# Written Submission to House of Lords Communications Committee following oral evidence session with Myles Jackman and Javier Ruiz

**Alex Haydock, Javier Ruiz, Myles Jackman**

*"Democracy does not simply mean that the views of the majority must always prevail. A balance must be achieved which ensures the fair and proper treatment of minorities and avoids any abuse of a dominant position"*

European Court of Human Rights Young, James, and Webster v United Kingdom (1982), at para. 63

## Summary

Our primary point is that users have a right to publish and need the ability to take legal responsibility for their work when it is identified for removal; and that systems of issuing notice to platform and user and counter-notice to the platform and complainant ("notice and counter-notice") provide a basic framework to achieve this. However, with the exception of libel law, these systems do not exist in the UK and EU. Additionally, the current framework already makes platforms liable for content when they are notified; this leaves users in a vulnerable position where they cannot defend their publications on platforms.

We also detail ad-hoc regulation by Police, Nominet and UK law enforcement agencies to remove content and domain names which lack accountability and oversight. A further 'quick win' would be for bodies that deal with Internet regulation, including the BBFC, IWF, National Crime Agency, and National Trading Standards to be brought within the scope of Freedom of Information legislation, and for Nominet to introduce an independent appeals process for domain suspensions.

# 1a. Is there a need to introduce a new regulatory framework for the Internet?

Arguably, the current regulatory systems that constrain the internet already function reasonably well.

Data protection, e-Privacy, electronic commerce and defamation laws serve different and extremely important purposes. Laws of course evolve and more protection for privacy is particularly needed, as are protections for the right of users to publish lawful content. In practice, there is not enough scope within current legal frameworks to protect users' right to publish on platforms and few systems of notice and counter-notice exist to allow users to take legal responsibility when their content is challenged.

Internet regulation is a complex web of various stakeholders and laws which interact with each other through a multi-stakeholder governance model. As the Internet is not a single entity and is comprised of tens of thousands of private actors, it would be difficult to establish a single new framework for regulation.

Laws must be targeted in scope towards a particular problem or set of problems, as the necessary complexity of legislation will depend on what is being regulated. The wider the scope of a particular piece of regulation, the simpler and less specific it is going to be. For example, the Electronic Commerce Directive (ECD) protects platforms and intermediaries against incurring liability for the actions or users. It is a critically important piece of law but is very simply drafted. Similarly, data protection laws are very important but are drafted very widely as they are unable to address the narrow and particular privacy risks seen by specific industry sectors.

Current debate in this area appears to be focused on the role of large platforms like Facebook and Google, evaluating what kind of role they can play in policing online content. This effectively involves eroding their liability protections by creating a looming threat of more formal regulation if they do not take action to remove unwanted content.

From a user's perspective, ensuring that online platforms are protected from liability is critically important. A user's right to publish and to defend their legal right to publication is critical to the open web. When the law does not properly recognise the right of users to defend this right to publication, we experience arbitrary censorship.

Often the Internet and platforms are identified as a politically acceptable arena in which to intervene, without regard to the effectiveness of that intervention. Policy makers at all times can focus on platforms; persons creating a problem; or other social factors that generate the behaviour. Of the three, platforms may be the easiest to push into taking action, but this is likely to be less effective in real

terms than dealing with the people or criminals directly, or taking action to deal with root causes. Instead, platforms are treated as a root cause, even though this is rarely the case.

## Necessity

The question above, which regards the perceived need to regulate the Internet, explicitly references the test of necessity. Necessity is the legal principle that any new law should be capable of being justified from an objective perspective.

This is defined within the context of personal data protection by the European Data Protection Supervisor (EDPS) as follows. Although this definition comes from data protection law, it also applies more generally:

*"Necessity is a fundamental principle when assessing the restriction of fundamental rights, such as the right to the protection of personal data. According to case-law, because of the role the processing of personal data entails for a series of fundamental rights, the limiting of the fundamental right to the protection of personal data must be strictly necessary.

Necessity shall be justified on the basis of objective evidence and is the first step before assessing the proportionality of the limitation. Necessity is also fundamental when assessing the lawfulness of the processing of personal data. The processing operations, the categories of data processed and the duration the data are kept shall be necessary for the purpose of the processing." *

The legislature must be satisfied that any proposed Internet regulation is necessary before moving on to consider the test of proportionality.

In questioning whether a piece of legislation may meet the test of necessity, the Government should consider whether the regulation of a particular platform or of the Internet is necessary to achieve the goals of the legislation. We are aware that this Committee heard recently of the issues surrounding the FOSTA and SESTA legislation in the United States. FOSTA and SESTA sought to address some of the real-world problems presented by sex trafficking through the regulation of online platforms. The regulation of the platforms does not solve these problems, and can only serve to make them worse.

