Submission to House of Lords Select Committee on Communications Inquiry:

"The Internet: to regulate or not to regulate?"

NINSO (The Northumbria Internet & Society Research Interest Group)[1]

Summary	
1.	• An assessment of existing laws and regulatory approaches should be undertaken. Existing regulation should then be amended, taking an evidence-based approach • There should be consideration of online norms and the role of the law in shaping norms • Education must be a key consideration
2.	• A tailored approach should be applied with reference to size, resources, technical means and content • Determination of liability should go beyond the 'notice and takedown' mechanism • A platform should be liable where it has knowledge of unlawful content or the technical means to ensure legality
3.	• Moderation processes are generally opaque • There are limited options available for individuals who disagree with a platform's decision • Alternative systems include an online optional dispute resolution platform • A tailored approach to platforms is required based on size and resources
4.	• Users should be responsibilised; education should be integrated as part of the online user experience • Users could establish and maintain online norms • Large organisations could consider introducing a review panel composed of independent users
5.	• The right to privacy should also be protected by any measures introduced • Measures should be appropriate to the resources of the platform • Additional safeguards should be introduced to protect children • Education must be a key consideration
6.	• A summary of key information should be provided followed by a detailed explanation • The method of informing users is of equal importance • Platforms must ensure a level of clarity sufficient for users to make a clear choice • The issues of power imbalance and genuine choice should be given consideration • Education must, again, be a key consideration
7.	• Adherence to principles of fairness, accountability, transparency, privacy and user-friendliness is required • The algorithm should be disclosed in full in certain circumstances
8.	• The issue of power imbalance between the user and the platform should be considered • A holistic approach should be applied
9.	• The existing jurisdictional problem of fragmentation of internet laws is likely to be worsened • The UK cannot afford a fundamental divergence from the EU position on matters including cross border transfer, geo-blocking and portability of digital content • Participation in relevant EU initiatives should be considered

[1] NINSO (The Northumbria Internet & Society Research Interest Group) is multidisciplinary enterprise consisting of researchers from law, business, social sciences, computer science, engineering, and architecture, with a research interest at the intersection of internet and society. For more information please see: https://www.northumbria.ac.uk/about-us/academic-departments/northumbria-law-school/law-research/ninso-the-northumbria-internet-and-society-research-interest-group/

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

1.1. The scope of this question appears to be very broad. It is considered noteworthy that the question asks whether it is necessary to introduce specific regulation for the 'internet' whilst subsequent questions refer to 'online platforms'. If the intention is to regulate 'the internet' then this is clearly more complex than regulating a specific part of the internet; very different issues are raised when one considers the different types of online platforms now available (for example: large social media entities such as Facebook, Instagram and Snapchat; sites which offer opportunities to buy online including Amazon, eBay; online gaming sites; dating applications; discussion forums, websites and social media pages operated by individuals to allow other members of a sporting club or village to gain information about interests of specific relevance to that group). There is no 'one size fits all' answer that can be applied to all of these platforms and a tailored approach is necessary.

1.2. In addition, the scope of any regulation should be considered in order to ensure a more focused application. In 2014/5 the HL Communications Committee report published on social media and criminal offences considered, at that time, that the criminal law was generally appropriate for the prosecution of offences committed using social media. It is therefore queried whether the intended scope of the current call for evidence is focused on civil regulation. This would make the project more manageable and seems sensible, though consideration should be given to the intended approach (e.g. from the standpoint of ecommerce or for the protection of individuals, or both).

1.3. In answer to the question of whether it is desirable or possible to regulate the internet, it is submitted that the internet is already heavily regulated in the UK where there exists, for example, the ICO in relation to online data protection and privacy; Ofcom in respect of online streaming services and ASA with regard to online advertising standards. The first step should be to collect all existing laws and regulations and assess whether they are consistent. Secondly, one should try and take a holistic, evidence-based approach and amend existing laws accordingly.

