Can the law effectively regulate social media? Should it?

In the 16th century, the first printing presses transformed Martin Luther’s *Ninety-five Theses* into the first ‘viral post’ – with unforeseeably seismic consequences. In the 21st century, unregulated social media enables everyone to become their own free, global, instantaneous printing press - with potential consequences so profoundly undesirable that some regulation is needed. As Zuckerberg hoped in 2009, unfettered global interconnectivity has made “a really big change in the world”¹, but total liberty within this ‘marketplace of ideas’ is now a discredited ideal. Zuckerberg’s utopian vision will morph into a quasi-dystopian reality unless three areas are addressed effectively. Firstly, social media is threatening democracy through micro-targeting users and allowing the dissemination of fake news. Secondly, social media is threatening public safety and harmony, because it can be exploited by terrorist groups, abusers, and hate speech provocateurs. Thirdly, social media sites (which derive most of their income from the private data provided by their users) are not giving adequate privacy to user data. These three areas require regulatory responses but, because there is no international consensus on a common approach, each country (or political bloc) must decide what regulation, or threat of regulation, is most effective for it. They will have to strike a balance between the conflicting concerns outlined below, whilst accepting that no domestic regulations can be globally ‘effective’ because of the difficulty of enforcing them beyond frontiers. A supranational body such as the UN can, nevertheless, be of use in coordinating and facilitating different countries’ regulatory efforts.²

---

¹ Zuckerberg, M. Personal interview. (2009, May).
Social media threatens democracy: initiatives such as Facebook’s *Building a Better News Feed for You*³ narrow the scope of political exposure online, reinforce existing views and build resistance to differing ideas. Through micro-targeting, social media sites sort users into like-minded groups, amplify their views in echo chambers, and thereby develop a closed and uninformed political psyche. Sunstein comments: “We are living in different political universes – something like science fiction’s parallel worlds”⁴, in a prison of our own design, trapped in self-insulation. However, excessive regulation or censorship also threatens democracy so, to avoid this, Sunstein proposes an “architecture of serendipity”⁵, in which sites would expose users to randomly selected political posts to help them form unbiased views. This proposal would counteract growing political fragmentation and polarisation by promoting informed democracy. Three attempts in line with this proposal have been made: PolitEcho (showing news feed bias), The New York Times’ site *Right and Left: Partisan Writings You Shouldn’t Miss* (exposing readers to alternative viewpoints), and Facebook’s reworking of its newsfeed (offering pages such as *Related Articles*).

Dissemination of fake news is another threat to democracy and, if it hasn’t already swung elections, its potential to do so is clear. For example, Internet Research Agency, a pro-Kremlin troll factory with 80 employees and a monthly budget of $1.25 million, aimed to undermine the 2016 US Presidential Election. This threat will increase exponentially once AI-driven ‘fake videos’ hit the mainstream – as they are poised to do. University of Washington researchers have generated a highly realistic video of Obama ‘talking’ about terrorism⁶. This technology, only in its infancy, will make it even more difficult to distinguish

---

³ See: https://newsroom.fb.com/news/2016/06/building-a-better-news-feed-for-you/
⁵ Sunstein. *op. cit.* p.5.
between fake and real news – a horrifying prospect. Moreover, criminalising the dissemination of fake news runs the risk of curtailing freedom of speech. The Malaysian Government’s March 2018 proposal to introduce a maximum 10-year jail sentence for anyone peddling fake news has alarmed activists; they warn that this could stifle reports on alleged government misconduct. Trying to keep platforms sufficiently secure from malign disseminators (by, for example, developing algorithms that remove fake news) will be a never-ending and expensive arms race. However, if social media sites do not make sufficient efforts then, in the interests of democracy, the law should require them to do so.

Social media can threaten public safety and harmony. For example, 90% of organised online terrorism uses social media\(^7\) both as a global recruitment, publicity and proselytising tool, and for covert communication via encrypted and/or self-deleting messages. However, the protection given by Article 19 (right to freedom of expression) of the Universal Declaration of Human Rights\(^8\) complicates the task of websites and regulators in deciding which (‘bad’) content should be deleted. Each country must balance its particular need to reduce hateful, dangerous, or extremist content against the universal requirement to protect individual freedom of expression. Germany, possibly acting as global precursor, passed a pioneering law\(^9\) prohibiting online hate speech, extremism and neo-Nazism. Since coming into force on January 1\(^{st}\) 2018, this law has been very effective; officials received only 5% of the predicted complaints about sites failing to delete posts. On March 1\(^{st}\) 2018, the EU Commission took a softer approach; it gave Facebook, YouTube and Twitter three months to show that they are removing harmful content within an hour of notification, or face

---


\(^9\) *Netzwerkdurchsetzungsgesetz.* (2017, June).
legislation forcing them to do so. AI, which threatens to hugely sophisticate fake news, could be used very effectively to counter cyber terrorism; the Home Office recently tested a mechanism that detected 94% of ISIS propaganda, and removed it with a 99.995% success rate.\(^\text{10}\) The dark web, the easy availability of internet anonymity, the impenetrability of sites (such as Telegram) where messages are encrypted and self-deleting, and the difficulty of enforceability beyond frontiers, preclude any initiatives from being totally effective. Nevertheless, effective mainstream regulation to preserve public safety and harmony should still be achievable by initiatives such as those described above.

