Department of
Media and
Communications

Roundtable on the Draft Online Safety Bill

Report

Wednesday, October 27, 2021, 3:00 PM – 5:00 PM

- On October 27, 2021, the LSE Department of Media and Communications hosted an online roundtable on the Draft Online Safety Bill (OSB)[1] that brought together leading academics and industry experts.
- The event was aimed at providing a platform for exchange on the questions of anonymity and age verification online, and on ways to improve the framing of these issues in the Draft OSB.
- Many views were expressed in the meeting; its aim was not to achieve consensus. This report has been prepared by the LSE as a record of some of the key points.

Event Chairs: Professor Lee Edwards (LSE), Damian Collins MP (Select Committee)

Participants: Debbie Abrahams MP, Lord Anderson QC (Brick Court), Andy Burrows (NSPCC), John Carr (UK Council for Child Internet Safety), Florian Chevoppe-Verdier (Yoti), Iain Corby (Age Verification Providers Association), Julie Dawson (Yoti), Alastair Graham (Age Verification Providers Association), Stephen Kinsella (Clean Up the Internet), Professor Sonia Livingstone OBE (LSE), Dr Joe Mulhall (Hope Not Hate), Boris Radanovic (UK Safer Internet Centre), Dave Rich (Community Security Trust), Warren Russell (Age Verification Providers Association), Andrew Strait (Ada Lovelace Institute), Matt Tindall (BBFC), Alison Trew (NSPCC), Dr Carissa Veliz (University of Oxford), Dr Heather Wardle (University of Glasgow), Professor Lorna Woods (University of Essex)

Committee Members: Lord Tim Clement-Jones CBE, Darren Jones MP, Dean Russell MP, Lord Wilf Stevenson, Beeban Kidron

Observers: Andrea Dowsett (Committee Clerk), Chloe Grant (Ofcom), Elizabeth Holloway (Ofcom), Jacquie Hughes (Committee Specialist Adviser), Hammad Khan (Ofcom) Leah Selig Chauhan (Ofcom), David Slater (Committee Clerk), Nicola Spooner (DCMS), Richard Wronka (Ofcom), Zoe Hayes (Committee adviser), Josh Robinson (DCMS)

[1] The Draft Bill can be accessed via https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

Key Findings

- Participants largely agreed on the **importance of preserving anonymity online.** Not only do children benefit from anonymous communication but removing anonymity would also put vulnerable groups and individuals (women, minorities, dissidents) at risk. Furthermore, evidence on whether real-name policies mitigate online disinhibition effects is mixed.
- Some speakers also questioned the overall usefulness of anonymity as an all-or-nothing concept, pointing out that there is a continuum between **anonymity, pseudonymity, traceability**, **and full verification**. Graded solutions are conceivable, whereby user identities are safely stored by platform providers and/or third parties but remain invisible to the general public (and/or platforms).
- A range of standards and technology options exist for **age verification**. These include hard verification via **identity documents, facial recognition systems,** or **age estimation**. While all technologies come with trade-offs, the significance of finding **privacy-preserving solutions** was highlighted.
- There was broad consensus among participants about the risks of platforms being granted too much leeway regarding risk assessments and age verification. Without clear guidelines on the powers of Ofcom, there is a **danger of companies setting their own standards.** Likewise, a strict separation is necessary between verification providers, their clients, and advertisers.

Potential amendments to the Draft OSB suggested by participants

Amendment proposal	Relevant Clause(s)/sections	Raised by
Strengthen Ofcom's powers regarding the enforcement of risk assessment duties	Clause 7	Professor Lorna Woods
Clarify Ofcom's assessment obligations with regard to freedom of expression and privacy	Clause 61	Professor Lorna Woods
Clarify basis on which Ofcom devises risk profiles and provides guidance	Clause 62	Professor Lorna Woods
Clarify whether Ofcom is under an actual obligation to look at platform functionalities	Clause 135	Professor Lorna Woods
Broaden scope of bill to incorporate platforms that choose to drop user-generated content	Clauses 13 (2) (b) and 14 (2) (b)	Iain Corby
Empower Ofcom & clarify enforcement powers to avoid multiple court appearances	Chapter 6	Iain Corby
Add penalties from Digital Economy Act	Chapter 6	Iain Corby
Empower Ofcom & clarify enforcement powers to avoid multiple court appearances	Chapter 6	Iain Corby
Add a section about user verification duties to Chapter 2	Chapter 2	Dr Damian Tambini
Introduce a duty to cooperate	n/a	Damian Collins MP
Personal responsibility of and criminal sanctions for senior executives and managers	n/a	Dave Rich
Address online spaces and groups where hostility becomes the norm; give law enforcement powers to go after such groups	n/a	Professor Sonia Livingstone

Main discussion themes

Panel 1 – Anonymity (Chair: Professor Lee Edwards)

Duty of care and risk assessments

Professor Lorna Woods opened the session by underlining that the structure of risk assessments in the Draft OSB needs improvement. Current provisions are too weak, as they leave little leeway for Ofcom to enforce assessments in case of company negligence (cf. Clause 7). It also remains unclear on what basis the regulator should devise risk profiles and provide guidance about risk assessments (cf. Clause 62). Woods expressed doubts about whether Ofcom is really obliged to look at functionalities (cf. Clause 135), and whether company duties to consider freedom of expression and privacy (cf. Clauses 12 & 24) also extend to Ofcom's risk assessment obligations (cf. Clause 61).