1.4. Whilst regulation should be kept to a minimum, not all regulation stifles innovation. Regulation is fundamental when it is industry practice to violate fundamental rights by contractual means (e.g. privacy and consumer protection). More evidence is needed to assess which of the following approaches is the ideal one: regulation, co-regulation, or self-regulation. In regulating, one should keep in mind the inherent jurisdictional problem; therefore, emphasis should be given to private international law and conventional initiatives.

1.5. Whilst it may be appropriate to regulate some aspects, it may be less appropriate to impose strict rules in respect of others. Two particular issues for consideration are set out as follows:

1.5.1. *How information is used by online platforms and those who offer services via the internet***.**

It is arguable that this is an area which both should and could be subject to regulation. Whilst arguably these platforms are already subject to data protection regulation, the recent issues with Facebook and Cambridge Analytica suggest there is scope for greater regulation of the use of individual's personal data. One particularly significant issue that has been identified is that there is a substantial power imbalance between users and the operators of online platforms. Users frequently have no capacity to moderate terms but instead have the 'choice' of accepting all terms (which might include giving away significant amounts of personal data) or simply not using the service. This is not providing a real choice. Alternative models are explored below at 6.3.

1.5.2. *How the rights of individuals to exercise their rights to freedom of expression are balanced with the rights of individuals whose information is posted online, particularly where that information is posted online without their knowledge or consent*.

The heavy censorship of countries, such as China and Bahrain, is not considered desirable. However, it is suggested that consideration does need to be given to ensuring that there is effective regulation in place to enable individuals to challenge a breach of their right to privacy. There are potentially difficulties in regulating the speech of individuals given the global nature of the internet. However, the case of PJS v Newsgroup Newspapers (2016) suggests that to some extent legal regulation of the internet can be effective even in the face of worldwide disclosures.[2] The bigger issue here, perhaps, is not, however, a lack of regulation. As noted above data protection regulation already exists. As the Information Commissioner has made clear, however, they will not consider complaints made by individuals against other individuals who have posted information online in a personal capacity. This is at odds with the approach in many other European countries.[3] It is, however, a pragmatic response to limited resources.[4] By contrast, recent empirical research, whereby a group of 45 parents were asked about their knowledge and understanding of the law and how it could be used to protect their family's privacy suggests that many individuals already believe that regulations exist which would allow them to request the deletion of online posts which they have not consented to.

1.6. Reference is made in the call to the comments in the Government's Internet Safety Strategy that 'what is unacceptable offline should be unacceptable online'. This is not disputed. What

[2] *PJS v Newsgroup Newspapers* [2016] UKSC 26

[3] See: David Erdos 'Beyond having a domestic: Regulatory interpretation of European Data Protection Law and Individual Publication' Computer Law and Security Review (2017) 33(3) 275-297

[4] See: ICO, Social Networking and Online Forums – When does the DPA apply? https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf [accessed 4 May 2018]; and
The Law Society and others v Rick Kordowski [2011] EWHC 3185 (QB))

needs to be considered, however, is whether, in fact, in some situations, a greater level of regulation is needed in the online sphere than in the offline sphere. In interviews with parents, a significant number of parents expressed concern that the impact of online disclosure is significantly greater and longer lasting than offline disclosure. It was clear from these interviews that what some individuals find unacceptable online they may in fact consider to be acceptable (or treat as mere gossip) offline. By contrast, however, some individuals, who are regular users of online platforms may be happier for information to be disclosed online. The extent of technology use, the extent to which users trust those with whom they associate online, age of users, anonymity of platforms etc. are all relevant to individuals' views. So many people use the internet in so many different ways it may be difficult to establish a 'norm'.

1.7. Before any decision can be made about regulation, therefore, careful consideration needs to be given to what online 'norms' are and the role that the law plays in shaping norms. As noted above many individuals believe that they should be able to control what information is posted about them online; they understand that they already have a right to redress where posts are made without consent. There is therefore an issue not only of regulation here but also of providing guidance to individuals and managing expectations.

1.8. It is submitted that one of the key concerns should be education and raising of awareness so that individuals have a clearer understanding of the control over personal data and possible redress available (especially in light of the GDPR). This is considered in more detail below at 6.

