children's charities' coalition on internet safety
10 Great Queen Street, London, WC2B 5DG

Comments on the Online Harms White Paper

Children are not a small or marginal group of internet users

Today one in five of all human internet users in the UK is a child[1]. Children are a permanent and substantial presence in cyberspace. We need to establish a new narrative, help create a new settlement, one which recognises the online world as a consumer or family product or service every bit as much as it can be an instrument that serves other purposes.

Implicit in this approach is a clear determination to entrench or bolster new norms in terms of how society thinks about the internet and what is considered to be appropriate behaviour in relation to it, in respect of corporate or commercial interests, communities and individuals.

The internet's value to children and to society as a whole is beyond dispute but here is not the time or place to dwell on things that are going well. Here we need to focus on issues that still need to be resolved to make the internet an acceptably safer, better, rights-enhancing place for children.

In the new settlement the best interests of children should be dominant considerations. This principle is long-established and followed in a great many other shared spaces where children can reasonably be expected to be present at scale and on a regular basis. There are no grounds for saying the internet should be an exception.

No adult need feel or be deprived of any rights they currently have to access places or content designed or intended only for persons over 18. However, it is recognised that in online environments meant *only* for adults, certain formalities which are not currently commonly enforced might lead to short delays while proof is provided that allows the service provider to have reasonable certainty the would-be user meets the qualifying age threshold. Such formalities likely as not need only be completed once on the first occasion the person engages with the service in question.

This type of authentication is already frequently used in the physical world. Almost all adults accept such processes are designed to achieve a larger social good and, for that reason, they happily go along with them. The challenge on the internet lies in determining what is required in environments where one could reasonably expect both adults and children to be present in the same spaces on a regular basis. However, again, this is not wholly new. In the physical world we have "watersheds" on TV, limits on the kind of advertising that can be displayed on hoardings located near schools, restrictions on window displays in High Street shops, checks at the doors of cinemas pubs and clubs, but it is acknowledged that finding a way to deliver anything similar in cyberspace will present challenges. However, in order to meet such challenges, it is first necessary to want to meet them.

[1] https://www.unicef-irc.org/publications/pdf/idp_2016_01.pdf

There is precious little evidence that such a desire exists where it perhaps matters most i.e. among leading internet companies.

The White Paper's aspirations are crystal clear

The children's organizations applaud the Government's decision to publish the Online Harms White Paper. It recognises self-regulation has failed as the core principle for addressing the challenges facing children as internet users. It sees a statutory Regulator as an essential feature of the future landscape. As a statement of intent, the White Paper's aspirations are crystal clear, and the Government is doubly to be commended for publishing it, written as it was in the face of nearly zero meaningful co-operation from a great many important high-tech companies.

No real commitment to multistakeholderism

These businesses may habitually sit in the same room as Ministers, civil servants and children's groups, they may proclaim their support for "multi-stakeholderism"[2], support education and awareness initiatives – i.e. programmes designed to help parents and children address problems their services helped create[3], problems which, sometimes, by their own admission, arose from their own mistakes or oversights, but most of the truly important things we know about the threats facing children online are derived from external sources.

This is because the companies themselves refuse to allow any independent, external evaluation or examination either of the scale of different problems faced by children using their services or of the efficacy or proportionality of the systems they have put in place to counter or mitigate behaviours which adversely impact children.

Non-disclosure agreements and money buy silence and sustain opacity

Businesses are, of course, entitled to enjoy confidential, privileged relationships with their own employees and external advisers. However, in the technology space a practice has emerged of having or consulting with "Advisory Boards". These give the appearance of being a source of independent advice to the company but may, in reality be anything but. This is because Board members or their organizations will often be compromised by being in receipt of significant sums of money from the same company and be tongue tied by being required to sign non disclosure agreements. Information is ***not*** shared in a way that would allow the online community as a whole, the Government or civil society to have a better understanding of how to deal with the remaining child protection and child rights challenges.

