Solicitors & Attorneys

The House of Lords
Select Committee

By e-submission.

11 May 2018

Dear Sirs,

Re: Call for Evidence on Internet Regulation

Please accept our submission below. In summary, we do not believe that regulation is currently necessary. We do have concerns about pressures being applied to ISPs to regulate speech in return for immunity and based on soft law, at best, and the impact on freedom of expression. We also believe the UK fails to provide an effective remedy in many cases given our very serious access to justice issues, and suggest these need very careful thought, not knee-jerk reactions or headline-making initiatives.

1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

a. *Is there a need to introduce a new regulatory framework for the internet? Is it desirable or possible?*

(i) No. There is no present need. See below.

(ii) It is possible with some limits. These tend to be territorial and/or jurisdictional. There is still no comprehensive international treaty for enforcement of foreign judgments[1] and while this has not caused serious issues to date, this is in part as many US companies have decided to voluntarily comply with UK court orders or pre-action demands. However, there are some serious issues that will need to be addressed. Sooner or later, we will need to look at those who are targeting the UK while deliberately avoiding our laws and jurisdiction. Some US platforms that host reviews for example are avoiding UK libel laws and fighting even Norwich (disclosure) orders very effectively on First Amendment grounds for John Doe defendants. This plus the US libel shields (the State and Federal Libel shields, including the SPEECH ACT Law 111-223, 124 Stat. 2480, 28 USC 4101 and protection domestically without takedown under the §230 of the Communications Decency Act 1996) mean that these parties are publishing here with impunity

[1]There is the Hague Convention on Choice of Court Agreements but this is limited in scope to respecting jurisdiction clauses and so party autonomy on jurisdiction selection in commercial contexts.

and have an advantage over other speakers. Sooner or later we will have to look at blocking these people –perhaps on a strikes basis. What this means in practice is that the ordinary person can only seek relief takedown from Google (or other search engine) or other intermediary and while this may provide some relief under the new personal data tool, companies will not get takedown. See further below.

There are no easy answers here. We can look at the example of commercial international disputes more generally and see that the New York Convention and its near ubiquitous adoption led to the selection of international arbitration as the main choice for cross-border disputes. It has the advantage of avoiding local state courts and judges which may prefer a domestic party plus internationalised procedural rules and norms. In some ways, having a new chapter of the Convention to deal with cross-border internet related disputes might be a way forward but there are issues and the New York Convention allows challenges to awards on grounds of public policy –which is circular in that it will take us back to local speech norms or laws. There is a need for international co-ordination and a rule-making forum. Many states are signatories to the UNDHR and there is a level of harmonisation at a Human Rights law level on art. 10 ECHR and its parent, art. 19, with margins of appreciation for signatory states. It should be possible to distil some level of basic rule harmonisation into a treaty. See further below.

(iii) Is it desirable?

No. On the whole, things have worked in practice reasonably well so far. However, this has in part been due to a desire by the big players to be seen as good actors and avoid regulatory attention and sanction. This cannot be counted on indefinitely and we are also arguably now seeing smaller players now who are more prepared to game the rules. See above and further below. There was a wise recognition early on by the UK and US courts and legislatures that nascent technologies and business models should not be regulated into an early demise or quashed. One learned US judge said that after 100 years we should start to think about regulating the internet. There is often a rush to it, but good laws evolve over time and are first tested in the market. English commercial law, for example, has been honed over centuries of trade usage. We can look back and see that without the e-commerce immunities for notice and takedown, the early intermediaries would have been sued out of existence very early on.

b. *In your view, should we encourage self-regulation or employ more direct means such as co-regulation or direct (command and control) regulation?*

The UK's approach from the start -the same rules online as offline –with light touch regulation has worked well and facilitated London as a home to tech, with many industry leaders based

here. This also reflects international norms and the UN Human Rights Council affirmed in Resolution 32/13 that "rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice."[2] Good laws are technology and actor neutral and focus on behaviours and not actors, so the first question should remain what happens offline? The UK has laws dealing with intellectual property, revenge porn, privacy and data, harassment (criminal and civil), obscene publications, malicious publications and communications. We also have the Public Order Act (Incitement to Racial Hatred), the Race Relations Act and the Racial and Religious Hatred Act, the Terrorism Act, the Sexual Offences Act and the Protection of Children Act and laws governing advertising and commercial communications, etc etc. Most of these are technology neutral and so, in short, we believe the law is currently adequate and there is no pressing or obvious need for additional legislation. The current approach works well when dealing with regulated speakers, print or broadcast media –where there are co-regulatory and self-regulatory systems which include complaints procedures or arbitration or other means of effective remedy.

