Open Rights Group

# Response to the Lords Communications Committee enquiry into freedom of expression online

## 15 January 2021

Open Rights Group are grateful for the opportunity to provide our input to the Lords Communications Committee enquiry into freedom of expression online. Open Rights Group are a digital rights campaigning organisation. We seek to help build a society where rights to privacy and freedom of speech online are respected, protected and fulfilled. We have over 20,000 engaged supporters across the United Kingdom. We advocate evidence-based policy, guided by respect for fundamental human rights.

In our response below, we have combined several questions for the purpose of the narrative, and have also included information about actions the Government have taken that limit free expression online, that also lack oversight and scrutiny. We also call the Committee's attention to the transcript[1] of the 9 December 2020 hearing on freedom of expression held by the Joint Committee on Human Rights, which included testimony from our Executive Director, Jim Killock.

[1] https://committees.parliament.uk/oralevidence/1387/html/

# Executive Summary

1. Free expression in the UK is under threat online from government over-regulation, informal regulation, lack of processes and safeguards for users, and automated takedowns. The proposed Online Safety Bill adds to these threats by attempting to push private enforcement against illegal content, and removal of legal content deemed to be risky to users. (pp 7-10)

2. We draw particular attention to previous government initiatives to reduce the availability of terrorist content, to remove fake goods websites, to reduce access of children to inappropriate websites through filtering, and to block pornographic websites through administrative orders, which have lacked proper process, oversight and transparency. These have left a legacy of damage to free expression which the government has not sought to address, while asking for new restrictions in current proposals. Government needs to set high standards of process, oversight, and transparency for itself, while demanding it of private companies. (pp 46-62)

3. Private companies are in a position of power to determine the limits of free expression which needs independent supervision. However, this needs to be independent of political influence, just as courts are. Thus we favour independent, non-state regulation of content removals, rather than the use of Ofcom, which is a state regulator. State regulation of legal online content is highly undersirable online, just as state regulation of the press is. (pp 26-30)

4. Legal duties for platforms to take due regard of free expression and other human rights, anchored in existing human rights laws, are an important idea that should be more fully explored in the online harms context. (pp 16-19)

5. The debate about online anonymity has been very unfortunate. Anonymity in practice is usually psuedonymity and easily removed by legal means when necessary. True anonymity is hard to obtain, but vital for whistleblowers and press freedom. Likewise, psuedonymity is vital for marginalised individuals such as members of the LGBTQ community seeking to explore their identity safely without identifying themselves to everyone they know. The debate on online anonymity must not be used as leverage to force mandatory account, age, or identity verification. (pp 20-25)

6. Moderation policies, automated takedowns, notice procedures, and safeguards to stop the abuse of takedown procedures have yet to be clarified at this stage of the Online Safety Bill debate. These issues, in contrast, are now advancing in the EU at pace with the Digital Services Act. The DSA additionally places judgment calls about harmful content at a distance from state regulators. Overall there is a lot to learn from that proposal, but there is also a risk that the UK will need to accept the DSA as a *de facto* standard which will supercede the UK's proposed approaches. (pp 43-45)

## Is freedom of expression under threat online? If so, how does this impact individuals differently, and why? Are there differences between exercising the freedom of expression online versus offline?

7. Freedom of expression online is under a great deal of societal and political pressure, as the result of its boundaries being treated, by government and law, primarily as a private and commercial consideration. Private spaces can choose their own standards for free expression; however a small number of these private spaces now contain a great deal of what forms our public discourse. Additionally, their free-to-use business models platforms are based on advertising paying for an 'attention market'. This model can drive the prioritisation of potentially unwanted but popular content. It also incentivises low content moderation costs. It fuels exploitation of personal data to these ends.

8. Thus questions of accountability for content have arisen both as the result of concerns about takedowns and what content is deprioritised, while others wish to see platforms remove more material, especially content that is "lawful but [potentially] harmful". We are especially concerned that this is driving the state to take a proactive regulatory role in setting limits around access to legal content, without seeking to legislate against the content itself. Such an approach has been repeatedly ruled out of scope regarding the press, but is currently ruled in scope when governing the speech of millions of UK residents.

