary verification measure, with accompanying options to filter non-verified accounts, would give the blocking user additional options to prevent further unwanted interaction. Measure 9A would therefore be a much more effective measure in protecting users if combined with a voluntary verification measure.

- **Measure 10A Removing accounts:** Ofcom is recommending to platforms a measure to remove accounts operated by or on behalf of a terrorist group, and consulting on a further measure to also block the accounts of users that share CSAM. Both these measures will be less effective because of “phoenix accounts” – as described above, the potential for users circumventing a ban by creating a new account. A voluntary verification scheme would preclude “phoenix accounts” from gaining verified status, ensuring that they were labelled non-verified and that users had enhanced options to filter them out, and therefore limiting their reach and ability to do harm. Measure 10A would therefore be a much more effective measure if combined with a voluntary verification measure.

Evidence of verification schemes being effective in other relevant circumstances

As part of the Online Fraud Charter announced in 2023, the UK Home Office identified offering users “the choice to verify their identity on platforms to allow other users to know they are genuine, allowing users to opt to interact with verified people only” as an effective measure for tackling online Romance Fraud, and secured a commitment to this measure from stand-alone dating platforms. Romance Fraud does not only occur on stand-alone dating platforms - other user-to-user services including general social media platforms are also used, with fake profiles crucial to the deception.[3]

Clean Up The Internet have had our own conversations with dating platform company Match Group, who already offer users verification options across many of their platforms and have committed to extending this offer under the UK government’s Online Fraud Charter. They confirmed to us that their user research has shown that many users consider their verification measures to make them feel safer, and that they see fewer reports of harmful behaviour concerning verified accounts.[4]

In Ofcom’s consideration of a mandatory verification measure, it noted that it had identified “some evidence suggesting that IDV can reduce the level of illegal content available on

[3] https://assets.publishing.service.gov.uk/media/65688713cc1ec5000d8eef96/Online_Fraud_Charter_2023.pdf

[4] Conversation with Match Group, 20 December 2023

services hosting pornographic content" from Aylo, formerly known as Mindgeek, who had stated that "ID measures since January 2021 are deterring illegal uploads."

In making recommendation 9C, concerning "notable user" and "monetised" verification schemes, Ofcom itself appears to accept the potential effectiveness of voluntary user verification schemes to prevent forms of fraud which entail impersonation of notable figures, subject to them being effectively implemented and properly labelled.

Some of the major user-to-user platforms also appear to accept that ID verification can be effective in preventing harms. X described the purposes of ID verification (which it currently only offers bundled with a premium subscription, and not in the UK) as being "to increase the overall integrity and trust on our platform" and "to ensure the safety and security of accounts on our platform", whilst Meta, in its promotional material for the "Meta Verified" premium subscription, describes the service as offering "added protection".[5] [6]

Evidence of public appetite for verification as a safety measure

There is considerable evidence that UK internet users perceive a strong link between anonymous and fake accounts and the prevalence of harms, and that they perceive verification as a measure which could protect them from such harms.

Ofcom's 2022 research into online scams found that the public ranked a "warning from the platform that content or messages come from an unverified source" as the single most helpful action a platform could take.[7]

In 2021, a poll conducted by Opinium for Compassion in Politics found 81 per cent of social media users said they would be willing to provide a piece of personal identification to a social media platform in order to receive a "verified" account. The same poll found that nearly three quarters (72 per cent) of those surveyed said they would choose to remove all unverified user-content from their feed if that option was available.[8]

In 2023, a poll conducted by Opinium for Clean Up The Internet found that just under four-fifths (78%) of UK social media users believe it would be helpful to be able to see which social media accounts have been verified to help them avoid scams. Almost as many also say being able to see which accounts have been verified would help with identifying bullies

[5] https://help.twitter.com/en/rules-and-policies/verification-policy

[6] https://help.instagram.com/738055111270671/

[7] https://www.ofcom.org.uk/__data/assets/pdf_file/0025/255409/online-scams-and-fraud-summary-report.pdf p17

[8] https://www.compassioninpolitics.com/4_in_5_back_efforts_to_curb_toxic_anonymous_social_media_accounts

or trolls (77%); spotting false or misleading news stories (72%); or buying products or services (68%).[9]

This evidence of public appetite obviously does not guarantee real-world take-up of a specific verification scheme. Whilst verification should be optional, platforms should be required to design schemes which are user-friendly, accessible and attractive. A scheme which is not designed to encourage substantial take-up should not be considered compliant.