Where there is a real issue is how to provide a low-cost remedy/self-help measure more generally against other businesses and unregulated speakers. At present these can only be advanced as data issues to the ICO as there is no other authority in town. Access to specialist lawyers and/or the courts or litigation process is not affordable/possible for so many (arguably a violation of the state's art.6 obligations). So if a well-founded takedown notice is given and ignored, the only option is the courts. Ofcom/DCMS probably need to facilitate the establishment of an arbitration procedure for removals on other grounds –this would be self or co-regulatory.[3] This could be based on the domain name dispute resolution procedure for the UDRP (Uniform Dispute Resolution Policy) as administered online by WIPO and CAC and the Forum –all of whom offer paperless and software facilitated platform procedures. This is one of the internet's real success stories. Online justice at its best. It is cheap and fast yet the panellists or arbitrators are all independent experts. It is an excellent model. In the interests of disclosure, I note that the writer is a panellist for CAC and other panels. The public need something like this dealing with removals on various legal grounds where there is currently no effective remedy.

[2]See UN Human Rights Council 'Resolution 32/13 on the Promotion, Protection and Enjoyment of Human Rights on the Internet' (18 July 2016) A/HRC/RES/32/13, para 1.

[3]Ofcom regulates TV and while we don't want the internet regulated under the same codes, Ofcom is the backstop internet regulator under the Communications Act yet does nothing and offers no more general remedy. Note that Mr. Justice Leveson in his Report on the Regulation of the Media was also happy that Ofcom should be the final regulator for the print media if it had failed to join a recognized standards body within a year of being required to do so (as it was they set up and joined IPSO instead which refused to apply for recognition in contrast to Impress).

This would be preferable to leaving the ISPs to do it –particularly as they are incentivised to protect themselves and obtain an immunity/safe harbour defence by removal.

Those grounds however should be found in or extrapolated from existing law. There are obvious issues and problems with restricting speech based on anything less than hard law, see the art.10 jurisprudence on soft law.[4] There are problems with introducing new restrictions that need definition over time. Existing law has already been interpreted and has known contours. Furthermore –the law already has what is needed.

There are also issues if interpretation and enforcement is left to private interested actors entirely. See the recent decision in *NT 1 & NT 2 v Google LLC* [2018] EWHC 799 (QB) demonstrates this. That decision, was about the very important societal principle of rehabilitation through the *spent conviction*--the ability to serve your time and move on to a second chance under the Rehabilitation of Offenders Act (ROOA). In that decision, the judge decided that only one of the offenders deserved a second chance as only he was remorseful and there was no obvious risk to the public as he was no longer in business and so dealing with the public. The second offender was denied his second chance as he showed a lack of remorse (in the view of the judge) and was still offering services to the public –who had an interest in knowing his criminal past. That denial means he will never be allowed to move on and any search of his name will forever bring up his past—like a permanent tattoo on his name. This decision was about the Right to be Forgotten (RTBF) where the first decisions are taken by the search engine. Recourse may then be had to the ICO and finally, as happened here by the court. Frankly, in our view this decision makes very bad law. It may have some justification (spent convictions may be mentioned if there is a public interest under the ROOA) but how is Google or any other search engine going to assess remorsefulness or judge whether an offender is worthy of moving on? It has an interest in traffic and is not independent. The decision is a licence to refuse the RTBF to any party dealing with the public –which will include tradesmen. Many many people will be denied their second chance by Google on this basis. We believe this is wrong. There are already many serious challenges for offenders who must re-enter society and support themselves and their families and that was what led to the passing of the ROOA in the first place. In a similar vein, from experience in practice, while the law recognizes that companies have valuable reputation protected by the law of defamation, see per *Jameel v Dow Jones & Co. Inc.* [2005] QB 946 and the Defamation Act 2013, in our experience, Google will not grant a RTBF to a company as it is

[4]And see *Malone* v United Kingdom App.8691/79 the court stressed that the law must indicate the scope of a discretion of the executive and the manner of its exercise with sufficient clarity to give the individual protection against arbitrary interference. English law was so obscure and subject to such differing interpretations particularly as to the dividing line between the conduct covered by rules and that by discretion that it lacked the minimum degree of legal protection required to qualify as law.

a personal data right for individuals. There are also issues as to the scope of any relief even where granted. [5]

We examine further below but note here the fact that ISPs are incentivised in their own interests to remove content in order to benefit from defences and the only recourse is to the courts which is not an option for many.

In summary, there are many issues with leaving the matter wholly to the private sector where they get to mark their own homework and/or are self-interested and we believe that the UK state/government should offer an effective remedy to online rights and that the lack of such a remedy is the real issue. We propose an arbitration procedure based on the UDRP model as offered by WIPO and CAC perhaps via existing arbitral institutions but funded and supported by the state and perhaps facilitated by DCMS/Ofcom. This accords with the obligation of the UK under the ECHR to provide an effective remedy under art. 13 to persons whose convention protected rights and freedoms have been violated. The corresponding provision in the UDHR is art.8. Given the widely accepted issues in the UK about access to and affordability of traditional court justice[6] and the risks involved, there is a strong case for saying that there is in real terms a lack of an effective remedy for the art.10 and art. 8 and art.6 rights engaged.

2. What should the legal liability of online platforms be for the content that they host?
a. *Should online platforms be liable legally for the content that they host? In your view, are online platforms publishers or mere conduits?*

(i) Publishers and conduits. The current position.

