House of Lords, Select Committee on Communications, *The Internet: To Regulate or Not to Regulate?*

Summary of Response

1.The internet is too complex for a single regulatory framework. We, therefore, suggest that the current laws and regulations are kept in line with the EU laws and developed for the benefit of the open Internet, driven by human and user rights.

2. The legal liability of online platforms, remains quite low based on Article 15 of the E-Commerce Directive. This is further supported by a growing body of legal scholarship which indicates that online platforms should not be required to proactively monitor, filter and block content uploaded by their users. There is also the argument that notice and staydown measures could be incompatible with both the EU Charter and CJEU/ECtHR case law.

3. Whilst online platforms reflect efficiency in moderating content they host, the procedures in relation to transparency and fairness can be improved, particularly, in relation to appeal processes and complaints mechanisms. In this sense, the UK can also learn from the US (DMCA 1998) and some EU countries where users are notified of takedowns requests and are given the opportunity to send counter-notices reflecting 'put-back' processes.

4. In the context of users, it must be recognised that online communities whilst sharing some key characteristics with offline communities are fundamentally different in their composition, and in what is deemed as acceptable behaviour. The Internet Safety Strategy document sets out the Government's intent to improve safety online; however, simply imposing a code of conduct on online communities will not satisfy this desire. Involving users in establishing and maintaining community standards is a way forward.

5. Freedom of expression (FoE) and freedom of information (FoI) are two very important rights, which needs to be protected online although they are not the only two online rights – all rights ought to be protected. Platforms need to balance FoE rights whilst maintaining standards for content, behavior and participation rights.

6. Platforms should be attentive in relation to providing information to users as required by the GDPR 2016 and the Data Protection Bill 2017 thereby abiding by the principles of transparency and accountability. It is also essential that platforms provide information regarding the use of the deceased's data, which is currently lacking.

7. It is imperative that platforms clearly explain their business models and the manner in which they use personal data of their users, as well as the effect the processing involving algorithms can have/has on individuals. If their business model is not based on using personal data for advertising, it should still be set out in clear terms.

8. The 'Big Four' – Google, Amazon, Facebook and Apple (GAFA) will continue to have powerful influence on the way we work and live. Yet, it is not the GAFAs one should be concerned about. China's internet giants Baidu, Alibaba and Tencent (the BATs) are now taking the lead and regulation in this area will need to go beyond competition law.

9. UK's departure from the European Union raises various questions on regulation as well as deregulation. However, the confirmation that the Charter of Fundamental Rights of the European Union 2000 will be retained in UK domestic legislation after Brexit, will mean that equivalence, adequacy or compatibility of UK law will be assessed by the European Commission in view of the interpretation of UK law by the CJEU after Brexit – which is a step forward.

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

1. The internet is too complex for a single regulatory framework, as it includes the infrastructure (regulated by telecoms law and policy), standards and protocols (regulated by organisations such as the Internet Engineering Task Force, W3C and ICANN) and content (regulated at a national level, e.g. privacy, e-commerce, libel, criminal and intellectual property laws). These terms should not be confused and the focus of this inquiry should be on the regulation of content, platforms (intermediaries as they are commonly known in our scholarship), and some aspects of telecommunications law.

2. We acknowledge that the current drive to regulate the internet comes from data and ad-driven platforms with market dominance, mainly American, and being perceived as powerful enough to affect and manipulate the democratic process. Some of the issues we have seen recently, e.g. Cambridge Analytica and the US elections, relate to very different areas of law, such as electoral laws, privacy and access to information. These concerns should not result in the entire complex structure of the Internet being regulated as one entity.

3. We support the principle that "the same rules apply online and offline", but we also note that rules need to be applied in a way that takes into account the implications of technology.

4. One of the key problems is that the Internet mainly consists of private infrastructure, therefore a lot of regulatory interventions works through private companies. These companies and platforms have to make decisions about user rights, they interpret and enforce the law and courts are seen as the last resort (e.g. privacy, copyright or libel).

5. We also note that there have been numerous problems with self-regulation, especially in the area of privacy and data protection (e.g. cookies and online advertising witnessed a complete failure of industry self-regulation).

6. We, therefore, suggest that the current laws and regulations are kept in line with the EU laws, and further developed for the benefit of the open Internet, driven by human and user rights.

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

1. Laws such as libel, intellectual property and e-commerce provides provisions for liability for online platforms hosting infringing content or in violation of human or private rights. For example, the *Defamation Act 2013* (extending to England and Wales only) requires that an online platform removes infringing material when notified or requires that the website will cease to distribute, sell or exhibit material. However, this requirement becomes active following a court judgement.

2. Such provisions also exist under intellectual property laws, where following a court judgement, the infringer will be required to cease operating or host counterfeit or pirated content.

3. However, the *Defamation Act 2013* provides a defence to online platforms which can establish that it was not they who posted the comment or content. The defence is defeated if the online platform had notice of the content and was slow to respond.