The companies themselves typically do little to compensate for the opacity with which they surround themselves. For example, simply being told a company has x number of human moderators is of little use. It may even flatter to deceive. With no idea how and by whom the moderators are actually employed, under what conditions, with what training, management and support and with what brief, what can anyone deduce from "knowing" an unverified number? How does the cost of x human moderators compare, for example, with the cost of other aspects of a company's operations? This would allow at least some sort of judgement to be made about relative priorities. If Artificial Intelligence is being deployed as an aid to human moderation or for some other protective reason, how well is it working? Are some AI solutions better than others? If so why?

Recommendation: Consideration should be given to establishing large datasets to be held by a

[2] https://en.m.wikipedia.org/wiki/Multistakeholder_governance_model

[3] As often as not, by their own admission, only because they made mistakes or didn't think things through

public interest body in a way that would allow qualified researchers and businesses lawful access to test various hypotheses or develop new solutions. This will help avoid a situation where monopolistic ownership or control of large datasets gives established big businesses a permanent, market stultifying in-built advantage.

To act or not to act?

In the face of the information blackout with which the Government was confronted, it had a choice. They could accept they were paralysed and incapable of doing anything worthwhile because they did not have a perfect understanding of the terrain.

Or they could make reasonable judgements and proposals based on such intelligence as they could glean from academic research, police or court reports, expert advice, Parliamentary enquiries, investigations by tenacious journalists and by listening to parents and children themselves. More recently they have also been able to draw on evidence which is emerging from the IICSA hearings[4].

The children's organizations are glad the Government opted for the latter course of action. Those voices expressing doubts or reservations about this or that aspect of the White Paper need to bear in mind the responsibility of the internet companies themselves for helping create the conditions which led to it.

Facebook's denial of service

Facebook's unambiguous refusal to collaborate in a UKCCIS Evidence Sub-Group research project is a perfect illustration of the case in point.

In 2014 three UK Government Ministers wrote to various companies asking them to cooperate in a project that was designed to gain a better insight into children's experiences when using different platforms. We knew what children were telling us happened when they sought to engage with companies in respect of something that troubled them, but how did things look from the companies' perspective? Were there any significant disparities or disjunctions between what the external data revealed and how the businesses saw things? Within companies, how well did different processes work for dealing with matters raised by children and within what kinds of timeframes?

After local, UK staff, initially agreed to take part in the study Facebook finally withdrew saying their Californian HQ had ruled they "would not provide the British Government with any information they were not legally obliged to publish or supply". They are not legally obliged to publish or supply anything that touches on children's online safety.

But it goes beyond that. Even when companies make a claim or they allow people to believe something that is said about them, it can turn out to be significantly at variance with the actualité.

Things are sometimes not what they are believed to be

Look what happened in the case of Blackberry handsets[5].

In 2005 the mobile phone networks proclaimed in an industry code of practice that all mobile networks were restricting access to child sex abuse material (csam) and to adult content. That was substantially true, but not completely.

[4] https://www.iicsa.org.uk/
[5] https://johnc1912.wordpress.com/2011/12/09/blackberry-has-some-explaining-to-do/

At the relevant time (2010/11) there were about 8 million Blackberry handsets in use in the UK. The company had a significant share (one-fifth) of the total smartphone market. It turned out that, with the exception of the 700,000 Blackberry users who were on TMobile's network, the other 7,300,000 Blackberry users on all the other networks were not shielded from adult content, neither were they protected from the possibility of being exposed to child sex abuse material. This was because the Internet Watch Foundation's (IWF) list of urls and the adult content filters would not work on Blackberry devices unless, as with TMobile, special arrangements were made. They hadn't been.

This was particularly unfortunate because at that time Blackberry handsets were hugely popular with children as they had pioneered "free" messaging services. Yet for quite some time (until this lacuna was discovered) neither Blackberry themselves nor any of the networks made clear to their existing customers or would be purchasers of Blackberry handsets that if they used the device on any network other than TMobile they would not benefit from the protections trumpeted by the industry code of practice. This was misrepresentation by inaction or silence.

A similar situation arose at one point with companies who joined the IWF and took receipt of their list of urls. The implication was these businesses were actually deploying the list and were therefore actively engaged in restricting access to csam on their services. Most were. Some weren't.