1.9. The importance of education also extends to the organisations which process the data, to which education on safe working practices, existing laws on privacy, freedoms, crime etc. should be provided. This could also be combined with a code of practice guided by a set of principles that include respecting and using personal data appropriately, making sure people understand the rules that apply to them when they're online and putting in place protections to keep people safe online. This should also ultimately contribute to a system of compliance based on the key concept of 'privacy by design'.

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

2.1. Again, a 'one size fits all' solution would not be suitable for every platform and a tailored approach would be more appropriate taking into account the size, technical means and resources of the platform. A similarly tailored approach should also be applied to different content, with more extreme content necessitating more extreme measures. Online platforms should be liable not merely for illegal contact but more generally should be liable for unlawful content i.e. posts that defame, breach privacy laws including the provisions of the GDPR, result in nuisance of harassment and the violation of copyright.

2.2. Determination of liability should go beyond the 'notice and takedown' mechanism; a platform should be liable if it has knowledge of the unlawful content or it has the technical means and resources to ensure the legality of the activities carried out on the platform while striking a balance between the different interests involved, including freedom of expression. Platforms which de facto or de jure monitor users cannot invoke immunity (so-called safe harbours).

2.3. If content is from third party sites, then it should not be the responsibility of the content provider platform; accountability should lie squarely on those generating the content in the first instance. As mentioned above, however, if content provider is aware of the inappropriate content then they should have the responsibility of removing content.

2.4. Consideration should be given to issues regarding policing of sites, reduction in privacy, freedom of expression and information.[5] Moreover, there should also be consideration of whether contract law at its current state is sufficient to establish liability between content providers, online platform/interface, host, ISP, site and app developers. Potential standardization of terms of service for ISPs and search engines used within a jurisdiction could provide a consistent and transparent system in disclosing information held/monitored and how the site will process these. The GDPR will be of value in this regard.

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?**

3.1. At present, online platforms are often over-effective when it comes to intellectual property infringement and non-effective when it comes to other forms of content, for example in relation to terrorism.

3.2. Furthermore, moderation is often opaque and one of the real issues that users face is a lack of guidance as to what policies online platforms operate. Even when platforms do provide an accessible policy it is not helpful to the ordinary individual and indeed may be considered misleading. As an example of this, see Facebook's community standards page which states that 'you may not publish the personal information of others without their consent.'[6] Many individuals do, of course, publish other individuals' personal information without consent, for example when posting photographs. Facebook states elsewhere that it 'provides people with ways to report photos and videos that they believe to be in violation of their privacy rights. We'll remove photos and videos that you report as unauthorized if this is required by relevant privacy laws in your country.'[7] Since few people know what the actual legal position is, it will not be clear to the average

[5] See also E-Commerce Directive Art 12, 13, 14;
Digital Content Directive; Digital Single Market; European E-Commerce Reforms 2018
[6] Facebook Community Standards https://www.facebook.com/communitystandards/ [accessed 4 May 2018]
[7] Facebook Image Privacy Rights https://www.facebook.com/help/428478523862899 [accessed 4 May 2018]

individual whether or not they have a right to seek removal of a photograph and such a statement is not, therefore helpful. Transparency is key in this matter; however, careful consideration should be given to how 'transparency' is defined, covering what is meant by 'effective' and 'fair' in this context.

3.3. In any event, whilst in principle online dissemination of an individual's personal information without consent might be considered to breach data protection provisions (which will of course emphasise the importance of consent still further from 25 May 2018) it appears that Facebook's position on removal of posts is far more limited, and focuses on matters such as hate speech, incitement of terrorism, but not a photo of mundane activities in ordinary life[8]. This is perhaps understandable given the EU position as detailed in the European Commission's Recommendation of 1.3.2018 on measures to effectively tackle illegal content online[9] and the Information Commissioner's current approach to the DPA and social media as detailed above at 1.5.2.

