The Internet: to regulate or not to regulate?

Contribution from Dr. Olivier Crépin-Leblond on behalf of the Internet Society UK Chapter
Date: 11 May 2018

The Internet Society UK Chapter was invited to speak at the House of Lords Inquiry on "The Internet: to regulate or not to regulate?"[1] on Tuesday 8th May 2018. The Chapter circulated the Inquiry to its membership base, triggering a wide range of feedback. In his spoken address, Dr. Konstantinos Komaitis, Director of Policy Development for the Internet Society, addressed many of the points raised in our local Chapter's consultation. The responses included in the present document, seen below, should serve an additional input from the Internet Society UK Chapter, drawing from the input and participation of our members as well as the years of experience in Internet regulation since its founding in 1992. Such policy papers may be consulted on https://www.Internetsociety.org/resources/policybriefs/

Overall, the Internet Society favours collaboration of all actors, to reach solutions that involve a multi-stakeholder framework. We would highly suggest reading of the Internet Society paper "Internet Governance – Why the Multi-Stakeholder Approach Works"[2].

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

The "Internet" is a very broad term, when referring to "regulation". In essence, it really depends on what "layers" one means by referencing "the Internet".

When considering regulation for the Internet it is important to distinguish between 'regulating the Internet infrastructure', i.e. the underlying communications backbone that facilitates the sending and receiving of information 'packets' (colloquially referred to as 'the pipes' and the "lower layers"), vs. 'regulating services that are built on the Internet' (e.g. media and commerce platforms and services.) which constitute the higher layers.
https://en.wikipedia.org/wiki/Internet_protocol_suite

Some layers (such as layer 1 and 2 that include spectrum allocation and physical properties of connectivity) are already significantly regulated. The lower layers are indeed probably not the target of this inquiry and are covered by a list of Internet Invariants which are described in a paper by the Internet Society called "Internet Invariants"[3]. Regarding Internet infrastructure, the

[1] https://www.parliament.uk/business/committees/committees-a-z/lords-select/communications-committee/inquiries/parliament-2017/the-Internet-to-regulate-or-not-to-regulate/
[2] https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/
[3] Internet Invariants - https://www.Internetsociety.org/policybriefs/Internetinvariants

focus should be on *facilitation of access*, which includes regulator support for the concept of Net Neutrality[4].

The focus of this inquiry is therefore about the way in which we address online responsibility for users, their safety (broadly defined) and maintain their trust in the Internet.
For services built on the Internet, e.g. platforms, the primary focus needs to be on appropriate application of existing offline regulation to online service providers. Regulation (and application of regulation) should focus on the function that is provided, not the medium through which it is delivered. Thus, a business that facilitates chauffeured private car hire services should be regulated the same way, regardless if the service is provided via an online app (e.g. Uber) or an offline phone centre (e.g. traditional 'radio car' service) .

A key challenge is the international nature of seamless cross-border service delivery of many online services, which can cause confusion regarding who has jurisdiction over what? This is a fundamental issue that has been recognized and addressed in the GDPR by focusing on where impact of processing occurs, i.e. the location of the data subject. The same jurisdiction issues that GDPR is addressing for personal data also apply to questions regarding copyright enforcement, taxation, hate speech, etc. associated with online businesses.

Specific consumer protection concerns arise in dealing with unbounded "in-game" purchases. Certainly for children controls need to be in place to prevent excessive charging. Given the child is not the bill payer, it could be viewed as negligence on the part of the service provider to not provide the bill payer with the controls necessary to cap such payments, something the credit card industry could champion backed by the threat to refuse to honour payments.

The fact that online platforms are increasingly becoming the information gateway for people, especially younger generations who get much of their news from online platforms via mobile devices, raises social and political concerns similar to traditional news media. Concerns about media empires with too much dominance in newspapers or TV coverage, should equally apply to online platforms where it is now common for a single provider to dominate a service sector (Facebook for social networks, Google for search). As shown by Facebook's own study (2012 US elections impact on likelihood to cast a vote[5], they have the power to influence voting behaviour.
Social concerns also arise from the fact that the majority of online platforms are developed in the US (Silicon Valley) and therefore operate under US (Silicon Valley) oriented social values which can differ significantly from EU/UK values, as for example with attitude towards the precautionary principle for consumer products or data protection laws.

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

[4] https://www.gouvernement.fr/en/the-digital-bill
[5] https://theconversation.com/can-facebook-influence-an-election-result-65541

Online platform should be reactive to requests from law enforcement regarding take down notices whilst being cognizant of due process that respects laws.

On the whole, legal liability might hinder competition, as large platforms are more likely than smaller platforms, to be able to invest in resources to (a) fight litigation, (b) develop tools and algorithms to police their platform and (c) actively employ people to police their platform. When considering that historically, innovation has been shown to be brought forward by new players, hindering the ability of new players to grow through the increased risk of legal liability might hinder innovation. Furthermore, it will serve to trigger a shift of online platform hosting providers from having their servers based in the UK to migrate them abroad to more lenient regulation regimes.