4. Similarly, most online platforms will benefit from Articles 12-15 of E-Commerce Directive [1] which provides a safe harbor provision to internet intermediaries such as, hosting services platforms by offering them immunity from liability. One of the conditions for such immunity is that under Article 14 of the E-Commerce Directive intermediaries act "expeditiously to remove or to disable the information" upon obtaining the knowledge of infringement. This provides a legal base for the widely adopted practice of "notice and take down". In other words, when a person identifies an infringement of their rights – whether it be a violation of human rights (e.g. privacy) or violation of their private rights such as intellectual property laws (e.g. copyright, trade marks), the relevant person can notify the intermediaries requesting that they take down the infringing information from their platforms.

5. Whilst this appears to be an efficient mechanism, it does not always work as well in practice. In most cases, the content is removed *after the harm* has occurred. On the other hand, the use of ''notice and staydown'' measures, which involve the real time monitoring, filtering and blocking of user uploaded content can easily lead to mistakes, specifically the blocking of lawful content (false positives) or the passage of unlawful material (false negatives).

6. What is controversial is regarding how the internet intermediaries should *acquire knowledge* of illegal activity or information. At the moment, the burden on online platforms is quite low and this is in part due to Article 15 of the E-Commerce Directive, which sets out that online platforms have no general obligation to monitor all the activities which take place on their platforms. For example, in a recent case concerning *Google* the court ruled that a search engine is not expected to monitor all the activities of all their users.[2] Moreover, in *Sabam v Scarlet*[3] *Sabam v Netlog*[4] and *Mc Fadden*[5] the CJEU found that notice and staydown measures, which involved the real time monitoring, filtering and blocking of user uploaded content failed to strike the right balance between, on the one hand, rightholders' rights, and on the other, internet intermediaries and users' rights. The use of unregulated private sector surveillance and censorship of information would also be incompatible with the ECtHR case-law - see for instance *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017). Equally, the notice and staydown approach has also been heavily criticised by the UN Special Rapporteur on Freedom of Expression for its total disregard of human rights (see Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda at pg 2).

7. On the one hand, academics such as, Mendis[6] and Lucas-Schloetter[7] argue that this is an area that needs consideration and the online platforms should be placed with a higher burden to monitor users' activities such as, relying on notice and staydown measures. They claim that there has to be a greater burden on online platforms to moderate harmful content and the legal liability for online platforms should differ according to the harm suffered. The more prominent online platforms have software to detect material that is deemed harmful and therefore will not be posted. Such measures should be adopted by all online platforms thereby making a distinction between avoiding harm on the one hand and bearing the liability in accordance with the harm caused due to lack of swift action on the part of the online platform.

8. Conversely, a growing body of legal scholarship has warned of the risks and challenges associated with content recognition and filtering systems. They argue that under Article 14 and 15 of the E-Commerce Directive, EU law and CJEU case law, online platforms should not be required to proactively monitor, filter and block content uploaded by their users.[8] Equally, Member States have argued that notice and staydown measures could be incompatible with both the EU Charter and CJEU case-law. For example, Belgium, Czech Republic, Finland, Hungary, Ireland, the Netherlands[9] and Germany[10] have claimed that in *Sabam v Netlog* and *Sabam v Scarlet* the CJEU declined to impose a duty on service providers to automatically monitor the contents disseminated by their users on the basis of Articles 8, 11 and 16 of the Charter. Additionally, current research has found that notice and staydown measures could also violate the rights of online platforms and users under Articles 6, 8 and 10 of the European Convention on Human Rights.[11]

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?

1. When signing up to the use of online platforms, users inadvertently, sign up to various terms and conditions – which for most users can be confusing and complex and may not always be clear to the average user. Yet, when an issue arises, an online platform can point to the terms and conditions, with ease.

2. In 2015, a commissioned report for the UK Intellectual Property Office exploring online platforms and user behaviour in the context of platforms dedicated to the sharing of 3D files, established that 65% of users did not license their work, leaving their creations vulnerable and open to infringement whilst losing the ability to claim authorship (Mendis and Secchi, 2015) [12]. When an issue arose in relation to the copyright content, the online platforms considered in this Study were able to point to their terms and conditions and user agreements, thereby avoiding liability for the content that they host. Therefore, *transparency* could be improved.

3. This could be achieved by online platforms providing more awareness and understanding of their terms and conditions, and offer it in a manner that is more user friendly. For example, the nuances relating to each licence, could be explained in clear and simple language, rather than simply ‘encouraging’ the user to adopt a particular type of licence.

4. In terms of efficiency, online platforms have a legal liability to take swift measures to stop an infringing activity, rather than resorting to court procedures. However, there is no quantified requirement from statutes or jurisprudence regarding how *quickly* the information should be removed upon obtaining such knowledge. In practice, internet intermediaries tend to swiftly respond and remove the infringing information. For example, in the case of counterfeited goods, intermediaries have been known to remove the material within three days or even shorter.