Four defences are available to internet intermediaries facing claims from third-party defamatory content: (1) the horizontal immunities under the E-Commerce Directive and implementing Regulations, (2) the statutory defence of secondary responsibility under §1 of the Defamation Act 1996, (3) common law innocent dissemination and (4) the Website Operators defence under

[5]See *Equustek v Google* 2017 SCC 34 and see the EU's Article 29 Working Party issued guidance in November 2014 stating that when the RTBF is granted, results ought to be de-listed worldwide (so from .com domains too) in order to comply with the CJEU ruling in *Google Inc. v CNIL* Case C-136/17 (links to defamatory material should be removed from Google's worldwide sites on the penalty of the payment of fines by its French subsidiary). We understand that Google has so far resisted this move to implement the "right to be forgotten" on a global scale. See also *Google France Sàrl v Louis Vuitton Malletier SA* (C-236/08 to C-238/08) and *L'Oreal v eBay,* C-324/09.

[6]This is particularly so in the case of libel –where cases must be bought in the Queens Bench of the High Court and so under the full costs regime and requiring highly specialised lawyers.

§5 of the Defamation Act 2013.[7]The bottom line is that currently, anyone can be turned into a publisher by *actual* notice, even mere conduits, and that notice will provide such conduits with *actual* knowledge at which point they lose the immunity and other defences above, see *Twentieth Century Fox Film Corp v British Telecommunications plc* [2011] EWHC 1981 (Ch) (28 July 2011), *L'Oreal v eBay* [2009] EWHC 1094 (Ch) and *EMI Records* [2013] EWHC 379 (Ch)(blocking KAT, H33T, Fenopy)] and see also *Cartier International AG v British Sky Broadcasting Ltd* [2014] EWHC 3354 (Ch)(re trade mark infringement affirmed).[8] We set out briefly below, the position prior to such notice—by reference to trade mark cases (IP) and libel.

In any case, it depends on what the platform has done as to their legal status. If they cross a line they may lose their neutrality and become liable. With libel –that line can be continuing to publish once on notice of libelous content. With trade mark infringement cases, Google and others have been held to act as hosts when providing keyword services—on the basis that the search triggers the hosted ad. See *Google France Sàrl v Louis Vuitton Malletier* SA (above) and *L'Oreal v eBay* (above). However, in both cases the court stressed that to benefit from the Ecommerce Directive immunity, the host had to be neutral, that is, its role must be merely technical, automatic and passive and without knowledge or control. Assistance in drafting commercial messages or selecting keywords might well step over the line and provide knowledge and so jeopardize the immunity, and it was a question of fact for national courts in each case. In *L'Oreal*, the court was also asked what impact on eBay's covered hosting activities, other "unprotected" activities had, but merely reiterated that if the ISP takes an active role of such a kind as to give it knowledge of, or control over, those data then the immunity will be lost.[9] To date UK courts have compartmentalized hosting activities from other activities to give effect to the E-Commerce immunities. Other activity will not therefore necessarily jeopardize the neutrality and the immunity. See *Kaschke* [2011] 1 WLR 452 (denying summary judgment),

[7]At present, ISPs find it challenging to rely on many primary defences as they may lack the co-operation of the authors, direct knowledge and evidence of the truth or otherwise of the allegations. Further, defences are fact intensive and expensive to prove. This renders the intermediary defences all the more attractive.

[8]The intellectual property cases have the underpinning of art. 8(3) of the Information Society Directive 2001/29/EC and the implementing §97A of the Copyright Designs and Patents Act 1988, and art. 11 of the Enforcement Directive 2004/48/EC.

[9]The failure to address the question more directly is notable as the Advocate General characterized Google as having wrongly anchored the immunities to neutrality—and disagreed that this was the correct test and contrary to the Directive's focus on the activity—not the nature of the entity, noting that in practical terms, current business models often spanned a number of the relevant activities in an industry in the process of constant change.

where editorial and user generated content were combined. See also *Mulvaney v Betfair* [2009] IEHC 133 where the defendant provided a betting exchange website which also contained a chat room hosting user generated content. See also *Imran Karim v Newsquest Media Group Ltd* [2009] EWHC 3205 (editorial and user generated content), cited in *Kaschke* and *McGrath* (above), (Amazon sold books but also hosted reviews).[10]

While moderating is not fatal to the Website Operators defence, it will defeat the other defences and has been applied to the other defences in a variety of cases,[11] any manual review (by human eyes) will lose an ISP the defences --the notorious "Catch-22." Classic moderating is a form of editorial control and will render an ISP a publisher. There is no sensible way around this except as taken in the Website Operators defence. Further publishers and publication have long settled meanings in libel law and we cannot see that it would be worth tinkering with these.

