Research Program
on Digital Constitutionalism
Project Aristotle

United Kingdom

Country Report

December 2021

Authors

Manasa S Venkatachalam, GNLU Centre for Law and Society
Pravah Ranka, GNLU Centre for Law and Society
Aman Garg, GNLU Centre for Law and Society
Shubham Tiwary, GNLU Centre for Law and Society

Institute
for Internet &
the Just Society

project
Aristotle

Research Program on Digital Constitutionalism **Project Aristotle**

United Kingdom

Country Report

Authors
Manasa S Venkatachalam, GNLU Centre for Law and Society
Pravah Ranka, GNLU Centre for Law and Society
Aman Garg, GNLU Centre for Law and Society
Shubham Tiwary, GNLU Centre for Law and Society

December 2021

Inquiries may be directed to digitalgovdem@internetjustsociety.org

DOI: 10.5281/zenodo.5792089

About us

The Institute for Internet & the Just Society is a think and do tank connecting civic engagement with interdisciplinary research focused on fair artificial intelligence, inclusive digital governance and human rights law in digital spheres. We collaborate and deliberate to find progressive solutions to the most pressing challenges of our digital society. We cultivate synergies by bringing the most interesting people together from all over the world and across cultural backgrounds. We empower young people to use their creativity, intelligence and voice for promoting our cause and inspiring others in their communities. We work pluralistically and independently. Pro bono.

Project Aristotle is the flagship project of the Digital Constitutionalism cycle of the Institute for Internet and the Just Society. Together with our international partners, we publish a research guide on what a structure of governance for the digital realm can look like when it is informed by interdisciplinary country-specific legal and policy research and analysis. We believe that delving deep into these bodies of knowledge, as shaped by a people within a particular national context, has much to offer in response to the pressing questions posed by the digital ecosystem.

A. Digital Constitutionalism and Internet Governance

I. Traditional Constitutional Concepts in the United Kingdom

"The very notion of a master legal instrument that one might call 'the constitution' is alien to the British legal tradition. No clear boundary divides what is constitutional from what is not."[1] What counts as constitutional in practice has never been codified, but is scattered about in sundry documents spanning ten centuries. The undefined margins have the potential to become as fuzzy as quantum mechanics. Without definite articulation of the rules and norms that govern the digital world, the protection of fundamental rights and, ultimately, the safeguarding of human dignity with respect to the digital environment might become difficult, and create room for arbitrary exercise of power. Besides a negative, limitative approach, claiming the restriction of the power of rulers by law and the institution of a system of checks and balances, constitutionalism also developed a positive aspect, revolving around individual empowerment.[2] The *Magna Carta* has placed limitations on the arbitrary power of the crown.[3] It has created greater inclusion and democratization, similarly a charter of digital liberties must be made to avoid arbitrary use of sovereign power and protect fundamental liberties. Therefore, the first and foremost factor for grounding Digital Constitutionalism in the traditional concepts should be the creation of a charter of digital liberties.

The *Bill of Rights 1689*, also known as the *Bill of Rights 1688*, is a landmark act in the constitutional law of England that sets out certain basic civil rights.[4] Therefore, Digital Constitutionalism must have an internet bill of rights, which safeguards an individual's digital freedom by providing a set of principles that are about giving users more control of their online lives, protecting their right to privacy and creating a healthier and safer environment. One of the thirteen provisions mentioned in the English *Bill of Rights* is that "the freedom of speech and debates or proceedings in Parliament ought not to be impeached or questioned in any court or place out of Parliament."[5] Therefore, the internet bill of rights must have provisions which guarantee freedom of speech and expression in the digital atmosphere.

The *Representation of the People (Equal Franchise) Act 1928* widened suffrage by giving women electoral equality with men. It gave the vote to all women over 21 years old, regardless of property ownership.[6] The voting age was further lowered to 18 in 1969. These acts aimed at increasing representation in decision-making processes and a representative government. As a result, Digital Constitutionalism must ensure that all stakeholders are given the representation they deserve.