5. With regard to appeal processes, users should be provided with complaint mechanisms in the case of disputes and any technical solution should also be compatible with the rights of online platforms and users to a fair trial under Article 6 of the European Convention on Human Rights. Specifically, pursuant to the Strasbourg Court equality of arms principle, online

platforms should be required to quickly notify users when material that they generated, uploaded or host might be subject to a technical measure.[13] Moreover, following this principle, users should also be given an opportunity to respond to any technical measure.[14] For instance, as in the US (DMCA 1998) and some EU countries, users should be notified of takedowns requests and be given the opportunity to send counter-notices to the service provider requesting that their uploaded content be reinstated, thereby relying on 'put-back' processes. The courts or the data protection supervisory authorities such as, the Information Commissioner's Office could be responsible for overseeing this - in this context see eg Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [123]; and *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [122].

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

1. It must be recognised that online communities whilst sharing some key characteristics with offline communities are fundamentally different in their composition, [15] and in what is deemed as acceptable behaviour. It would therefore be a mistake to try and impose one set of standards on all online communities but also to expect that they will adopt the same standards in respect of behaviour that we see offline.

2. Where considerations of user involvement in establishing and setting standards for content and behaviour are made, this is in itself likely to mean that there are different standards for each online platform. Users feel part of communities where they engage online – in some online communities, experiments concerning governance have involved users setting standards. [16]

3. Involving users in establishing and maintaining community standards should offer the opportunity to enhance the standards adopted. Ultimately, there are already standards for content and behaviour set out by social media platforms and other online communities.[17] The problem here is that users often fail to read the documents outlining these standards[18] but beyond that, where there is a contravention, then the enforcement of these standards is often problematic – in that the standards do not address the objectionable behaviour, or the platform seeks not to enforce measures against the user in contravention.[19]

4. The Internet Safety Strategy document sets out the Government's intent to improve safety online [20] – establishing and maintaining online community standards for content and behaviour should fall within that remit. However, simply imposing a code of conduct on the online communities will not satisfy this desire. The EU IT Companies Code of Conduct [21] is one aspect of establishing standards but it is only one aspect and does not involve users.

5. Given that users of these online communities are the ones who will be either upholding or breaching these standards of behaviour, it is important that their opinions be canvassed. That said, it is important to note that simply because something is offensive, it is not necessarily something which is illegal and this is a fine line which needs to be recognised in

establishing standards, and which is consistent with the established principles of freedom of expression.

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

1. Any measures adopted – such as those including reporting and reviewing – must maintain a proportionate balance between posts which are removed, and those which are upheld on the basis of being questionable but not posing a problem.

2. Simply adopting measures does not mean that the rights will be protected.

3. Freedom of Expression (FoE), and Freedom of Information (FoI) are not the only rights which ought to be protected online. All rights ought to be protected but nevertheless the FoI provisions are likely to be enhanced following the introduction of the GDPR (see below). The FoE rights need greater protections given that filtering, moderating, and muting [22] are arguably all threats to FoE online.

4. Platforms need to balance FoE rights with maintaining standards for content and behaviour, but also whilst maintaining participation rights [23] The freedom of participation is also essential for the Internet and for users of online communities / platforms and therefore this must also be considered alongside FoE and FoI.

5. It is essential that the UK does not follow the example of Germany and introduce measures replicating that of NetzDG [24] which is a direct challenge to FoE online. Such measures are not conducive to maintaining online safety whilst protecting rights. Reporting, flagging and reviewing posts and online content is the predominant method by which unacceptable content is addressed – notably through takedown steps. Whilst this does not ensure the FoE rights are upheld, it is a retrospective – and therefore reactive – approach. The current approach in terms of 'illegal content'[25] is not an ideal solution but is one which has shown results in respective of extremist content[26]. This approach could be rolled-out to incorporate an assessment of the balance between FoE / FoI and online safety.

6. Some of these measures are outside of the control of social media platforms e.g. No Hate Speech Movement[27] – there is also a place for these campaigns.

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

1. First and foremost, platforms need to provide information as required by the General Data Protection Regulation 2016 (GDPR) and the Data Protection Bill 2017 (DP Bill). Platforms need to abide by the principles of transparency and accountability, enshrined in GDPR and representing crucial changes in the revised data protection regime [28].

2. Practically, this means that they need to explain the use of personal data in a concise, transparent, intelligible and easily accessible manner, using clear and plain language [29].

This must be in it must be in writing “or by other means, including where appropriate, by electronic means”, orally if requested by a data subject as well as free of charge [30].

3. Information that need to be provided to data subject under the law include: the identity and contact details of the platform; contact details for the data protection officer; the purposes and legal basis for the processing; where legitimate interests (Article 6.1(f) GDPR) is the legal basis for the processing, the legitimate interests pursued by the data controller or a third party; categories of personal data concerned; recipients of the personal data; details of transfers to third countries and the details of the relevant safeguards; the storage period (or criteria used to determine that period), the rights of users to: access; rectification; erasure; restriction on processing; objection to processing and portability (articles 15-22 GDPR); where processing is based on consent, the right to withdraw consent at any time; he right to lodge a complaint with the ICO; whether there is a statutory or contractual requirement to provide the information or whether it is necessary to enter into a contract or whether there is an obligation to provide the information and the possible consequences of failure; the source from which the personal data originate; the existence of automated decision-making including profiling and, if applicable, meaningful information about the logic used and the significance and envisaged consequences of such processing for the user [31].