5. Methods of verification

As Ofcom notes in its consideration of a mandatory scheme, (in comments that would apply equally to a voluntary scheme) "there are various methods of identity verification, and solutions are continuously developing. The identity verification process usually starts with gathering from the user certain claimed attributes and evidence of these, followed by validating that evidence, then establishing that the person with those attributes is the one seeking access." Ofcom also notes the presence of a variety of existing standards and guidelines, including the UK digital identity and attributes trust framework, the UK Cabinet Office and Government Digital Service "Good Practice Guide 45", and EU's eIDAS and eIDAS 2.0 regulations.[10]

The onus should be on platforms to develop and implement verification processes which are appropriate to their characteristics and risk profile, including by being sufficiently robust, sufficiently accessible to a wide enough range of users, and privacy respecting. Ofcom should stipulate minimum standards, but leave platforms flexibility to implement systems which work best for them.

A number of options would be available which could offer a sufficiently high level of assurance to be effective in reducing the level of harm associated with fake and anonymous accounts. Many of these are already in use by some user-to-user platforms in some circumstances. Verification methods which could be used include:

- **Verification by checking a user's claimed identity against some form of photographic ID.** This method is already used by a range of platforms in a range of circumstances - for example Meta's monetised premium subscription, "Meta Verified", requires this. Because the UK does not have a universal, government-issued identity card, for UK users such schemes rely on a range of other voluntary documents. The range of documents accepted has implications for how accessible such an approach is. Approximately 77% of UK adults have a driving licence, 86.5%

[9] https://www.cleanuptheinternet.org.uk/post/new-research-78-of-social-media-users-say-being-able-to-see-who-s-verified-would-help-avoid-scams

[10] https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

possess a passport.[11] [12]. Accepting a wider range of documents would increase the accessibility of this method – for example the wider range of documents accepted as voter ID in the UK under the Elections Act 2022 are held by 96-98% of voters[13]. However there may be trade-offs in rigour if documents with less security features are accepted. To be robust, such verification systems need to be able to check both the ownership and the authenticity of the ID, which may involve additional processes such as requiring a user to upload a video selfie, and checking the provided document against lists of lost/stolen IDs.

- **Verification by checking a user's claimed identity against digital identity credentials already held by a trusted third party.** Users verify their identity to a platform by sharing credentials from a reusable digital ID which they have created and verified with a third party. There are a growing number of providers of digital identity services in the UK, and a growing number of use cases. For example, Services like Digital ID Connect, built by Yoti, Post Office and Lloyds Bank, offer apps which enable users to verify their ID using government ID documents and encrypt it on their own smartphone[14]. UK company OneID offers identity verification by checking a user's credentials against those already held by their banking provider[15]. This takes advantage of the fact that 97% of UK adults have a bank account, and that banks are already required by law to conduct rigorous identity verification, as part of their Know Your Customer and Anti-Money Laundering obligations.

- **Verification by seeking confirmation of a user's claimed identity by other trusted individuals, often known as "vouching".** This method is commonly used in more "analogue" situations - for example signing the back of a passport photo to verify the true likeness of someone - and is also commonly used to include people whose vulnerabilities make them less likely to be able to afford or access other forms of verification (e.g. no fixed abode).[16] In some use cases, this method requires the individual providing the vouch to have some form of professional status e.g teacher, lawyer or doctor. Alternatively, or additionally, the provider of the vouch could be required to themselves be a verified user, with a certain period of stable use of the platform. Further safeguards against abuse could include limits on the number of

[11] https://www.ethnicity-facts-figures.service.gov.uk/culture-and-community/transport/driving-licenses-and-access-to-vehicles/latest/#main-facts-and-figures

[12] https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/internationalmigration/bulletins/internationalmigrationenglandandwales/census2021

[13] https://assets.publishing.service.gov.uk/media/609a5105d3bf7f2886e29f44/Photographic_ID_research-_headline_findings_report.pdf

[14] https://www.digitalidconnect.com/

[15] https://oneid.uk/

[16] See for example https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity

vouches any one user/individual can provide, or potential consequences for the user providing the vouch if the vouched-for user violates the platform's terms of service. This could be offered as a "last resort" method for vulnerable users for whom other methods are not accessible.

A related consideration would be whether the verification process is conducted by the platform itself, or by a third party provider, and therefore who handles and/or retains any relevant user data. There are examples of "monetised" and "notable" schemes that take each approach. For example "Meta Verified", which requires users to provide government ID documents, appears to be conducted in-house, whereas X Premium, not currently available in the UK, states that it uses a third party provider, Au10tix.[17] [18]

The UK government aims to encourage the development of more reusable digital identity products and services, which could be used for social media verification processes. It has developed a UK digital identity and attributes trust framework to support this, and is now allowing digital identity services to be used for right to work, right to rent and DBS checks.[19] Almost 50 Digital Identity Service Providers (IDSP) have now been certified against the trust framework and offer identity checks for Right to Work, Right to Rent, and DBS Schemes.[20]

Whilst all relevant privacy and data protection rules should apply whoever administers the scheme, some users may feel more comfortable sharing their data with a trusted third party, or others may feel more comfortable sharing their data directly with a platform which they are already familiar with. Offering users choices, including choices of both mechanism and provider, would help maximise accessibility and therefore take-up.