9. As with the press, the right approach to platforms can be achieved by allowing independent co-regulatory models which are independent from both government/the state and corporations, but are robust enough to hold those corporations to account. We address the substance of these points in questions throughout this consultation response.

10. The right to freedom of expression online in the UK has already been adversely impacted by several government initiatives. There are serious concerns about the accountability of government agencies which are already empowered to remove or restrict online content, such as the Counter Terrorism Internet Referrals Unit, and domain suspensions made in bulk by the Police Intellectual Property Unity and others. In addition Government has persuaded ISPs to filter adult content, causing much content to be blocked incorrectly for around 20% of UK households. The Government also tends to prefer 'administrative' powers for website blocking, rather than court processes, as envisaged for BBFC for adult websites. As these concerns do not immediately fall into the questions below, we explain the issues in full at the end of our submission.

## How should good digital citizenship be promoted? How can education help?

11. While ORG is not an educational organisation, we are well aware that education has an often-neglected role regarding online life. Risks cannot be eliminated by government

policy, especially when the core issue is the interaction of individuals with each other and their expressions. The life skills which allow people to deal with situations, and have opportunities to discuss the implications of moderated digital discourse, are extremely important, but very neglected. We would welcome a shift in thinking from an attempt to eliminate risks and harms altogether, to working to help people of all ages to understand and mitigate risks they will inevitably encounter online.

12. Equally as important to digital citizenship is creating an online environment where it is clear that moderation guidelines are enforced, abusive and harmful conduct has consequences, and criminal activity is dealt with through the rule of law. However, these values, again, are neglected in current approaches, which seek instead to incentivise the removal of content and user accounts via corporations, and indeed, task corporations with law enforcement responsibilities, rather than ensuring that criminal behaviour can be reported to and is properly dealt with by law enforcement.

13. We are also concerned by the rise of automated detection as a policy of surveillance. Society should not feel constantly watched and supervised. If it is, this inhibits freedom of expression. When content takedowns are automated, inaccurate, and in practice hard to rectify (as is often the case with copyright claims for instance), this creates social frustration with a bureaucratic, petty and unfair online environment. None of these are good models for online citizenship.

## Is online user-generated content covered adequately by existing law and, if so, is the law adequately enforced? Should 'lawful but harmful' online content also be regulated?

14. Many laws are in place to adequately deal with most content issues, but these laws can prove difficult for individuals and law enforcement to understand and enforce, just as is the case in the offline world. Consistency is key. We have recently made a submission to the Law Commission's review of the online communications offences in which we stressed that there should not be separate laws for online offences which do not have a real-world equivalent.[2] Speech which is illegal offline should be illegal online. This should not be complicated any further, in a way which will further detract from enforcement of those laws and the protection of those harmed by the offences.

15. In our submission to the Law Commission, we also noted that there is a case to look at ensuring the Public Order Act applies equally online as offline, to ensure that threatening behaviour is criminalised regardless of the medium. We are concerned about the existence of  "grossly offensive" tests for criminal speech in the Communications Act, and believe this needs to be repealed.

[2] https://www.openrightsgroup.org/publications/open-rights-group-response-to-the-law-commission-reform-of-the-communications-offences/

## Should online platforms be under a legal duty to protect freedom of expression?

16. Freedom of expression is currently protected in law in the UK through the Human Rights Act of 1998, which incorporates Article 10 of the European Convention on Human Rights. The UK is also an original signatory to the UN Declaration on Human Rights, which requires member states to protect freedom of expression in spirit and in law.

17. We are aware that the future of the Human Rights Act, following the UK's exit from the European Union, is in doubt.[3] Parliament has made it clear that the Act is not safe.[4] The Committee should ensure that regardless of the Act's future, or Article 10's European provenance, its provisions on freedom of expression must be equalled and maintained in any current or future legal framework.