4. Practically, this could be done using innovative visualisation techniques, such as layered privacy statements/notices (link to the various categories of information which must be provided to the data subject as suggested above in order to avoid information fatigue), [32] ‘push’ and ‘pull’ notices[33] and privacy icons [34].

5. It is crucial that the UK follows standards for digital and online advertising as set by the ongoing EU reforms as well as in accordance with GDPR and consumer protection laws. It is important that platforms acknowledge relationships and overlap between these areas of law and how they affect user rights to privacy and freedom of speech. This necessity is often disregarded in practice and even in the academic discourse.

6. However, as recent scandals show (Cambridge Analytica in particular), providing all the information required by the law is far from sufficient. Platforms need to be clear as to what business model they use and what does this mean for user and their fundamental rights more generally, not limited to the right to private and family life. There should be clear prohibition of manipulative practice, akin to Cambridge Analytica, which may influence democratic processes, user autonomy and the ability to make an informed decision about their participation in social and economic processes.

7. It is also essential that intermediaries provide information regarding the use of the deceased’s data and their related policies. Many platforms lack these policies, and a lot of the existing policies are not compliant with the UK data protection, copyright and succession laws.[35] Whole identities are created and stored online, so users should be able to decide what happens to data on these platforms after they die, otherwise we risk seeing more conflicts between platforms, friends and the deceased’s family, who wish to access different accounts. All this of course notwithstanding any public interests, such as historical and archival purposes for example. This information needs to be clearly presented to users in an intelligible and simple manner, using some of the techniques described above.

8. Looking beyond data protection laws, intermediaries also need to explain how they use user data in managing requests related to copyright infringement, defamation and the law enforcement, as noted in answers to the previous questions. Some reference to the UK law should be in place here, presented in an easily understandable language, as suggested above.

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

1. Individuals may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes, including the use of AI, machine learning and algorithms. It has been evidenced that profiling may be unfair and generate discrimination, (by denying individuals access to employment opportunities, credit or insurance, or targeting them with excessively risky or costly financial products).[36] Generally, platforms need to explain their business models and the way they use personal data of their users, as well as what effect this processing can have/has on individuals. If their business model is not based on using personal data for advertising, it should still be set out in clear terms.

2. To improve transparency and address shortcoming of GDPR with regards to the use of algorithms,[37] transparency should not be limited to GDPR-related obligations only and mostly to public bodies.[38] Also, platforms should not only be requiring to provide information only about the use of purely personal data but also aggregate data they claim to be anonymous (and there is much evidence that any data can be linked back and reidentified, if adequate techniques have not been used to anonymise the data fully).[39]

3. Providing a complex mathematical explanation about how algorithms or machine-learning work is not helpful for an average user, as they would not be able to grasp the full meaning of these. Instead, platforms should consider using controller should consider using innovative solutions to provide information to their users, such as, for instance visualisation tools, simple design and adequate notices as discussed above.[40]

4. As suggested by the Article 29 Working Party, the information provided to users about profiling and automated decision-making should include for example: the categories of data that have been or will be used; why these categories are considered pertinent; how any profile used in the automated decision-making process is built; why this profile is relevant to the automated decision-making process; and how it is used for a decision concerning the user.[41]

5. In addition, it is not sufficient to explain how the decision was made but also whether there is an opportunity for a revise by a human and in its absence, why not. A user should be able to access the results, correct and challenge the decision made by an algorithm (going beyond article 22 GDPR, which focuses on automated processing ***with significant or legal effect*** on data subjects, not authorised by consent or contract, but by member state law). As suggested by Veale, Binns and Edwards, safeguards should include a meaningful right to explanation; a requirement for meaningful human involvement in certain decisions; and a right to complain and seek effective judicial redress as a result of the consequences of an automated decision.[42] We support this stance.

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

1. Frequently labelled as the ‘Big Four’ of the tech moguls, it is arguable that, in the future, Google, Amazon, Facebook and Apple (the GAFAs) will continue to have powerful influence on the way humans work and live. It is likely that the GAFAs will keep acquiring clever startups, which serve as a business alternative to the usual service in the internet era. Since 2001, Google has acquired more than two hundred startups such as, DeepMind. In 2016, Google CEO Sundar Pichai stressed that developments in AI, data management, infrastructure and

analytics would be carried out in the cloud. Similarly, in 2017, among its nine acquisitions, Amazon purchased Graphiq. This was remarkable as an AI-based tech business, which created charts relying upon searchable data sets. By the same token, according to Facebook CEO Mark Zuckerberg, AI can and should be employed to better humanity. In addition to Facebook's acquisition of Instagram, the social network's purchase of companies such as the virtual reality service Oculus clearly feed into this plan. Additionally, in 2017, of the seven purchases and teams-ups by Apple, particularly significant were the acquisitions of Lattice Data that concentrates on processing unstructured data, and Initial, a messaging virtual assistant. The latter employs natural language processing (NLP). Equally, Apple's services SensoMotoric and Regaind specialize in computer vision.[43]

