A REGULATORY FRAMEWORK FOR THE INTERNET?

House of Lords Communications Committee

Cybersalon

11th May 2018

1. The Open Web and the closed platform

1.1 There is a clear distinction to be made when we speak of the internet. On the one hand, proprietary platforms[1] and the ecosystems which surround them, the walled gardens of Facebook, Instagram, Amazon, and on the other the open web, a tapestry based on open standards, Wikimedia, Creative Commons, the Mozilla Foundation and the software and protocols that form the foundations of the World Wide Web. Whilst the wider discussion is chiefly concerned with dealing with problems caused by undesirable content and behaviour on social platforms, lawmakers should be very careful not to place undue restriction on the open web, the open standards and infrastructure of the digital economy and culture that we so value and take for granted now.

1.2 The internet is a panoply of networks, built upon shared protocols that form the basis and foundation for websites and digital services to operate from. Facebook, Google, Amazon, Apple use but are not part of the Open Web, nor do they embody the internet, they may be regulated as online-based digital examples of existing businesses ranging from broadcasting and advertising to retail. We need not enshrine new precedents and categorisations in legislation that leads to unexpected loopholes and unintended consequences.

2. The extension of fundamental rights into the digital age

2.1 This submission is predicated on an understanding of the successive development of rights and freedoms, that the new digital age, defined by an ever increasing role of the internet and digital platforms in our lives, warrants a new debate over how to construct a new constitutional settlement which nurtures today's emerging forms of digital citizenship.

2.2 Fundamental rights laid down in the 17th and 18th century liberal formulations of political and civil freedom were grounded in widespread economic exploitation. Such fundamental rights, in practice, were often the privilege of the few. At our current impasse we risk a similar submission to power in this new digital age, from the rise of the phenomenon of platform dominance from the likes of Facebook and Google who now play a key role in mediating the civic, political and economic life of the nation and the world[2].

2.3 The following pages detail a set of recommendations that constructively and proactively set out the case for user rights, in opposition to the current state of platform dominance.

3. GDPR is good, but Britain can do better

---

[1] Open Web - Wikipedia https://en.wikipedia.org/wiki/Open_Web

[2] Digital Citizenship: from liberal privilege to democratic emancipation, OpenDemocracy https://www.opendemocracy.net/richard-barbrook/digital-citizenship-from-liberal-privilege-to-democratic-emancipation

3.1 GDPR as an EU Regulation will apply unilaterally across the EU, but it does contain provisions for member states to expand and withdraw from the Regulation in certain ways. Germany has already legislated with the Federal Data Protection Act. The UK can follow suit, acting to close loopholes present in the legislation such as the 'escape' of data outside of the EU for example by handing over personal data via transactions to non-EU organisations without adequate protections, the loss of GDPR protections by non-EU organisations selling data to third parties not related to the offering of goods and services and so on. These are just an example of where the UK can improve upon and enhance existing legislation.

3.2 Fundamentally, GDPR leaves too many opportunities for data leakage. Users must have confidence in the overlapping systems, policy instruments and legislation that are purported to protect their online privacy and personal data when using the internet. As we presume innocence until proven guilty, we must presume that the user has the right of control and use over his or her data.

4. Curatorial versus editorial control

4.1 Algorithms are merely rules and processes. They are designed by humans, composed of human decisions, and in the case of platforms, human decisions informed by corporate goals and directives. Facebook and other major platforms hide behind the obfuscation that their platforms and the content served on their platforms is automated, that it is presenting posts and inputs as they are submitted to the platform. This is not the case.

4.2 Let us be clear, they are not just curating our social experiences, but rather taking on an editorial role. Take the example of Facebook's recent alteration governing which content from which sources are served to the user's newsfeed, the Facebook timeline. This change altered the distribution of content on the news feed weighting in favour of posts and media from friends and family over organisations and companies. Facebook and other social networks are presenting a very specific view of the world; they are mediating and filtering engagement in the online space. They have taken on the role of the editor, but claim they are merely re-presenting inputs, a curatorial role.

4.3 Facebook, Twitter, Instagram and others are closer to that of online magazines, where the magazine is edited by a team of editors; the Facebook newsfeed is edited by algorithms, rules and if-statements, developed by humans, reflecting human goals. Facebook's own Community Standards are an example of hands-on editorial control[3]. As a result they should be held accountable under existing laws as would any other publisher for the content therein.

