



Law Society
of Scotland

Consultation Response

Regulation of the Internet

11 May 2018



Introduction

The Law Society of Scotland is the professional body for over 11,000 Scottish solicitors. With our overarching objective of leading legal excellence, we strive to excel and to be a world-class professional body, understanding and serving the needs of our members and the public. We set and uphold standards to ensure the provision of excellent legal services and ensure the public can have confidence in Scotland's solicitor profession.

We have a statutory duty to work in the public interest, a duty which we are strongly committed to achieving through our work to promote a strong, varied and effective solicitor profession working in the interests of the public and protecting and promoting the rule of law. We seek to influence the creation of a fairer and more just society through our active engagement with the Scottish and United Kingdom Governments, Parliaments, wider stakeholders and our membership.

We welcome the opportunity to consider and respond to the House of Lords Select Committee on Communication on the consultation: The Internet: To Regulate or Not To Regulate? We have the following comments to put forward for consideration.

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

The internet continues to generate new possibilities and opportunities but also new challenges, including challenges to those concerned with regulation and protection of consumer interests across a host of areas.

However valuable the internet is, in embracing it, consumers can be exposed to risk because of the change in the business model. In moving online, the consumer did not choose to give up rights and protections and expose themselves to greater risks. Generally, they are not aware of what is "lost" or the exposure to risk.

Some, simply by circumstance, are more impacted by this change than others - those in rural areas more than in urban conurbations; vulnerable members of the community required to undertake the activity online.

Many of the potential challenges faced in a digital context arise in other contexts as well but the difficulties are compounded by the sheer scale of the online environment, the ability to capture, analyse and exploit data, including personal data, the immediacy of communications and intangible nature of entities operating in the online environment and indeed of the products they sell.

However, this does not necessarily lead to the conclusion that "the internet" needs to be regulated. Many regulatory frameworks can be applied in both an online and offline context – for examples competition law or rules governing unfair contract terms. A large part of the internet can therefore already be said to be regulated.

There is also considerable existing regulation focused specifically on digital issues. For example, the E-Commerce Directive liability regime works well; it is activity based rather than business model based. This helps to provide clarity and certainty for all parts of the ecosystem, balances rights of various stakeholders.

The better option may be not to look at “regulating the internet” but instead to test new regulation and review existing regulatory frameworks to ensure that they are applicable to digital environment. Taking a sectoral approach to regulation also guards against the unintended consequences and potential negative impact on both businesses and consumers which can come from attempting a one-size-fits-all approach to disparate areas.

Furthermore, “internet” is a very broad term and covers a huge range of different stakeholders all with different models and with different roles in the overall system. This consultation focuses issues around online platforms, which are only one aspect of the internet economy. Many are viewed positively and can offer significant benefits to both the businesses and consumers they connect. Furthermore, “online platforms” are not a homogenous group: the potential harm of one type of platform may be very different from the risks associated with another.

However, regulation to promote better business practices, may prove helpful. The European Commission has proposed a Regulation on promoting fairness and transparency for business users of online intermediation services.

Recent events also suggest that regulation of social media platforms could be an area for further investigation and consideration.

However, any change or new framework needs to be evidence-based and proportionate. There is a risk that increased, or even divergent regulation will damage UK as attractive place to set up and invest, particularly post-Brexit.

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

- Balance of interests

The crux of this issue is ensuring a fair balance of interests between the online platform, the content authors or owners, and anyone affected by that content – be it consumers/readers or natural or legal persons who form the subject of that content. This is a complex equation and policy, or political views will play a significant factor in directing where the lines should be drawn in any given situation.

- Control

Liability is usually linked to an element of control, a criterion which ties in with instinctive notions of “fairness”. It does not seem just that a person or entity should be liable for something out with its control. However, in the context of platforms this raises considerations of effective control – both in terms of the

extent of “ownership” of content and decision-making power and logistical questions around e.g. screening obligations.