2. Despite the fact that trust in these tech moguls is being questioned due to concerns regarding fake news, misuse of personal data and tax avoidance, arguably a potential next step would be for the GAFAs to leverage a mixture of customer, product and global economic data to provide economic advice and targeted product information.[44] As Fintank has noted, *'using mapping data from Google, iTunes information from Apple, social media content from Facebook and customer choices from Amazon, this vast customer insight could lead to highly personalised financial advice and solutions.'*[45]

3. However, a case can be made that it is not the GAFAS the tech moguls that one should be concerned about. China's internet giants Baidu, Alibaba and Tencent (the BATs) are now taking the lead, interacting with customers beyond China's boundaries and posing a risk to the global financial marketplace.[46] In fact, the BATs seem to be much more active and dynamic than the GAFAs.[47] Yet, if the BATs were to expand beyond Asian borders, these internet giants will need to do so under the same burdensome legal regimes, which the GAFAs work. Perhaps, whilst the GAFAs will influence the concept of global banking, financial institutions will have to move to the places in which clients spend their time that is, the GAFAs' apps. App usage largely focuses on social networks, Google and utilitarian apps like messaging and maps. Thus, in the future, banks will likely find themselves wholly engaged in the apps their clients use the most. For instance, services such as Google Maps, Facebook's Messenger and WhatsApp as well as Amazon's Alexa virtual assistant.[48]

4. We believe that these issues of dominance cannot be addressed by competition law only, as this area of law is reactive and *post factum*, and it does not take into account vendors lock-in, network externalities and economies of scale and scope. Regulation here should rather be *ex ante,* focusing on the measures that would improve interoperability and the mobility of users.

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

1. The UK government plans to exclude the Charter of Fundamental Rights of the European Union 2000 from 'EU retained law' after Brexit.[49] Instead, underlying principles and rights will continue and will be substitute reference points in pre-Brexit case-law making reference to the EU Charter.[50]

2. However, when it comes to the regulation of the internet, this raises a number of issues. For example:

- Will the UK depart from aspects of the E-commerce Directive 2000/31/EC once it is transferred into domestic law? A specific problem would be that Article 15 of Directive 2000/31/EC[51] has not been transposed into the UK E-commerce Regulations. Therefore, it will not be retained under the Withdrawal Bill. We believe that this needs to be addressed in law.
- What will the position of UK internet intermediaries be in terms of their operation in EU27? Simple incorporation of EU law as domestic law will not work as from an EU law point of view, the UK may (without a 'deal') be a third country and so an intermediary is not established in a member state.[52]

3. More generally, there will be great pressure for deregulation after Brexit. A key issue is the e-Privacy Regulation Proposal, currently discussed in the EU and the fact that the UK will exit before it comes into effect.[53]

4. Perhaps unsurprisingly, in 2017, the Lords Select Committee on the EU stressed that it was 'struck by the lack of detail' on what effect will the UK leaving the EU have on internet law.[54] In fact, the Committee warned that there was no prospect of a 'clean break' from the EU.[55] It is noteworthy that, as of 23rd April 2018, peers in the House of Lords voted by a majority of 71 opted to retain most of the Charter of Fundamental Rights of the European Union 2000 in UK domestic legislation after Brexit.[56]

5. Moreover, it should also be observed that the legally binding character of the EU Charter in 2009 did not deprive the European Convention on Human Rights 1950 of its role as a source of fundamental rights protection in the EU. The Treaty of Lisbon 2007 has paved the way to EU accession to the ECHR. However, in 2015 the Court of Justice of the European Union found that the negotiated agreement neither provided the CJEU's exclusive jurisdiction, nor sufficient protection concerning the EU's specific legal arrangements. Thus, although both the European Parliament and the European Commission stress the need for EU accession, as of today, a new draft accession agreement is still waiting.[57]

6. Furthermore, it is worth pointing out that the CJEU interprets the instruments, directives and regulations in line with the EU Charter. This means that equivalence, adequacy or compatibility of UK law will be assessed by the European Commission in view of the interpretation of UK law by the CJEU after Brexit. Accordingly, when such assessment is carried out, the CJEU case-law must be 'taken into account'.[58]

7. Importantly, in assessing the relationship between the ECHR and the EU Charter, in the CJEU decision in *Tele2/Watson*, the Advocate General Saugmandsgaard-Øe advised that, according to Article 6(3) Treaty on the European Union 2007, human rights as enshrined in the ECHR, constituted general principles of EU law. However, the AG acknowledged that since the EU had not acceded to the Convention, the latter could not be considered a legal instrument, which had been formally incorporated into the Union's law.[59] The AG elaborated that EU law did not preclude the Charter from offering more extensive protection than that available in the Convention.[60] Thus, AG Saugmandsgaard-Øe concluded that when it comes to assessing human right issues, it would not be legally correct to impose a different test on Member States such as the UK, depending on whether the ECHR or the EU Charter was being examined.[61] Indeed, in addition to *Tele2/Watson*, the CJEU ruling in *Digital Rights Ireland*[62] also reflects how the case-law of the Strasbourg and Luxembourg Court is increasingly becoming carefully 'aligned'.[63]

8. It should be noted that the European Court of Human Rights and CJEU alignment of case law appears to be also increasingly acknowledged by the UK courts – see for instance the internet law decisions in *Cartier International AG and Others v British Sky Broadcasting Limited and Others* [2014] EWHC 3354, *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2016] EWCA Civ 658 (06 July 2016), *The Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2017] EWHC 480 (Ch) (13 March 2017) and *SSHD v Watson & Others* [2018] EWCA Civ 70. Thus, in view of the above, it is perhaps arguable that the UK government would be wise to abandon its plans to scrap the EU Charter after Brexit.