Woods noted a number of gaps, including the obligation to keep risk assessments up to date by reference to triggering events, rather than doing them on a rolling basis to see what has changed; a lack of detail about requiring companies to measure success; and the status of situations where a company has taken action but willfully ignored evidence - the wording in cl 80 is that the provider has 'failed or is failing', which leaves interpretation open and raises the risk of litigation. Overall, Woods argued that a balance needs to be struck between general duties and specificity. While adopting a framework approach to the Bill might make it more flexible and therefore future proof, getting too prescriptive might have the adverse effect of platforms not actually thinking through their policies.

Stephen Kinsella reiterated that under the current proposal, too much is left to platforms' own discretion. He stressed that rather than policing content, assessments of risk profiles should be based on structural factors and design elements. Otherwise, context sensitivity would be lost. Platforms should be obliged to identify risks, including anonymity, and come up with detailed proposals to mitigate such risks. Iain Corby suggested that the Bill needs to incorporate measures that mitigate against platforms bypassing their operational duties by removing user-generated content and thereby becoming 'out of scope' (cl 13 (2) (b) and 14 (2) (b)).[2] For non-compliance, he suggested penalties could parallel the Digital Economy Act (e.g. blocking websites and access to payment services, removing support services such as search engines and hosting sites). A deadline should be imposed as a starting point for enforcement (e.g. 6-months from formal notification).

Dave Rich and Joe Mulhall highlighted that most extremist content can be found on smaller (category 2) platforms and that introducing differentiated rules and duties might be an open goal for extremists to exploit, because they have multiple accounts on several platforms and will often search for the safest harbour for their content online. The two-level arrangement in the draft OSB misunderstands the ways these actors circumvent big platform regulations and build audiences across alternative spaces online.

[2] https://metro.co.uk/2020/12/16/pornhub-deletes-80-of-videos-after-claims-site-is-infested-with-child-abuse-13759151/

Damian Collins suggested considering a duty to cooperate, whereby category 1 platforms could be obliged to notify the regulator of suspicious or harmful traffic on category 2 platforms which is being redirected to a larger platform, thereby triggering an intervention[3]. This was supported by a number of participants.

Anonymity, harm, and vulnerability

Participants generally agreed some level of anonymity online is crucial because vulnerable groups may be harmed if they have to expose their identity and there was no clear evidence that identifiability mitigates the incidence of harm. Dr Carissa Véliz argued in favour of mechanisms allowing people to be pseudonymous,[4] as a midway approach between full anonymity and identifiability and in light of evidence that identifiability does not necessarily mitigate abuse and aggression but might have adverse effects.[5] Andrew Strait noted that in a context of de-anonymisation, additional risks to individual security could arise in the case of data breaches. Professor Sonia Livingstone added that the original argument about social norms in the digital space was that people feel disinhibited online, a rationale that was also behind Facebook's real-name policies. However, she questioned this line of thinking and suggested the focus of the Bill should be on contexts where people can foster hate and abuse and hostility becomes the norm. Overall, Livingstone and others stressed that anonymity needs to be protected, especially for young people.

Joe Mulhall pointed to potential ways of introducing friction that could reduce harm, e.g., having to be on a platform for a prolonged period without a breach of terms of service before obtaining certain privileges, which could incentivize people to change their behaviour online. In the chat, Mulhall also highlighted the dangers of holding platforms accountable for anonymous accounts. Such a step could present a slippery slope towards major platforms completely removing anonymity, thereby creating a two-tier social media ecosystem where communities relying on anonymity would be marginalised even further in the digital space.

Layered responses to online anonymity and privacy

Several speakers underlined the need to transcend the anonymity-identifiability binary and think of other ways to prevent online harm. Sonia Livingstone asserted that being anonymous from one's peers or the public should be kept distinct from anonymity vis-a-vis the platform. John Carr traceability was more important than anonymity. He stressed the need to devise a system that can rapidly, accurately and inexpensively identify people who have crossed the line of criminal

[3] In response, Nicola Spooner (DCMS) noted the government does not share the view the provisions are insufficient. She pointed to clause 19 of the bill which outlines risk assessment duties and clause 82 which outlines enforceable requirements. If a company does not complete the risk assessment, as defined in the Bill, enforcement options are available. However, Professor Woods subsequently challenged this via email. She argued that the Bill does not impose any obligation on OFCOM to have regard to freedom of expression when coming up with its guidance or codes, although its status as a public body makes it subject to the Human Rights Act. She argued that privacy and freedom of expression both incorporate terrain that goes beyond just not violating rights (as the HRA requires), and this isn't currently covered in the Bill.

[4] See https://onlinelibrary.wiley.com/doi/10.1111/japp.12342

[5] https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0155923

law. Similar to number plates on a vehicle, mechanisms could be designed whereby users are effectively anonymous but can nonetheless be held accountable for their actions.