Instead of seeking the 'easy solution' of placing sanctions on online platforms, lawmakers should attempt to tackle issues head-on. Addressing the problems Congress had identified with sex trafficking should have taken part as part of a broader policy discussion focusing on those issues, rather than deferring such problems to online platforms to solve, by making them liable for anything that could constitute "facilitation" of sex trafficking.

Following FOSTA and SESTA, sex workers as a whole are now unable to advertise for clients online using platforms which had been established for many

years and had community reputations. With the loss of these avenues for advertising, sex workers are being forced to soliciting clients on the street, which is far more unsafe, and leaves Congress with less of an ability to control the situation. A study published in November 2017 by the universities of Baylor and West Virginia highlighted that in cities where Craigslist had opened online boards for advertising erotic services, the rate of homicide against women in general fell by 17 percent.

In the US case, this problem will affect many sex workers in the UK and elsewhere, as they will be unable to use US-based platforms. Nevertheless, over 76,000 Twitter users, for instance, recently signed up to an Australian Twitter-style service called Switter, which aims to cater to sex workers and clients. This illustrates the difficulty of simplistic bans. In any case, while the aim of FOSTA and SESTA was to tackle sex trafficking, the impacts have been on sex workers as a whole. It would be hard to imagine a ban on migratory farm workers using Internet platforms as the result of concerns about forced labour and modern slavery, yet this has been a politically acceptable approach in this case.

## Proportionality

Proportionality is also defined within the context of personal data protection by the European Data Protection Supervisor (EDPS) as follows:

*“Proportionality is a general principle of EU law. It restricts authorities in the exercise of their powers by requiring them to strike a balance between the means used and the intended aim. In the context of fundamental rights, such as the right to the protection of personal data, proportionality is key for any limitation on these rights.”

“More specifically, proportionality requires that advantages due to limiting the right are not outweighed by the disadvantages to exercise the right. In other words, the limitation on the right must be justified. Safeguards accompanying a measure can support the justification of a measure. A pre-condition is that the measure is adequate to achieve the envisaged objective. In addition, when assessing the processing of personal data, proportionality requires that only that personal data which is adequate and relevant for the purposes of the processing is collected and processed”.*

A clear case of disproportionality can be found in the UK’s Digital Economy Act 2010, which proposed suspending access to the Internet for ISPs’ users who had received three allegations of downloading copyright infringing material. Account suspension could have disrupted education, job seeking and access to government services for whole families and seemed wholly disproportionate.

In this case, online copyright infringement was held by lobby groups to be so severe that TV, video and music industries simply could not compete against ‘free’ services. This was delayed and did not take place.

Thankfully, the plan was never put into action, and the problem has subsequently been resolved through proper supply of services such as Netflix, Amazon Prime, BBC iPlayer, Spotify, Deezer and others. The market has reduced infringement primarily through the supply of good services, as we suggested it could at the time. The calls for 'urgent' regulation of the Internet could have resulted in serious harm for individuals and, though heeded in 2010, were pushed into the long grass.

### Is it desirable?

Clearly the child protection imperative with regards to child pornography (Indecent Images of Children as defined under the Protection of Children Act 1978) is necessary and proportionate in a democratic society.

However, other technical infringements of freedom of expression must also be demonstrably necessary and proportionate; and consideration of the impact of regulation on communities who receive information, as well as the individuals who impart it, must be given.

### Is it possible?

This question raises the spectre of practical workability.

For example, the current age verification régime, as dictated by the Digital Economy Act 2017, has been acknowledged as unworkable in practice; in the sense that it is easy to obviate using tools such as Tor, Virtual Private Networks (VPNs), or proxies.

Given the current rate of technological development, it seems likely that advances which allow tech-literate users to simply "get round" regulation will continue apace.

## 1b. In your view, should we encourage self-regulation or employ more directive means such as co-regulation or direct (command and control) regulation?

We have concerns that self-regulation in practice often consists of Government forcing the hands of platforms by making platforms feel that they have to take steps to regulate of their own volition, otherwise they will face legislative regulation for which there may be sanctions or penalties for failure.

This leads to a culture of “privatised enforcement”, where the will of Government is carried out by private actors under a self-regulatory framework. The lack of a threat of penalties or sanctions for failure means that there is a lack of incentive for platforms to invest the necessary resources into getting things right.

Fundamentally, this is about how we deal with crime and victims. Encouraging an entirely self-regulatory regime risks the danger that we give up on the direct enforcement of criminal activity and merely try to disrupt the criminal activity online rather than pursuing criminals. This is due to the fact that platforms can only disrupt and have no law enforcement powers. Facebook and Google do not operate courts or prisons. Direct enforcement action against criminal activity should not be something that is lost track of when considering alternative forms of regulation.