On discovering this the IWF introduced a self-certification scheme and a mechanism for checking whether or not, in fact, the list was being used by companies that were taking it. One might have expected the IWF to have anticipated eventualities such as these but once again we see that, left to their own devices, organizations are quite willing to take advantage of the absence of proper checking or due diligence even if, or especially if, it delivers them entirely undeserved credit.

A different example once again concerns Facebook. In evidence given to the IICSA hearings on 14 May, 2019 the company representative acknowledged (p82) that back in 2014 they had started discussions with the IWF about deploying the url list to block access to csam. Most people engaged with online child protection were aware of this and just assumed this would be dealt with swiftly. Speed is a hallmark of the internet and everybody knows about Facebook's famous commitment to "moving fast".

Certainly, subsequently, many people made speeches which Facebook staff heard because they were in the room, or they read articles in which it was said Facebook was among a righteous group of companies that were doing everything then known to be possible at a technical level to restrict the availability of csam, meaning using hashes and the IWF url list. Facebook did nothing to correct that false impression.

Is this really a criticism of those who were too trusting or gullible? Or is it once again a reflection of the fact that absent any independent means of verifying a claim a company makes, everything said should be treated with a pinch of salt? Either way that is not a good position to be in.

Even in respect of the deployment of filters by domestic broadband suppliers, mobile networks and WiFi providers, there is no properly resourced, independent mechanism for checking or confirming the efficacy of these measures or the extent to which they are in place and being taken up. That is a major, continuing shortcoming that ought to be corrected. The Regulator could do that.

The position of the Regulator and the codes of practice are going to be key

Referring back to the fact that the White Paper was necessarily written on the basis of the Government having only partial information and referring also to the way in which, hitherto, there has been no independent means to verify, evaluate or vouch for any of the online safety claims made by internet businesses, it seems clear that the Regulator must have the legal power to compel companies to answer questions in a way which would allow the Regulator to determine whether or not the business's approach to dealing with children is satisfactory and, in the event they find it isn't, to give directions, levy fines, or both.

Recommendation: Just as companies are required to make audited or certified declarations in their annual company reports about compliance with a variety of financial, equalities, human rights and environmental laws and regulations, for relevant businesses compliance with online child safety standards should also be made subject to regular inspection and certification by the newly created Regulator.

The auditable practices of online businesses should be guided and underpinned by the codes of practice which will be developed following the adoption of various key proposals in the White Paper.

The codes will be developed and refined by the Regulator on the basis of the information received from companies and its own evaluations and determinations.

Recommendation: Recognising the critical importance of the codes of practice referred to in the White Paper, it is anticipated an iterative process will emerge to aid their development. The overall intention and scope of each code will need to be crisply stated. Procedural matters will also need to be clearly set out. However, there should be no doubt that, particularly in the early days, and perhaps forever in respect of alleged harmful content, there are always likely to be edge cases that throw up challenges.

There is no suggestion there should be any kind of prior restraint but, equally, it is recognised there will need to be a process established, possibly within or linked to the Regulator, which can make decisions in disputed cases. This process will be judicial or quasi-judicial in nature. Other media regulators operate in a similar way.

Over time a corpus of cases and settled knowledge will emerge which provides the required degree of certainty for the medium to longer term. It is destructive "impossibilism" or obstructionism to demand complete certainty from Day 1.

There will always be margins for interpretation, particularly with the sort of issues raised in the White Paper where the UK is engaged in pioneering a radically new, comprehensive approach to online child safety and children's rights. Professor Sonia Livingstone of the LSE has compared the period we are living through to the time that existed when "horseless carriages" first started to appear on public highways and a person had to walk in front of each vehicle waving a red flag.

As we chart this new territory we are, in effect, being asked to declare how we see the future. In that future nothing should be off limits when it comes to the protection of children or children's rights. Nostalgic hankering for the "Wild West freedoms" of yesteryear has to be abandoned.

The internet has inserted itself too deeply into the fabric of children's lives and into how we all now live for the old ways, limitations and uncertainties to be acceptable. To repeat an earlier point: the internet is a consumer product, operating in the consumer space, often acquired as an adjunct to or as part of a TV package. It must conform to the reasonable expectations of products and services which are sold or provided to consumers.