Several participants agreed that whatever the system introduced, it should not reinforce big platforms' ability to collect data and/or provide access services for smaller platforms. Solutions involving independent third parties need to be found, with regular audits and certification. Prof Woods also highlighted the potential for guidance and codes of practice to be layered, and for allowing some choice within a given framework. Platforms could tweak specific mechanisms according to their user base, and users would be given a range of services to choose from.

Warren Russel remarked that technical solutions are available to layer anonymity, including options such as complete transparency/identifiability, being publicly anonymous but known by the platform, being anonymous publicly and vis-a-vis the platform but identifiable by a third party, and complete anonymity. He argued that the scope of the Bill should cater to different privacy requirements according to platform category and the nature of their audiences.[6] Steven Kinsella argued that possessing a right to speak must come with a right to choose who we want to hear, and floated the idea of being able to block abusive accounts. Dave Rich argued that compliance duties need to be streamlined in relation to cases where platforms are unable or unwilling to cooperate with police and law enforcement, to facilitate prosecution. Potential options include fines or sanctions levied on senior executives.

Dr Damian Tambini pointed out that there is a legal continuum between enforcing identity verification and leaving things to guidance, and suggested that a section about user verification duties could be added to chapter 2 of the Bill. However, Tambini also argued that user incentives could be changed, and where users repeatedly breach guidelines, platforms could be obliged to undertake more comprehensive measures than they currently do.

Damian Collins closed the discussion by reiterating that the law can play a decisive role in stopping the spread of harmful content. Many areas within the scope of the Bill are areas where existing legal arrangements simply do not work.

Panel 2 – Age verification (Chair: Damian Collins MP)

Age verification technologies

Iain Corby argued that different technologies are already available to carry out 'age checks', including hard age verification (passport or driver's license) and age estimation. However, Corby conceded it was difficult to do hard age verification at age 13 (a common limit for online participation) and suggested that sites check to determine a user's 18th birthday.

John Kerr suggested the adoption of an approach used by the Gambling Commission since September 2007, where industry enforcers pretend to be children and place bets on gambling websites. If they are successful, the service risks losing its license. Similar sanctions could be applied to platforms that fail age verification tests.

Boris Radanovic cautioned that age verification mandates for large platforms would drive users to smaller platforms with less stringent mandates. He supported the risk-based approach

[6] Julie Dawson referred participants and committee members to this articlereflected the different levels of anonymity https://institute.global/policy/social-media-futures-anonymity-abuse-and-identity-online

to age assurance and verification, as proposed by Ofcom in its guidelines to video-sharing platform (VSP) providers.[7]

Third-party verification providers

Participants generally agreed that transparency is critical to the age verification process and that a strong, independent third-party age verification sector could be more carefully regulated and scrutinized than if platforms do their own verification.

Iain Corby suggested the Bill makes provisions for the regulator to stipulate verification standards. Independent certification bodies could audit age assurance providers to ensure their information is accurate, and privacy is being protected. Julie Dawson emphasized the need for more benchmarking companies to assess age verification technologies, such as the UK's Age Check Certification Scheme. Participants referred to BSI Standard PAS 1296, a code of practice dealing with the provision and use of online age check services. Those standards may be broadened to include the creation of an international standard and IEEE standard. Corby added that under the EU consent project,[8] Facebook and Google are part of an advisory board discussing interoperability. As part of proposals, if a user proves their age to one platform provider, other providers can rely on that information. A 'test age set' was also recommended.

Drawing on discussions about the Digital Economy Act John Kerr cautioned that businesses able to commercially benefit from age verification processes should not provide age verification services. Prof Woods recommended ownership limits for age verification providers, and that the Broadcasting Act could serve as a model. The UK's Communication Act (2003)[9] also provisions for media ownership in chapter 5, paragraph 391 and schedule 14. Parameters could include being independent of advertising companies, brokers and similar entities.

Child protection

Participants agreed that more should be done to protect children from adult content. Dr Heather Wardle suggested the development of a graded system, which clearly identifies adult only activities, to form the basis of age verification structures. Prof Woods argued adults could be prevented from participating in platform services designated for children in some instances.

Professor Sonia Livingstone emphasized that child-only spaces will only work well if extensively moderated. She pointed to scandals involving Habbo Hotel and Club Penguin, where minors were exposed to illicit and explicit content.[10] [11].

[7] https://www.ofcom.org.uk/__data/assets/pdf_file/0027/216486/consultation-vsp-harms-draft-guidance.pdf

[8] https://euconsent.eu/

[9] https://www.legislation.gov.uk/ukpga/2003/21/contents

[10] https://techcrunch.com/2012/11/27/after-losing-over-half-its-9m-users-in-a-pedophile-scandal-habbo-hotel-hopes-for-new-life-as-a-gaming-platform/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKyA_GLIwKPRowc2-Vdei7UTwS15OEbsuWCu896RQOjHKRN5GN6v-ratJvXBjWqD3nTRm12V-BTI3eK25W64OeyOP1ad97gQoxS9ZhXUGT6m2MRfriEyQOCz9BzxMMXc4mDkBbn5_luZvYbzHm0GLtS6NTTE95yZS-0VLagZwOzf

[11] https://www.bbc.co.uk/news/technology-52677039

Damian Collins questioned how a regulator could hold a platform accountable, if by nature of its ecosystem, user-generated data pushes adult content to children. John Kerr noted that American-owned platforms have a legal obligation to remove persons who are below the sign-up age of 13. Professor Livingstone countered, however, that there is no law in the UK which says children under age 13 cannot access websites or social media platforms. She said there is an American law to protect children from data misuse and marketing, and that provision is incorporated in the terms and conditions of platforms.