18. The EU's recently announced Digital Services Act[5] intends to place a duty upon providers to take due regard of human rights considerations in their terms and conditions as a matter of law. This would mean that the protection of free expression, and other related rights such as the right of association, and regard for impacts on these, would need to be reflected in the practices of platforms. The DSA backs up this approach with concrete measures to improve processes including notice and takedown systems, appeals, and measures to stop the abuse of takedown systems, for instance by "reputation management" companies asking for "libellous" content to be removed.

19. In contrast, the UK government's full response to the online harms white paper[6] has begun the work of identifying means to protect free expression, but has not fully developed these. There is to be an obligation to protect "controversial viewpoints"; however, this is just one kind of expression. There is to be a means for users to challenge takedowns which unduly restricts their free expression; however, this has not yet taken account of the difficulties of making appeals, and the scope for abuse of takedown mechanisms. If platforms and service providers are to be under a legal duty to protect freedom of expression, those obligations must be clear in law from the beginning. They cannot be an afterthought.

[3] https://commonslibrary.parliament.uk/how-might-brexit-affect-human-rights-in-the-uk/

[4] https://www.parliament.uk/business/lords/media-centre/house-of-lords-media-notices/2019/january-2019/human-rights-act-is-not-safe-after-brexit/

[5] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

[6] https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response

## What model of legal liability for content is most appropriate for online platforms? To what extent should users be allowed anonymity online?

20. Anonymity, on its own, is not the issue. Indeed, anonymity is vital to ensure the safety of those experiencing abuse, exclusion, or any number of situations beyond their control. It is also a vital safeguard on freedom of expression. The issue should be what forms of recourse exist for those who are adversely impacted by anonymity, and whether they are sufficient. That issue is equally applicable to the legal liability models for content, which by definition, means *content which is already illegal*. This largely refers to content associated with violence, abuse, and terrorism, in addition to obvious issues pertaining to children. True anonymity is hard to obtain, but vital for whistleblowers and press freedom. Likewise, anonymity is vital for individuals seeking to manage different public identities, so especially important for people in minority groups such as parts of the LGBTQ community who may wish to separate their identities in different parts of their life, for instance in order to feel safe at work, or explore their identity safely without identifying themselves to everyone they know.

21. Most 'anonymous' content is not truly anonymous, but provisionally so. We may therefore term it 'psuedonmyous', as the individual can be identified via details held by a platform or in combination with details from an ISP. A number of policy and legal options therefore already exist to give users, and law enforcement, a form of recourse when online content, whether attributed to a user or left anonymously, is misused as a vector for abuse, harassment, or criminality. These include the provisions of the Investigatory Powers Act, and Norwich Pharmacal Orders. Options for recourse also include direct engagement between law enforcement and platforms which are used to send abusive messages. We would therefore stress that legal liability models already exist to deal with the vast majority of criminal misuses of attributed speech or online anonymity. The question is why they are not being used to their full extent, and consequently, what government would hope to achieve with any new regulations which are not possible under current laws.

22. The upcoming Online Safety Bill, as it has evolved from green to white paper to policy proposal to government response, has at times risked creating a legal liability structure for platforms and companies for both illegal *and* "legal but harmful" content. That model would hold a web site operator responsible for something said on the site, but not necessarily the person who said it. It also would contain the threat of imposing actual criminal liability onto managers and directors of sites for that content but again, not necessarily the person who said it. We have been clear[7] that this regulatory model would be completely unacceptable. It would create a freeze on freedom of expression which would inspire less democratic and civic minded nations to follow our example, making the UK a leader in criminalising speech.

[7] https://pictfor.org.uk/pictfor-online-harms-stakeholder-input-report/

23. On anonymity, the upcoming Bill will require platforms to tackle anonymous illegal abuse. This must not be used as leverage to attack anonymous “legal but harmful” speech, which may be subjective and contextual, nor should it be used as leverage to require mandatory identity verification processes on platforms.

24. One frequently raised suggestion proposes to link online accounts to a form of identification, such as a utility bill or a bank account, thereby enabling a positive form of digital identity verification. However, these requirements would immediately disenfranchise those on low incomes, the unbanked, the homeless, and people experiencing any number of other forms of social exclusion from being able to use the internet, and consequently, to build their lives up to a level where utility bills and bank accounts are possible. Policy solutions to misuses of online anonymity cannot create a digital and social underclass.