In many situations - particularly some fraud, bullying, and harassment cases - relying on disruption tactics to remove offending posts and content from platforms results in criminals being left to go free where it is possible for them to be prosecuted. Determined criminals and serial bullies or harrasors are free to continue what they are doing.

Of course, it must be recognised that the Internet is a global network, and it is not always possible to take action beyond disruption if perpetrators are located outside of the UK. However, if offenders are based in the UK or other legally-cooperative countries then this should not be the case.

In response to this question, we can also consider the failures of self-regulation when it comes to privacy. One example is mandatory cookie warnings and online advertising; a complete failure of industry self regulation. Most cookies don’t need a banner and when they do there is not enough info.

# 2. Should online platforms be liable legally for the content that they host? In your view, are online platforms publishers or mere conduits?

## Online platforms and liability for the content they host

The general legal position is that online platforms are currently liable for hosting unlawful content if they do so knowingly, though defences are available if the platform does not know they are hosting the content.

In current EU law, liability defences are not attached to an entity, but to specific content and actions. An online newspaper running uncurated comments below articles will generally receive protection from potential liability arising from what their users write. Similarly, an online platform which generates its own content will not be afforded the same liability protection.

The main liability protections for online platforms currently come from the Electronic Commerce Directive, implemented domestically as The Electronic Commerce (EC Directive) Regulations 2002. As “hosting” providers, platforms are currently offered protection from liability under Article 14 ECD. Platforms are neutral providers that host the content of third parties and users, but do not generate the content themselves or undertake editorial decisions.

An exception for persons acting as a “mere conduit” - as this question refers to - can be found in Article 12 ECD, although it should be noted that this refers primarily to Internet service providers and other intermediaries who do not store the content they are transmitting and is thus not the correct term to use when discussing online platforms.

## Libel

More specifically, when dealing with libelous content, additional protections are available for platforms in England and Wales under the Defamation Act 2013. Under the Act, it is a defence for a platform operator to show that they were not the person who posted the defamatory statement on the website. Liability for defamatory comments rests with the originator of the comment.

The Defamation Act outlines a system of notice and counter-notice, which allows an original poster of a potentially defamatory statement to defend their right to publish. This applies where the original poster consents to their personal details being passed back to the complainant.

This should serve as a model for the other areas of law we have identified in this document as lacking any similar mechanism.

## Patent law

The main law surrounding patents in the UK can be found in the Patents Act 1977.

Once again, the general liability exemption that might apply here, for ISPs and platforms, are the Electronic Commerce Directive exemptions for “caching”, “hosting” and “mere conduit”. It is worth noting that the “hosting” exemption only applies where a provider does not have “actual knowledge” that they are hosting unlawful content. Once a notice is received, the hosting platform is liable for the content.

UK law also provides a statutory right of redress against unjustified or groundless threats to sue for patent or trade mark infringement. According to the Law Commission, “If a threat to sue for infringement is made where there has been no infringement, or the right is invalid, it is said to be groundless or unjustified. Any person aggrieved, that is whose commercial interests suffer because of the threat, may apply to court for a remedy. These are an injunction to stop the

threats, a declaration that there has been no infringement and/or damages for loss caused by the threats."

The default position of the law in favouring online platforms presents difficulties for UK businesses who sell goods through the eBay platform who have their listing removed through notice by third parties in response to allegations of patent infringement.

We have seen this clearly with our campaign against printer manufacturer Epson's tactics in persuading eBay to remove store listings for third-party ink cartridges which fit Epson printers. As a trusted member of eBay's Verified Rights Owner (VeRO) programme, Epson was taken at their word over a highly technical patent claim while the accused were denied a proper chance to defend themselves. eBay are in a difficult position, as they cannot realistically assess a patent claim, nor can they pass the legal responsibility to the person making the listing.

Here, a system of **notice and counter-notice** would allow eBay's customers to assume legal responsibility. Ebay would notify the customer of a complaint; the customer would file a counter-notice in which they would assume legal responsibility for the listing. The customers' details would be passed to Epson, so that Epson and the cartridge reseller could resolve the issue between themselves, if necessary in a court.

Without a legal framework, this is not an option.

## Trade mark law

A trade mark is a graphical sign used to distinguish one party's goods or services from those sold by others. To protect their brand or image, the owner of a trade mark is granted the power to seek legal remedies if another party makes use of that mark in the course of trade.

A person can protect their trade mark by registering it with the UK Intellectual Property Office (UKIPO), which makes legal remedies for infringement available under the Trade Marks Act 1994. If a trade mark is not registered, then some protections may still be available under the common law of 'passing off'.