5. Algorithm accountability and access

5.1 Software and computer code are often put into escrow when commercial suppliers need reassurance that software a buyer commissions will still be usable if the supplier fails

[3] Community Standards, Facebook
https://www.facebook.com/communitystandards/

financially[4]. Alternatively, information and patents are held in escrow, set aside whilst competing parties vie for their claims. We argue a similar instrument can be used by Parliament or a new monitoring body to provide access to platform code and algorithms for researchers to examine.

5.2 Such instruments and monitoring bodies with access to the algorithms of platforms allow Parliament and civil society, under certain conditions, to gain an understanding of the intentions and aims of platforms and their use of data, including socio-economic goals. Parliament cannot legislate effectively, cannot scrutinise effectively what it does not understand. As a result policy responses in this sphere have largely been reactive rather than proactive based on an educated evidence-based approach. Given the monopolistic nature of these companies that govern and harvest the daily activities of billions of people, such an approach is not unwarranted given the current threat of their activity further undermining the established supremacy of Parliament and the democratic process.

6. The case for moderation

6.1 We often think of the internet as a self-managed community, and by extension expect online moderators to work for free. This has come from the historical fact that the original online forums such as Usenet were specifically not-for-profit. Moderators then were part of a self-governing community of non-commercial groups. In other cases commercial services such as AOL offered free use of their service in exchange for moderation.

6.2 Facebook, Twitter and the platforms are commercial entities, earning millions leveraging user content. Facebook does not have services it can provide in kind, except the use of its platform without processing the user's data. It should employ moderators and pay them. In addition to this, lawmakers should bear in mind the kind of content moderators are obliged to expose themselves to, from child pornography to extreme gore and hate crimes, and factor this into their decisions.

6.3 As things stand, social platforms are left to exercise their own judgement when it comes to taking down offensive content. We back the view of the Independent Committee on Standards in Public Life with regard to their recommendation to shift the liability for illegal content onto social media firms. We add that platforms should be forced to remove offensive content within legally defined time limits and recommend the Santa Clara principles of moderation[5].

7. Social Network Ombudsman

7.1 "Free" platforms are not covered by existing UK ombudsmen. Ombudsman services are available only in cases where money is paid or financial transactions take place for goods

[4] Software Escrow, SBA Research
https://www.sba-research.org/research/projects/software-escrow/
[5] Santa Clara Principles, Digital Social Contract
https://digitalsocialcontract.net/what-proportion-of-social-media-posts-get-moderated-and-why-db54bf8b2d4a

and services. Users of social networks are consumers of the services of the social platforms and they pay for the “free” service with their data. However, because this is a non-financial transaction, social users have no recourse to dispute and complaint resolution when their user rights, or consumer rights, are challenged.

7.2 Alternatively, existing ombudsmen such as CISAS need to reframe their definition of “consumer” to include users who trade their data for services, such as Facebook, Twitter etc. This is important to state, given that the user relationship with platforms can be read as a supplier relationship. Facebook makes approximately £15 per user in the UK per year. Accordingly, users need a supplier contract and supplier protection.

8. Digital Citizens Advice Bureau

8.1 As it stands, despite internet usage now extending to above 80% of the UK population, internet users have no dedicated advice services. We recommend Parliament consider the establishment of a new internet user rights service, providing assistance and expert advice to British internet users regarding their online rights, privacy concerns and advice with how best to secure their online presence, similar to Childline. This would be particularly valuable internet users, both young and old.

9. Platform users have rights to their own content and remuneration

9.1 The content individuals post and share via online platforms belongs to them. We suggest Parliament consider the licensing of user content under Creative Commons. If content is used by the platform, such a scheme could include negotiated pay percentages based on usage data by the platform. Platforms economic value are predicated on the exploitation of colossal amounts and flows of individual’s personal data and content.

10. Russia, China and the right to interrogate foreign company use of user data

10.1 Recital 23 of the General Data Protection Regulation provides a loophole, through the specific wording of *“offering goods and services”,* allowing for foreign companies to ‘escape’ data out of the EU area by the means of marketing, rather than the selling of products. Put simply, a global company wanting to exploit this loophole and extract personal data belonging to British and EU citizens can set up a marketing company in the EU presenting a range of products and services, before taking the EU customer to a non-EU payments portal, transferring payment and personal data to a non-EU business. From that point on the personal data are “outside the law” and there are no barriers to the UK/EU citizen’s personal data being sold on to any other non-EU company.