3.4. There are of course issues with online platforms 'self-policing'. At present there are limited options for individuals who disagree with the decision of a social media giant unless they have the financial capacity to bring court proceedings. In terms of remedies, an online optional dispute resolution platform managed by a trusted independent third party should be available. This should not replace judicial redress. It should be recognised that most of the decisions taken in this context fall under the GDPR, Article 22. However, it is crucial to make sure that remedies are available also beyond the GDPR, e.g. when no personal data is processed or if the decision is not solely automated. A task force with members of the national Data Protection Authority and of the Consumer Protection Authorities should oversee this (though again the current stance of the ICO to the Data Protection Act and social media poses problems). A further alternative might be to adopt the suggestion made by the Children's Commissioner to put in place a children's digital ombudsman, to mediate between under 18s and social media companies, and/or to put in place a digital ombudsman to support any individual.[10]

3.5. It must not be forgotten, of course, that there are many different types of online platforms including smaller platforms, for example websites operated by sporting groups or from community interest, which will also operate their own moderation policies. Online platforms vary widely in how they have been developed, their functionality and what their objectives are, and each have various business models for operation. Given that such groups will rarely be able to benefit from the legal

[8] See for example: Revealed: Facebook's internal rulebook on sex, terrorism and violence https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence [accessed 4 May 2018]

[9] Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177)

[10] Growing Up Digital, A Report of the Growing Up Digital Taskforce (2017) https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf [accessed 4 May 2018]

advice available to large corporations, a tailored approach to regulation or at least guidance for such groups would undoubtedly be helpful.

3.6. The agenda should be evidence-based and research-informed; therefore, academics should play an important role and should be consulted.

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

4.1. Users should be reasonably responsibilised. Long, unfair, and opaque privacy policies and usage guidelines are not a good way to achieve this. Education and advice should become integrated as part of the online user experience reminding users of the privacy options available. Users should also be held responsible and accountable to adhere to age restrictions, publishing content that is appropriate/inappropriate such as photographs, messages that are libellous, offensive, illegal, damage to reputation, bullying and humiliating.

4.2. In addition, it might be seen as appropriate for users to establish and maintain online community standards (acting together as part of a responsible community). The difficulty in the online sphere is that we have yet to see the establishment of norms of disclosure i.e. what it is appropriate to disclose online, as discussed above at 1.7.

4.3. There is again a distinction to be made between the establishment of standards on platforms operated by large corporate entities and small sites. Even on smaller sites, however, significant differences of opinion are often evident between the moderators of such sites. On bigger sites one possibility that might be considered could be a review panel composed of independent users, who vote and report on decisions which have been appealed by a user of the site. Consideration would need to be given to the definition of the users appointed, the method of appointment and the steps that should be introduced to ensure that membership registration is a legitimate attempt to join the site and not merely an attempt to exert influence over standards and their enforcement. Matters such as diversity, bias, confidentiality and relevance should also feed into the discussion.

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

5.1. This is a very broad question. Online safety and freedom of information are very different issues and would require very different measures. Furthermore, it is interesting that this question focuses on freedom of expression and freedom of information yet makes no reference to rights to privacy. Rights to privacy should be considered alongside and recognised to be of the same fundamental importance as rights to freedom of expression.

5.2. Moreover, it is important that measures differ depending on the resources of the platform. Regulatory initiatives should be taken bearing in mind the risks of over-protection of certain interests (e.g. IP holders). In no instance, however, should platforms be allowed to invoke

immunities based on the lack of knowledge if they carry out forms of private surveillance e.g. for advertising purposes. Preventive measures should be a last resort and they should have a sound empirical basis.

5.3. As noted above specific consideration needs to be given to the rights and vulnerabilities of children, who would benefit from the support of their own digital ombudsman. It is suggested, however, that additional consideration needs to be given by large platforms to whether a user is a child and indeed whether a post relates to a child. A duty of care might for example be imposed upon large organisations with significant resources, such as Facebook, Instagram, Snapchat, Twitter, with, for example, privacy settings being set to respect privacy, as a default, when images or information relate to young children with a limitation also imposed on the extent to which information and images relating to that child can be copied, re-contextualised or disseminated further.

5.4. An alternative measure, which may be easier to implement, could be to incorporate a system whereby a user receives a pop-up message each time information featuring an individual's image is shared, which informs and reminds the user of the rights, restrictions and obligations in relation to data privacy. This method also strikes a balance between privacy and freedom of expression through the use of 'nudges' rather than more severe methods such as filtering, censoring or blocking of content.