Another related consideration will be account security. Given that a voluntary verification scheme would make anonymous and fake accounts less potent tools for criminality, we could reasonably anticipate bad actors increasing efforts to hack and steal verified accounts. Platforms could combine the verification process with requirements that users implement security measures such as stronger passwords and two-factor authentication. Reporting mechanisms for hacked and stolen verified accounts would need to be sufficiently resourced and responsive.

6. Costs of verification

This measure would entail some level of implementation costs. Whilst some economies of scale may apply, it is likely that the larger the number of users using a verification process, the greater the total costs. This means platforms with the largest user bases, and therefore

[17] https://about.meta.com/technologies/meta-verified/

[18] https://help.twitter.com/en/rules-and-policies/verification-policy

[19] https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version

[20] https://www.gov.uk/government/publications/digital-identity-certification-for-right-to-work-right-to-rent-and-criminal-record-check

both the greatest resources and the greatest scale of potential harm to prevent, would face the largest costs.

The exact unit cost of verifying would be contingent on method, rigour, and the scale at which it was being done. But we can confidently say it would be a matter of pence per user, not pounds. For example, OneID quotes on its web site a price per verification starting from 16p, whereas Yoti quotes from 30p.[21] In its 2022 impact assessment, the UK government arrived at an estimated cost of 7p per user.[22]

Other industries where an ID verification is required tend to absorb this cost. For example, online banking platforms are required by law to follow rigorous identity checks before accepting a new customer, and do not apply a charge to the customer for this. Given that this is a safety feature, and should be accessible to all users, we do not think it would be appropriate for users to be charged to verify.

Given the wide range of harms which this measure would help address, and the severity of the impact of those harms, the direct costs of this safety measure are proportionate. To take one example for which the government has recently attempted to quantify the societal cost - the Home Office's most recent estimate of the total cost to society of fraud against individuals (2019-20) in England and Wales was estimated to be at least £6.8 billion.[23] Whilst the societal costs of non-financial crimes is more challenging to estimate accurately, Ofcom notes estimates of many millions of pounds for other harms linked to anonymous and fake accounts. The government's 2022 impact assessment, includes attempts to quantify the cost of many of the harms linked to anonymous and fake accounts, including CSAM, hate crime, drugs, modern slavery and cyberstalking. The estimates, which it acknowledges do not cover all relevant harms, and "are likely to underestimate", added up to £5 billion/year.[24]

A measure requiring platforms to offer all UK users verification options, as a core safety feature, would have some potential indirect impact on some platforms' business models, because of an overlap with monetised subscriptions such as "Meta Verified" or "X Premium". However, in all these cases, identity verification is only one feature in a bundle of other features, which a platform would continue to be able to offer to differentiate any premium offer. It's surely a proportionate interference with a platform's business model to require it to make a safety feature, which will help protect users from serious harm and serious

[21] https://oneid.uk/pricing and https://www.yoti.com/business/identity-verification/

[22] https://assets.publishing.service.gov.uk/media/6231dc9be90e070ed8233a60/Online_Safety_Bill_impact_assessment.pdf p56

[23] https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf

[24] https://assets.publishing.service.gov.uk/media/6231dc9be90e070ed8233a60/Online_Safety_Bill_impact_assessment.pdf pp64

criminality, widely available – no one would consider it acceptable for a car manufacturer to offer brakes only as part of a premium subscription bundle.

A voluntary verification scheme could potentially have some further indirect impacts on platforms' business models, because a platform's total user numbers is often such an important figure for both investors and advertising customers. The introduction of widespread user identity verification would raise new questions about how many of these users were verified and what that might suggest about the credibility of total user number claims. This could have business benefits for platforms with high uptake of verification - for example a platform with a higher percentage of verified users might find itself more attractive to advertisers.

7. Rights impacts

In its consideration of mandatory verification, Ofcom notes that such a measure would be "likely to affect users' right to respect for their private life and correspondence", and that "the usual trade-off is that the higher the level of assurance, the more intrusive the method is likely to be and the higher its impact on privacy."