However, it is also necessary to differentiate between different types of online platforms

- Public broadcast type - like open Web sites
- Private group type - like communication services such as WhatsAp
- Centralized vs. decentralized content moderation and/or recommendation such as Wikipedia

The test for legal liability must be based on an assessment of the factual role that the platform takes, not self-assessed claims regarding business sector (e.g. Facebook statement that they as a ‘technology company, not a media/advertising company, should not be the determining factor in setting the regulatory regime that is applied).

Algorithmic content moderation (e.g. setting the effective visibility of content through filtering or ranking) is an editorial engagement with content, even though it does not involve direct human intervention. The platform provider controls how the algorithm is set up, what its prioritization metrics are. Platforms that provide private (encrypted) communication between closed groups should be assessed differently from platforms that provide publicly visible content broadcasting. Encrypted private communication is more similar to telephone communication, with the platform acting as neutral carrier. Net neutrality ‘carrier protection’ should apply to them.

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?

Online platform are notoriously unclear about their content takedown process. Information regarding content moderation policy of platforms is usually provided as part of the long and complicated Terms of Service document that users typically click through without reading. Introductory demos that interactively guide new users through the features of the platforms highlight the existence and use of means by which the user can flag inappropriate content, but it is often not clear what happens once content is flagged.

Traditionally a major focus of content moderation for platform providers has been on identifying and removing copyrighted materials. In contrast to moderating of fake or hate content, where algorithmic approaches are only recently being introduced, ‘pro-active’ algorithms that search through the content on the platform to find potential violations of copyrighted material have been in place for many years. Just as with proposed ‘fake/hate’ material detection algorithms, this copyright enforcement suffers from detection errors where non-infringing material is taken down, also known as “false positives”. This often occurs for content that is allowed in the US ‘fair-use’ copyright exemption, such as critical commentary. The process of challenging a take-down notice can however be very intimidating since this raises the chances of leading to a legal confrontation in a (US) court. This constitutes what is known as a “chilling effect”.

One improvement that might be needed is the process to reverse decisions. Platforms have been accused of providing very little opportunity for a customer services contact with a real human. This brings a lack of transparency, where end users often feel as though they are dealing with an algorithm rather than a real human being.
Content takedown processes of platforms needs to introduce more transparency and processes for independent appeal.

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

On the whole, end users should be associated with content takedown standards, but there are some circumstances where this is not possible.

On closed group communication platforms it is common that users have an active role in setting and maintaining standards for content and behaviour. On large open platforms, such as Facebook and Twitter, users generally do not have the means or a sufficiently global picture of what is going on in order. Responsibility must therefore lie with the platform provider. Sub-groups within the larger platforms, e.g. sub-Reddits, Facebook groups etc., do often set their own unofficial content and behaviour standards which are moderated by the users of these groups through collective responses to and infringement of those standards.

The current approach to moderation of hate-speech and only abuse, heavily relies on reporting by the abused users to trigger an investigation by the platform to determine if the content violates the platform standards. This approach makes sense as a way to avoid undue censorship of content by automated means that are likely to produce a high number (due to large volumes even a small percentage results in a high absolute number) of false-positives (the system things it is content that violates the standards even though this is not the case) and simultaneously miss many cases of actual violations. Automated methods are still not capable of reliably identifying contextual cues that can shift the meaning of content between abusive and non-abusive.
It should be noted however that regardless of failures to distinguish context, and thus producing errors, automated content moderating of copyright infringement is used by the major platforms.

A significant problem with user initiated content moderation is the response time by the platform investigation of the flagged content. Especially in cases on online abuse, any delay in action by the platform can result in increased abuse through copy-cat behaviour.
One approach could be a shift towards a model where content that users flagged as infringing of community standards is automatic temporarily quarantined, pending investigation by the platform, and released if the investigation find that the content is does not merit removal. In this case also it is imperative that the investigation by the platform must happen quickly in order to minimize the ability of malicious actors to interfere with free communication by falsely flagging content as abusive.

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

Online platforms should publish clear guidelines on how their process for content takedown and appeal works, indicating clearly how to appeal. Platforms should also provide clear information about why content is removed or made more/less visible to users, in light of the need to protect freedom of expression.

Currently it is not uncommon that users may find that a message they posted appears not to be seen by anyone, leading to theorizing about reason why the platform might have removed or suppressed the content. It is very difficult for people to actually know if and how their content is visible to their intended audience. The same is true for companies that sometimes find out about a change in takedown policy through a sharp drop in customer engagement.

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

One of the main problems with online platforms arises from the centralized architecture where data from/about the user is transferred to the platform provider, resulting in a loss of control over the data by the user and a strong power imbalance in favour of platform providers. Users are often confronted with an all-or-nothing choice in which they must accept complete surrender of control over their data, even if they wish to use only certain parts of the platform services. This can results in discontent and/or suspicion by the users, who might nevertheless feel compelled to use the service due to peer-pressure (fear of missing out) or lack of alternatives (for many online services there is only a single large player in the market; closed systems make it impossible to interact with users of the platform without buying in to the platform as well). The problem is often confounded by the use of an advertising based revenue model where consumer data becomes the ‘gold’ that is mined by the platform.