25. Additionally, any discussion which could lead to policy decisions to restrict anonymity must take into consideration the impact of age verification and age assurance requirements, as have been recently requested in several public and private policy forums, ostensibly for child protection purposes but impacting all users in all scenarios. These proposals would mandate age verification (an exact form of identity confirmation linked to public and private data sets) or age assurance (a rough form of identity confirmation linked to general characteristics) for all users, situations, and content, in order to identify child users for the purpose of applying different security standards to them. Government must understand the chilling effect that these procedures will create for free speech and expression, where grown adults will be afraid to express what may be wholly innocuous and subjective opinions on matters both public and private, because their words can be linked directly to them through processes created in order to (quite literally) treat them like children.

## How can content moderation systems be improved? Are users of online platforms sufficiently able to appeal moderation decisions with which they disagree? What role should regulators play? How can technology be used to help protect freedom of expression?

26. The current debate on the use of technology as a means of protecting freedom of expression tends to centre around automated content moderation systems, such as machine learning or artificial intelligence. This is always viewed as a positive. We would call the Committee’s attention to the ways that technology can be used to moderate content in unfair, excessive, or simply incorrect ways. We have noted these issues at the end of this submission.

27. We also ask the Committee to note the means for notice and takedown and appeal mechanisms, which exist as safeguards around content which has been either been “machine-flagged” or is the subject of high-profile moderation decisions - an issue which has been in the news as of late following the Capitol insurrection and the deplatforming of Donald Trump. We believe that decisions about content, even in a case as egregious as

that, need to be held to independent account.[8] This oversight should be done either by the courts, or by an independent, non-state regulator.

28. While the UK's online harms proposals do include mechanisms for appeals against takedown decisions, these ultimately rely on the terms and conditions of the platform or online service. If a particular kind of content is disallowed, the appeals would need to be made on the basis of those restrictions, rather than the law. Thus the contest could easily become about the limits of terms and conditions, and whether these need to be more restrictive or permissive. The door is open to political pressure on the regulator to rule that terms and conditions need to be made more restrictive in selectively chosen areas for reasons of 'safety', meaning that terms and conditions can effectively become weaponised in the interests of the ruling political party of the day.

29. Notice and takedown systems are open to gaming by people who simply desire content to be removed, at no risk to themselves. Appeals, on the other hand, are relatively burdensome for people whose content is wrongly and unexpectedly taken down. The result is that appeals are not taken up very often, under any notice and takedown system. Notices can be particularly dangerous when content is automatically removed as the result of a notice, without the chance of an objection. Notice systems therefore need to take account of bad actors, and penalise people who abuse these systems.

30. As the Online Safety Bill takes shape, its drafters would be careful to design systems that do not politicise oversight and undermine trust. Independent external oversight for content moderations, in a way which is as equally accessible to the everyday user as it is to a head of state, is a key to this safeguard, but the online harms proposals do not yet establish it . Yet they could: particularly if they move away from a state regulator, and look to a model like co-regulation which is less susceptible to political interference.

## How do the design and norms of platforms influence the freedom of expression? How can platforms create environments that reduce the propensity for online harms? To what extent would strengthening competition regulation of dominant online platforms help to make them more responsive to their users' views about content and its moderation?

31. Many of the problems with the online environment caused by unwanted content and experiences can be related to the lack of choice users have over which platform or service to use. Online platforms are operating as *de facto* monopolies in the cases of Facebook, Google, and Twitter. Rather than addressing that lack of choice, much of the online harms debate has focused instead on placing regulatory obligations onto platforms and service providers to monitor and moderate content. That proposed model creates a regulatory burden which can only be achieved by the largest platforms and companies, and would drive smaller services, platforms, aspirants, and startups out of the market. It would, in other words, achieve the exact opposite of what it wants to achieve.