10.2 It is within the purview of Parliament to lobby the CJEU to rule that Recital 23 is a misinterpretation of EU law, and that “offering” should have the same interpretation as applied in competition law.

11. Combating shadow profiling

11.1 Facebook is understood to have built up profiles of non-Facebook users. Information about non-Facebook users is captured or inferred from the information posted to Facebook by their family and friends: they may be included in photographs, and their lives and jobs may be discussed in postings. The photos may also be passed through facial recognition algorithms. All of this happens even though they have not granted Facebook their consent.

11.2 This is possible and alarming because of the limited number of data points required to identify someone. Countless non-users are swept up and their data stored and used by the company, through simple acts of a new user uploading their phone contacts into Facebook to search for new friends through Facebook's People You May Know service. This extends to Facebook's Like and Share buttons on websites external to Facebook; these all track non-users through the internet, building up a Shadow Profile.

11.3 When users ask Facebook to delete their account, they expect the company to delete the information they have uploaded since their profile was created. However, the information Facebook has inferred and collected about them, for example, from their activities on the web - that is, their Shadow Profile - remains on Facebook's servers. When we talk about scrutiny of algorithms, algorithm escrow and the consideration of new forms of monitoring to better understand these systems, we are arguing that policy makers must educate themselves about precisely this kind of activity by internet platforms.

12. Risks and capacity of current oversight

12.1 The Information Commissioner's Office has limited capacity with only 500 full time staff to oversee 500,000 companies that hold data and operate within the UK, the enforcement of FOI & GDPR rules, and for the 40,000,000 social network users. The ICO requires higher funding in line with the expansion of its portfolio of activities.

13. Unintended consequences

13.1 In the past when legislation has been written on the hoof, and without proper due diligence it has had unintended consequences. To cite two examples, FOSTA/SESTA, the anti-trafficking law in the US has effectively ended the rule of Safe Harbor, Section 230 of the 1996 Communications Decency Act[6]. The Computer Misuse Act has paradoxically made it difficult for security researchers to undertake their work in case of being implicated for the things they're working to prevent.

14. Conclusions

14.1 The new power of Facebook and Google is here to stay and is increasing. These new services and economies have brought about wonders, connecting the globe, empowering billions, providing next-generation services, toppling dictators, highlighting abhorrent behaviour with #metoo. But these new platforms also come with new costs and threats, to our democratic process via paid Russian Facebook trolls, the political polarisation of global

[6] A new law intended to curb sex trafficking threatens the future of the internet as we know it https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom

populations, the weaponization of personal data via Cambridge Analytica, the shaping of moods of entire populations via algorithms, a new torrent of unchecked hate crimes, a new generation of children socialised through the less than safe space of social media and YouTube, and the rise of hitherto untouchable economic monopolies based on the mass exploitation of personal data.

14.2 The current generation of platforms are companies that have been allowed to grow to monopoly status due to watered-down US anti-trust laws. Facebook owns Whatsapp, Instagram, Oculus and Messenger, an entire ecosystem that their users largely think are separate distinct entities. The size of the platforms matter. They affect millions of users, making them dangerous, and by and large, they are unchecked by regulation.

14.3 Because of their size, with a few dominant players, governments regulate these companies through conversations and backroom chats with a handful of corporate representatives, rather than legislating and making arguments publicly. The UK Government is not immune from this.

14.4 The approach of collaborating via the back door is not working, and as a result there are areas where the law is silent because platform giants won't collaborate and they refuse to engage. Mark Zuckerberg's recent refusal to speak to Parliament is a case in point. The government won't take a stronger line for fear of being shut out.

14.5 The supremacy of Parliament itself is under threat, an issue that will be exacerbated when, post-Brexit, the UK will be attempting to regulate or mediate platform monopolies from a national level rather than a pan-European one. This point is worth the House's consideration. Zuckerberg has already refused to answer the UK Parliament's call to testify - yet he felt obliged to speak in person to the European Parliament.

14.6 Democracy requires open public policy discussions rather than private discussions based on relationships with powerful companies that take place behind closed doors. We believe Parliament should reassert its sovereignty. The current system of regulating these companies is not compatible with the public interest. In our view, the UK needs a Digital Bill of Rights to consolidate the progress of GDPR and cement user rights in law[7].

[7] Digital Bill of Rights, Cybersalon.org http://cybersalon.org/digital-bill-of-rights-uk/