Response to DCMS and Home Office

Open consultation on the

Online Harms White Paper

On behalf of the UK Computing Research Committee, UKCRC.

Prepared by: Professor Chris Johnson,
School of Computing Science, University of Glasgow, Glasgow, G12 8RZ.
http://www.dcs.gla.ac.uk/~johnson

The UK CRC is an Expert Panel of all three UK Professional Bodies in Computing: the British Computer Society (BCS), the Institution of Engineering and Technology (IET), and the Council of Professors and Heads of Computing (CPHC). It was formed in November 2000 as a policy committee for computing research in the UK. Members of UKCRC are leading researchers who each have an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC and, as such, is an independent response on behalf of UKCRC and does not necessarily reflect the official opinion or position of the BCS or the IET.

Response

Question 1: This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

- [1.1] The UK has a broad range of regulatory models with very different degrees of engagement or consultation with industry. The White Paper provides minimal requirements for the creation of "transparency, trust and accountability across industry". However, annual transparency reporting will be retrospective. Other bodies such as the HSE have developed a reputation for prospective consultation and transparency – working with regulated industry to achieve consensus that often avoids the need for enforcement actions. For instance, Operational Guidance (0086) was published by the HSE before the assignment of their role as Competent Authority under the NIS Directive. This helped industry understand what they were working towards and offered a chance for feedback that gathered a degree of support not seen by some of the other Competent Authorities. This specific example illustrates the need for any Regulator to learn from existing best practice beyond the minimal framework developed in the White Paper.

- [1.2] More widely, we would urge that a limited trial be conducted to determine the likely impact of the proposals before they are fully implemented. In particular, to provide concrete examples of the services that fall within scope and to ensure that any published criteria are workable.

Question 2: Should designated bodies be able to bring ‘super complaints’ to the regulator in specific and clearly evidenced circumstances?

- [2.1] No. The term “super complaint” seems underspecified in the White Paper. The concept of a designated body without detail on the process of designation seems to contradict the aims of transparency and accountability.
- [2.2] There also seems a further contradiction in the White Paper – “We do not envisage a role for the regulator itself in determining disputes between individuals and companies, but where users raise concerns with the regulator, it will be able to use this information as part of its consideration of whether there may be systemic failings which justify enforcement action”. The decision to start an enforcement action would seem to imply a role in determining disputes.
- [2.3] A further concern is that without more developed guidance on expected norms of behaviour across the many different fields identified in the White Paper, it will be extremely hard for companies to know when they are likely to trigger enforcement action or indeed for the regulator to sustain any judgement in the face of a legal challenge.

Question 2a: If your answer to question 2 is ‘yes’, in what circumstances should this happen?

- [2a.1] N/A without further clarity on the process of designation or the legal status of a “super complaint”.

Question 3: What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

- [3.1] Users should have access to an on-line system that clearly identifies who in the regulatory organisation is dealing with their complaint and the likely timescales for each stage in the regulatory process.
- [3.2] It should be possible to create a fast track process where enforcement actions are speeded up in situations where delays might increase the perceived harm of the on-line activity to an individual or group.

Question 4: What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?

- [4.1] The leadership team of the regulatory body should present an annual review of the on-line risks to the UK with respect to the areas identified to the White Paper and to any emerging concerns. This approach follows the mechanisms that are widely followed by US regulatory agencies.

- [4.2] The leadership team should also be invited to submit a “top 5” most wanted reforms that would encourage the future safety of on-line activity across the UK – borrowing an idea favoured by the US NTSB. These items can then be tracked over time where they require action by Parliament through legislation or by other legal, regulatory bodies.

Question 5: Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

- [5.1] Even after several readings of the White Paper, it remains far from clear what services might fall within the scope of any regulatory change. It also seems unlikely that any enumeration will survive the pace of change in Internet based activities.
- [5.2] We would propose the creation of a series of principles that can then be interpreted by the Regulator and that these principles should be reviewed annually by Parliament to determine whether they are sufficient and to ensure that they are proportionate to the harm that might arise from any abuse.

Question 6 In developing a definition for private communications, what criteria should be considered?

- [6.1] As in [5.1] we advocate a set of principles that establish in broad terms the differences between private and public communication – acknowledging the need for interpretation and review as technologies change.
- [6.2] Many defendants often do not realise that their contributions fall under existing legal definitions of public communication. Of course, any claim of ignorance over the definition of public or private communication can be influenced by hindsight bias and cannot simply be taken at face value. Equally, it is important that the Regulator working with lead government departments helps to clarify the principles proposed in [6.1].

Question 7: Which channels or forums that can be considered private should be in scope of the regulatory framework?

- [7.1] This question may miss a key point – any definition of privacy put forward in law or other regulations/policies may not meet the reasonable expectations of legitimate users further exacerbating existing concerns over the role of government in areas relevant to digital free speech. More important is the legal challenge to any monitoring or other activities that might be engaged in by the regulator and the judicial approval that they might need to seek to support such enquiries. The consultations documents are silent on this issue and without more on these topics, the proposals will face widespread opposition.

Question 7a: What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

- [7a.1] Any monitoring by the regulator should be either approved in the same way that a physical search warrant is approved or should be subject to a detailed annual (judicial?) review to ensure that civil liberties are not inadvertently being eroded through a natural desire to expose and halt criminal harm on-line.

Question 8: What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?

- [8.1] A spate of recent consultations make use of terms such as ‘risk based’ and ‘proportionate’. These are technically vacuous concepts unless some explanation is provided as to how these terms are to be realised within methods and processes that direct intervention. The recent NAO report into the National Cyber Security Strategy is relevant here – arguing that the lack of objective metrics across government departments prevents an independent view of whether the response has either been proportionate to the risk or, indeed, cost-effective in terms of the money that the public have invested in countermeasures.
- [8.2] Metrics must be established to demonstrate value for money through the development of any more sustained regulatory framework.