[8] https://www.openrightsgroup.org/blog/trump-takedowns-need-accountability/

32. Competition policy is, in our view, a means to rebalance these concerns in favour of users, free expression, and a pleasant online environment, in a way that does not make big platforms even bigger while punishing smaller operators for the sins of others. Done correctly, good competition policy benefits freedom of expression by diversifying platforms and marketplaces, as opposed to mandating restrictive content moderation and harms rules which would reduce platforms and eliminate any sort of healthy marketplace.

33. Competition policy must push for interoperability - the technical infrastructure which makes it easy to move content and accounts to other services[9] - so that users could choose which platform to use. This would allow different services to offer different experiences, which includes the way that content is prioritised as well as what is removed. This also has the potential to drive the market in a different direction than the current "attention market" model, as users choose platforms that give them experiences that suit them as users rather than the platforms' desire for their time and interaction.

34. This is already taking place in some environments, particularly the Mastodon and Matrix networks. Mastodon, largely developed in France, seeks to create an environment like twitter ("Microblogging") where users choose sites that favour their style of discourse and moderation, but continue to interact with other sites as they wish. The initial drive for Mastodon was a concern about abuse of data and lack of civility among Twitter users. Some Mastodon sites are more open to un-moderated discussion, while others favour controls on what is said and how. Mastodon users and services are able to prevent sites with users who may break the law or spread hateful content from interacting with them, which they are far less able to do on Twitter or Facebook, despite these being closed and commercially patrolled environments. This gives a flavour of how interoperability in social media can be made to work to the benefit of users and their personal experience.

35. The Matrix network, developed by a British company, is similarly interoperable, but focuses on chat rooms and private discussions, rather like products such as Slack and Internet Relay Chat. It has robust means of identifying bad actors, and preventing them from accessing servers, according to the desires of the people operating the servers. Interoperability ensures that chat rooms can be accessed across all servers, and also different protocols, preventing any single company from dominating and deciding what content should or should not be accessed – this is the responsibility of the host. This again shows how interoperability can both create diversity of supply and enhanced content moderation policies.

36. Both Matrix and Mastodon are open source products, using published, open standards to exchange messaging, rather as email is based on open standards and protocols. Platforms like Twitter or Facebook could be obliged to adopt open standards for messaging in the same way, while remaining closed source with their own proprietary

[9] https://openforumeurope.org/publications/ofa-research-paper-the-technical-components-of-interoperability-as-a-tool-for-competition-regulation/

technology governing user experience. Instead of competing on the basis of who has most users, to encourage more people to sign up to communicate with them, these platforms would have to compete on user experience.

## How could the transparency of algorithms used to censor or promote content, and the training and accountability of their creators, be improved? Should regulators play a role?

37. Algorithms are fundamentally unable to be fully accurate. They are not humans, nor can they substitute for them; nuance, context, and culture are extremely important in making content moderation decisions.

38. Taking Facebook's policies as an example, content policies are set to work along very simple guidelines to aid decisions, whether those are made by human or machine. For instance, nudity is defined as exposure of a female nipple, or part of a female nipple. This relieves a moderator from needing to decide if content is meant to be sexually provocative, but of course can prevent pictures of breastfeeding or war crimes from being published. Likewise, as recent events have shown, content showing violence may be necessary journalistic reporting for the public record rather than gratuitous violence shown for its own sake, and its deletion on literal moderation guidelines can impede law enforcement and the progress of justice. Facebook has invoked policies to suspend takedowns when it expects such problems due to political disturbances, but this requires foresight.

39. Problems of these kind are magnified when they are made by machine, as they are more likely to make contextual and cultural errors, and miss the significance of content. In practice, machines can more easily identify pre-existing content copies than make their own decisions, but again this can lead to misidentification of content. For example, a "terrorist video" might be contained within a report about terrorism, or a copyrighted clip can appear within a review of that film.

40. Although moderation policies are often revised in the light of such problems, content can still be caught incorrectly. No policy can fully capture all circumstances and balance all considerations. Appeals that can apply flexibility to take account of free expression and other concerns are therefore vital with any content moderation system. Likewise, it is essential that people can reinstate material pending decisions, should they wish to do so.