Where a person's trade mark is infringed via an online platform - for instance, by a user of an online marketplace site offering counterfeit goods for sale - the trade mark owner may generally only take action against the party who is posting the content and not the platform itself. The operator of a service will generally be entitled to rely on the 'hosting' exemption of the Electronic Commerce Directive to indemnify themselves from liability.

As per the wording of the Electronic Commerce Directive, the service's liability exemption for 'hosting' ceases to apply if they are presented with "actual knowledge" of trade mark infringement happening on their platform. When presented with this knowledge, a provider would have to take action to remove the infringing content.

A service operator also cannot rely on the 'hosting' exemption if their service does deal with the trade mark infringing content in a neutral manner. If the operator can be said to have taken active steps with the content that would give it knowledge, or control over, the data stored. This is confirmed by the cases of L'Oréal, and Google v Louis Vuitton.

The case of Cartier, also confirms that patent-holders have the right to request that a court order ISPs in the UK to block websites which are infringing their trade marks and selling counterfeit goods. A pending judgment in the case from the UK Supreme Court will confirm whether ISPs are required to bear the cost of implementing the blocking for such sites.

## Copyright

In the UK, DMCA rules have often substituted for a codified legal process of notice and counter-notice for copyright claims. For instance, Youtube videos that are produced for use in the UK may receive copyright violation notices, which can then be contested by the UK user by agreeing to the jurisdiction of US courts and allowing their personal details to be passed.

This is dissatisfactory for a number of reasons, but in particular, a UK hosting company cannot legally allow users to provide a 'counter notice'. Instead, the UK host must either remove the content, or accept legal liability for it under the terms of the e-Commerce Directive, as they may have 'actual knowledge' as the result of notification.

This is the case with eBay. Again, under the terms of their VeRO programme, a rights holder can remove anything they like from eBay if they claim it violates their copyright. The reseller at eBay cannot contest this. eBay cannot rely on a DMCA notice and counter-notice system, because it does not exist in UK or EU law.

Current proposals in EU law (Directive 2016/0280 on the "Digital Single Market") would require all platforms to implement filters which would automatically detect copyrighted material being uploaded by users, and could take appropriate action to stop the content from being uploaded publicly. Such filters are wide-ranging and inaccurate and the potential for expression to be curtailed through the over-censorship of legitimate content is massive. There are many reasons why uploaded works may incorporate segments of others, such as criticism, review, or remixing. As it is currently framed, copyright holders are currently left to be the 'deciding voice' on whether the copyright filters are adequate and fit-for-purpose.

It is also very hard to see how this proposal does not amount to 'general monitoring' of users' communications which is prohibited under Article 15 of the Electronic Commerce Directive.

### Our concerns

We have concerns that, under the current regime, the shields protecting online platforms from incurring liability are too weak. As we have seen repeatedly through our work, it is very easy for content to be reported and face removal without the user being granted the ability to take responsibility for their own content through a standard system of notice and counter-notice.

### Online platforms as publishers

The classification of platforms as publishers should be approached with caution. Publishers claim exclusive rights over their content, and act as much narrower gatekeepers. Reclassifying platforms in this way would lead to an extremely concerning chilling effect and would jeopardise the concept of an open Internet.

Even with the current imbalance, we see problems for UK businesses and free expression. Users do not have a right to defend their right to publication, except in limited circumstances. By adding liability for users content to platforms, those companies would have a direct disincentive to allow users to take legal risks at the platform or companies' expense.

Furthermore, there is no need to reclassify platforms as publishers if the desired outcome is to prevent a platform from 'hiding behind' the Article 14 hosting defence. As indicated by Article 14(1)(b) ECD, a provider who obtains, or is provided, "actual knowledge" of the fact that they are hosting unlawful content must act "expeditiously" to remove the offending content, otherwise they will be unable to rely on the exemption.

## 3a. What processes do online platforms use to moderate content that they host? Are these processes fair, accountable and transparent?

The processes used by online platforms are opaque, unaccountable and unfair. We know very little about how their systems work, and what aspects of their moderation is automated, or involves humans. What criteria are platforms using? Who decides those criteria? Who arbitrates in decisions on borderline cases? What action can be taken, and who determines the action?

There is very limited information available to assist with answering the above questions.

Online platforms are not transparent about how they moderate, and do not offer accessible systems of redress for users to challenge moderation when it occurs.

# 3b. 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?

In our research into these bodies, our preliminary conclusions are that they frequently operate with: A lack of accountability; Little to no oversight; No prior authorisation for content takedowns; Often no independent appeals, or no appeals at all; In many cases, such bodies are not subject to Freedom of Information requests, or rely heavily on the 'crime' or 'national security' defences to avoid responding to requests.