---

[1] E-Commerce Directive, 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[2] Case 236/08 *Google France, Google Inc. v Louis Vuitton Malletier;* Case 237/08) *Google France SARL v Viaticum SA and Luteciel SARL*; Case C-238/08 *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others* (23 March 2010).

[3] Case 70-10 *Scarlet Extended SA v Société belge des auteurs*, *compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [53].

[4] Case 360-10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [51].

[5] Case 484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* [2016] [87].

[6] D Mendis and D Secchi, *A Legal and Empirical Study of 3D Printing Online Platforms and an Analysis of User Behaviour* (London: UK Intellectual Property Office; 2015)

[7 Lucas-Schoetter, Agnès. 2017. ‘‘Transfer of value provisions of the Draft Copyright Directive (recitals 38, 39, article 13).’’ http://www.authorsocieties.eu/uploads/Lucas-Schloetter%20Analysis%20Copyright%20Directive%20-%20EN.pdf

[8] See for instance Senftleben et al. 2017. ‘‘The Recommendation on measures to safeguard fundamental rights and the open internet in the framework of the EU Copyright Reform.’’ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3054967; Stalla-Bourdillon et al. 2016. ‘‘A brief exegesis of the proposed Copyright Directive.’’ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2875296; Angelopoulos. 2017. ‘‘On online platforms and the Commission’s new Proposal for a Directive on Copyright in the Digital Single Market.’’ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2947800; Angelopoulos and Smet. 2016. ‘Notice-and-Fair-Balance: How to reach a compromise between fundamental rights in European intermediary liability’ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944917; Giancarlo Frosio. 2017. ‘‘Reforming intermediary liability in the platform economy: a European Digital Single Market Strategy.’’ *Northwestern University Law Review* https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2912272; Bridy and Keller. 2017. ‘‘US Copyright Office Section 512 Study [Docket no 2015-7] Comments of Annermarie Bridy and Daphne Keller.’’ https://www-cdn.law.stanford.edu/wp-content/uploads/2017/08/SSRN-id2920871.pdf; Jennifer M Urban, Joe Karaganis, and Brianna L Schofield. 2016. ‘‘Notice and takedown in everyday practice.’’ *BerkeleyLaw University of California*: 1-147. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628; Evan Engstrom, and Nick Feamster. 2017. ‘‘The limits of filtering: a look at the functionality and shortcomings of content detection tools.’’ Engine: 1-32. http://www.engine.is/the-limits-of-filtering/.

[9] Council of EU. 2017. ‘‘Document 12127/17, Interinstitutional File 2016/0280 (COD), Proposal for a Directive on the European Parliament and of the Council on Copyright in the Digital Single Market – Questions by the Belgian, Czech, Finnish, Hungarian and Dutch Delegations to the Council Legal Service Regarding Article 13 and Recital 38.’’

[10] Council of EU. 2017. ‘‘Document 12291/17, Interinstitutional File 2016/0280 (COD), Proposal for a Directive on the European Parliament and of the Council on Copyright in the Digital Single Market – Questions by the German Delegation to the Council Legal Service Regarding Article 13.’’

[11] Romero-Moreno. 2018. ''Notice and staydown' and social media: Amending Article 13 of the Proposed Directive on Copyright.' *International Review of Law, Computers & Technology* (in press) - email f.romero-moreno@herts.ac.uk for a free copy.

[12] D Mendis and D Secchi, *A Legal and Empirical Study of 3D Printing Online Platforms and an Analysis of User Behaviour* (London: UK Intellectual Property Office; 2015)

[13] Refer to the Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21287&LangID=E at pg 4; see also *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [133].

[14] See Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21287&LangID=E at pg 4; see also the CJEU C-314/12 UPC *Telekabel Wien GmbH v Constantin Film Verleih GmbH and anor* [2014] All ER (D) 302 (Mar) [57].

[15] See for example, K Barker & C Baghdady, 'Building online hybrid identities' in N Lemay-Herbert and R Freedman (eds) Hybridity: Law, Culture and Development (Routledge, 2017).

[16] K Barker (2016): Virtual spaces and virtual layers - governing the ungovernable?, Information & Communications Technology Law, 25:1, 62 70; J Dibbell, 'A Rape in Cyberspace' 23 December 1993, http://www.juliandibbell.com/texts/bungle_vv.html.

[17] See for example: Twitter Rules & Policies https://help.twitter.com/en/rules-and-policies#twitter-rules.

[18] A point widely commented on e.g. D Berreby, 'Click to agree with what? No one reads terms of service, studies confirm' The Guardian, 3 March 2017 https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print.