41. Automated copyright identification is a particular problem regarding out-of-copyright musical works, as a new performance has a copyright, while the music or words do not. A performance of Beethoven from 1925 can easily be claimed by a company with a more recent, in-copyright performance. The same is true of short clips released for review purposes. Such content is often "monetised" by copyright claimants, to the detriment of the real creators. Copyright removals have also impacted people recording themselves cheering in pubs at goals in football matches, and publishing their experience on Twitter.

This is clearly unimportant to copyright owners, and likely not a violation of copyright, but content has been removed nevertheless.

42. Copyright takedowns have been given some relief by the addition of an ‘exception’ to allow parody in the UK. Nevertheless, we remain worried that EU proposals to identify and remove content in an automated fashion could come to the UK in due course. This would require content used by individuals to be pre-licenced by platforms and paid for, or else removed. Thus cartoons, video clips and photographs often used in a parodical fashion in “internet memes” would be subject to licencing or removal, even when protected by law under parody exceptions. As a result, the EU is struggling to implement these changes. They are likely to be the subject of legal challenge.

## Are there examples of successful public policy on freedom of expression online in other countries from which the UK could learn? What scope is there for further international collaboration?

43. The UK has much to learn about attempts to regulate content which have proved unfeasible in constitutional law, such as France’s Loi Avia, or disproportionate to the need at hand, such as Germany’s NetzDG legislation. There are equal lessons to be learnt from recent high-profile experiences with American social media applications which took the concept of freedom of expression, and light-to-no moderation, to their most literal ends. All of these rules, and experiments in balancing freedom of speech with online civility, were paved with good intentions.

44. However, as with data protection regulation, the Committee and the Government should understand that there is no feasible way of the UK ‘going it alone’, with a third way of standalone regulation for a third way’s sake, in a regulatory landscape which is transnational and multistakeholder, particularly in light of the EU’s plans for the Digital Service Act. Any UK initiative which creates more restrictive rules on freedom of expression than the DSA will risk platforms and service providers opting to withdraw from the UK market altogether. Additionally, companies which will be facing a DSA compliance process will not feel inclined to embark upon a completely separate process for the smaller UK market in areas such as content moderation and obligations over “legal but harmful” content. It may prove inevitable, despite the UK’s exit from the EU, that the DSA will create the *de facto* standard on freedom of expression and that these guidelines, having proved good enough for the EU, will prove good enough for Ofcom.

45. Despite the inherently international nature of freedom of expression online, we note that the UK must deal with the issues which are squarely in front of it. This must mean not allowing our domestic dialogue on online harms, content moderation, and freedom of expression to be roped into or tainted by grievance issues, culture wars, or astroturfed debates borne in other countries or political environments. Our problems, and our solutions, must be our own.

## Other issues the committee should consider: Government initiatives to remove content that lack oversight and due process

46. The Committee seeks to understand threats to free expression online. At its heart, this is a question of legal practice. If content is removed, there should be legal recourse for that. This makes Government initiatives to remove or restrain content especially impactful.

47. We are concerned by the lack of external accountability for three major Government takedown and filtering efforts, which are entirely informal in nature. These are the CTIRU notifications made by police about terrorist content, the domain suspension system operated by Nominet, accessed by a number of law enforcement agencies, and ISP adult content filters.

48. All three examples show the potential for Government policy to have adverse free expression impacts, and especially to bypass necessary systems of review and accountability, by placing the burden for policy implementation on private companies alone.[10] The issues with UK ISP Internet filters also demonstrate the likely problems with machine identification of content. **In the Committee's work on free expression, we recommend that the lack of due process and oversight around each of these three informal procedures used or promoted by Government is examined.**

**(1) CTIRU**

49. The CTIRU assesses 'terrorist content' for legality in the UK and the terms and conditions at platforms. When content is in its view in breach of both, it notifies platforms that content should be removed. Over 300,000 pieces of content have been removed according to statistics given to Parliament. As far as we are aware[11], the quality of these notifications is not reviewed externally. There is not public information as to how accuracy is assessed. However, it is clear that at this scale, mistakes will be made. It is unclear that platforms receiving these notifications, especially the smaller ones, will always be able to correctly identify such mistakes and refuse inaccurate takedown requests.