Transparency is essential

In amongst its other powers and obligations the Regulator must be able to reassure the public that named companies are conforming to the guidelines contained in the codes of practice. In order to do that the Regulator must be in a position to specify transparency standards. Simply providing some kind of generic kitemark or seal of approval is unlikely to be sufficient for the foreseeable future.

Recently Facebook and Google have started issuing their own enhanced transparency reports. These are a welcome recognition of the growing importance of publishing more information about what is happening on internet platforms, but insofar as these reports are about those companies saying to parents, children, the Government and the general public "this is what we think you need to know and this is what we are willing to tell you" they are not acceptable as the basis on which to proceed in the longer term.

The future of self and co-regulation

Quite rightly there is now almost zero support for self-regulation as the core principle on which the internet is managed within a given jurisdiction. Most online businesses now accept there needs to be a framework of legally enforceable rules, obligations and accountability.

That said, nothing in this submission should be read as implying there is no future at all for self-regulatory or co-regulatory measures. Neither is it being suggested that every existing statutory regulatory mechanism which impacts on children in the online space should be collapsed into or be taken over by the new Regulator. However, henceforth, certainly in respect of self-regulatory and co-regulatory mechanisms, the new Regulator should, in effect, act as a "super-Regulator" i.e. act as a guarantor or inspector of any continuing self-regulatory, co-regulatory or other initiatives relevant to online child protection. This would reassure the public that the processes established are working satisfactorily and delivering what they purport or seek to do.

Recommendation: Where there are existing statutory regulators with responsibilities which engage or overlap with online child protection or children's rights online e.g. in respect of privacy, gambling or limiting access to pornography, a Memorandum of Understanding should be prepared and published setting out how the arrangements will work and who has principal responsibility for doing what. The Regulator referred to in the White Paper should be given lead responsibility for negotiating the Memorandum.

Recommendation: Self-and co-regulatory bodies exercising functions which address the welfare or rights of children on the internet must be subject to Freedom of Information requests. In addition, the Regulator must have the necessary powers to require information from the same bodies and the power to investigate and report on their conduct and efficacy.

Recommendation: It should be made clear to the IWF they owe a duty of care to children which extends beyond and is superior to any and all obligations they have to their fee-paying members or to other bodies.

Specifically, there should be a presumption the IWF will publicly name individual companies that persistently fail to observe reasonable standards in respect of those issues which are within the

IWF's areas of competence. This obligation applies irrespective of the jurisdiction within which a company may be domiciled.

The IWF should set out the circumstances where it will *not* publicly identify companies found to have persistently fallen short of best practice in relation to the removal of child sex abuse material (csam) or preventing it being uploaded in the first place.

The "chilling effect"

Critics of the White Paper speak of their fears of the "chilling effect" of aspects of what may emerge from it. Generally, they are referring to the potential to restrict free speech. This is a concern that is shared by children's organizations, but everyone needs to keep in mind the "chilling effect" of leaving things as they are.

At risk of being repetitive, it has to be acknowledged that the internet has evolved. It is a long way from being what it once was. No longer the sole preserve of adult geeks and academics, it is absolutely central to the way society works across a broad spectrum. Driven in no small degree by the operation of free market forces, the internet has become central to the way children live their lives. The rules have to change to adapt to these new conditions.

Since the free market now seems to be incapable of making the necessary adjustments, on the contrary it shows every sign of being deeply attached to the status quo, the state has to step in. This is a pattern that has been repeated many times, with many different industries. It can be disruptive and painful. Change often is. That is not a reason for ducking it or listlessly kicking the can further down a road which stretches towards a barely visible horizon.

A matter of confidence

Recommendation: The Regulator must enjoy the confidence of the tech world, civil society, the media and law enforcement. If it is inevitable the Government must appoint the person who will be its head, there is a strong case for this appointment being subject to approval by Parliament with all-Party agreement that whips will not be applied.

Alternatively, consideration should be given to using a system similar to the process for appointing senior members of the judiciary.

Recommendation: While the Secretary of State clearly needs to have a power to direct the Regulator to look at a particular problem, it is unacceptable also to stipulate that the Secretary of State has the final word on any code of practice that might result from such a direction.

Recommendation: Parliament must approve whatever codes of practice the Regulator proposes.