The following is non-exhaustive list of bodies with an interest in content regulation:

## Current Regulatory Framework

### Crime

**CTIRU:** produces a single statistic of takedown requests. Appears to lack any formal oversight of their takedown requests and refuses any transparency relating to their work, applying FoI exemptions to everything they do. CTIRU also make requests for domain suspensions to Nominet, again without supervision.

**National Police Chiefs' Council:**has a role co-ordinating counter-terrorism police work, including that of CTIRU. The NPCC is not subject to the FoI Act although it does respond to requests.

**Home Office**: administering CTIRU's list of websites to block across the public estate, with no oversight of the list or where or why it is applied. No oversight of any potential monitoring or information flow relating to persons making visits to sites on the list. No oversight of relationships with vendors within the programme.

**National Crime Agency**: does some takedowns, entirely exempt from FoI. Unclear what if any oversight takedown or suspension requests require.

**Internet Watch Foundation**: a private company and charity, lacking FoI obligations but acknowledging they act as a state authority when blocking child

abuse material. Unclear what their current presentation of block pages is, and whether this is any help for victims, people thinking about breaking the law or correcting errors.

**Crown Prosecution Service**: Prosecutes cases, on basis that can be unclear, despite guidelines.

**General**

**Nominet**: a private company, subject to DEA 2010 clauses that allow the government to disempower it in the event of it failing to meet public objectives. Not subject to FoI in relation to these public objectives. Transparent in general terms, but recently reduced transparency about its governance. No transparency surrounding the 16,000 domains suspended via PIPCU and others, except in numerical terms. No longer transparent in terms of governance.

**Ofcom**: subject to high levels of transparency and accountability, but as of yet no clear policy or accountability around Net Neutrality complaints and violations.

**Consumer protection**

**PIPCU**: subject to FoI, have been very co-operative in this regard. No formal oversight of their takedown work. Removing over 13,000 domains annually via Nominet. These are mostly related to trade mark violations, fake goods and fraud.

**National Fraud Intelligence Bureau**: makes domain suspension requests to Nominet. No formal oversight of these requests.

**Veterinary Medicines Directorate of DEFRA**: makes domain suspension requests to Nominet. No formal oversight of these requests.

**Metropolitan Police Fraud and Linked Crime Online (FALCON)**: makes domain suspension requests to Nominet. No formal oversight of these requests.

**Medicines and Healthcare Products Regulatory Agency (MHRA)**: makes domain suspension requests to Nominet. No formal oversight of these requests.

**National Trading Standards**: a private company not subject to FoI or external oversight, which coordinates local trading standards' work. Makes domain suspension requests to Nominet.

**Gambling Commission**: regulates gambling for the UK, and requires non-UK hosted Internet gambling to hold a license, which includes an obligation for age verification.

**Intellectual property**

**Intellectual Property Office (IPO)**: the IPO supports PIPCU's work and has a role in their governance, as well as having a role in wider IP enforcement. Unclear if e-Commerce advice and policy development for IP takedowns are their remit, or a question for another body.

**Court order blocks**: these delegate responsibility for identification of duplicate sites for blocking to various private organisations with copyright or trade mark claims, such as the BPI or MPA. No oversight of transparency of the lists of blocked URLs (other than ORG's detection tools). No transparency over their role in error correction on block pages. Confusing block pages at ISPs.

**Federation Against Copyright Theft (FACT)**: FACT have issued domain seizure requests to registrars and redirected domains to a redirect page.

**Child protection**

**ISP Soft blocking**: lacking any legal requirements for user choice, error correction or visibility of what is blocked. Probably in violation of net neutrality laws barring ISPs from interfering with Internet traffic.

**BBFC**: a private company, with statutory duties in different legislation. Acquires new duties for blocking under DEA 2017. Generally reasonably transparent, but not subject to FoI. Provides limited accountability for specific mobile operators' website blocks, and publishes reasons for decisions about specific complaints.

**UK Council for Child Internet Safety**: responsible for industry co-ordination, but often tasked with patching up problems generated by government-pushed policy, such as Internet filters. Transparent and subject to FoI, as a government initiative; but unclear in its accountability as its measures generally count as industry self-regulation.

**Internet Matters**: an industry-led initiative to educate parents in matters of child protection, but also provides advice to website operators about getting sites unblocked.

**Are these processes fair accountable and transparent?**

The processes employed by law enforcement agencies often do not focus directly on a criminal actor, but on innocent third party intermediaries, seeking to place liability on those intermediaries. They are rarely fair, accountable, or transparent.

Firstly, these processes are often shrouded in secrecy, with the excuse that revealing information about how they would would jeopardise effective law enforcement by allowing criminals to see when their content is being censored, or to learn how any blocks are implemented so they can be circumvented.