Professor Livingstone agreed that platforms can ascertain the age range of users, but pointed out that platforms can also use that knowledge to benefit or protect children and that children have a legitimate right to participate in the digital world, that should be protected.

Cross-cutting themes & general comments

Dangers of platforms marking their own homework

Several speakers stressed the fact that the current moment presents a window of opportunity to invest Ofcom with the appropriate legal powers to effectively carry out its oversight functions. Ofcom needs to be given "cover and confidence" to deal with resistance from platforms, otherwise substantial powers will default to the providers themselves. The same holds true for age verification mechanisms, which should be kept separate from platforms' own operational scope.

Business models and algorithmic design

A repeatedly invoked issue was the business model underlying platforms' operations. Several speakers highlighted the need to focus on companies' motives to behave in certain ways, and particularly the commercial incentive to manipulate user data in the favour of platforms. There was consensus that the provisions contained in the OSB should not lead to platforms being able to harvest more data and use it for their own benefit instead of for the benefit of data subjects themselves. As Damian Collins pointed out, the regulator could potentially be given powers to challenge a platform over the way they process user data.

Protecting Privacy

Safeguarding privacy was integral to remarks by several participants. Dr Véliz suggested an approach similar to that of the 'Solid project' led by Professor Tim Berners-Lee at the Massachusetts Institute of Technology (MIT). Solid,[12] according to its website, aims to change the operations of web applications to improve privacy, among other things. In this approach, third-party age verification providers would only have knowledge of an individual's age, and no other personal data. She cautioned against following China's pattern[13] of using facial recognition to verify the age of individuals.

[12] https://solid.mit.edu/

[13] https://www.bloomberg.com/news/articles/2021-07-08/tencent-uses-facial-recognition-to-ban-kids-gaming-past-bedtime

Further reading

Rost, K.; Stahel L. & Frey, BS. (2016), Digital Social Norm Enforcement: Online Firestorms in Social Media. PLoS ONE 11(6): e0155923. https://doi.org/10.1371/journal.pone.0155923

Tony Blair Institute for Global Change (2021), Social Media Futures: Anonymity, Abuse and Identity Online. https://institute.global/policy/social-media-futures-anonymity-abuse-and-identity-online

Véliz, C. (2019), Online Masquerade: Redesigning the Internet for Free Speech Through the Use of Pseudonyms. Journal of Applied Philosophy, 36: 643-658. https://doi.org/10.1111/japp.12342

Appendix 1: Chat transcript

15:15:17 From John Carr to Everyone:

The question of anonymity certainly touches or can touch on the issue of age verification but the two issues are not coterminous. One can operate age verification without having to disclose a person's identity, at least not on screen.

15:25:18 From Heather Wardle to Everyone:

Regarding the functions of how risk assessment may work, it may be worth looking at other attempts to get industry operators to perform their own risk assessments and the efficacy of the processes around that. In my field, the Gambling Commission attempted to get the gambling industry to produce local area risk assessments to use to mitigate gambling harms, but it was poorly instituted, the GC had very little/no powers/resources to check or audit and it rapidly became a more check box exercise - because of poor infrastructure to monitor.

15:29:00 From Andrew Strait (Ada Lovelace Institute) to Everyone:

On this point re: Facebook's real name policy, isn't that an example that attempts to remove anonymity doesn't help prevent toxic/harmful behaviour?

15:29:12 From John Carr to Everyone:

Always being mindful of the rule of proportionality, why can we not go back to an overarching duty of care which applies to everyone? And Ofcom must satisfy itself that the standards being used by platforms e.g. in respect of risk assessments, meet an acceptable/recognised standards.

15:31:45 From Stephen Kinsella to Everyone:

Our proposal would not ban anonymous accounts but would give us all a right to be verified, if we choose, and then to choose not to hear replies from unverified accounts. In other words, not interfering with free speech but balancing it with a right to decide what we hear.

15:32:01 From Lorna Woods to Everyone:

In my view anonymity is a risk factor and companies should think about how to mitigate if it (in whatever format) is permitted - but this then come back to how we check the effectiveness of the measures - so this comes back to OFCOM's oversight/enforcement.

15:34:25 From Iain Corby to Everyone:

We will discuss age verification later - in itself, its a process that puts a very high premium on protecting privacy and is anonymised - but the process itself could be a firm "nudge" to bad actors who will have had to supply ID or even just a selfie as part of that process (even though its data that need not actually be retained for the AV process).

15:35:38 From Lorna Woods to Everyone:

There is a concern that requiring traceability should not reinforce the big platforms' ability to collect data. So a third party market in digital identity should be encouraged (and those providers should be independent from data broker business) and some sort of interoperability needs to be required. Note that without this, we might find that the bigger platforms provider access services for (some) smaller ones and things like single sign on can be a mechanism for tracking people across at least some of the internet.