For all platforms that do not require log-ins, a simple process to obtain one’s personal datafile should be established and published.
For platforms that offer a log-in and therefore private accounts, each account holder/user should be able to enter an area named “what do you know about me?” where all data held by the

platform about the account holder/user is displayed. Where the datafile is very large, the end user should be able to download it to their own device. They should have access to all their data and how it is being used. The uses to which data is being put should be based on fully transparent Terms of Service (ToS) and an opt-in basis. In other words the user has the ability to select and deselect the uses to which their data is being put.

Platforms should provide a clear, easily accessible overview of the various businesses, organizations and people who have received or accessed personal data of the users. This must include information that the platform has algorithmically inferred about the users, e.g. employment status inferred from times/locations of content the user posted on the platform.
Information given to the user must be in a standardized, human and machine processable format so that third party apps can be created that help users better understand the data

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

Algorithms are often considered a confidential, proprietary business asset. It is therefore unlikely that the exact workings of an algorithm be opened and transparent. However, online platforms should be clearer about where algorithms are used.

Service ‘personalization’ is frequently used to ‘optimize’ the customer interaction, this involves filtering/recommending the products/services the customer is presented with.

It is, however, often not clear what exactly is being optimized for. Is the content on the platform being shaped to provide content that will increase customer wellbeing, or is it shaped to maximise time spent on the platform and/or number of interactions with adverts even if this is to the detriment of the user?

In order to do the personalization the platforms collect a wide variety of information about the customer, including past behaviour on the platform, location tracking, scanning of content posted by the user, tracking of over websites visited by the user via ‘cookies’ and ‘tracking pixels’. Larger platforms can do a lot more with the data than smaller platforms.

The collection, use and trade of this user data, including personal characteristics inferred from this data, has potentially far reaching consequences as most vividly shown by the recent Cambridge Analytica controversy.

Concerns regarding lack of transparency about the kind of data that is collected and the purposes for which it is used apply not just to personal data about individuals but also to data about businesses.

The European Commission is currently exploring the potential for abuse of such data about business by platforms, such as travel bookings sites and online game stores, especially in cases of vertical integration where the platform provider is also a competitor in the same market (for example, the games manufacturer Valve which is also the provider of Steam, a major game selling platform.

Data-driven algorithms are an increasingly important element in determining the customer experience when using online platforms. The algorithms filter and rank which information is presented to the user and where it is presented, which affects the likelihood that a customer will notice and interact with the data. The high volumes of data available online means these algorithms are vital for enabling users to find the relevant information, be it search results, news stories of product offers. Accountability or algorithm inferences, or lack thereof, affects the development process behind the creation of the algorithms. In the current environment where the platforms are not accountable for algorithm behaviour, there is little incentive to focus on the interpretability of algorithmic processes. Due to the large number of parameters that are used by the algorithms, even the engineers who constructed the system are often not able to explain why the algorithms made specific decisions. This is even more so in the case of adaptive systems that learn from continuously evolving example data sets, as is the case with deep-learning and similar systems. We do know however, that all data-driven systems are susceptible to bias based on factors such as the choice of training data set. Since the dominant online platforms are US based, it is likely that training data sets will contain biases that reflect US culture. As demonstrated by various cases of discriminatory behaviour of algorithmic service (e.g. gender discrimination in Google Ads for high paying jobs[6]) even supposedly neutral algorithms that are based purely on observations of Internet usage statistics are not value-neutral. Rather they tend to reinforce an existing status-quo which might not be in the interest of the values that the UK society is striving for

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

The dominance of a small number of online platforms, resulting in big data, is detrimental both to plurality of data and fair competition. Competitors struggle as their return on investment are not offset by the income generated by the data analysis that comes with big data.

Thus we are in a self-perpetuating circle where local actors are seeing their local market destroyed by massive multi-national corporations that can always undercut them with better information and considerably more firepower to promote their products.

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

The UK will be able to introduce local legislation that is independent of European Union legislation. Unfortunately, it is sometimes attractive to regulate too much, or too heavily, thus curbing innovation, freedom of speech and human rights. The European Union has pan-European institutions that might mitigate legislation, such as the European Court of Human

[6] https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html

Rights. The UK should continue to be a member of such organisations, wherever possible, as they are a back-stop to a healthy democracy.

International coordinated regulation is required in order to have impact, specifically on large corporations which have emerged within the US's specific regulatory framework. In this regard the EU has been an important player, where the UK will be a minor voice unless it continues to coordinate and support EU action in this area.

In data protection the status of the UK as a non-member 'third-party' participant in the EU's Digital Single Market will have implications for UK digital economy, as free flow of data between the UK and the European Single Market will be impacted.