50. We do know, however, of a number of notifications that have been refused by larger plaforms, as a few of these have entered the public domain.[12] In one example, a WordPress.com blog ("UKIP Voices") attempting to satirise or defame UKIP leaders as racists was notified as being in breach of terrorist legislation.[13] While the site was disatasteful, it was unlikely to be terrorist in nature. In another more recent case, CTIRU

[10] https://www.openrightsgroup.org/publications/org-regulation-report-ii/ and https://www.openrightsgroup.org/publications/uk-internet-regulation/

[11] https://wiki.openrightsgroup.org/wiki/Counter-Terrorism_Internet_Referral_Unit

[12] https://wiki.openrightsgroup.org/wiki/Counter-Terrorism_Internet_Referral_Unit/Lumen_reports

[13] https://lumendatabase.org/notices/13651135 Also summarised above

notified Google to remove part of their Transparency Report referencing a CTIRU takedown. It is unlikely that Google's Transparency Report was in breach of terrorism legislation.[14]

51. In order to protect free expression and prevent over-reach, police notification systems need checks and preferably a mean for individuals or companies to ask for their notices to be reviewed. Otherwise, a company or individual is left in the difficult position of being notified that they are breaching terrorism legislation, in the view of the police, and accepting criminal liability for that. In any case, individuals should be able to ensure that police decisions are of the highest standard. In at least some cases, they clearly are not.

### (2) Nominet Domain suspensions

52. Nominet have suspended up to 30,000 .uk domains on advice of the police and other agencies, such as medical and fraud agencies. The vast majority of requests are filed by PIPCU, on the basis of likely trademark violations by sellers of watches, shoes and handbags falsely bearing upmarket branding. However, there is room for error in this work[15]. Occasionally, 'grey market' sellers may be misidentified as breaking the law, or domain owners may be unaware that their domains have been hijacked for lawbreaking. Nominet will refer people identifying mistakes to the agency that made the request, but as yet have not created a standing, independent appeals process. This may leave the credibility of appeals in doubt.

53. Nominet have made advances to ensure that there is better transparency about suspensions, and recently adopted our 2019 recommendation to introduce splash pages at domains that are suspended, partly to help consumers who had been adversely affected. Nominet do not however include information about rectifying mistakes or making appeals on these splash pages.

54. In our view, domain seizure is a very powerful and disruptive tool, that is potentially very damaging for a business or publisher reliant on that domain. Such takedowns should be subject to a court or tribunal decision, rather than reliant on an informal notification from the police.

### (3) Adult content filters at UK ISPs

55. Finally, the Government in 2017 pushed for ISPs to implement content filters. Around 20% of households now use these filters. Content filters are sometimes enabled by default, and can be difficult for ISP customers to understand. When businesses are blocked by filters, their experiences tend to be very bad, as they cannot practically ask all of their customers individually to remove their site from filters. The kinds of businesses and

[14] https://transparencyreport.google.com/government-removals/overview?authority_search=country:GB&lu=request_country&request_country=period:;authority:GB;p:2

[15] https://wiki.openrightsgroup.org/wiki/Nominet/Domain_suspension_statistics

organisations that are routinely incorrectly blocked include charities,[16] advice sites, or counsellors,[17] including those aimed at children and teenagers[18], because of keyword mismatches around 'drugs', 'sex' and 'alcohol'.[19] LGBTQ sites are disproportionately incorrectly blocked, also as likely graphic content.[20]

56. Businesses selling legal cannabis-derived products are also routinely blocked for similar reasons.[21] For reasons that are rather unclear, 1300 photographers and 4,000 wedding-related sites were blocked in 2019, Even websites relating to building supplies have been found to be blocked.[22]

57. There are also issues with over-broad categories. TalkTalk for instance recommend that customers block sites relating to 'alcohol' and 'tobacco'. This includes websites run by local pubs and restaurants, and vineyards that offer holidays to tourists. It is unclear that harms are likely to proceed from a child visiting a website about a pub or a vineyard.