15:36:04 From Stephen Kinsella to Everyone:

Agree with Joe that more friction would also help mitigate some of the harms. Also we should be focusing more on how to limit harms occurring, reducing burden on law enforcement etc, rather than how we detect and prosecute after the event, because the reality is that the resources will never be devoted by the state to carrying this burden.

15:36:09 From Iain Corby to Everyone:

If Parliament favours measures to tackle anonymous trolling online, the tokenised architecture of age verification offers a mechanism which could be duplicated to achieve this without the platforms themselves being given access to the full identity of the user.

15:36:32 From Andrew Strait (Ada Lovelace Institute) to Everyone:

On this point about regulating amplification, Daphne Keller has written a great piece on the challenges with doing so https://knightcolumbia.org/content/amplification-and-its-discontents

15:37:33 From Andrew Strait (Ada Lovelace Institute) to Everyone:

And this is the study Carissa is referring to: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0155923

15:38:56 From Warren Russell to Everyone:

Anonymity, like identity/age verification can, and should have multiple levels, all of which can be achieved technically. Complete transparency; Publicly anonymous - but the platform knows the account holder; publicly and platform anonymous but a third party provider can establish the account owner; and then completely anonymous. There is a place for all, depending on the arena in question, one size does not fit all and the scope of the bill can apply to all categories and can cater for all privacy requirements. - Warren Russell, Co-Chair AVPA

15:40:36 From Stephen Kinsella to Everyone:

We did a review of the literature on the disinhibition effect, (available on our site), but we believe that the German study cited by Carissa is an outlier - that's why it keeps getting cited in this debate. But in any event it doesn't seem helpful to get distracted by debating whether more harm is caused by anonymous or open accounts, if we are in a position to take sensible action to limit harm caused by the former.

15:40:52 From Lorna Woods to Everyone:

This is not a full academic study but rather a Buzzfeed story, talking to the people who were convicted of s 127 Communications Act offences- they got involved because they were chasing likes based on trending topics. Anonymity or otherwise doesn't seem to have been an issue.

15:41:31 From Carissa Véliz to Everyone:

Here is an open access, short paper, that proposes a system of pseudonymity that would, on the one hand, stop abusive speech, and on the other hand, protect people's identity (thereby protecting vulnerable citizens):

15:41:33 From Carissa Véliz to Everyone:
https://onlinelibrary.wiley.com/doi/10.1111/japp.12342

15:42:35 From Joe Mulhall - HOPE not hate to Everyone:

In case of interest, this is a briefing Hope not hate produced with the think tank Demos outlining our thoughts on Anonymity and possible alternative solutions.
https://hopenothate.org.uk/wp-content/uploads/2021/10/HnH-Online-Safety-Bill-Anonymity-2207.pdf

15:45:03 From Julie Dawson, Yoti to Everyone:

There does not seem to be enough shared understanding of the tech options available. As a suggestion, a workshop of tech experts could be given the set of challenges and then review and come up with granular responses as to the art of the possible e.g. the selective sharing of data minimised credentials e.g. a 13+ or 18+ attribute with a verified name, could still allow a pseudonym to be used. eg. a liveness check and biometric template (not face photo) where someone does not have or does not wish to use a form of ID - could 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... Julie Dawson, Yoti

15:47:43 From Lee Edwards to Everyone:

Thank you all for the contributions in the chat - they will be incorporated into the report as part of the discussion.

15:48:15 From Lee Edwards to Everyone:

However, if you'd like to raise the issues addressed in more detail, please do raise your hand.

15:50:14 From Joe Mulhall - HOPE not hate to Everyone:

I think that holding platforms accountable for anonymous account is one of the less harmful options. However, the danger is that most/all major platforms would thus remove anonymity creating a two tier social media ecosystem where communities that rely on anonymity (LGBT+ people, undocumented people, sex workers, people seeking health advice and/or end of life care, victims of domestic abuse or persecution etc) who are already severely marginalised in society would be even further marginalised by being confined to a small group of platforms that continue to allow anonymity. And its likely that these platforms would be small. Voices already ignored in public debate will be further marginalised.

15:52:35 From Lorna Woods to Everyone:

I agree that the fixed nature of the Cat 1 boundary is problematic. Another mechasnism could be to link higher obligations to risk profiles, so that the fact that different risks might arise on different platforms and that this is not necessarily about the size of the platform.

15:53:11 From Iain Corby to Everyone:

and the tech for traceability is ready to go today - we can have that DVLA equivalent by duplicating the AV architecture for this purpose (AV would remain an anonymised process by default of course) Iain Corby Age Verification Providers Association

15:53:59 From Joe Mulhall - HOPE not hate to Everyone:

One of the main reasons people value anonymity is precisely to avoid traceability. This can result in negative behaviour but it also gives a voice to people like undocumented people/whistleblowers/sex workers/etc who want to be anonymous and untraceable.

15:54:20 From John Carr to Everyone:

Some uber geeks think few if any internet users have complete or true anonymity. And btw the introduction of E2EE is not going to changed that position fundamentally. Or rather, what the uber geeks say is, if a "powerful adversary" wants to find out who is doing what online they will. OK we are here more concerned with mass market applications e.g. social media sites but we should discuss the issue against that background.