There is already clear liability on online providers to act in certain circumstances – i.e. when they have actual knowledge of problem content (the so called “notice and takedown” regime). There already plenty of reports showing the amount of investment in take-down and the material that is being removed as a result. Improvements in AI etc will probably increase performance even more over coming years. This balanced regime has led to the ability for providers to invest, innovate and grow.

- Defective products

One scenario where liability arises is in relation to product sales – both tangible products and intangible ones, e.g. software downloads. In both of those situations it is important that the consumer knows who to pursue if there are problems with the goods or services they buy.

- Defamation

Another issue is where the content refers to an individual or legal person and makes false or defamatory statements about them, their products, services or business practices. Again, liability must be established to ensure access to justice and identify the person against whom a claim should be brought. However, establishing who is a primary or secondary publisher, and who should be viewed as author, editor or publisher of a particular statement, is much more complicated in an internet context. Furthermore, there is a balance to be struck in relation to protection of individual’s reputations on the one hand and freedom of expression on the other. Any regulatory framework must protect this important human right as well.

Furthermore, as we noted in our response to the Scottish Law Commission’s consultation on the draft Defamation and Malicious Communications Bill in relation to commercial publishers (specifically referred to in the draft bill), it is not clear whether for example an individual with say a YouTube channel with over 100,000 followers (not uncommon) receiving YouTube royalties would be considered a commercial publisher. We anticipate that there will be many examples similar to this where drawing a line between commercial businesses and private individuals is difficult. This is an example of an area where general legal rules should be applied but must be configured to take account of the internet environment.

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?

There is no single or simple answer to this first question and of course a wide variation in the effectiveness, fairness and transparency of online platforms in relation to moderation of the content they host. The concept of moderating content is also closely linked to questions around liability: the first must be determined before powers or duties to moderate can be properly assessed.

The processes that should be implemented for individuals who wish to reverse decisions to moderate content will depend on the nature of the content. If it relates to personal data, then many of the issues are likely to be covered by the new rules coming into force on 25 May under the GDPR.

Furthermore, as noted above duties or ability to moderate will often be linked to liability but can also impact upon freedom of expression. If you try and increase liability on providers, there is a clear and obvious danger that they will become arbiters or controllers of what we can all see. In addition to the threat this poses to freedom of expression it can also chill investment incentives and increase legal risk on providers. There is a clear danger of unintended consequences if they decided to pursue the most prudent options.

It is not clear what other situations are envisaged and the appropriate oversight body may well depend on the nature of the issue. Without further detail, it is difficult to provide a useful response to this question.

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

One option would be to create a code of conduct which users could sign up to. If they failed to comply with those standards, the platform might have a power to eject them. However, this could be difficult to monitor and enforce.

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

As noted above, there is a danger that unduly restrictive regulation could in fact result in threats to the freedom of expression and freedom of information. At the same time, to the extent that regulatory obligations are introduced which would increase the scope of liability for online platforms in respect of content, there is a risk that this could result in a potentially negative impacting freedom of speech through a reduction in available platforms or barrier to new entrants in the market. This should be considered along with other factors in assessing how to regulate platforms.

Even if platforms are not to reduce in number, the easiest way to mitigate risk by taking a restrictive approach to what they will accept as online content and remove anything which could generate complaints or be viewed as illegal eg in respect of laws governing hate speech. This is an increasingly important topic with the European Commission publishing a communication directed at tackling online abuse and enhancing the responsibility of online platforms in September 2017. However, it may be difficult to determine what is or is not hate speech: effectively delegating this responsibility to corporate entities, with no means of appeal for those whose content has been removed, has generated concerns among some human rights advocates.

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

The GDPR sets out a robust framework which should guarantee high levels of transparency and protection for personal data.

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

Businesses should be encouraged to operate in a transparent manner where this is appropriate.

We note that the European Commission is investigating how best to encourage transparency of algorithms – a concern which has already been addressed in some EU legislation.

Use of personal data in line with the requirements of the GDPR is a good example of this. GDPR does itself include obligations on being transparent about use of automated decision-making and profiling, which might go some way towards addressing the issues around algorithms.

