

## **Andrew Lea—written evidence (FEO0050)**

### **House of Lords Communications and Digital Committee inquiry into Freedom of Expression Online**

#### **Summary and Introduction**

1. This matter concerns the technological outworking of an ethical and philosophical issue. This submission therefore firstly outlines the ethical perspective (section 1), considers technological implications (section 2), and finally suggests measures for HMG to consider (section 3).
2. I take the libertarian position that freedom of expression is fundamental, and therefore technology should enhance, rather than stifle, that freedom. Freedom of expression on-line (and off-line) is being eroded, and it is for HMG to halt that erosion. Freedom of expression does not imply a duty to listen to others, but is balanced by a freedom to not listen.
3. I argue that technology can enable either censorship or freedom of expression. Specifically *content classification* provides the protection society needs from undesirable content without the loss of freedom that censorship brings.
4. My key recommendations are (i) that dominant micro-blog service providers should not be permitted to censor content, except for content which causes or incites predictable, objective, substantive and unlawful harm to others; (ii) to encourage service and app providers to classify content so users can avoid content they consider harmful; and (iii) a variety of measures should be taken to strengthen privacy in so far as privacy has implications on freedom of expression.
5. I am submitting this evidence in a personal capacity because as a local councillor (at Mid Sussex District Council and West Sussex County Council) I have a deep interest in freedom of expression as a foundation of democracy; as a long-term practitioner of Artificial Intelligence (and Head of AI at HelloDone Limited) I design technologies, such as text and data understanding, which could be used to enhance or frustrate on-line freedom of expression; and I am a member of the BCS' Specialist Group in Artificial Intelligence committee and have an on-going interest in the societal implications of AI.

#### **1. Ethical Basis**

6. Freedom of expression is the fundamental freedom that underpins all others, because it allows wrongs which would otherwise remain hidden to be exposed and addressed, and allows society through public debate to develop new ideas and refine existing ones. The election of governments and freedom of expression are the cornerstones of democracy. It should

therefore be restricted only where absolutely necessary to prevent direct and objective harm.

7. There is, and should never be, a “right not to be offended”. This is because my right not to be offended impinges on your right to freedom of expression, and therefore undermines that fundamental freedom. Offence is, of course, a subjective harm. Worse yet, there is the issue of who should be empowered to decide what should and should not be said: it is more power than human beings can handle.
8. Censorship, except where to prevent direct, objective, substantive and unlawful harms, is in opposition to freedom of expression. Amongst its many pitfalls is, of course, the question as to who gets to decide what may or may not be expressed. Related issues are the way in which much of the media now perceive their role to be that of forming, rather than informing, public opinion; and of the growing prevalence of “no-platforming”.
9. Alongside freedom of expression is the need to judge the provenance of the facts. We should promote the expression of genuine opinion, but oppose deliberate deception.
10. Freedom of expression does not imply a duty on others to listen to what is said; there is an equal and opposite right to not listen, or to express in turn differing views.
11. Finally, because privacy and anonymity impinge on an individual’s ability to have meaningful freedom of expression, they are included in this discussion.

## **2. Technology Implications**

### **2.1 Definitions and Principles**

12. There are two forms of **fake news**: intentional fake news, simply invented to sell; and news with which one simply disagrees and labels as fake to discredit it.
13. **Meta-data** is data about a communication or individual, and is often used in data mining.

### **2.2 Technical Impact on Freedom of Expression**

14. Whilst the internet allows undesirable influences to gain traction, it also allows people to hear the opinions of, and facts from, others in an unprecedented direct manner. This leverage is the difference between freedom of speech online and offline.
15. On-line **censorship** is escalating, and deprives individuals of the freedom of expression as well as others of a freedom to listen. Dominant and near-monopoly micro-blog and social media companies should not be allowed to

ensor content.

16. The exception is removal of that narrow band of material which causes or incites predictable objective substantive unlawful harm to others. These are the same class of materials, or expressions, which would already be illegal in the off-line world.
17. Unlike censorship, **content classification**, allowing consumers to avoid content, does not reduce freedom of expression, provided that categories are treated in a similar way. It can be readily automated for text, and is becoming increasingly viable for video or image. Automated classification can be anonymous. *Content classification can provide the protection society needs from undesirable content, whilst avoiding the loss of freedom from censorship.*
18. **Artificial Intelligence content filtering** will in general either mimic the views of those who wrote its rules, or the content on which they chose to train it. When used online to block content it is, of course, a form of automatic censorship. However, end-users can use AI under their own control to avoid receiving content they do not wish to see. This is not censorship, but the right to not listen.
19. AI could also be used to identify intentional **fake news**: fictional news deliberately made up to sell. It would not be able to do so with 100% reliability.
20. On-line **technology can enable anonymity**, and there is a balance to be struck in terms of freedom of expression. Attributed posts are of course reasonable, and so are anonymous posts provided they are labelled as such. What is not reasonable is posts with fake identities.
21. **Technology can easily violate privacy**. Several popular services go to great lengths to construct detailed profiles of their users. Whilst not a reduction in freedom of expression *per se*, it will inhibit that expression.
22. Natural language understanding can be used by services to understand, and "data mine", posts and communications of their users.

### **3. Regulations, Actions, and Enforcement**

23. Regulations should be crafted as if all forms of electronic communication were readily machine understandable, not just text and meta data, because that will soon be the case.
24. HMG should consider the following regulations and actions:-
  - 24.1. Dominant and near-monopoly micro-blog and social media companies should not in general be allowed to censor content. HMG should specify the narrow band of user generated content which may be deleted by those services, which should be those which cause or

incite predictable objective substantive unlawful harm to others, referencing the offences its distribution causes.

- 24.2. Service providers, and app developers, should be encouraged to classify material so that consumers may avoid categories they wish to avoid.
- 24.3. Anti-monopoly or unfair contract provisions should be examined to ensure that dominant suppliers are unable to insist on terms and conditions which effectively force users to agree to censorship or large scale data-mining enabled privacy violation.
- 24.4. General Data Protection Regulations might be extended to prevent data collection, even where consent is given, if it is actually unnecessary (rather than simply being mentioned in terms and conditions) and intrusive. This could be subject to a test of "what has the intrusive data item been allegedly collected for, has it been actually used, is that use itself legitimate, and was no other less intrusive data item available which would have achieved the same objective". HMG would need to define a list of "intrusive" data items, with location (except for good purpose to the benefit of the user) being an obvious example.
- 24.5. Terms and Conditions, where a consent is required, should have a clarity test: they can be written to deliberately befuddle the user into giving consent they would otherwise not. This might be achieved by having a "void for incomprehensible consent" provision in contract law.
- 24.6. The Communications Act 2003 (127.1.a) makes it an offence to use "a public electronic communications network" to send a message "that is grossly offensive or of an indecent, obscene or menacing character". This is over-broad, since the judgement of offensive is subjective and therefore restrictive of freedom of expression. It should be reduced in scope, and made to apply only to those messages which may cause or incite predictable objective substantive unlawful harm to others.
- 24.7. Law enforcement should be directed to only investigate substantive objective unlawful harms in the social media world.

*15 January 2021*