15:55:23 From Iain Corby to Everyone:

traceability would need to be well regulated, and only reveal ID where there is just cause (e.g. court order). Hence better to use independent third parties which can be regularly audited and certified.

15:57:59 From Carissa Véliz to Everyone:

Regarding what John Carr said before: If we had a robust system of pseudonyms, people could be identified (by authorised institutions/people) rapidly, accurately, and inexpensively. It is a mistake to consider only two alternatives: either total anonymity or total identifiability. It’s a false choice. Pseudonymity is a midway approach that avoids the worst effects of full anonymity and identifiability. Pseudonymity is a low-level form of anonymity, and a low-level of anonymity is crucial, not only for children and teens, but also for healthy political debate and social interaction (from people debating about politics, to them seeking help in health forums, etc.).

16:00:12 From Julie Dawson, Yoti to Everyone:

This article from TBI details some of the shades from pseudonymity through to anonymity to verification - we need a chart with the 20 possible shades https://institute.global/policy/social-media-futures-anonymity-abuse-and-identity-online

16:00:19 From Iain Corby to Everyone:

We are neutral on the policy question here - but be assured that the tech can deliver pretty much any policy objectives that are selected by Parliament.

16:00:40 From Lorna Woods to Everyone:

There are issues for the right to choose what we hear. It seems harmless enough when we think about it in the context of anonymous accounts, but what about concerns about misinformation/ahte speech - it might lead to the suppression of counter narratives for example.

16:01:56 From John Carr to Everyone:

Rapid, inexpensive and accurate, but the platforms or whoever should also be obliged to hand over the data immediately. Think traffic offences and car number plates. Regulated by law. Supervised by the courts.

16:02:26 From Lorna Woods to Everyone:

The use of ANPR actually has no specific legal base - and I think that's a problem!

16:02:50 From Andrew Strait (Ada Lovelace Institute) to Everyone:

To Dave’s point, I do worry that suggestion of passing criminal sanctions onto platforms may create a perverse incentive in which platforms may in turn remove anonymity to prevent any liability.

16:03:07 From John Carr to Everyone:

so give it one. It appears to work anyway

16:03:47 From Stephen Kinsella to Everyone:

Agree with Lorna, we try to simplify this for a debate of this nature but there are always going to be tradeoffs.

16:03:50 From Lorna Woods to Everyone:

Following on from Andrew, it may also be a blanket response - are we talking about this happening for all sorts of law, or just criminal?

16:04:12 From Stephen Kinsella to Everyone:

I agree with Carissa we could envisage a range of levels of verification from anonymous, to pseudonymous, to verifiable or identifiable, to open - and give all of us users the right to decide which of those categories we are comfortable interacting with, or allowing to reply to us.

16:04:13 From Dave Rich to Everyone:

Andrew, I take your point, but I suspect you will get a range of responses from platforms in terms of how much of that legal risk they want to take on.

16:04:25 From Lorna Woods to Everyone:

I meant to say some of the hate speech will not trigger the criminal law

16:04:36 From Carissa Véliz to Everyone:

On the police not being able to track abusers. Admittedly, I don't have as much experience as Dave Rich, but I have had friends brutally abused online by people who were identified, and when they went to the police, it didn't work either. To what extent is police inaction due to difficulties to identify people, and to what extent is that used as an excuse because police are not sure what to do in these kinds of cases? Genuine question.

16:05:03 From Stephen Kinsella to Everyone:

As Lorna said earlier we could have graduated duties but as Dave says there is enormous risk if we give a free pass to certain platforms who have smaller user numbers, because we will still be talking about large numbers in absolute terms.

16:07:04 From Andrew Strait (Ada Lovelace Institute) to Everyone:

+1 to Carissa, I'm also not sure police/legal action is the best remedy for abuse online, and whether we should focus more on efforts to (a) prevent, identify, and rapidly disable abuse (an enormous moderation challenge, given how context dependent and gray this can be in many cases) or (b) as Carissa and Stephen have mentioned, focussing more on design choices that reduce the capability to send or view harmful content (though it's very hard to know if this works and what its impacts would be without careful testing)

16:07:16 From Iain Corby to Everyone:

you also need a way to stop banned users opening a fresh account (again quite possible technically in a privacy preserving manner)

16:09:17 From Iain Corby to Everyone: A relevant cartoon to amuse you in the break https://avpassociation.com/thought-leadership/2194/

16:14:19 From Stephen Kinsella to Everyone:

Apologies for the flurry of messages just now but I spotted that a number of my replies had gone only to one recipient.

16:15:20 From Lorna Woods to Everyone:

On the duty to cooperate, the phrase was being used in 2 contexts: (1) duty of platform to tell regulator about problems on other platforms (or perhaps also to cooperate in regulator-coordinated discussions about horizon scanning for new problems); and (2) duty to cooperate by handing user data over to the police (with appropriate safeguards in place). We should perhaps think of some different labels to distinguish the two. Also in re (2), this would only come up when the police are investigating a would-be crime - as I mentioned earlier a lot of hateful speech is either not criminal, or not prosecuted for various reasons. So does a duty to cooperate arise at all in other context or are we relying on victims to take legal action (Norwich Pharmacal order) to get it?