Although different positions have been taken within the EU, the English courts treat search engines as conduits rather than hosts, see *Metropolitan Schools v DesignTechnica* [2009] EWHC 1765 (QB) (before notice as a search engine, Google's wholly automatic functions performed by its algorithm could not render it a publisher and it had no need of any defence). Owing to the futility of suing search engines, primary publishers often find themselves facing additional claims for the foreseeable republication by the search engines, see *Budu v BBC* [2010] EWHC 616 (QB). See *Slipper v BBC* [1991] 1 QB 283 (liability of original publisher for foreseeable

[10]Following *Kaschke*, if a service consists of the storage of the particular information complained of (that is, the particular post or entry complained of), the service provider is not precluded from invoking the hosting immunity merely because he also provides some other—unprotected—services, provided that the nexus between the activities does not require them to be considered together. There is little or no guidance on the boundaries rendering the nexus too proximate.

[11] In *Kaschke* (above), a host and the operator of the site corrected and amended language in user posts, and the court rightly characterized this as the exercise of editorial control. What saved the defendant in that case was the failure to edit the particular post in issue. The fact that the defendant took posts down of his own volition, scored them and rated them was not the subject of in-depth separate analysis in *Kaschke*; however, this conduct is classic moderating and a form of editorial control. In *McGrath*, Amazon narrowly escaped liability as a primary publisher as it had a moderation policy of limited pre-publication control by an automatic filter for forbidden words or blacklisted users which if found would escalate the post for manual, human review. None of the postings complained of failed either of these tests, so they were displayed without any human intervention. As Amazon took no steps in relation to the content and no part in any decision to publish, except by way of the automatic process referred to above, it was bound to succeed under the Directive—and the claim against it was struck out. The judge noted that if there had been a manual review (human eyes) the position might have been very different, and noted the notorious "Catch-22."

republications). See also the decision of the appellate court in *Tamiz* [2013] EWCA 68 (distinguishing Google's passive role as a search engine from its role as a host. The court noted that after a takedown notice, Google as a host could be a secondary publisher). However, while this may be the case prior to notice, *after notice* even search engines must be liable based on the Blocking Order cases.

This is not as absolute as it may seem. Where there is control and financial benefit, art. 10 jurisprudence will uphold liability even *prior to notice* for hosts per *Delfi v Estonia*(No.64569/09 ECHR 2015) and *MTE and Index .hu v Hungary* No. 22947/13 (the provision of notice and takedown procedures can itself satisfy the balancing and proportionality required for the fundamental rights analysis). Note that in *Delfi,* there was effectively a finding of constructive knowledge as the hits on the site went crazy and the ad revenue with it.

Where there is a notice both ways so that the intermediary cannot tell who is right and whether there is any unlawfulness, it does not have to take any action. See *Davison v Habeeb* [2011] EWHC 3031 Parks QC (blogger.com was like a giant notice board and Google could not be familiar with postings until notified, rejected the Law Commission's gloss that unlawful meant "prima facie unlawful" and found that while Google had received a takedown notice alleging defamation, where it faced conflicting claims it was in no position to adjudicate it could not know whether there was a defence to defamation or not. Unless it knew there was a libel, it was not on notice of unlawful activity according to the Directive).[12]

(ii) Should there be liability?

Notice and Takedown works very well indeed in most cases –subject to those out of the jurisdiction as noted above. It is a decent self -help remedy. Another particularly British model is the Website Operators defence in §5 of the Defamation Act 2013. This evolved from the practice

[12]This was followed at first instance in *Tamiz* [2012] EWHC 449 on the e-commerce defence (Eady J. found that a bare notification that statements were defamatory would not make it apparent that they were unlawful, where no details of falsity were provided or substantiation of bare assertions, and it had no ability to consider the availability of defences to defamation, citing *L'Oreal v eBay* for the finding that art.14. of the Directive was not to be rendered redundant in every situation where notice or facts reveal an issue, given they may turn out to be unsubstantiated and imprecise). The issue was not subject to the appeal. See also *McGrath v Dawkins* [2012] EWHC 83 (a hosting case where the claimant failed to address the merits of any defences and make it apparent that the statements were unlawful under the Directive, Amazon was not on notice of libels where its processes were automated, where takedown notices were defective as to the defences and otherwise).

of certain operators when dealing with anonymous posts. It is a facilitation model, the operator gains the defence if he forwards the complaint to the poster/author (who has to decide whether to default, consent (to takedown) or disclose (his identity to the complainant or just to the operator pending a court order for identity disclosure—and with it some court scrutiny on serious harm and real and substantial tort). The final version passed was not as good as the original proposal which was broadly as follows.

(a) For attributed statements

(i) ISPs should be obliged to publish complaints (beside the statement complained of)[13] and leave both up in order to benefit from the intermediary immunities/safe harbours and defences.

(ii) A complainant seeking removal had to apply to a court for a Takedown order –by means of *an expedited and inexpensive paper based procedure* (emphasis added).

(b) For unattributed statements

(i) Statements to be takedown on receipt of complaint unless the poster/author identifies himself, in which case the statement is treated as in (a) (i) above.

(ii) The ISP could of its own volition apply for a Leave-Up or Stay-Up order on public interest grounds.

