children's charities' coalition on internet safety

Submission to House of Lords Select Committee on Communications

The Internet: To Regulate or Not To Regulate?

Is there a need to introduce specific regulation for the internet?

With the development of easy to use web browsers in the early to mid-1990s the internet started its journey from the confines of academia and limited adoption by business towards a mass consumer market. Unanticipated problems were not far behind. The increased availability of child sex abuse materials was one of them.

Questions about how or whether to regulate the internet first arose in public forums in the UK in 1996. This was the year Internet Watch Foundation was established.

At the time there was very little knowledge within Parliament, the Civil Service and the police about what the internet was and how it worked. Would this new-fangled technology take off or was it a passing craze? How much effort should be put into trying to understand it? There was therefore an almost palpable sigh of relief on the part of the Government when, after some difficult conversations, the industry agreed to "sort things out". Thus, the IWF came into existence *faute de mieux.* It was not a carefully selected option, chosen from a range of available possibilities.

The internet industry then consisted principally of a handful of ISPs. There was opposition to the idea of forming the IWF but the majority view prevailed. Industry leaders were pleased to be left to their own devices. It married with a strong prevailing ideology among internet pioneers that, by building out the network, they were also building a new and better way of running the world.

John Perry Barlow's "Declaration of the Independence of Cyberspace" spoke of *"Governments of the Industrial World, you weary giants of flesh and steel…..On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."* This was an extreme exemplification, but it had resonances in many different virtual quarters.

Within industry circles there remains a strong attachment to self-regulation in everything that is connected to the internet. Undoubtedly this is rooted in part in an acknowledgement of the unique complexities presented by cyberspace, but it also picks up on, maybe exploits, a larger acceptance of the notion that smaller government is better government which, similarly, is connected with a diminution in confidence in public institutions generally.

However, the way events have unfurled since the mid-1990s, in particular the manifest failure of the internet value chain to find a way to reassure the public that the industry is both willing *and* able to find solutions to some of the problems that have developed, suggests the current arrangements for managing the internet in the UK are not working well enough.

Such internet regulation as exists in Britain today lacks coherence and consistency. It has grown up piecemeal, on an ad hoc basis not infrequently, as in the case of the IWF, following a crisis of some sort. As a result, we have a patchwork of powers and responsibilities distributed between different organizations, with varying degrees of transparency and apparent effectiveness.

On one count there are twelve different bodies[1] with a claim to being involved in regulating online activity. Moreover, there are limits to the extent to which these self-regulators, co-regulators and statutory regulators can or are willing to co-operate with each other.

Having twelve different organizations is not in itself the issue. However, our strongly held belief is someone somewhere should step back and take a view about what would be the *optimal* way to serve the public interest in this field. If the Select Committee cannot undertake this task perhaps it will be minded to recommend such an idea.

It may well be the case that in relation to certain types of activity self-regulation could continue to be the best possible answer to ensuring the public interest is properly safeguarded, but self-regulation has lost its historic right to be considered the default option. Henceforth, self-regulation should only be acceptable if it can be shown to adhere to processes and systems which allow members of the public to feel confident things are working to an agreed standard.

The lack of coherence and consistency in relation to internet regulation is by no means a peculiarly British problem. This does not mean the UK is powerless to act to protect or enhance its own best interests. Aside from anything else the value of the UK market to many online businesses means they will be unusually attentive to openly declared public policies and if they have the force of law behind them every significant online business will be keen to comply.

There will always be “tiddlers and rogues” who flourish around the edges or seek to exploit loopholes, but that ought not to deflect from mainstream concerns. It is possible to spend forever chasing the longtail when, by any reckoning and in accordance with the principles of proportionality, what the larger enterprises are doing is what matters to the vast majority of users. As smaller businesses grow so they will be drawn in. This may seem to be a little bit untidy, but the internet is untidy.

We have to start somewhere

It is a deeply entrenched myth in the liberal democracies that policies to address problems on the internet have to be internationally negotiated, agreed and implemented if anything lasting

[1] Ofcom, ICO, PSA, IWF, ASA, BBFC, CMA, DMA, GC, FCA, PRA, IPSO

and worthwhile is to be achieved. This has the effect of paralysing Governments and legislatures and some companies, or lets them off the hook, providing an alibi for inaction. It serves to preserve, or at any rate prolong, the status quo. Cui bono?

Of course in some areas the greater the degree of international harmonization the more likely it is companies will voluntarily align (there are no certainties here, look at the story of IPv6) but equally it is true that in an environment where the ability to innovate is so highly prized, the role of leadership and rigorously thought through experimentation cannot be over-emphasised. If the UK develops an approach that is seen to be effective others will follow and eventually the "international community" will recognise and embrace it.

When BT first introduced "Cleanfeed" back in 2004, as a tool to restrict access to child sex abuse material on web sites, it did not consult the whole world before pressing ahead. It was criticised at the time by and in practically all parts of the internet, both here and abroad. BT nonetheless did what it thought was right and was technically feasible. "Cleanfeed" was seen to work. The practice is now widespread in all parts of the world and the idea behind it has even gained recognition within a 2011 EU Directive.

Similarly, when Prime Minister David Cameron announced the "We Protect" initiative in 2016 and arranged for £50 million to be put at its disposal he did not wait for the blessing or the opinion of the UN, the EU, ICANN, the IGF or anyone else. The Prime Minister did it and the current Government continues with it because they believed it was the right thing to do and would add value. The initiative is now widely recognised as ground-breaking.