16:16:20 From Stephen Kinsella to Everyone:

A thought, but on eg Twitter there would be nothing (at least under our proposals) to stop a user having a verified account for some public-facing purposes and an anonymous one to use when exploring sensitive issues.

16:19:36 From Joe Mulhall - HOPE not hate to Everyone:

Thanks for a really nuanced discussion about anonymity. Really informative and interesting. One final point I thought worth adding is that usually the people who most value anonymity aren't on calls like or wouldn't be able to give evidence to to a PLS committee so there is always a danger that their perspective is underheard in this debate. Just a small thing to add.

16:20:42 From Julie Dawson, Yoti to Everyone:

Regulators such as OFCOM could undertake adhoc or periodic audits using age assurance tools - see in this blog how the BBC documentary nudes for sale did this and found that on an 18+ platform 32.9 % of users on a given day were under 17 https://www.yoti.com/blog/nudes4sale-supporting-bbc-expose-underage-porn-anonymous-age-estimation-technology/

16:21:35 From Lorna Woods to Everyone:

@ Carissa, I think the issue about police inaction is a mix of things - partly lack of understanding/training but also lack of resources. There is also a question of legal threshold and one interesting point is that the CPS guidance says that in general it is not in the public interest -given the importance of freedom of expression - for low level social media offences to be prosecuted. My guess (and it is a guess) is this sends a message to the police that unless it is within the hate speech offences (rather than just being generally hateful) that dealing with these issues is not a priority.

16:23:20 From Carissa Véliz to Everyone:

@Lorna: Thanks, that fits my perception. But then let’s not blame it on anonymity, because identifiability won’t fix that.

16:25:52 From Iain Corby to Everyone:

The AVPA has endorsed Baroness Kidron's Age assurance [minimum standards] bill - if it does not get govt backing perhaps it can be integrated to the OSB

16:26:18 From Julie Dawson, Yoti to Everyone:

Here is a link to the organisations reviewed by ACCS to review age approaches https://www.accscheme.com/registry

16:27:04 From Andrew Strait (Ada Lovelace Institute) to Everyone:

Apologies, I’m afraid I have to leave to make a train, but thank you so much for this wonderful discussion.

16:27:05 From Julie Dawson, Yoti to Everyone:

And link to white paper with new data in terms of facial age estimation for under 13s accurate to 1.3 years of accuracy https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-October-2021-20211026.pdf

16:28:00 From Stephen Kinsella to Everyone:

Is it hard to be certain about the impact of any measures because the platforms have the data and won't readily share it. But if verified accounts were enabled to decline to receive replies from unverified accounts, we certainly know (and companies like Signify can show this) that it would reduce the incidence of harmful communications. The police don't have the bandwidth or appetite for all these cases.

16:28:40 From Matt Tindall to Everyone:

Picking up on Julie's comments re: the need for audits of AV tools, this is the approach that the BBFC would have taken as the Regulator under Part 3 of the Digital Economy Act. We would have been investigating and testing adult sites' age-verification arrangements on a daily basis, and also checking that sites were not hosting illegal extreme pornography. Active investigation and (as Iain notes) swift enforcement is essential for maintaining a level playing field to ensuring sites are not given a commercial incentive to circumvent the regulations

16:29:50 From Iain Corby to Everyone:

We work to the BSI Standard PAS 1296:2018

16:30:21 From Iain Corby to Everyone:

doing AV in house is marking your own homework!

16:31:46 From Iain Corby to Everyone:

Here's a non exhaustive list of Age assurance methods https://avpassociation.com/avmethods/

16:34:03 From Iain Corby to Everyone:

There is a combination of other legislation driving an almost universal requirement for age assurance - AudioVisual Media Services Directive, Age Appropriate Design Code and this Bill - we have reached a tipping point.

16:35:02 From Julie Dawson, Yoti to Everyone:

It is worth being clear as to the difference between facial analysis and facial recognition. There is no authentication or recognition of an individual with facial age analysis. See this chart by FPF to see the difference. https://fpf.org/blog/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/

16:35:33 From Iain Corby to Everyone:

www.euCONSENT.eu is a project funded by the Commission to deliver an interoperable network for AV providers across Europe (including the UK). This will allow you verify once and use the same check many times, with little or no impact on user experience

16:36:20 From Carissa Véliz to Everyone:

@Julie. But even facial analysis is a huge threat for privacy.

16:37:12 From Lorna Woods to Everyone:

One sticking plaster to the online porn issue would be to amend the Comms Act so that the country of origin jusrisidiction test comes out (replacing it with a similar jurisdicition test to the draft OSB), so that the ODPS content rules would apply to overseas providers.

16:37:34 From Iain Corby to Everyone:

You need to apply age assurance proportionately - our standards define 5 "Levels of Assurance" which increase the certainty about the check. So legal checks to sell a knife might require very strict checks; opening a twitter account might be a lower bar.

16:38:02 From Iain Corby to Everyone:

and don't forget lootboxes!

16:39:17 From Iain Corby to Everyone:

We would like the Gambling Commission to specify PAS1296 so operators know the standard expected of them in that industry - this can be considered for other industries too with Ofcom giving guidance on the level of assurance expected

16:39:58 From Julie Dawson, Yoti to Everyone:

It is worth reviewing the options. Facial analysis estimates age without identifying or recognising any individual person.