See the earlier versions of the draft regulations and the *travaux preparatoires*.[14] Art. 10 is better served in the draft model than the final. On the other hand, we know from the US copyright model, the Digital Millennia Copyright Act (DMCA) that no-one ever avails themselves of PUT BACK (which has to be done under pain of perjury) and the material is just posted elsewhere if there are strong feelings. Arguably we have a similar rule –one is always free to re-phrase and re-post and that works too and serves freedom of expression. In practice, there is nothing a complainant can do to force a Website Operator to use the defence. So it is entirely at his

[13]Known in libel law as Louchansky notices, see *Loutchansky* [2002] EWHC 2490

[14]See http://www.parliament.uk/business/committees/committees-a-z/joint select/draft-defamation-bill/news/publication-report/

discretion and many are not using it. This follows the general rule –it is a defendant's decision which defence to elect.

While we note that the UN, OSCE, OAS, and ACHPR in a Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda, as well as the Manila Principles on Intermediary Liability emphasise that 'Intermediaries should never be liable for any third party content.' With respect, we think that the current position whereby the intermediary has a choice to continue to participate in the acts complained of after being put on notice is a pragmatic and sensible one that works well for parties who are professionally represented and dealing with platforms and intermediaries within the jurisdiction.

On fake news and offence etc, it is also important to remember that art. 10 protects the right to offend, see *Handyside v the United Kingdom* App No 5493/72.[15] The ECHR has affirmed that art.10 of the Convention also protects/does not prohibit discussion or dissemination of information even if it is strongly suspected that this information might not be truthful, see *Salov v Ukraine* App no 65518/01 (ECtHR, judgement of 06 September 2005), para 113. We must be careful not to create an environment where only approved or widely held views can be online. UN Guiding Principles on Business and Human Rights state that enterprises 'should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.'[16]Note that *Magyar Tartalomszolgáltatók Egyesülete and Index.Hu Zrt v Hungary* (above) sets out the extent to which intermediary service providers can be liable for content related to their services. The ECHR found that a 'notice-and-take-down-system could function in many cases as an appropriate tool for balancing the rights and interests of all those involved. We agree –subject to our comments above about effective remedy thereafter, but more thought needs to be given to speech related removal requests and the safeguards for art. 10 and chilling concerns.

3. How effective, fair and transparent are online platforms in moderating content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

[15] (ECHR, judgement of 7 December 1976), para 49. (the right to freedom of expression protects 'not only "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population').

[16]UN Guiding Principles on Business and Human Rights, principle 11.

a. *What processes do online platforms use to moderate content that they host? Are these processes fair, accountable and transparent?*

There are still issues with moderating and ecommerce defences. Moderating does not prejudice the Website operators defence under §5 of the 2013 Defamation Act (although it is a qualified privilege and subject to malice) but the other defences would all be lost. Moderating is uncomfortable unless it is complete removal. It is editing and the paradigm activity of a publisher as noted above. Particularly with some of the US platforms, all that they will do is request you follow their moderation procedures and then decline the request for takedown. Your choices then are to turn to Google here or get a Norwich (disclosure) order here with leave to serve out of the jurisdiction (but which may be ignored in the US), you can seek the assistance of the US court, but may run into the state and federal libel shields as well as first amendment issues. See 1. above. The moderation processes are not remotely transparent. It seems in many cases that US law is applied even to content published in the UK by and about UK residents and targeting the UK and earning revenue in the UK. There is no appeal or review function and even legal letters are ignored. See 1 above.

b. *What processes are employed by law enforcement agencies and other bodies such as the Internet Watch Foundation in overseeing the regulation of online content? Are these processes fair, accountable and transparent?*

No – these processes are most certainly not fair, accountable and transparent in the UK and there has long been a serious art.10 ECHR problem. These parties (IWF and Nominet and Law Enforcement Authorities) arbitrarily restrict speech and act without any regard for basic due process.

They also fail to comply with the rules for interference with the right to freedom of expression based on the three-part test, which provides that a limitation on freedom of expression must: (a) Be provided for by law (legality); (b) Meet a legitimate aim (legitimacy); and (c) Be necessary (necessity). Limitations should always be exceptional and only be implemented if they are compliant with all the criteria. The Human Rights Committee guidance is that "the relation between right and restriction… must not be reversed."[17] It has explained that 'when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself.' The starting point is that the individual is entitled to the full exercise of the right. It is then up to the state to establish – based on the criteria described above – the permissibility of a

[17]Human Rights Committee 'General Comment No. 34, Article 19: Freedoms of Opinion and Expression' (12 September 2011) CCPR/C/GC/34, para 21.