A measure which requires only that users are offered a choice as to whether they verify hugely reduces any negative impact on a user's privacy rights, because users can choose whether or not to go through the process. Any remaining impact would be mitigated further by ensuring services having in place robust measures to comply with their data protection obligations, and by giving users choices as to how they verify, including choices to verify via third parties as users could then choose a method and a provider that they feel comfortable with.

In its consideration of mandatory verification, Ofcom also noted implications for users' rights to freedom of expression and freedom of association. Ofcom observed that "being able to speak anonymously enables individuals to express themselves without fear of repercussion from employers, insurers, family members or their community. Being able to receive such communications enables everyone to become aware of information and ideas which may otherwise not become public. This is particularly true of political and journalistic speech, which are afforded the greatest degree of protection by the law." It noted that certain groups could be particularly impacted by a loss of anonymity, including whistle-blowers, journalists, activists, minority groups, and survivors of illegal harms including sexual and domestic abuse."

Again, the voluntary nature of our proposed measure significantly mitigates the potential negative impact on users' rights to freedom of expression and association: users can continue to choose not to verify, and therefore retain the ability to communicate and associate anonymously. Indeed users could have one verified account alongside an unverified account that they used when they felt the need for that privacy.

There would, however, still be some residual potential negative impact for users who chose not to verify. The combination of voluntary verification with labelling of verification status, and options for users to choose to filter interaction from non-verified accounts, would likely have some impact on the reach, and in some cases the credibility of users who chose anonymity. These features would disproportionately impact accounts that wished to misuse anonymity for example to deceive or send unsolicited, hateful content. But there might be circumstances where a perfectly law-abiding user who has chosen not to verify for perfectly legitimate reasons finds it takes longer to build a following or reach an audience because of the filter, or where it takes longer for them to build credibility or overcome scepticism as a result of their non-verified status being visible.

If a verification system is not designed with accessibility in mind, there would be a risk that some of these negative impacts could fall disproportionately on already marginalised groups. For example Black people are less likely to hold a driving licence (58%) than the general UK population (77%) so a verification scheme which relied on this document alone would disproportionately exclude them.[25] Whilst with a voluntary verification scheme the negative impact of being unable to access it is far less severe than with a mandatory scheme, platforms should still carefully consider equality and accessibility. Offering users a choice of methods of verification, including methods which will cater for otherwise marginalised groups, will mitigate these risks.

Overall, as Ofcom has noted, the rights which verification schemes could impact “are not absolute rights” and that conclusion must be even more compelling in relation to a voluntary scheme. The limited potential for a negative impact on some users who are unwilling or unable to verify must be balanced against the broad range of illegal harms for which anonymous and fake accounts increase the risk, and the negative impact the prevalence of these harms has on other users’ rights. Given the potential of this measure to prevent a significant amount of crime, and to mitigate a significant amount of harm to users which itself impacts their rights to freedom of expression and privacy - as well as many other Convention rights which Ofcom, as a public body, must always have regard to - this limited level of interference appears proportionate to the aims pursued.

8. Conclusion

Anonymous and Fake Accounts are identified by Ofcom, in its risk profiling, as one of four functionalities which “stand out as posing particular risks”. It goes on to note (correctly) that these functionalities can also carry benefits for some users, and that just because a functionality carries risks does not mean it should be banned – rather, the goal of the regulation should be “to get services to put in place safeguards which allow users to enjoy the benefits they bring while managing the risks appropriately.”

[25] https://www.ethnicity-facts-figures.service.gov.uk/culture-and-community/transport/driving-licenses-and-access-to-vehicles/latest/

Ofcom’s current set of proposed recommendations doesn’t yet meet the test it has set itself, because, having explored and rejected mandatory verification, Ofcom doesn’t then consider recommending any alternative “safeguards” which could “manage the risks appropriately”. Despite anonymous and fake accounts having been identified as a “stand out” risk factor, associated with 15 different offences, only one of Ofcom’s recommended measures (9C) makes any direct attempt to mitigate the illegal harms associated with fake and anonymous accounts. This measure addresses only one subcategory (fraud involving impersonation of a notable individual) of one of these 15 offences.

We believe that recommending platforms offer voluntary identity verification, accompanied with different labelling for verified and non-verified accounts, and options for users to filter non-verified accounts, would strike a more appropriate balance. Anonymity would not be banned. Users would be able to continue to choose to post anonymously or pseudonymous, and to choose to interact with other anonymous or pseudonymous accounts – i.e. “enjoy the benefits”, if in their judgement they believe these functionalities to be benefits. But users would also be able to choose to verify their own identity, to see who is and isn’t verified, and to choose to limit their interaction with non-verified accounts – giving them more choices and control to “manage the risks appropriately”.