Secondly, law enforcement are increasingly turning to unofficial methods of censoring content, which are not performed under a particular statutory authority. Law enforcement appears to prefer to outsource such interferences with expression, as private entities are not curtailed by human rights laws when it comes to censoring speech on their platforms.

In our work, the notable examples we have encountered to illustrate the above points include the Counter-Terrorism Internet Referral Unit (CTIRU), and the Police Intellectual Property Crime Unit (PIPCU), and domain suspension enabled by Nominet.

CTIRU in particular cannot be said to be accountable or transparent. CTIRU's aim is to remove material promoting terrorism from the Internet. This is not done under any statutory authority and appears to consist of contacting platforms directly and requesting that they remove the content by notifying the platform in question that the content is in breach of the platform's own terms of service. ORG have submitted Freedom of Information Act requests to obtain more information about how CTIRU operates, but these requests have been persistently refused for national security reasons.

More recently, following an investigation by the ICO into one of our FoI requests, the Metropolitan Police Service stated that CTIRU do not keep internal statistics about their operations, except for their claim to have removed over 300,000 pieces of extremist content. This represents a major concern for accountability and transparency. Although CTIRU are not submitting statutory requests to remove content, they are a publicly-funded organisation whose aim is to remove content from the Internet, thus transparency and accountability should be paramount.

Furthermore, CTIRU 'requests' have the legal effect of removing liability protection at platforms by providing potential 'actual knowledge' of an offence. A decision by a platform to leave the content as published is to accept legal liability for it. This requires accountability. It should include the possibility for a user to accept legal responsibility for it, through a system of notice and counter-notice.

Additionally, it is unknown what a 'piece' of CTIRU content may mean. We suspect that one web page may involve many 'pieces' of content, and thus the 300,000 'pieces' of content may in fact be a much smaller number of web pages or web documents. For this reason we have asked CTIRU for their methodology via FoI.

PIPCU operate an "infringing websites list", which they share with advertisers in an attempt to prevent them from advertising on known "pirate" sites, so that they can starve the sites of income.

PIPCU's list is secret, and the Police claim that they do not force advertisers to withdraw their advertisements, and that any restriction on freedom of expression

is therefore not their problem. Advertisers in turn claim that the responsibility lies with the Police for compiling the list and they are just doing their duty once they are informed.

PIPCU and a number of bodies, as listed above, are involved in a programme of domain suspension in cooperation with Nominet, the registry for all sites using the .uk country code top level domain. The number of domains suspended has doubled annually since 2015, now standing at over 16,000 a year. Nominet make the actual suspensions after notification by an agency that they are associated with criminal activity.

Appeals are directed back to the agencies who requested the suspension. There is no independent appeal process, nor any external oversight. Most of the agencies have no published policy about when and why they suspend domains. Several have no formal policy, according to FoI requests we have made. Some of the agencies, such as National Trading Standards, a private company, are not subject to the Freedom of Information Act 2000, and others including the National Crime Agency, are exempt from FoI.

In other countries, such as Denmark or the USA, a legal process is required before domains are suspended or seized.

With each of these cases – CTIRU, PIPCU's Infringing Website List, and Nominet domain suspensions – the UK has established no real accountability, oversight or independent appeals processes, despite the potential impacts on free expression, the right to property and to run a business. While the number of errors may be small, they will exist, not least because of the scale of the takedowns and removals.

## 3c. What processes should be implemented for individuals who wish to reverse decisions to filter or block content? Who should be responsible for overseeing this?

Ideally, platforms would put in place processes which mean individuals are able to challenge decisions to filter or block their content.

On online platforms, existing processes of content removal generally include three parties: the platform, the user as originator of the content, and a third actor who wishes for the content to be removed. Currently, many of the existing processes are not designed to consider all three users fairly and do not give enough weight to the platform user as the originator of content.

All sides of a dispute need to have the ability to assert their rights or raise the dispute in court. It is unfair for anyone to be unable to raise their side of an issue in a court of public opinion.

In answering this question, the first thing to determine is who is asking for a decision to filter or block, and why. Different reasons require different processes. Copyright is very different to harassment, defamation, or terrorist content, for example.

Content removal from platforms is largely a contractual matter, and the difference in bargaining power between the platform and the user is massive. In practice, the only party who can interpret the contract is the platform. If somebody objects to their content being removed, the only practical recourse is to embarrass the platform into changing and restoring it.

One visible example of this was Facebook's removal of the Pulitzer Prize winning image "The Terror of War", depicting a young girl burned by napalm during the Vietnam War. Facebook removed the image initially to comply with its rules on nudity, and the image was only restored to the platform after significant media coverage was generated surrounding the removal. Recently, a "Volunteer Army" of content creators have also been forced to assist with appeals to YouTube on behalf of content uploaders who have had their content removed from the platform without access to appeal.