A matter of money, equality of arms and the ability to participate going forward

If we set on one side the (anyway unknown) costs of companies deploying technologies which help them avoid unwittingly aiding and abetting the distribution of csam, facilitating grooming or other forms of crimes against children[6] or harms, it is impossible to say what monetary value to attach to the sum total of all child safety-oriented activities currently provided by all the private sector

[6] It is a strange world where we congratulate people for not helping with the commission of a crime.

stakeholders in the UK. These mainly take the form of supporting education and awareness initiatives and some research. However, on the most generous estimates the amounts are unlikely to approach anything like the sorts of numbers the UK gambling industry seems to think are needed to address their issues.

It appears at the moment the industry contributes £10 million per annum to combat problem gambling and while the Regulator thinks that sum ought to increase to £70 million, the industry itself has suggested its contribution could rise to £100 million within 5 years. Maybe there are better comparators but when thinking about the level of a levy to finance the Regulator and its associated works the Government ought to be ambitious.

Recommendation: It is vital to ensure the Regulator can do what it has to do without risking becoming financially dependent on, beholden to or captured by industry interests or becoming in any way reliant on them for their voluntary cooperation in essential research or technical evaluations. This suggests, if a levy is to be collected and used for these purposes, it must be secured in a way that is sustainable in the longer term and which isolates the Regulator from any sense that it is obligated to the companies paying it.

Money matters and civil society's views matter. The whole idea of multistakeholderism is premised at least in part on the notion that the opinions of all the parties will be listened to both in terms of being able to initiate policy proposals or being able to respond to consultations that emanate from or arise within the processes.

Yet how is any of this possible if some of the parties e.g. children's organizations, cannot even afford to attend the meetings? Preparing for the meetings or other discussions, sustaining a potentially prolonged engagement in online exchanges of emails, lists and drafts, initiating research which they think is necessary to support their engagement, these are all integral to multistakeholder processes. It is not just about "being in the room". But the resources necessary to do this are well beyond the means of too many children's groups. This reduces the idea of multistakeholderism to a fiction, a veil which seeks to disguise an unpalatable truth. Those with the money generally get their way and can present their victory as having an unwarranted democratic patina.

To put that slightly differently, having a theoretically level playing field is all well and good but if one team consists solely of players drawn from the Premiere League while the other team's would struggle to win a spot playing at the lower end of the National League South it is likely to be a very unequal and unrewarding match.

Faced with a decision about whether or not to divert scarce resources which could help a child or a family in immediate need, as opposed to preparing a brief or travelling a long distance to an event to discuss a proposition which may, only *may*, at some indeterminate, probably distant point in the future, help some of the richest companies in the world do a better job, most children's organizations will have no choice but to meet the immediate need. This does not mean they do not appreciate the importance of the forum or the issues being discussed. It is just a cold, hard question about cash and how to use it. Moreover, if the high-tech companies were serious about it, if they truly valued or wanted a body of vibrant, engaged, well-informed children's groups participating in policy making processes, with all the money at their disposal they could find a way to make sure it happened without making children's groups feel beholden to them. But they don't.

Recommendation: The principle of "multistakeholderism" is well established and is a sound basis for determining policy in respect of children and the internet. However, it implies that all stakeholders have the wherewithal to enable them to participate in a meaningful way in the associated processes. Yet at present that is very far from being the case. It is impractical to imagine there could ever be full equality of arms as between the giants of the tech industries and UK children's organizations, but the current asymmetry is so pronounced as to mock the very idea. Thus, when considering future arrangements for activities in this area, the Government should ensure children's organizations are provided with sufficient financial and other forms of support. Any funding provided should not compromise the independence or the integrity of the recipients.

Recommendation: In the same vein, particular attention needs to be given to finding ways to support and improve the participation of children's organizations in appropriate international multistakeholder internet infrastructure and consultative or policy bodies.

Remote participation may be fine if all you need to do is listen or watch, but it is a very poor substitute where there are matters up for discussion which are complex and nuanced and the participants do not have a pre-existing relationship of some kind. In such circumstances remote participation gives the illusion of engagement, gives the illusion of being democratic, and in limited circumstances or in emergencies there is no doubt it can play a role. But if remote participation were so good why would any senior official or company executive ever trouble to attend any distant meeting in person?