Question 9: What, if any, advice or support could the regulator provide to businesses, particularly start-ups and SMEs, comply with the regulatory framework?

- [9.1] As mentioned in previous sections, existing regulatory bodies provide good models. In particular the HSE have established mechanisms and guidance that companies can use to determine whether or not their activities are likely to violate regulatory requirements BEFORE they start. These documents focus attention on the harm that might be caused and do provide the objective methods of risk assessment that are needed here (see comments in [8.1] and [8.2]).

Question 10: Should an online harms regulator be: (i) a new public body, or (ii) an existing public body?

- [10.1] It should be a new public body. The existing regulators in this space lack funding and find it extremely hard to retain staff – for example, look at some of the teething issues that have arisen in standing up the regulatory response to the allocation of responsibilities for Competent Authorities under the NIS Directive.
- [10.2] A new public body would avoid situations where existing staff are asked to take on new burdens with their existing roles just because new personnel cannot be found. There is some evidence that regulators have struggled to meet their existing obligations when faced with also staffing the new requirements under NIS.

Question 10a: If your answer to question 10 is (ii), which body or bodies should it be?

- [10a.1] N/A

Question 11: A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

- [11.1] Similar schemes have been developed – for example by the US FCC and in this case, the fines levied on companies were directly used to fund regulatory intervention. This creates tensions with existing recovery mechanisms and may also make industry less willing to cooperate with the regulator. However, the alternative is to continue to place additional tasks on existing regulators in the digital space leading to a dilution of finite resources when the future UK economy depends on the work of a very small number of key individuals.

Question 12: Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?

- [12.1] The regulator should have no powers for active cyber defence. However, they should have the ability to work with the NCSC and GCHQ supported by the SCA to direct the existing work of their active cyber defence teams to those organisations, sites and resources that create harm. Otherwise there is a danger that a regulator inadvertently undermines the activities of parallel actions being taken by the police and intelligence agencies.

Question 13: Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

- [13.1] Yes but… There is a strong likelihood that the UK public will expect access to on-line services provided by companies that have no interest in meeting these requirements. In such circumstances, the regulator and associated government departments might be directly perceived to be blocking technological innovation. Any revision to the consultation should clearly explain how such situations might be handled.

Question 14: In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

- [14.1] Strongly yes (see previous answers).

Question 14a: If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?

- [14a.1] In general, the consultation lays out some strong ideas but it lacks detail in terms of the areas of conflict that are likely to arise between the regulator, companies and the UK public; for instance over the definition of privacy or the emerging services that might be in scope. This is yet another example – as in previous sections, I would look at the appeal mechanisms provided by Ofcom but also the CAA and HSE to determine the 'best fit' with tried and tested mechanisms that are also applicable to digital technologies in a highly dynamic marketplace.

Question 14b: If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

- [14b.1] It seems likely that principles will require considerable interpretation to particular instances within the very wide scope of the proposals. It also seems that some principles may not be applicable to some legitimate services – this has already been seen in, for example the NIS CAF framework established by NCSC where cyber security indicators of good practice are having to be refined by individual industries because they are simply too general as principles. The 'merit' based approach carries much weight until there is something resembling a case law that can develop in step with the digial markets.

Question 15: What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

- [15.1] Government must defend funding for UK Computing research which is leading most of the technological 'safety measures' cited in the supporting documents for this consultation. The potential loss of access to European funding sources and the uncertainty for many leading researchers over recent months has had a damaging effects in the core areas identified here and these need to be redressed.
- [15.2] It is important not simply to focus on algorithmic interventions. Many of the issues raised by the consultation are socio-technical in nature and require input from a range of disciplines. For example, some of the technologies identified in the consultation have suffered from 'false positives' leading to the suppression of sites that contained legitimate material. It is also the case that the evolving use of digital technologies means that there will always be 'false negatives' where the use of machine learning lacks appropriate training sets to identify new forms of terrorist or pornographic material. Hence it is likely that we will need to supplement the safety measures with human intervention at least in the short to medium term.
- [15.3] It is essential that all work in this area coordinated with NCSC.

Question 16: What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

- [16.1] Like the terms 'proportionate' and 'risk based' – 'by design' is over-used in recent consultations. Too often there is a lack of understanding of the implications of this approach to software engineering. Typically, to achieve safety or security by design it is necessary to place additional constraints on companies and engineers. For instance, by following particular processes or by using particular technological features, including APIs and libraries. This can be entirely appropriate but it can also stifle innovation and lead to a form of myopia that fails to challenge whether the 'by design' approach really does offer safety and security. Companies need guidance on situations where it is appropriate to innovate in areas that might not match the orthodoxy – in the US regulatory agencies handle such situations by issuing waivers to the Code of Federal Regulations – this enables Waymo and Uber to test autonomous vehicles under the National Highway Traffic Safety Administration or drones within the National Air Space under the US FAA.

Question 17: Should the government be doing more to help people manage their own and their children's online safety and, if so, what?

- [17.1] Yes but this should be the subject of sustained research – not simply into the safety technologies but also the socio-technical aspects of risk communication in a digital age.

Question 18: What, if any, role should the regulator have in relation to education and awareness activity?

- [18.1] There are significant opportunities for the regulator to set the direction for UK computing research to provide the evidence base that is needed to ensure any public money achieves a measurable effect in these areas. UK research also acts as a bridge between government agencies and wider education bodies – the direct relationship with government has not always been good.