If courts are to safeguard liberty, their independence must be paramount.[7] This principle is considered so important that it has been constituted as a fundamental principle of the British constitutions.[8] Assent to judges' independence of the pleasure of the crown was formalised as a condition for acceding to the throne of Great Britain by the *Act of Settlement (1701)*.[9] Therefore, Digital Constitutionalism must be grounded in the system of checks and balances to protect the democratic spirit in the digital environment.

II. Defining Digital Constitutionalism

In 2015, Gill, Redeker and Gasser published a working paper on Digital Constitutionalism wherein they proposed to use this denomination 'Digital Constitutionalism' as an umbrella term to connect a set of documents seeking to establish a bill of rights for the internet.[10] They argue that these texts, which have emerged in the last twenty-five years, are very different, but that they could be regarded as a part of a broader 'pre' or 'proto-constitutional discourse', as "intellectual building blocks for the constitutional material of the digital sphere" whose ultimate aim is to define comprehensive set of rights, principles, and governance norms

---

[1] Parau CE, 'Core Principles of the Traditional British Constitutions' <https://www.politics.ox.ac.uk/materials/Core_Principles_of_the_British_Constitutions.pdf> accessed 25 March 2021.

[2] Celeste E, 'Digital Constitutionalism: How Fundamental Rights Are Turning Digital' (*Convoco!* 26 January 2021) <https://www.convoco.co.uk/digital-constitutionalism-how-fundamental-rights-are-turning-digital/> accessed March 27 2021.

[3] English Bill of Rights, 1689.

[4] ibid.

[5] English Bill of Rights, 1689.

[6] The Representation of the People (Equal Franchise) Act, 1928.

[7] Parau CE, 'Core Principles of the Traditional British Constitutions' <https://www.politics.ox.ac.uk/materials/Core_Principles_of_the_British_Constitutions.pdf> accessed March 25 2021.

[8] ibid.

[9] The Act of Settlement, 1701.

[10] Celeste E, 'Digital Constitutionalism: A New Systematic Theorisation' (*Sutherland School of Law, University College Dublin, Dublin, Ireland*) <http://doras.dcu.ie/24697/1/E.%20Celeste_IRLCT_Digital%20Constitutionalism_AM.pdf> accessed March 12 2021.

for the internet. Besides a negative, limitative approach, claiming the restriction of the power of rulers by law and the institution of a system of checks and balances, Digital Constitutionalism has also developed a positive aspect, revolving around individual empowerment.[11] Under *Article 10 of the Human Rights Act 1998*, "everyone has the right to freedom of expression". But the law states that this freedom "may be subject to formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society". Therefore, a balance is created between the private parties and the sovereign by protecting the rights, and putting reasonable restrictions on them. Therefore, Digital Constitutionalism in the context of the UK would adopt the path of creating a balance where it puts reasonable restrictions on the actions of private parties and also protects their digital freedom.

III. Core Tenants Of Digital Constitutionalism

The first and foremost core tenant of Digital Constitutionalism in the UK is the inclusion of a wide range of legal instruments and institutions. 'Digital constitutionalism' is a common term to connect a constellation of initiatives that have sought to articulate a set of political rights, governance norms, and limitations on the exercise of power on the internet.[12] Such documents can be traced back at least twenty-five years, with authors that include international political bodies, national governments, technology firms, civil society groups and some of the world's most influential leaders in internet governance.[13] Therefore, it can be fairly concluded that Digital Constitutionalism has not been restricted to just a body of laws. Moreover, it must be borne in mind that the legislation documents in the UK are one strand of an ongoing part-codification of the British constitutions, which, however, is not limited to the acts of Parliament. Hence, Digital Constitutionalism must also include the judgments given by the judiciary. The impact of Supreme Court decisions extend far beyond the parties involved in any given case, shaping our society, and directly affecting our everyday lives. For instance, in their first legal year, the justices gave landmark rulings on access to legal advice for Scottish suspects, the rights of gay asylum seekers, and the weight to be given to pre-nuptial agreements.[14] In *Copland v United Kingdom*, the European Court of Human Rights qualified an employee's use of the internet as part of her private life and correspondence.[15] In consequence, state control over private internet use and content including emails amounts to interference. The same is true for an obligation of internet providers to store internet that as laid down in *Article 3 of the European Directive 2006/24/EC* on the retention of data generated or processed in connection with the provision of publicly available electronic communications services. Even a person who does not use the internet may be compromised by the internet publication of information relating to him or her. If public authorities publish such information, or if legislation imposes a duty to publish it, the state interferes with private life, as the European Court of Human Rights rightly stated in *Wypych v. Poland*. Legality therefore depends on a special justification.[16]