Duty of care, platforms' liability, terms and conditions and scope

In the absence of essential information it is impossible, right now, to say what individual codes of practice should say or to prescribe particular approaches to the specific problems that currently preoccupy children's organizations, but there were three clear and overarching ideas in the White Paper which ought to be included on the face of whatever Bill makes its way to Parliament.

First among these is establishing a *"duty of care".* This is a core proposal in the White Paper and the children's groups strongly support it.

There is scope within the existing eCommerce Directive to allow Parliament to establish a duty of care in respect of intermediate platforms[7]. The only wonder is why this has not happened sooner?

Moreover while the White Paper appears to suggest that judging whether or not a platform has adequately discharged its duty of care is a matter for the Regulator, it ought also to be made clear and underlined that platforms continue to owe a long-established common law duty of care to each and every individual user or other entity upon whom their actions could reasonably foreseeably have an impact.

Recommendation: Parliament should invoke that part of the EU's eCommerce Directive which permits a national jurisdiction to create obligations on platforms in the form of a duty of care.

[7] Recital 48. "This Directive does not affect the possibility for Member States requiring service providers who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

Recommendation: In addition to the Regulator having a power to act, individuals should also have a power to act in respect of breaches of the new duty of care. There ought also to be scope for class actions on behalf of groups of consumers to enforce a duty of care or obtain compensation for breach. End users should also be reminded of their common law rights in respect of negligence.

Being in consumer markets brings with it a set of expectations that are far from being met at the moment. To the extent adults have different or additional rights or needs in relation to the internet as compared to children then, of course, they should be provided for. What is important, though, is to get away from the practice which to a large extent has existed hitherto where the position of children as users of a device or service is only thought about following a calamity of some kind.

Every technology company needs to adjust the way it thinks before "putting it out there". Back in the 1990s Professor Ross Anderson remarked[8] that a typical attitude was "ship it Tuesday, fix it by version 3". This gave rise to techies generally advising people never to buy Version 1. Whatever view one took of that then it surely has no place in a world where children are known to be present at scale. Yet it persists, finding a modern echo in the famous dictum of Mark Zuckerberg "move fast and break things", or his updated version, "the fast shall inherit the earth". These are metaphors which give businesses permission to be careless and, in respect of children, they rest on the assumption that the burden for policing their products is shared equally or to a substantial degree with parents and teachers. The legal or economic incentives to be careful have been absent up to now. On the contrary, the legal protections provided by platform immunity and the economic incentives provided by capitalising on "network effects" point in exactly the opposite direction. This must change and the White Paper suggests that is what will happen. Bravo.

Recommendation: Arising from the second overarching idea, without necessarily going so far as to impose a general obligation on online businesses to monitor all activity on a site or platform, although views on that are weakening, businesses should be under an explicit obligation to analyse every aspect of the services they provide so as to anticipate or identify issues or problems that might arise which are likely to have an adverse impact on children's rights. Arguably this is already a requirement under the GDPR and is further supported by the UK ICO's Code on Age Appropriate Design.

Recommendation: Thirdly, and closely linked to the above, if platforms and services wish to preserve immunity from civil or criminal liability, they must be required to show they have taken reasonable and proportionate steps to enforce their own stated Terms and Conditions of Service. Terms and Conditions of Service should not be reduced to the status of marketing hype.

Recommendation: Being mindful of the rules about proportionality, companies should be expected to deploy available technical tools to detect, mitigate or eliminate illegal and harmful activity insofar as these are prohibited by their own Terms and Conditions of Service and insofar as they are likely to give rise to harms to children.

Private messaging

In relation to scope: the intentional exclusion of "private messaging" is perplexing and must be changed. To the extent that private messaging services are a means by which illegal images can be

[8] http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf> (page 2)

exchanged or other harmful acts against children initiated or extended they cannot be declared to be outside the range of concerns the White Paper or the Regulator will address.

Professor Hany Farid[9] has made clear that, for example in respect of encrypted messaging services, forms of encryption can be used which in every degree maintain the privacy of the content of the message but nevertheless retain a facility to identity known illegal child sex abuse images.