Similarly, in 2013, ORG worked with a Turkish digital rights group - the Alternative Informatics Association (AIA) - who were representing activists who had been operating a Facebook page, Ötekilerin Postasi, which was removed without warning. ORG and AIA worked to arrange a conference call with Facebook in Ireland to allow the page's administrators to appeal for their content to be restored.

Both the Vietnam image example and the example of the Turkish activists highlight an important issue with the moderation approach of online platforms - namely that the "ordinary citizen" is highly unlikely to be able to challenge the removal or moderation of their content unless they can generate significant media exposure, or can involve third party rights groups in the process.

An example we have seen in our work on our Blocked! project - which documents websites blocked by ISP-level adult content filters - is that sites can be accidentally blocked without necessarily containing any content that is inappropriate to minors, and site owners may be legitimate businesses and may be unaware of this fact. We built our tool to allow site owners and interested members of the public to directly appeal to the Internet service providers to request the unblocking of particular sites which did not host any adult content.

The above example of the Blocked! project perfectly highlights a problematic system in which users who may be affected by content filtering or blocking are

not provided adequate knowledge that they may be affected by a decision to block, and are not provided easy avenues of recourse to reverse such decisions.

For this reason, we would like to see independent processes to interpret the meaning or community standards particularly when those platforms are particularly important for the dissemination of information.

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

If users are to be expected to establish and maintain online community standards for content and behaviour, this should vary from platform to platform. Even within platforms, community standards will differ. Large platforms like Facebook cannot reasonably be considered to be a single community. Rather, particularly large platforms can be considered to be sets of smaller communities, each of which may have their own individual standards.

Some platforms already allow in their design for users to maintain and establish community standards. Facebook and Reddit make clear attempts to devolve moderation and ownership to people controlling pages and groups.

It must be recognised in response to this question that legal standards for content are very different to standards for behaviour. Additionally, posts which are individually lawful may become unlawful or otherwise unacceptable as part of a pattern of behaviour.

Often, we find that users are not best-place to establish community standards. Users tend to exhibit a ‘mob mentality’ and opt to remove content which is lawful, rather than focusing on ensuring that policy or fundamental rights questions such as freedom of expression are at the forefront of their consideration.

## 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?

It should be noted that criminal law applies online as well as offline. Criminal behaviour should not be tolerated. Criminals should be prosecuted. Measures of disruption are problematic because they evade the prosecution of criminals, and the rights of redress and due process.

Platforms can and do take measures to reduce the occurence of unwanted behaviour. The main issue for policy makers is that much of this behaviour is unpleasant but legal. Trolling – in the traditional sense of deliberately provoking unpleasant arguments – is hardly illegal. Bullying behaviour does eventually become harassment and intimidation, but a certain threshold has to be reached.

Modifications to platforms can and should be made to devolve moderation, report and flag abuse, and to incentivise good behaviour. However, the corollary of reach and availability is that gaming and abuse are potential factors, whether it is the familiar email spam and fraud, or groups of immature individuals attempting to provoke or bully people they do not like. While platforms must try to reduce these behaviours, not least so their products do not become poisonous and unpleasant to use, it may be hard to eliminate them entirely.

Given that platforms do have incentives for good behaviour and customer experience, it is somewhat surprising that these have become apparently very serious issues for some users. Similarly, the rights of users to participate and exercise their right of free expression should not be overlooked.

Platforms are attempting to find technical solutions through pattern recognition (machine learning, or “artificial intelligence”) to reduce unwanted behaviour. This has its place, but also contains risks of mis-identification, particularly of behaviours like anonymity, incomplete personal details, use of privacy technologies or sporadic posting, as equating with bad posting. Platforms take it upon themselves to be the sole interpreter of their contracts, except when facing publicity storms. In short, there is the potential for reasonable content and behaviour to be mis-identified.

We must also recognise that there is no right to avoid offence. Sometimes free expression depends on the ability to offend. Without the right to offend, there would have been no enlightenment, no Galileo, and no science. Technologies must avoid equating controversy with poor behaviour.

The further question is whether there are interventions governments can or should make. So far we have not heard suggestions that seem proportionate and effective, without creating serious harms to free expression.

# 6a. What information should online platforms provide to users about the use of their personal data? How should it be presented?

The GDPR is the key starting point here. There are several concrete prescriptions for information that must be presented when collecting data from individuals, what is collected and for what purposes, etc.

There are some good example of how and when to provide information. Context specific reminders are particularly effective.

There is one area where the situation is less clear. GDPR mandates companies to provide information on automated decision making and profiling in an attempt to stop the growth of a black box society, where individuals are at the mercy of opaque computer systems.