The *Data Protection Act 2018*, which is the UK's implementation of the General Data Protection Regulation (GDPR) can be considered to be a part of UK's Digital Constitutionalism, but it has been found to be ineffective to protect privacy on its own.[17] Therefore, another core tenant could be having an internet bill of rights. Digital Constitutionalism should be to create and execute internet bills of rights in the United Kingdom. The bill would aim at achieving both data privacy and net neutrality at once. The bill would ensure that it restricts any form of discrimination, and make the internet accessible and available to all. Furthermore, a committee can also be established monitoring net neutrality to adopt an assimilative, analytical and participative approach to address this issue. The goal of Digital Constitutionalism should be to ensure that the UK's domestic legislation can control current and future advances in the digital realm.

The Digital Constitution should also ensure that it is in sync with the National Laws of the Country. The constitutional law principles in the United Kingdom include The *Habeas Corpus Acts of 1640 and 1679* drew on *Magna Carta* principles, which are among the most important acts in the constitutional history of all times,

---

[11] Celeste E, 'Digital Constitutionalism: How Fundamental Rights Are Turning Digital' (*Convoco!* 26 January 2021) <https://www.convoco.co.uk/digital-constitutionalism-how-fundamental-rights-are-turning-digital/> accessed March 27 2021.

[12] Lex Gill, Dennis Redeker & Urs Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' (2005) <https://dash.harvard.edu/handle/1/28552582> accessed April 4 2021.

[13] ibid.

[14] 'Significance to the UK - The Supreme Court' <https://www.supremecourt.uk/about/significance-to-the-uk.html> accessed March 27 2021.

[15] Copland v. United Kingdom (2007) ECHR 6267.

[16] Wypych v. Poland, (2005) ECHR 2428.

[17] Burgess M, 'What Is Gdpr? The Summary Guide To GDPR Compliance in the UK' (*Wired U. K.* 24 March 2020) <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018> accessed March 27 2021.

echoed in Dicey's remark that they "declare no principle and define no rights, but they are for practical purposes worth a hundred constitutional articles guaranteeing individual liberty." As a result, it creates a society in which liberty is given the highest regard.[18] It is suggested that in the creation of Digital Constitutional discourse and the design of digital policies, Digital Constitutionalism may learn from the experience of national legislation in the United Kingdom and adopt analogous methods, to the extent feasible.

IV. Digital Constitutionalism: A Constitutional Model For the People, By the People, and Of the People

Initially, pressure for reform came from the wealthy and powerful who wanted to gain a political power to match their economic influence. After the French Revolution, this notion reached wider audiences. The first *Reform Act of 1832* extended voting rights to males who rented land of a certain value.[19] After World War I ended in 1918, a proportion of women were able to vote – the *Representation of the People Act* granted the voting rights to women over 30, but only if they met a certain property qualification, for instance, if they were wives of householders or university graduates.[20] This act also enabled all men over the age of 21 to vote and eradicated the previous property restrictions in place. Universal suffrage was finally achieved through the *Equal Franchise Act of 1928*, when all women over 21, of all classes, were able to vote, increasing the female electoral number to 15 million. The voting age was further lowered to 18 in 1969. The acts passed reflect the need for a representative and inclusive government. Therefore, Digital Constitutionalism in the United Kingdom must have the representation of all stakeholders. It should also take into consideration their opinions and interests since representation and inclusion hold prime importance.