58. Fairness questions also arise. A small grocery shop selling beer and wine may be blocked under TalkTalk's policy,[23] but it is extremely unlikely that Tesco will suffer the same classification.[24] Similarly, antique shops selling tobacco memorabilia may be blocked,[25] while antique tobacco memorabilia will not be blocked by TalkTalk when sold on eBay.[26]

59. In our view, a better policy would be to restrict such recommended blocking to sites promoting major alcohol and tobacco brands, that might promote products to children, rather than classifying everything related to alcohol and tobacco as potentially harmful. In any case, categories need to be consistent, rather than favouring major providers at the expense of smaller businesses.

60. In response to these problems, especially where blocks are against ISP policy, Open Rights Group created a service which tests for blocks in real time, called blocked.org.uk[27] ISP had provided a basic manual request system for site owners through Internet

[16] https://www.blocked.org.uk/list/2019_report_all_charities 98 UK charities blocked in 2019

[17] https://www.blocked.org.uk/list/2019_report_all_counselling UK 112 Counselling sites blocked in 2019

[18] https://www.openrightsgroup.org/app/uploads/2020/03/top10vpn-and-org-report-collateral-damage-in-the-war-against-online-harms.pdf

[19] https://www.blocked.org.uk/list/2019_report_all_addiction 185 UK sites blocked in 2019 relating to UK addiction advice

[20] https://www.blocked.org.uk/list/2019_report_all_lgbtq UK 114 LGBTQ sites blocked in 2019

[21] https://www.blocked.org.uk/list/2019_report_uk_cbd 112 Legal cannabis sites blocked in 2019 (mostly cannabis oil and cannabis foodstuffs)

[22] https://www.blocked.org.uk/reported-sites?category=Builders+and+Building+Supplies 32 sites relating to building supplies incorrectly blocked

[23] https://www.blocked.org.uk/site/http://floriosditalia.com Florio's d'Italia, Italian grocery shop, blocked by TalkTalk filters

[24] https://www.blocked.org.uk/site/http://www.tesco.com Tesco, selling groceries, tobacco and wine, not blocked by TalkTalk filters

[25] https://www.blocked.org.uk/site/http://tobaccocollectibles.co.uk Site selling "Old Tobacco Tins, Vintage Cigarette Packets and Tobacciana." blocked by TalkTalk filters

[26] https://www.ebay.co.uk/b/Tobacciana-Smoking-Supplies/593/bn_1838390 UK ebay section selling tobacco products, not blocked by TalkTalk filters https://www.blocked.org.uk/site/http://www.ebay.co.uk

[27] https://www.blocked.org.uk/

Matters.[28] Our website allows anyone to check for errors through real time tests and report them to ISPs. When a block is reported and found, a request for a review is sent to ISPs at their publicly available email addresses provided for this purpose. We believe ISPs are finding this useful. We certainly know that website owners and operators are, with around 2000 requests being made and 1200 blocks being removed so far.[29]

61. ISPs have variable records in responding to requests to rectify mistakes. Replies can be intermittent or inappropriate from ISPs, suggesting for instance that the complainant should switch the filters off if they wish, or whitelist the site so they can access it. We are currently chasing down problems with poor responses from Sky, for instance.

62. Additionally, while mobile operators have an independent review system, whereby BBFC reviews content decisions, the fixed line providers rely solely on their suppliers for decisions. This means that more subtle problems cannot be resolved, and sites that are not in breach of ISP's blocking policies can remain blocked indefinitely. **We recommend that the Committee ask fixed line ISPs why they have not implemented independent appeals processes beyond supplier review.**

[28] https://www.internetmatters.org/info-site-owners/ Explains that: "If you're an individual site owner and you would like to check the status of your site across BT, Sky, TalkTalk and Virgin Media's network filter settings, you can email us at report@internetmatters.org. Please include the URL of your site, your name, and company name, if relevant. If you run forums or social media sites you may want to request a check of these URL's separately as well as your domain name. "Internet Matters will then liaise with the four ISP's to establish the status of your site and we will email you with the details of your site's classification with the four ISPs."

[29] https://www.blocked.org.uk/ See footer for headline statistics