When Microsoft developed and released PhotoDNA in 2009 they did so entirely of their own volition and it now ranks, globally, as one of the most significant advances in online child protection in recent years and it has been adapted to address other types of illegal content.

None of this is to minimise the importance of international institutions. On the contrary it is a matter of great regret that those that exist are not more energetically engaged in finding solutions to outstanding problems and some have a particularly lamentable history – here ICANN deserves a special mention. However, it is inevitable that geo-politics, diplomacy and the need to fund travel and find the time to attend international conferences are major limiting factors in terms of their speed and efficiency.

Children are not a small or marginal group

Whoever undertakes the sort of review we have in mind ought to be mindful of the fact that in the UK roughly 1 in 5 of all internet users is a child, that it to say someone under the age of 18. Globally, the proportion is 1 in 3, rising to nearly 1 in 2 in parts of the developing world. It is therefore the case that children are probably the largest single identifiable constituency of internet users, and even if that is not literally the case, they won't be far off.

Either way, there is no doubt that the internet is a medium for children every bit as much as it is a medium for anything else. This humdrum, ordinary fact is normally overlooked in the loftier climes of global internet policy making and by many individual internet businesses. Children are too often seen as an irritating, trivial concern, the responsibility of "someone else", usually parents, schools, the police, or all three, whereas our contention is that in any discussion about policy and the internet, in each and every forum, the fact that children are online in such gigantic numbers should be front and centre.

Two key US laws

One of the reasons children became marginalised as a factor in internet policy making circles can be traced back to two US laws.

s.230 of the **Communications Decency Act, 1996**, was the first legislative measure in the world to establish broad immunity from liability for intermediaries. The UK and the EU did not exactly copy it (eCommerce Directive) but they did not depart from it in a major way.

Recent changes in the law in the USA and in Europe have made some difference here but the core principle remains in place.

Immunity for intermediaries may have been critical in the early days of the internet, when there was a great deal of uncertainty about how the new technology would develop and there was justifiable concern about the prospect of law suits scaring off investors and slowing down innovation, but those days are long gone.

The internet is no longer a green field site. No one should be able to develop or market new products or services and plead ignorance in respect of well-known hazards. Yet the immunity laws are still in place. They have become a refuge for scoundrels.

The Children's Online Privacy Protection Act, 1998, introduced an incentive for companies to ban persons under the age of 13 from their services but the law did not create any obligation on businesses to enforce the age rule. No obligation meant zero incentive.

In the UK over 75% of all 10-12 year olds have accounts with social media platforms that specify 13 as their minimum age. In other countries the percentage is even higher. The social media companies could have chosen to police the perimeter. They didn't because they were not required so to do.

In effect this law and the immunity law combined to give online businesses permission to forget about children and many of them did. The GDPR will change the landscape but it is still too soon to say how.

What should be the legal liability of online platforms for the content that they host?

It would be unjust for any online platform to be held liable for any 3rd party content or behaviour where it did not have and could not have had any actual knowledge of it.

However, CHIS believes that in future, in order for a platform to maintain its immunity in respect of 3rd party content or behaviour, in either civil or criminal matters, it must show that, being mindful of available technologies, it had taken all reasonable and proportionate steps to prevent, limit or mitigate the scope for its service to be used for unlawful purposes AND that it has taken all reasonable and proportionate steps to ensure its stated terms and conditions are being honoured.

Terms and conditions of service which are not linked to any requirement to make good faith efforts to enforce them can be seen as being a pious hope, a marketing ploy or a deceptive practice. They convey the impression to a would-be user, or the parent of a would-be user, that certain things will or will not be happening or available on a site or service whereas in reality the service provider has no way of knowing if that is the case and they make no attempt to find out. That cannot be right.

How effective, fair and transparent are online platforms in moderating content that they host?

Online platforms vary enormously in their purpose, functionality and intended audience but CHIS cannot think of a single one where we could say we are confident their moderation policies are fair and effective, precisely because there is little or no transparency. Without an independent element which can verify that the statements a platform makes about its moderation practices are a true and fair reflection of what the company has actually done – rather as an auditor does with the commercial operations of a business – it will be impossible for us to take a different view.

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

This sounds like a laudable democratic ambition, but our short answer is it depends on the nature of the platform and its functionality. If children are an intended audience or are in fact present in any appreciable numbers certain minimum standards should be applied and be enforced. Obviously consulting with users will always be a good and necessary part of sound business practice but the intention to consult or referring to the results of an apparent consultation should never be a reason for diluting, avoiding or delaying the adoption of acceptable minimum standards.

What effect will the United Kingdom leaving the European Union on the Government's regulation of the internet?

In the Max Schrems case the mighty USA was forced to change its laws in order to bring themselves into line with EU law. The alternative was US businesses would be barred from allowing EU customer data to cross its borders. We suspect the same will apply when/if we leave the EU. If we want UK businesses to continue being able to buy and sell things to people and businesses in the EU, if we want British young people to be able to communicate online with young people in other countries, our laws will have to correspond with the EU's in several important respects. In this context the GDPR is likely to be the most relevant and since we are broadly pleased with GDPR from a child protection perspective, that is fine with us. It is obviously the case that, post-Brexit, the UK may have some greater latitude to develop new approaches and providing these do not collide with anything that matters to the EU this may work to the advantage of children in the UK. Time will tell.

---ooo---

John Carr OBE
Secretary
Children's Charities' Coalition on Internet Safety
10, Great Queen Street
London WC2B 5DD

27thApril, 2018.

www.chis.org.uk