Social networks such as Facebook, Instagram and Twitter all process user data to generate advertising revenue. Such data is the nucleus of their lucrative business models, and users typically grant these sites a license to use their data freely. Billions of users have thus accepted the receipt of micro-targeted advertisements as the price of being able to use these sites for free. It is accordingly unsurprising that these sites have hitherto attached little importance to preserving the privacy of this data, and have had little incentive to be transparent about how they process, and third parties can access, such data. Facebook’s porous privacy policy led to Cambridge Analytica obtaining detailed data from 50+ million users, possibly influencing the Brexit vote and the 2016 US Presidential Election. It is now apparent that social media sites collect non-users’ data to create a ‘shadow profile’ without their consent. It would therefore be naïve to assume that social media sites will put society’s need for privacy ahead of their own desire to generate profit and so self-regulation is unlikely to be effective without legislation in this area.

In 2012, Obama’s proposed Consumer Privacy Bill of Rights was blocked by fiery opposition, mainly from the US online industry. Possibly because this industry has less influence in Europe, the EU has introduced the General Data Protection Regulation (GDPR) which will come into force on 25th May 2018. This legislation is set to be the most comprehensive privacy regulation in the world, and aims to make individual users the masters of their own private data. Careful analysis of the GDPR reveals that it could break the quasi-monopoly of power that some transnational social media and online search sites currently enjoy. Two key GDPR articles are Article 15 (Right to Data Portability), whereby a data subject can transmit their data to another controller, and Article 18 (Right to be Forgotten), whereby a data subject can have the data controller erase, cease further dissemination of, and potentially halt processing of, their personal data.\textsuperscript{11} Users are only valuable to social media sites if they can process their data, and if users move and/or erase their data, this life-blood drains away. Such sites will thus have to make more of an effort to keep users, and may decide that semi-covert tracking by shadow profiling without consent is too unpopular and/or illegal to be worth continuing. Furthermore, a new fine of up to 4\% of global annual turnover of a company transgressing the GDPR should be highly effective in making social media sites comply with this necessary legislation.

When describing the fight against al-Qaeda, General Stanley McChrystal said: “it takes a network to defeat a network”\textsuperscript{12}. The comment could also apply to the challenges posed by social media, because global issues should ideally receive a global response. As the foremost international legal body, the UN would be a suitable choice to frame a common supranational approach, and in 2012 it hosted the World Conference of International

\textsuperscript{11} See: https://www.eugdpr.org/key-changes.html
\textsuperscript{12} McChrystal, S. It Takes a Network (Foreign Policy. 2009, February)
Communications. The nonbinding Final Acts recognised that “all governments should have equal responsibility…for ensuring the stability, security and continuity of the existing [and future] Internet.” However, only 89 out of 144 countries signed these Acts, with the US, Canada, the UK, France and Germany declining to do so, thus demonstrating the UN’s inability to pass an efficacious supranational convention for the foreseeable future. There is little chance that the US and Russia will soon agree on the same ‘effective’ regulation of social media, with the former conscious of the need to protect freedom of expression, and the latter prepared to erode free speech rights (by, for example, banning Telegram on 13th April 2018) when the status quo is threatened. A supranational convention enforced by the UN is a quixotic dream, but the UN could still be a useful identifier of abuses, researcher into effective methods of regulating social media, and catalyst for international harmonisation - a trend that is already occurring, with Argentina, New Zealand, Israel, and Colombia having already adopted the EU’s GDPR approach.

In conclusion, the law can effectively regulate social media but, to avoid overly damaging welcome connectivity, should only do so when these sites cannot self-regulate effectively. To preserve democracy, social media sites should both break the mould of self-insulation and political polarisation through a restructuring of how online politics is presented, and reduce fake news (probably through algorithms). To preserve public safety and harmony, social media sites should again self-regulate by immediately removing offensive or dangerous material (possibly through the use of AI). In the two aforementioned areas, the interests of governments, users and sites are aligned because sites derive little or no revenue from anti-democratic, terrorist-inspired or hateful content, which could attract

---

governmental regulation, drive away users and tarnish their brand. Sites are well aware of the need to keep themselves ‘clean’; Facebook has promised 20,000 content moderators by 2019. In these two areas, (costly) self-regulation should accordingly be tried initially, with regulation only being introduced if the sites’ efforts are insufficiently effective. On the other hand, private data is best protected through laws such as the GDPR because social media sites have given no convincing indication of prioritising societal needs of data privacy and transparency over their revenue - and can never be expected to. In all three cases, given the lack of international consensus, each country will have to decide what threats or regulations (if any) are most ‘effective’ for it, and multiple responses are thus likely. The UN could play an important role by providing research and by acting as a diplomatic catalyst for international cooperation and consensus. The emergence of a more connected world in 1517 led to over 100 years of warfare. The emergence of a hyper-connected world some 500 years later could lead to greater peace and understanding – but only if regulators strike the right balance between preserving the global freedom and connectivity afforded by social media and reducing the dangers that such hugely popular and free-to-use benefits inevitably entail.

2000 words (including all footnotes, not including title and bibliography)
Bibliography

Ferguson, N. *Why Twitter, Facebook and Google are the antisocial networks*. (2017, October).


Rudd, A. *New technology revealed to help fight terrorist content online*. (2018, February)


See: [https://www.forbes.com/sites/techonomy/2012/05/16/mark-zuckerberg-social-revolutionary/](https://www.forbes.com/sites/techonomy/2012/05/16/mark-zuckerberg-social-revolutionary/)