Recommendation: actions relating to private messaging services must be within the scope of the White Paper's aims and the Regulator's powers.

The international dimension

In almost every major international arena in which Governments participate, with or without the simultaneous presence of industry, attitudes towards the internet and the proper role of the state in relation to its regulation are highly diverse and contested[10]. Moreover, there is anyway room for considerable doubt about how much attention is paid to the pronouncements of international organizations by Board Rooms on the West Coast or in Shanghai. In a world where "moving fast and breaking things" remains a major driver companies march to the beat of a different and faster drum. Lest we forget, it is also the case that Post-Snowden not just US companies express considerable reservations about the boundaries of voluntary co-operation with Governments as well as other businesses. In addition, there are concerns about the emergence of what might be seen as cartels dominated by immensely wealthy mega-corporations. Anti-trust suits are to be avoided at all costs.

Thus, any call to defer or delay any new policy initiative until a "global solution" can be found is either Utopian or it disguises a deeper desire to maintain the status quo for as long as possible. Cui bono? Not children.

Rather, faced with a high degree of paralysis or sluggishness on the part of international organizations, individual nation states can lead by example. If something is tried and is seen to work reasonably well or show promise, others will take it up and either adapt or copy it. In that way a bottom up consensus will emerge despite the absence of any express prior endorsement by traditional internet governance or Treaty-making bodies. They can catch up later.

The UK has, rightly, obtained a reputation globally for being a leader in the field of online child protection. That reputation has been won in part by participating in all of the major international forums, listening to and learning from opinions and research published in all parts of the world. Typically, the UK is a signatory to all the major accords, communiqués, conventions and declarations which have emerged from the principal forums which consider such matters. However, while recognising the desirability of achieving greater international harmonisation of standards in terms of how to implement the principles adumbrated in the accords, communiqués, conventions and declarations, rather than allowing that to become an alibi for inaction, rather than wait for the slowest or least likely states or companies to climb on board, the UK decided to act in accordance with its understanding of what was required. This is one of the reasons why in the findings reported

[9] https://www.foxnews.com/opinion/hany-farid-facebook-end-to-end-encryption-security-privacy
[10] This is one reason why the "5Eyes" and similar machinery are growing in importance

by the Economist Intelligence Unit to the ITU-UNESCO Broadband Commission in early 2019 the UK came out as the world's No. 1 in a table of nations addressing online child safety[11].

That said, it would still be a mistake to think the UK has a perfect or near perfect record in every area connected with the way the international dimensions of the internet work.

Internet industry infrastructure bodies

While accepting the White Paper's primary focus is on businesses which allow interactivity via user generated content, there are key parts of the broader internet landscape which need to be brought within scope. In particular we have in mind the position of browser companies and any business which may engage with the operation of the DNS[12].

Alongside the companies that provide services via the internet there is an ecosystem of internationally based infrastructural and standards bodies which have been responsible for developing the technical rules that allow the internet to function. Two of the key ones are the IETF and ICANN .

Whatever the shortcomings of these bodies might be, and we are certainly not going to attempt to suggest any alternative or better models, it seems to us too many national Governments, the UK included, have not always been sufficiently engaged with them. At times their involvement has been tokenistic and therefore (predictably) ineffectual. This is particularly unfortunate because the commercial and other interests with a material stake in the results of decisions made by these bodies are never under-represented.

The way the DNS over https standard emerged through the IETF is one example. Another of equal importance concerns the way WHOIS has been allowed to be degraded by ICANN although in the latter case, more recently, they have been aided and abetted by scandalously negligent rulemaking by the European Union.

Web sites (sub-domains) continue to play a major part in a variety of forms of criminal activity on the internet. In the IWF's latest Annual Report (2018) they noted they had issued take down notices against 105,047 webpages confirmed as containing child sexual abuse imagery. Of these 6,941 (7%) were commercial in nature.

While these are comparatively small numbers, it should not be forgotten that a single url might contain anything between one and ten thousand or more individual images of a child being raped. But how can it be that even a single webpage containing child sex abuse material could be published on the web, much less be reaping a pecuniary benefit from its supply to others?