This information has been described as the right to an explanation, but its scope is unclear. In addition, modern machine learning systems defy explanations in the conventional sense. We simply cannot explain why the computer has made a decision.

## 6b. 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?

GDPR sets a baseline for data protection, but is not a solution for all sets of privacy risk. Some classes of data arguably demand stronger protection than the level provided by GDPR. In these scenarios, specific additional frameworks can be put in place to protect the data. An example of this is the PCI DSS standard, which is an information security standard which defines additional measures that need to be taken to secure payment card information.

At this point, we would also highlight the importance of addressing the lack of consideration of privacy in the proposed system of age verification for pornographic websites, as found in the Digital Economy Act 2017. Age verification requires all visitors to pornographic sites to take steps to actively prove they are above the age of 18. It is arguable that age verification data, which is capable of linking users' ID documents to the pornographic content which they visit, requires an even greater standard of protection than even payment data. There is currently no standard beyond data protection law for the protection of this data. We would strongly encourage the creation of a separate PCI DSS-style standard for the protection of age verification data.

## 7a. Is competition law effective in regulating the activities of these platforms?

Caution should be exercised when trying to use competition law to regulate the activities of online platforms. Platforms do not fit into the remit of competition law easily, as they are not abusing monopoly power in financial terms. There is no 'social media monopoly' that can be identified using competition law.

Additionally, actions under competition law are likely to need to be brought within the jurisdiction of the United States, as this is where the majority of large online platforms are based. The United States has shown little willingness to engage with the idea of breaking up large online platforms.

Furthermore, the idea of 'breaking up' a large online platform such as Facebook is difficult to implement practically. It is unlikely that it would be practically feasible to break up a platform like Facebook into a set of smaller entities which each took on some of the functions of the original platform.

In the digital world, people seem to have a preference for a 'single solution', whether that be open protocols like Email or the Internet Protocol, or centralised platforms such as Facebook. Thus, rather than attempt to break up platforms which appear to have a monopoly on services of their type, it may be more worthwhile to focus on creating open and interoperable standards. It is, however, difficult to know where to intervene to achieve that desired effect. Perhaps platforms could be forced to maintain a greater degree of interoperability and permeability - for example, so that people outside of Facebook can contact people using Facebook.

# 8. What effect will the United Kingdom leaving the European Union have on the regulation of the Internet?

One specific issue to be highlighted is the potential loss of the protections of Article 15 of the Electronic Commerce Directive after leaving the European Union. Please find enclosed along with this document a separate submission from us which highlights the critical importance of taking action to preserve Article 15 after Brexit takes place.

In addition, we have concerns that the DCMS and other Governmental departments may not have the necessary resources to cope with the reality of ensuring that all of the appropriate EU Directives and Regulations are incorporated into the UK regulatory framework after leaving the European Union. To highlight this point, GDPR faced over 3,000 amendments, and the recent Telecoms Package is facing similarly high numbers.

In the UK, the House of Lords acts as the scrutiny vehicle for legislation, but is not resourced with large staff research teams. Similarly, the Commons is not set up for line-by-line scrutiny and amendments of complex technical legislation which requires consideration of matters that are not yet in the public eye.

The temptation here will thus be for the Government to adapt and water down future EU legislation. The good but controversial parts such as consumer protections, strong regulatory powers, or commercial obligations are likely to be left out.

# 9. 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?

Here there is a difference between content, telecommunications infrastructure and the Internet. All of these could be improved, but there is no silver bullet.

## Telecommunications

The International Telecommunications Union regulates the basic infrastructure of cables and electromagnetic spectrum. Here governments have a big role to play and the UK could do a lot to ensure more democratic participation from civil society.

The EU plays a big role in standards because it can mandate some of these in their technical regulations through European Standards Organisations. Many of these EU standards become international standards. After Brexit, the UK situation will change. The British Standards Institute (BSI) is pushing to retain full membership of ESOs. This may be possible, but the link to EU policy will likely be lost.

## Internet

The technical details of the Internet proper are mainly decided at standards bodies such as there Internet Engineering Task Force and W3C, and some key governance institutions such as ICANN.

Governments - other than the US Government - are less influential in these spaces. The Internet Governance Forum is a UN-supported body that is meant to bridge this gap, but it is fair to say that it is not very effective.

The UK has tried several times to start its own processes of international governance, such as the Seoul cyber summit, but these have not worked. It would be better for the UK to spend its energies improving the governance of existing spaces.

## Content

Content regulation mainly works at national level, with some important influence from large geopolitical entities. The situation could be summarised in that the EU is setting the standards for privacy, and the US is for most content rules.

Other important elements of the landscape are the OECD recommendations on various issues, and the Council of Europe conventions, e.g. on data. For the UK the latter will be particularly important after Brexit.