limitation on such exercise. The legitimate aims pursued should also be interpreted *stricto sensu*. The 10(2) enumerated legitimate aims are: respect of rights or reputations of others, and protection of national security, public order, public health or morals. The rights and reputations of others', generally refers to 'human rights as recognised generally in international human rights law.' Neccessity implies the existence of a 'pressing social need, see the *Sunday Times* (above) and as proportionality, the Human Rights Committee has opined that '(r)estrictions must not be overbroad.'[18] Finally, the Human Rights Committee in *Fedotova v The Russian Federation* adopted the view that a limitation ground cannot be invoked for a discriminatory purpose or applied in a discriminatory manner[19] and this prohibits discrimination on the grounds of inter alia political or other opinion.[20] The ECHR often closely considers the context of the expression in issue, but the decisive factor can also be the nature of the penalties. The ECHR confirmed in *Handyside* (above) in relation to limitations to the right to freedom of expression, it 'leaves to the Contracting States a margin of appreciation' due to their 'direct and continuous contact with the vital forces of their countries.' Nevertheless, this margin is not unlimited. The ECHR 'is empowered to give the final ruling on whether a "restriction" or "penalty" is reconcilable with freedom of expression as protected by art. 10. The domestic margin of appreciation thus goes hand in hand with a European supervision.'[21] However, the extent of the restriction and form of expression and will bring more scrutiny to prior restraints which require safeguards and the court will also consider whether there was an alternative means of expression. More restrictive measures are permitted for broadcast due to the power of that media, and it has found that the internet can have a greater risk for art.8 privacy and data rights than the print press and so

[18]Human Rights Committee General Comment No 34, para 34.

[19]*Fedotova v the Russian Federation Comm* No 1932/2010 (Human Rights Committee, views of 31 October 2012) CCPR/C/106/D/1932/2010.

[20]This position is also articulated in the Committee's General Comment No. 34, which states that laws restricting the freedom of expression must not violate the non-discrimination provisions of the Covenant. Article 26 of the ICCPR.

[21]In the European context, there is usually an *inverse* relationship between the extent of the consensus among states on the substance and scope of a limitation ground and the extent of the margin of appreciation afforded to states; the greater the consensus among states, the narrower the margin of appreciation afforded to them, see See Magnus Killander, 'Interpreting Regional Human Rights Treaties' (2010) 7 (13) SUR International Journal of Human Rights 145, 151. Additionally, when applying the margin of appreciation doctrine, courts may consider the seriousness of the right infringed, whether there is a moral controversy at stake and whether broad and deep consideration has been given to the matter by national courts, see Dominic Mcgoldrick, 'A Defence of the Margin of Appreciation and an Argument for Its Application by the Human Rights Committee' (2016) 65 International and Comparative Law Quarterly 21.

different measures may be appropriate. The court has found there is no clear consensus in Europe on the form of permissible restrictions on the internet due to the rapidly changing environment, see *Yildirim v Turkey* App. 3111/10 (a restriction less than a ban was a violation given the importance of the internet as a tool for political expression).

More precisely, the actions of IWF and Nominet still lack a proper legal basis. That is, there is a failure of legality. Art.6 also protects from retrospective legislation and the law must be prescribed and knowable (in advance) so that citizens can regulate their conduct accordingly. An interference may count as 'prescribed by law' whether its source lies in statute or the common law but the law must be accessible and foreseeable. According to the ECHR in *The Sunday Times v the United Kingdom* App no 6538/74 (ECtHR, judgement of 26 April 1979).[22]More importantly, there is a lack of due process when the police are involved and so art.6 ECHR issues also arise. This is despite the fact that businesses can be shuttered and goodwill entirely destroyed in what may be a "taking" by the state. A notice and a hearing (before or after) must be provided at least. This is not happening largely as they police often treat the site/business as evidence or instruments of crime and seize them arbitrarily and without any process.

The public record shows and it is beyond question that Nominet is a public authority for the purposes of the Human Rights Act 1998 (HRA) and this status is reflected in the Digital Economy Act 2010 and it must act in compliance with the ECHR and the TFEU. Nominet holds .uk in trust for the nation as the delegee for the UK government. Nominet is therefore obliged to act for the public benefit and in the public interest. [23]

The legally acquired goodwill and reputation associated with the domain name cannot therefore just become illegally acquired retrospectively –just at the whim or discretion of Nominet or even law enforcement. We have the rule of law to protect us from this type of arbitrary conduct.

---

[22]At 49 "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail".

[23] This is the UK government's own view. See correspondence between BERR and Nominet Chairman at http://www.nic.uk/governance/review/. See also Digital Britain p. 193 & 194.

Both generally and given the lack of any judicial finding of any criminal or civil wrong and the lack of any due process or hearing and given the over-broad application to lawful goodwill and businesses and reputations, and also the chilling impact on Freedom of Expression -the domain name seizure and suspension is often in fact, unlawful and disproportionate. We have found in practice that the NCA/police and Nominet were not open to any review of their domain name seizures even where the issue was a technical one about the day a site ceased legal online sales and there was no actus or mens rea and no follow up arrest or charge. No process was offered and the only way to get relief would have been to sue.