There are several ways in which it happens but a major one is very easy to describe: criminals buy sub-domains and give false information about their real-world identity and their contact details. That makes it impossible or potentially very expensive and time consuming for law enforcement to track them down. That means, in turn, law enforcement doesn't even try other than in the most egregious cases. This encourages or permits a criminal sub-culture to continue flourishing online.

[11] https://www.accesswire.com/546163/Out-Of-The-Shadows-Index-Shining-a-Light-on-the-Global-Response-to-Sexual-Violence-Against-Children

[12] See below "Internet industry infrastructure bodies" for further comment on this aspect.

The last time anyone did a major study of the accuracy of the WHOIS information, they found that only 23% of all entries were fully accurate in the way ICANN's own rules required. In other words, accuracy was the exception rather than the rule despite accuracy being a fundamental requirement. Plainly ICANN has been asleep at the wheel. Why have they not been energetically seeking to enforce their own rules on accuracy? Their lack of focus has caused and continues to cause untold harm to untold numbers of children in all parts of the globe. Could it be that, for too many of those who provide the funding to ICANN, as long as they get paid, trying to ensure accuracy is just an annoying and potentially complicated overhead that simply discourages more people from buying more sub-domains? It definitely looks that way.

This situation has now been compounded and considerably worsened by the fact that, following the adoption of the GDPR, a set of rules has emerged which substantially restricts the ability of law enforcement and others with a legitimate interest to access ownership information (even inaccurate data can help track a perpetrator because they sometimes make telling mistakes).

It should be noted that at no point, in any of the legislative stages during the passage of the GDPR was the question of WHOIS mentioned. Not even once. The EU was therefore obviously also asleep at the wheel and one has to wonder what other stakeholders, particularly law enforcement, were doing at the time to allow this to happen? Once the defective GDPR was passed and interpreted by data privacy authorities with little knowledge of or background in online child protection concerns, ICANN seized and capitalised on the EU's negligence to weaken WHOIS further. Once more, cui bono? Not children.

Recommendation: The UK Government should legislate to make it a legal requirement for any and all Registries and Registrars operating within the UK jurisdiction to verify in a robust way the real world identities and contact details of the beneficial ownership and management of any entity purchasing or renewing a sub-domain through them. In addition, Registries and Registrars should be obliged to give that information to any law enforcement agency that requests it or to any other party that has a legitimate interest in receiving it.

Recommendation: Any part of the internet infrastructure, any platform or online service which can impact on online child safety or children's rights must be brought within the scope of the anticipated statutory regulatory framework. Specifically, this must include and embrace DNS resolvers.

Compensation and help for victims and more to deter would be or actual offenders

The Criminal Injuries Board Compensation scheme is not fit for purpose in relation to the needs of victims of child sex abuse in general. Neither is it fit for purpose in relation to the expanded harms specifically caused to a child when images of the abuse are published on the internet.

Recommendation: The Government should initiate a review of how best to compensate and support victims of child sex abuse, giving particular consideration to the needs of children who have had images of their abuse posted on the internet.

Recommendation: The Government should initiate a review of how best to minimise child sex abuse by, among other things, boosting public health and other educational initiatives. As part of this, greater support should be given to measures which will help deflect persons who are potential child sex abusers, or which reduce reoffending rates among individuals with convictions or cautions for relevant offences.

Recommendation: Any public health approach which seeks to address children's welfare and children's rights in the context of digital technologies must include a substantial component which seeks to enhance parents' and carers' ability to help their own children. Digital awareness and developing digital skills should become a standard part of an increased provision of parenting courses and programmes.

Recommendation: The Regulator needs to work closely with the Gambling Commission and the gaming industry both to minimise the extent to which otherwise legitimate gaming can become a way of socialising or normalising gambling in ways which impact on children and to restrict further the scope for children to engage in gambling activities.

Recommendation: In respect of practically everything that has been said in our submission, there needs to be a tight focus on the position of children with special needs or vulnerabilities, looked after children, and children from marginal communities. The position of children from linguistic minorities, perhaps particularly children whose parents do not have a good command of written and spoken English, needs specific attention.

---000---

1st July, 2019