[19] See for example, Twitter's criticism for failing to deal with hateful tweets: J Grierson, 'Twitter fails to deal with far-right abuse, anti-hate crime group tells MPs' The Guardian, 13 December 2016: https://www.theguardian.com/technology/2016/dec/13/twitter-fails-deal-farright-abuse-tell-mama-extremism-commons.

[20] HM Government, 'Internet Safety Strategy – Green Paper' October 2017.

[21] European Commission, 'European Commission and IT Companies announce Code of Conduct on illegal online hate speech' (31 May 2016) http://europa.eu/rapid/press-release_IP-16-1937_en.htm.

[22] Which are all mechanisms used by social media platforms to tackle posts and behaviour in breach of their respective terms and conditions.

[23] See for example, Internet Rights and Principles Coalition, 'The Charter of Human Rights and Principles for the Internet' (5th edn) 2018: http://internetrightsandprinciples.org/site/wp-content/uploads/2018/01/IRPC_english_5thedition.pdf.

[24] Germany's Network Enforcement Act (NetzDG) 2017. See: Beschlussempfehlung und Bericht [Resolution and Report], Deutscher Bundestag: Drucksache [BT] 18/13013, http://dipbt.bundestag.de/doc/btd/18/130/1813013.pdf; BBC News, 'Germany starts enforcing hate speech law' 1 January 2018: http://www.bbc.co.uk/news/technology-42510868

[25] EU Commission, 'Commission Recommendation on Measures to Effectively Tackle Illegal Content Online' 1 March 2018.

[26] EU Commission, 'Countering Illegal Hate Speech Online' (19 January 2018) http://europa.eu/rapid/press-release_MEMO-18-262_en.htm.

[27] No Hate Speech Movement: https://www.nohatespeechmovement.org/hate-speech-watch/focus

[28] Article 5 GDPR, related to articles 1, 11 and 15 TFEU, see also Article 29 WP Guidelines on transparency under Regulation 2016/679, WP 260, p. 5, at https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[29] Article 29 WP interprets intelligible as 'it should be understood by an average member of the intended audience' Article 29 WP Guidelines, p.7.

[30] See Articles 12-15 and 22 GDPR.

[31] Articles 13-14 GDPR and Article 29WP Guidelines on transparency, pp. 30 – 35.

[32] Article 29WP opinion p. 17; see also Office of the Australian Information Commissioner. Consultation draft: Guide to big data and the Australian Privacy Principles, 05/2016 says: "Privacy notices have to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. The very technology that leads to greater collection of personal information also presents the opportunity for more dynamic, multilayered and user centric privacy notices." https://www.oaic.gov.au/engage-with-us/consultations/guide-to-bigdata-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacyprinciples; Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0, 03/2017. Pp 87-88, March 2017. https://ico.org.uk/media/fororganisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[33] Push notices involve the provision of "just-in-time" transparency information notices while "pull" notices facilitate access to information by methods such as permission management, transparency dashboards and "learn more" tutorials. These allow for a more user-centric transparency experience for the data subject. Article 29WP Guidelines on transparency, p. 17.

[34] Article 12 GDPR Recital 166; Article 29WP Guidelines on transparency notes the need for more research around icons, p. 22 Opinion; ICO, Big data, artificial intelligence, machine learning and data protection version 2.0, pp 62-65.

[35] See e.g. Edina Harbinja, Digital Inheritance in the United Kingdom, 21 Nov 2017, *The Journal of European Consumer and Market Law (EuCML);* Harbinja, Post-mortem Privacy 2.0: Theory, law and technology, (2017) International Review of Law, Computers & Technology. 31 (1) p. 26-42.

[36] Article 29 WP, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, p. 10.

[37] Lilian Edwards and Michael Veale, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16 Duke Law & Technology Review 18 (2017); Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling, Computer Law & Security Review 34(2) 2018, 398–404, doi:10.1016/j.clsr.2017.12.002; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, 2017.

[38] Articles 13 and 14 require the controller to inform the data subject about the existence of automated decision-making, including profiling, described in Article 22(1) and (4). addressed in Articles 13 and 14 – specifically meaningful information about the logic involved, as well as the significance and envisaged consequences for the data subject), and safeguards, such as the right to obtain human intervention and the right to challenge the decision (addressed in Article 22(3)) p. 25.

[39] See President's Council of Advisors on Science and Technology. Big data and privacy. A technological perspective. White House, May 2014
http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_a

nd_privacy_-_may_2014.pdf and also El Emam, Khaled. Is it safe to anonymise data? BMJ, February 2015.

http://blogs.bmj.com/bmj/2015/02/06/khaled-el-emam-is-it-safe-to-anonymize-data/

[40] See also ICO, Big data, artificial intelligence, machine learning and data protection version 2.0, pp 87 - 88

[41] Article 29 WP, Guidelines on Automated individual decision-making and Profiling

for the purposes of Regulation 2016/679, p. 31.

[42] see Public Bill Committee, Written Evidence: Michael Veale, UCL, Dr Reuben Binns, University of Oxford, Professor Lilian Edwards, University of Strathclyde (DPB03), 14 March 2018, at https://services.parliament.uk/bills/2017-19/dataprotection/documents.html

[43] Nina Bryant, 'Blink of an AI' (ICAEW Communities, April 2018) < https://ion.icaew.com/itcounts/b/weblog/posts/blink-of-an-ai > accessed 29 April 2018.