It can support billions of people who do or do not own an ID document and so promotes social inclusion. Yoti openly states the accuracy for skin tone, age and gender in its whitepaper

Privacy preserving, data minimised No personal information is stored

Promotes data minimisation in line with GDPR

16:40:32 From Heather Wardle to Everyone:

Agreed Iain - and there are so many more practices with gaming/gambling intersection we could mention here. Very interesting that Twitch have now banned casino streaming, but others have not

16:41:28 From Iain Corby to Everyone:

I always remember the former problem gambler who found his 5 year old son playing is a casino on a slot machine he had built in a city building game!

16:42:30 From Iain Corby to Everyone:

The age appropriate design code (ICO) now requires services to consider children of different age ranges

16:42:45 From Iain Corby to Everyone:

AV can and does prevent adults accessing child safe areas#

16:42:54 From John Carr to Everyone:

AVMSD is not a brilliant model because it is tied to the country of origin principle. What matters is the country receiving the content, in this case, the UK

16:43:39 From Lorna Woods to Everyone:

A John - that's why I said change the jurisdiction test.

16:43:44 From Iain Corby to Everyone:

Can we just cut and paste Part III of the Digital economy act into the new Bill please? (it can be improved on but it does the job!)

16:44:22 From Lorna Woods to Everyone:

@ Iain I've wondered why we don't just delete cl 131 which repeals the relevant provisions but I assume that is politically unacceptable.

16:44:48 From Matt Tindall to Everyone:

The DEA Part 3 applied to all online pornography services operating on a commercial basis, wherever they are based. "Commercial basis" was defined in secondary legislation, and includes websites which offer pornographic content for free but which generate revenue through advertising or by upselling premium content. A similar definition could be used to bring all commercial porn into scope of the OSB.

16:45:32 From Tim Clement-Jones to Everyone:

I think the original part 3 needs to be more prescriptive about the type of 3rd party verification required.

16:45:49 From John Carr to Everyone:

Indeed it does

16:47:00 From Iain Corby to Everyone:

Our sense is ministers want Parliament to make the decision, rather than the government being associated with impeding access to pornography. Just not repealing Part 3 still leaves us awaiting a commencement decision which even the High Court could not extract.

16:47:39 From Lorna Woods to Everyone:

Yes, but you'll need commencement orders for the OSB when it gets enacted.

16:48:59 From Iain Corby to Everyone:

COPPA in the US is a major disincentive to platforms obtaining actual knowledge of age

16:49:11 From Carissa Véliz to Everyone:

Regarding Sonia's comment about empowering young people to exercise their rights: In our current data economy, it will be very hard to protect children's privacy. Personal data is being collected left right and centre by default. They collect every click, and are constantly inferring extremely sensitive data. As long as personal data can be bought and sold, we won't be able to protect children's (or adults') right to privacy.

16:50:53 From David Anderson to Everyone:

I need to disappear now but thank you to the organisers, to those who contributed both orally and in chat, and to Damian's committee whose digest and recommendations will in due course make all this so much easier for the rest of us. Could the numerous useful links in the chat to research and recommendations be provided in LSE's note of the session?

16:51:26 From Lee Edwards to Everyone:

Yes, they’ll be included, and thank you for your participation.

16:59:35 From ABRAHAMS, Debbie to Everyone:

Thanks

16:59:38 From Jacquie Hughes’s iPhone to Everyone:

Thank you to everyone; great contributions

16:59:55 From Julie Dawson, Yoti to Everyone:

Excellent session, thank you

Appendix 2: Email by Professor Lorna Woods [October 27, 2021]

Dear Lee,

I'd like to challenge something Nicola said at the end about OFCOM's duties to have regard to freedom of expression. There is no obligation on OFCOM to have regard to freedom of expression when coming up with it guidance or codes, although (as I originally said) OFCOM's a public body under the HRA and therefore can't infringe any of the Convention rights, and the Communications Act has OFCOM having regard to privacy and to freedom of expression in relation to its broadcasting role (see s 3(2)(f) and (4)(g) Communications Act) - note some of the other general duties might be applicable. Cl 56 draft OSB amends these provisions to introduce some general duties for OFCOM but doesn't mention either privacy or freedom of expression. I think there's some terrain that lies above just not violating rights that isn't then covered - more or less equivalent to those broadcasting provisions which almost saying try to optimise the balance of these rights.

I'd also like to clarify the point about OFCOM's powers in re risk assessment. Clearly OFCOM have enforcement powers (cl 80 + 82) in relation to risk assessments (cl 7) if the company does not do a risk assessment or does not cover all the ground in identified in cl 7, but it is less clear what the position is if the company has done something but wilfully ignored evidence - the wording in cl 80 is that the provider has 'failed or is failing'. There might be a qualitative element in there, or there might not- presumably there'd be a risk of litigation about it. I can't see the problem in clarifying if the policy team think that it should be in. There is less detail about obliging companies to measure success and the obligation is to keep the risk assessment up to date by reference to triggering events, not to do risk assessments on a rolling basis to see what has changed.

Lorna