5.5. Clearly, the importance of educating users should be integral when incorporating the concept of privacy by design.

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

6.1. It is important that individuals are provided with a summary of the type of data collected, the purposes for which every type of data is collected, how the data is processed and the third parties with whom the data is shared. The summary should be followed by a thorough explanation of all the data collected in compliance with the GDPR. Separate information is required for sensitive personal information, for example data regarding religious beliefs. The explanation should also describe the data which is provided by the individual directly, collected through use of the platform and inferred through further profiling and automated decision making.

6.2. It is equally as important, however, to consider how the information is delivered to individuals. In line with the requirement for privacy by design, the terms of service and privacy policies must be clear and easy to understand. Videos and infographics are goods ways to convey complex information such as this. The keywords should be in bold. The text should be readable, i.e. coefficient 8 Flesch-Kincaid. This policy should also comply with the Unfair Terms regime. Ultimately, the information should be delivered with a level of clarity that is sufficient to enable users to make an informed choice.

6.3. The concept of choice, as discussed above at 1.5.1 is an important issue which needs to be addressed. It is arguable whether users have a genuine choice as to whether to consent to processing given that, oftentimes, users are faced with the option of providing consent (which might include giving away significant amounts of personal data) or simply not being permitted to access the service, with no capacity to moderate the terms. Alternative models include:

- **i.** no data collection beyond collection of data needed for the user to receive the service;
- **ii.** default position is no data collection but data collection is possible with the user's explicit, valid, fully informed consent;
- **iii.** data collection is possible only upon payment to the individual; or
- **iv.** no data collection upon payment of a premium, free service individuals agree to provide data (this is not a model we support since it disadvantages the marginalised.

6.4. In any event more emphasis should again be placed on education and raising awareness of rights in relation to data minimisation. Again, privacy by design is an important principle in this regard.

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

7.1. Online platforms must adhere to principles of fairness, accountability, transparency, privacy and user-friendliness in relation to how decisions are made and the reasoning behind decisions. Article 22 of the GDPR can go to some lengths to determine these but not completely, particularly if machines are capable of self-learning.

7.2. There are also circumstances where a technical document which includes the algorithm used and a mere explanation of the logic in mathematical terms will not arguably meet the legal requirement under Article 22 of the GDPR. For example, in the context of court proceedings which are subject to obligations of confidentiality, platforms should disclose the algorithms themselves if they are used to make decisions affecting their users, to allow users to obtain expert evidence and therefore ensure access to a fair trial. The GDPR should be interpreted as the disclosure of the algorithm with an explanation in layman's terms about the rationale of the decision and criteria relied upon.[11]

7.3. Algorithms should also be auditable and audited frequently by an independent body.

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

8.1. The impact can be devastating. This again relates to the significant power imbalance between the user and the large organisation, where individuals are not able to negotiate the terms and there is in effect no real 'choice' at all. This issue should be considered in combination with the risk of 'lock-

[11] Guido Noto La Diega, 'Against the Dehumanisation of Decision-Making. Algorithmic decisions at the crossroads of Intellectual Property, Data Protection, and Freedom of Information' (2018) 9(3) JIPITEC 1

in effect' resulting from the disproportionate level of power in the hands of the oligarchy of online platforms whose business models rely heavily on the valuable currency of big data.

8.2. A holistic approach to personal data and big data, which also takes into account competition law, is necessary.

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

9.1. This is a question that can only realistically be answered once it is clear what shape Brexit will take and what steps the Government will take to ensure ongoing co-operation with Europe.

9.2. In general, there is a real risk that leaving the EU will worsen the existing jurisdictional problem of fragmentation of internet laws, across IPR, ecommerce, cyber security, and competition for UK businesses.

9.3. It is submitted that the UK cannot afford to have a fundamental divergence to the EU and a solution on cross-border data transfers, geo-blocking and on the portability of digital content must be a top priority.

9.4. Consideration should also be given to whether the UK will be able to participate in relevant EU initiatives, for example the Cloud Computing initiative and DSM.