Further, we have concerns about legitimacy and the balancing of the various rights required when carried out by these actors. Are the IWF, NCA and Nominet adequately applying the fundamental rights analysis and balancing the art. 8 rights of reputation and art. 10 rights to Freedom of Expression and property and business rights under arts. 16 and 17(2) of the ECHR and the Charter of Fundamental Rights (CFEU) and art.1 of the First Protocol -all of which may be engaged by these actors. The art.10 rights of customers and the public must also be considered. This balancing act is difficult even for the courts, which when it is aware from the evidence that the convention rights of persons other than the parties are engaged, then it is obliged, to take them into account. See also art. 3(2) of the Enforcement Directive and as to proportionality, *Twentieth Century Fox Film Corp v British Telecommunications plc* (No 2) [2011] EWHC 2714 (Ch), where the dangers of over-broad relief or blocking were warned against.

c. *What processes should be implemented for individuals who wish to reverse decisions to filter or block content? Who should be responsible for overseeing this?*

See above. Notice and a hearing (before or immediately after the blocking or seizure) must be provided at least.

4. What role should users play in establishing and maintaining online community standards for content and behaviour?

We don't address this question in any detail. While they currently have an important role in flagging issues for attention, there would be serious issues with art.10 if users/the community could restrict or restrain the speech of others. There is an issue with private actors determining fundamental rights where there is no effective remedy from the same. We already noted there is a right to offend protected by art.10. See above and below.

5. What measures should online platforms adopt to ensure online safety and the protection of community values or standards, while also protecting the rights of freedom of expression and freedom of information?

This is a problematic question. Art. 10 ECHR does not just protect commonly held values but also protects and enshrines the right to offend. See above. Community values today may be so liberal as to add nothing in any event. Soft law is problematic as a restriction on speech, see above. All the more so in the hands of private actors. The existing law really should be sufficient. We have hard law restrictions on offence, revenge porn, private information, libel, harassment and intellectual property, racial and religious hatred and discrimination.

The European Commission's Code of Conduct on Countering Illegal Hate Speech Online requires States to 'review the majority of valid notifications for removal of illegal hate speech in less than 24 hours.'[24] We note also the positive obligations that states have to prohibit incitement to hatred under the European Union's Audiovisual Media Services Directive (AVMSD art.6) states: 'Member States shall ensure by appropriate means that audiovisual media services provided by media service providers under their jurisdiction do not contain any incitement to hatred based on race, sex, religion or nationality.'

In the UK there is the Public Order Act (Incitement to Racial Hatred), the Race Relations Act and the Racial and Religious Hatred Act –and we believe the law is currently adequate and there is no need for additional legislation. We also note that international norms suggest that for speech to qualify as hate speech, the individual concerned should intend to incite violence or unlawful action, and those actions should be imminent. See *Brandenburg v Ohio,* [cite] (and its 'imminent lawless action' test) and *Gündüz v Turkey* App No 35071/97 (ECtHR, judgement of 04 December 2003) and *Rabbae v The Netherlands* Comm No 2124/2011 (Human Rights Committee, decision of 14 July 2016) CCPR/C/117/D/2124/2011 and developments in the African[25] and Inter-American systems[26] to establish a high threshold for limitations to freedom of expression, including to prevent hate speech. We note that the UK has laws dealing with revenge

[24]European Commission 'Code of Conduct on Illegal Online Hate Speech' (31 May 2016).

[25]See African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression in Africa', Art XIII (2), which provides: 'Freedom of expression should not be restricted on public order or national security grounds unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the expression.'

[26]See Inter-American Principles on Freedom of Expression, Principle 11.

porn, privacy and data, harassment, obscene publications and malicious publications. There is no need for any new legislation –in our view.

We need to consider however, the kind of environment for speech we will enjoy when enforcement is all by the private discretion of private actors. We need to think about how protections for speech offline can be fully mapped online.

Traditionally English law has been very cautious about prior restraints on speech as they may force the courts into a censor. For this reason, the rule was publish and be dammed (in damages) as it is always in theory possible to make a statement in a non-defamatory way and therefore going to the court for restraints before the language was final, was to put it in a position of censor .See *Bonnard v Perryman* (1891) 2 Ch 269 affirmed in *Green v Associated* [2004] EWCA Civ 1462 and *Mosley v UK* (ECHR considered a publisher's obligation of pre-notification of a potentially defamatory article and held that 'although punitive fines or criminal sanctions could be effective in encouraging compliance with any pre-notification requirement…these would run the risk of being incompatible with the requirements of article 10 of the Convention.' It found that such punitive fines would create a chilling effect which would be felt in the spheres of political reporting and investigative journalism, both of which attract a high level of protection under the Convention.'[27] The rule against prior restraint is not squarely applicable online –where publication is continuing, the restraint will be during and or after, restraint. However the same concerns remain –and are amplified by the fact that the restraining party will be a private actor— and one that is incentivised to remove material to obtain defences and immunities for itself.

Again, safety is something else. Criminal law applies online so this should be sufficient. If this is a question about how to protect the vulnerable or children –then it should be put as such. There are others who know about children and the internet and can address this.