[44] Simon Cadbury, 'Will a GAFA be your next bank' (Intelligent Environments) < https://www.intelligentenvironments.com/will-gafa-next-bank/ > accessed 29 April 2018.

[45] *Ibid*., accessed 29 April 2018.

[46] Alibaba's Ant Financial launched MyBank, a digital bank aimed at those who have restricted access to current banking systems and corporations seeking financing, in June 2015; Tencent launched WeBank, that is closely integrated with the notable Chinese instant messaging app WeChat, in January 2015; Baidu – 'the Google of China' – and partner CITIC Bank were given approval to launch a new joint banking operation last August - see *Ibid*., accessed 29 April 2018.

[47] Ant Financial is on the acquisition and expansion trail, investing directly in online wallets such as South Korea's Kakao Pay and India's Paytm, and attempting to purchase MoneyGram for $1.2bn; Tencent is leveraging WeChat to enlarge its geographic coverage; Baidu and its partners' ambitions exceed payments, with Baixin Bank leveraging Baidu's AI - see *Ibid*., accessed 29 April 2018.

[48] WeChat: China Construction Bank, Bank of China, and China Merchants Bank are just three of many banks, which have used chatbots on WeChat; Alexa: Capital One clients can manage their accounts via Amazon's voice-enabled chatbot; Facebook Messenger: Citibank's natural-language chatbot called Citi Bot permits clients to ask questions regarding their accounts, rewards and transactions - see *Ibid*., accessed 29 April 2018.

[49] Commons Library Briefing, 'Brexit and data protection' (10 October 2017) https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7838#fullreport at page 4.

[50] *Ibid*.

[51] Article 15 of the E-Commerce Directive has not been transposed in the UK E-Commerce Regulations. Thus, this means that it will not be retained under the Withdrawal Bill. However, it is important to stress that the Withdrawal Bill must 'take into account' the ECtHR and CJEU case-law. Accordingly, if Article 15 E-Commerce Directive is scrapped this would be inconsistent with the UK obligation to take into consideration the rulings of both courts. In this context see for example Case 70-10 *Scarlet Extended SA v Société belge des auteurs*, *compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4; Case 360-10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000; Case 484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* [2016]; and *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017); for an in-depth analysis of this issue see Romero-Moreno. 2018. ''Notice and staydown' and social media: Amending Article 13 of the Proposed Directive on Copyright.' *International Review of Law, Computers & Technology* (in press) - email f.romero-moreno@herts.ac.uk for a free copy.

[52] With special thanks to Professor Daithi Mac Sithigh.

[53] With special thanks to Dr Edina Harbinja.

[54] House of Lords European Union Commitee, 'Brexit: the EU data protection package' HL Paper 2017-19, 18 July 2017 https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf at pg 3.

[55] *Ibid*., at pg 51.

[56] Andrew Sparrow, 'May suffers three defeats in Lords over Brexit - as it happened' (The Guardian) < https://www.theguardian.com/politics/blog/live/2018/apr/23/brexit-no-10-rejects-claims-customs-union-vote-to-be-made-a-confidence-issue-politics-live?page=with:block-5ade16fae4b0d0cf980b8ee4 > accessed 29 April 2018.

[57] European Parliament Think Tank, 'EU accession to the European Convention on Human Rights (ECHR)' < http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282017%29607298 > accessed 29 April 2018.

[58] Oral evidence to the Select Committee on the European Union Home Affairs Sub-Committee, 1 March 2017, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48742.pdf at pg 8.

[59] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [AG 76].

[60] *Ibid*., [AG 80].

[61] *Ibid*., [AG 142].

[62] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others* [2014] WLR (D) 164.

[63] Legal opinion by the Legal Service of the European Parliament (confidential legal opinion 22 December 2014) 9 – with special thanks to Dr Sonia Morano-Foadi; for an in-depth analysis of the ECtHR and CJEU alignment of internet case-law see Romero-Moreno. 2018. ''Notice and staydown' and social media: Amending

Article 13 of the Proposed Directive on Copyright.' *International Review of Law, Computers & Technology* (in press) - email f.romero-moreno@herts.ac.uk for a free copy.

Response Prepared by:

Dr. Kim Barker, (Lecturer in Law, University of Stirling);

Dr. Edina Harbinja (Senior Lecturer in Law, University of Hertfordshire);

Prof. Dinusha Mendis (Professor of Intellectual Property & Innovation Law, Bournemouth University); and

Dr. Felipe Romero-Moreno (Lecturer in Law, University of Hertfordshire)

On behalf of the British and Irish Law, Education and Technology Association (BILETA).

Response Endorsed by:

Professor Abbe E. L. Brown, Law School, University of Aberdeen

Dr Maureen O Mapp, Lecturer in Law, Birmingham Law School, University of Birmingham

Dr Gavin Sutter, Senior Lecturer in Media Law, CCLS, School of Law, Queen Mary University of London

Bukola Faturoti, Senior Lecturer, The Law School, Robert Gordon University.