Of particular relevance are the rules contained in Section 4 (Articles 21 and 22) which protect individuals against arbitrary application of automated decision-making processes, which may function on the basis of an algorithm or algorithms. Similarly, there are EU rules for algorithmic decisions in relation to high-frequency trading on the stock market contained within the Markets in Financial Instruments Directive (MiFID II).

We also note that certain information which does not fall within the scope of the GDPR will be commercially sensitive or might fall within the scope of trade secrets: there is, and should be, no general rule that online platforms (or any other business) should publish every detail about its businesses processes.

At the same time, online platforms, like any other business, must comply with reporting obligations and relevant regulation including competition law. There has been increasing discussion around the intersection between data, competition law, consumer protection and privacy.¹

This aligns with a growing trend for regulators generally to demand greater transparency regarding the factors that are taken into account where algorithms are used in making decisions or generating search results. The CMA's 'CARE' principles are being used to tackle this in the digital comparison tools sector to good effect, and it is certainly possible to apply these kinds of requirements with a common-sense approach avoids the need for disclosure of commercially sensitive or proprietary technical information

¹ We note in this regard that one of the CMA's annual plan objectives includes a project looking at the use of algorithms.

regarding the algorithms themselves. Incidentally, the CARE principles are a good example of the benefits of taking a sectoral approach to regulation in the internet space.

On a broader note, openness and transparency in the context of algorithms/code will likely be helped over time as a result of increasing adoption of Free and Open Source Software (FOSS). This could be encouraged through government endorsement/support of FOSS, in particular within the education context where – anecdotally – the perception is that IT education continues to focus more on closed software, which means people are more likely to continue using this as they grow up/enter the workforce.

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

A small number of online platforms in certain online markets may raise competition and consumer concerns.

If there are only a small number of online platforms in a particular market, this necessarily gives a greater level of control to that platform. There is a danger of abuse of position, particularly where the platform operator is also a goods vendor in its own right. This can manifest itself in a number of ways which centre around the ability to collect and manipulate data.

For example, a platform sells a particular category of consumer goods. It collects data on the preferences of those consumers which it can use to predict market trends. But it can also use that data to identify the best-selling products in that category at the current time. It can therefore focus on those goods, reducing storage costs for less popular products, which in turn allows it to undercut competitors using the platform. From a consumer perspective, this can lead to a reduction in the range of available products. Furthermore, it may also be used to control content e.g. where a platform sells books or magazines, it may be able to use its position to promote its own content or even influence people's political views as can be seen in some of the recent analysis of the impact of social media platforms on election choices.

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

There are many benefits we are only just beginning to see from the Digital Single Market (DSM). The regulation of the networks that provide us with internet access are regulated by a framework of directives which the UK helped develop and the successor to which - the EU Electronic Communications Code - is due to come into force just after the UK exits the EU. As such the entire system of regulation of the mechanics of the internet and the access networks in particular is about to be brought up to date in the EU but the UK risks being left behind with the 2003 rules.

The UK has played a leading role in the development of these new rules (as we did with the last major

update in 2003) so it is vital that the same or similar rules are implemented here, regardless of UK withdrawal: the UK should ensure it will not be left out of step with a 15-year-old set of rules that is no longer suitable for 2018.

Furthermore, the Prime Minister has announced that we would be leaving the DSM. Industry has stressed the importance of updating our legal frameworks using the work done to date on the DSM rather than starting afresh with the option of “U.S. style regulation” which some commentators have proposed.

Alignment with EU regulation could also offer practical advantages for UK businesses trading with the EU/EEA. One of the challenges for internet businesses that have a global user base is dealing with the patchwork of overlapping legislation emerging within different jurisdictions – retaining alignment would minimise the regulatory changes which businesses need to tackle as a result of Brexit. Furthermore, it is important not to discourage new businesses from basing themselves or trading here: again, maintaining regulatory convergence with EU rules/principles could be helpful to businesses looking to trade on a pan-European basis.

For further information, please contact:

Carolyn Thurston Smith

Policy Team

Law Society of Scotland

DD: 0131 476 8205

carolynthurstonsmith@lawscot.org.uk