We note that art. 15 of the E-Commerce Directive, which states that Internet intermediaries may not be placed under a "general duty to monitor" has never been properly transposed into UK domestic law. Government has taken the position that this was not necessary, on the grounds that

[27] See also cite *Pihl v Sweden*[27] in this regard, where the ECHR found that an intermediary service provider's liability for third-party comments may have negative consequences on the comment-related environment of an Internet portal and thus a chilling effect on freedom of expression via Internet.' Similarly, *Muwema v Facebook Ireland Ltd* (High Court of Ireland, judgment of 23 August 2016) [2016] IEHC 519 (considered the liability of intermediary service providers for material published by users but decided the case based on the futility of prior restraint orders, as the information pertaining to the plaintiff was already in the public domain).

no UK law does place intermediaries under such a monitoring obligation. The lack of such transposition leaves UK operators exposed to the risk that law may be interpreted to allow the imposition of such a duty. This is particularly severe in relation to laws that grant courts a broad discretion to impose poorly identified duties on third parties, such as §94A of the Copyright, Design and Patents Act 1989. While the UK was a member of the EU, our ISPs had the comfort that even though art. 15 had not been transposed, UK courts were still under a duty to act in compliance with EU law. When the UK leaves the EU, this comfort is diluted (or removed, depending on transition provisions). The protection from a duty to monitor is part of the core acquis underlying Internet regulation in the UK and EU. We recommend that the government proceed to transpose it with prospective effect, as part of the preparations for leaving the EU.

6. & 7. Transparency

a. What information should online platforms provide to users about the use of their personal data? How should it be presented?

GDPR deals with this comprehensively.

b. Does the GDPR, in your view, provide sufficient protection for individuals in terms of transparency in the collection and use of personal data or do we need further regulation?

Yes --in theory. We will need to wait and see in practice. In fact, in our view, despite all the focus on social media, it is the offline players who are the worst. The banks and financial institutions are also sharing data in ways that deserve very close scrutiny.

c. In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

This is a very interesting topic. It is also applicable to government and has come up under the FOIA. Most parties using algorithms, including government and police and probation and others do not fully understand yet what and how they are making use of them. There are issues about fairness and bias and a myriad of issues here. No-one has got to grips with it. The GDPR makes some attempt. It is far too early to regulate in my view.

8. Competition

a. Is competition law effective in regulating the activities of these platforms?

It is too soon to intervene in these new markets in our view.

b. What risks are there for the UK post-Brexit in this regard given that most competition regulation in this field is currently carried out at the EU level?

This will be impactful if we do not adopt reciprocal EU law and standards. We may descend into a free-for all, without adequate protections. We find in particular, that EU Intellectual Property law and the ECJ decisions, always have competition concerns at their heart. This is not a local law focus and it will be a loss. English law often overly values the rights of vested interests and incumbents and property rights and we will need to be very aware of this. It's also relevant now to considerations about regulating at such an early stage. See below, but the ECJ has struck a very sensible balance in matters such as keyword use and trade mark infringement, see *Google v Louis Vuitton* (above) and *L'Oreal v eBay* (above) (keywords are not per se infringing unless the ad fails to make identity clear, as consumers usually can understand they are being offered *an alternative* to the searched for item). Similarly, in relation to linking and embedding and copyright infringement, we got a series of very sensible decisions to the effect that if the material was up online already, to link was not infringing unless there was a new public, see *Svensson* C-466/12, *Bestwater* C-348/13 and refining the rule for business users, *GS Media* C-150/16 (not infringing even if the original linked to was uploaded without right, unless a for profit use-when the rights should be investigated). Given the importance and ubiquity of linking to the web—this was all very sensible as the man in the street could not fathom that linking could be infringing. We see very sophisticated and holistic decisions—and would probably not get these domestically.

9. International

a. What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

This will be impactful if we do not adopt reciprocal standards and protections as we have from EU law. We may descend to an environment without adequate protection for the individual. US law and institutions can be focused on corporate and business interests and individuals are often not adequately protected—this is clear from their data protection failings and we see it in ICANN also. See below. The EU has been fairly proactive when it comes to enabling and facilitating the heathy development of online markets and in our view, has struck a good balance. With the Copyright Directive, the Ecommerce Directive, other harmonisation it has looked ahead and cleared the way for a truly single market. In specialist areas such as music licensing, it has been very pro-active and pro-competition. At the same time, with issues like net neutrality, it has looked for a sensible path also. In our view, this consumer-focused law and policy is one reason for the push to leave the EU, as it often does not suit vested business interests.

b. What should be the function of international organisations in the regulation of the internet? If so, what should be the role of the United Kingdom in these international organisations?

There is a need for international co-ordination and a rule-making fora. ICANN is totally unsuitable for this purpose in our view. It has no mandate for speech, moreover, it's approach is often driven by GAC (national per country government) representatives and would see a race to the bottom for speech. Its process is slow and subject to capture by vested business interests. It is not an acceptable model due to its flawed structure which privileges intellectual property owners and in our opinion, grants double voting privileges to business interests (through the IP constituency, Business constituency and Registrars constituency). We should disclose that we have in the past participated in the IP constituency and Non-commercial users constituency and in many ICANN working groups.

Yours faithfully,
Victoria McEvedy
McEvedys