Response to Call for Evidence –

House of Lords

SELECT COMMITTEE ON COMMUNICATIONS

The Internet:
To Regulate or Not To Regulate?

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 to Questions

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

[Paragraph 1] We would like to clarify confusion in the use of the term Internet; which refers both to the technical infrastructure - concerned with addressing hierarchies, routing policies, domain naming service, and other elements of the communications infrastructure – and the content and higher-level (web) applications delivered over that infrastructure. Attempts to regulate the latter are constrained by the open policies that dominate the former. For example, placing restrictions on Internet applications in the UK may only encourage people to manipulate the internal mechanisms to hide their location or to access those applications within the UK in ways that cannot easily be monitored or detected. We would encourage subsequent enquiries to honour this distinction in the usage of the term in such a vital area for the future of our connected nation.

[Paragraph 2] With this distinction between Internet infrastructures and Internet applications in mind, and in response to question 1, we note two different responses in different areas of industry. Large US Web application service providers (Google, Facebook, Amazon, Twitter, etc.) tend to argue in favour of the status quo; supporting 'net neutrality'. In contrast, the large telecom providers tend to argue in favour of regulation. This is not antithetical. Regulation may be necessary at the application level to ensure social goods: privacy, free speech etc., while Net neutrality sustains the Internet "pipes" and end-to-end communication service. In technical terms, we see a regulatory divide at the boundary between end-to-end Internet connectivity (in more technical terms the equivalent of the OSI Transport Layer) and the content and higher-level (e.g., web) applications

[Paragraph 3] The greatest danger is that the conflation of these different usages of the term 'Internet' create a regulatory environment in which it is possible for businesses to "own" vertical slices that control both application level services and the underlying communications infrastructures to the possible detriment of their competitors.

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

[Paragraph 4] Such a question cannot be answered except in terms of high-level principles that must be interpreted by a court of law or by devolving responsibility through a regulatory body/ombudsman similar to the Independent Supervisory Authority described in the General Data Protection Regulation (GDPR). The dynamic nature of Internet services makes it very difficult to draft detailed definitions of legal liability in this area. This creates concerns that law may be misapplied in a context that was never intended by those developing the original legislation.

[Paragraph 5] The existing organisations lack the resources to support the implementation of even existing legislation in any but the most extreme cases. Evidence for this can be provided through a research project led by our members[1]. The fast-changing nature of Internet communication and the number of people accessing shared resources around the globe undermine attempts by police, councils, news agencies, anti-harassment organisations, anti-bullying groups and schools to combat inflammatory, antagonistic or provocative material. ***Any regulatory agency must be adequately resourced to address existing public concerns and support those agencies already struggling to respond to complaints about Internet content.***

[1] The ESRC Digital Wildfire project[1] was an interdisciplinary collaboration between the Universities of Oxford, Warwick, Cardiff and De Montfort, see http://www.digitalwildfire.org/

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

[Paragraph 6] Existing platforms provide few or no guarantees over moderation. Most rely on self-moderation with explicit procedures only being activated after complaints are received. We also recognise widespread dissatisfaction at the result of requests for intervention. However, we recognise that this area is changing; for example, as a result of Mr Justice Warby's ruling in the High Court over the 'right to be forgotten' and as a result of GDPR (Article 16 on the right to rectification, Article 17 on the right to be forgotten).

[Paragraph 7] We recommend a code of practice that explicitly promotes transparency in moderation and provides a reference point for best practice. We do not advocate legislation for the reasons mentioned previously (see paragraph 4).

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

[Paragraph 8] On-line communities play a strong role in maintaining standards and this should be recognised. However, we cannot rely on them. These communities often reflect the particular interests of a subset of users. They often do not reflect the norms and values of society as a whole. There are tensions between the necessity to support free speech, the corrosive impact of perceived censorship and the need to safeguard expectations of public behaviour. A regulatory organisation, armed with a code of conduct, could mirror some aspects of the National Cyber Security Centre's work in educating on-line communities and providing case studies of the negative consequences of failing to act before an incident takes place.

5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

[Paragraph 9] This has been addressed in previous paragraphs. However, a transparent approach to moderation should be adopted – in line with a proposed code of conduct. We would also recommend that such policies by proportionate to the changing audiences – for example, the operators of online platforms should employ more active moderation in applications that attract a school-aged audience.

6. What information should online platforms provide to users about the use of their personal data?

[Paragraph 10] This is largely covered by GDPR but the public understanding of this directive remains very poor. As mentioned in paragraph 8, we welcome a strengthened regulatory organisation with responsibility for informing the public about their rights in this respect and also to ensure companies meet public expectations. This is an imperative if we are to go beyond the present difficult situation in which it takes a major breach of trust before many users realise the possible applications for the data they provided in response to on-line quizzes etc.

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

[Paragraph 11] Programmers often like to think that the algorithms they develop are "neutral". In practice they can create biases – e.g. in page ranks or what kinds of posts dominate social media streams. These influences are often subtle and unintended. There is a need for basic research to develop metrics and methods to discover these biases so that we can make developers more aware of the potential dangers. Similar comments can also be made about companies that deliberately seek to exploit these biases; as recent events have shown.

[Paragraph 12] There is a natural reluctance for companies to disclose IPR – it is important that UK legislation does not stifle innovation in the provision of data services that have the prospect of offering significant prosperity and public good. There is also a concern that the UK should not develop legislation that can simply be avoided by technical innovation in the underpinnings of the Internet – for instance through moving servers to other jurisdictions. Equally, for responsible operators, the proposed code of conduct could be associated with a traffic light system or some other suitable visualisation to help members of the public identify the degree of protection and moderations supported by a particular platform. We do not wish online platforms to divulge implementation details or innovative aspects of the algorithms they use. They ought to be more receptive to criticisms about any bias or dominance that the algorithms are observed to introduce into their results – and that an appropriate regulator might have the power to go and negotiate if and when users or relevant bodies complain.

8. What is the impact of the dominance of a small number of online platforms in certain online markets?

[Paragraph 13] This call is timely – it comes at a moment of significant change in the public perception of these dominant on-line service providers. It remains to be seen how they will respond. There is a concern, noted in paragraph 11, that some of these providers are responding by limiting third party access to all of their data – even when it is anonymous and appropriately aggregated. We should not underestimate the negative impact of these restrictions when, for instance, researchers are developing ways to speed the response and increasing

information available during emergencies using the information provided by the public through social media. There is a need for more and better informed public discourse about the risks and benefits of data sharing – for what purposes and with what level of guarantees of anonymity.

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

[Paragraph 14] This depends on the extent to which courts recognise each other's jurisdiction and to which UK legislation diverges from that across Europe. This submission has focussed on 'soft measures' – on a code of practiced and on informing companies and the public of expectations of behaviour. More stringent enforcement may be futile because of the dichotomy noted in paragraph 1: the application layer, which is the focus of public concern, is supported by technical infrastructures that do not obey geographical borders or legal jurisdictions. The costs of enforcement are likely, in such cases, to outweigh the public good.