The history of the United Kingdom has resulted in a democracy with universal adult franchise. As a result, it creates a society in which all stakeholders must be valued equally and have equal influence in the decision-making process. It is suggested that Digital Constitutionalism should learn from the United Kingdom's experience and adopt analogous approaches in the creation of Digital Constitutional discourse and the formulation of digital policy, to the extent practicable. While formulating the Digital Constitutionalism in the United Kingdom, the opinions and interests of the stakeholders and citizens should be taken into consideration.

V. Inclusive, Representative and Equal Online Spaces

In 2018, about 13.8% of the UK population was from a minority ethnic background with London having 40% of its population from the Black, Asian & Minority Ethnic (BAME) background. Digital exclusion is another facet of the deep inequalities, which run through the social fabric of the UK, and is more widespread than many people are aware of.[21]

The government's policies on regulation and competition play an important role in creating the foundations for universal access in the UK; the *1999 Electronic Communications Bill's* provisions on digital signatures and the auction of five broadband mobile communications licences are excellent examples, as are moves to liberalise the "last mile" of communications networks.[22] Yet, the digital divide in the UK persists. A report published by UK innovation foundation Nesta in December, 2020 said data poverty is a common problem among disadvantaged groups. Telecoms regulator Ofcom said that 2% of UK households with children have no access to the internet, 4% have only mobile access and 9% have no home access to a laptop, desktop or tablet. Many families across the country felt the financial strain of the pandemic last year, with almost one-fifth of households, 4.7 million in total, struggling to pay their broadband or mobile data bills.[23]

Based on the overall framework established at the international level, national governments need to identify their own social inclusion goals and objectives, incorporating their specific needs and context. Therefore, the

---

[18] Parau CE, 'Core Principles of the Traditional British Constitutions' <https://www.politics.ox.ac.uk/materials/Core_Principles_of_the_British_Constitutions.pdf> accessed March 25 2021.

[19] S. Zubair and others, 'Suffrage in the UK – a Brief Study of the History of the Vote' (*Kettle Mag* 6 June 2017) <https://kettlemag.co.uk/suffrage-in-the-uk-a-brief-study-of-the-history-of-the-vote/> accessed March 27, 2021.

[20] ibid.

[21] 'Opinion: Coronavirus Has Intensified the UK's Digital Divide' (*University of Cambridge*, 6 May 2020) <https://www.cam.ac.uk/stories/digitaldivide> accessed March 27 2021.

[22] Berg B, Page M and Melford M, 'Internet Access for All: The Uk Plan to Close the Digital Divide' (st*rategy+business* 1 April 2000) <https://www.strategy-business.com/article/16945> accessed March 27 2021.

[23] Collins K, 'When the Choice Is Internet or Food, Broadband Policies Aren't Working' (*CNET*) <https://www.cnet.com/home/internet/in-the-uk-some-families-must-choose-between-internet-access-and-food/> accessed August 27 2021.

UK requires broad social inclusion goals or objectives that need to be connected to the particular vision people have for their society – a positive image of an inclusive society of the future. This vision needs to be framed as concretely as possible, which allows effective monitoring and analysis, possibly using a set of indicators. It is useful to set a couple of principles to make social inclusion goals more explicit. Such principles may be: shared future, rights and civic responsibilities, mutual respect, respect for diversity, social cohesion, equality, equity, social justice, social contract, trust in the institutions as well as in neighbours, sense of belonging, inter-connectedness, etc.

VI. Role of Open-Source Intelligence in the Future

The Ministry of Defence in the UK provides a more specific definition of OSINT: "intelligence derived from publicly available information that has limited public distribution or access."[24] In particular, they state that OSINT material is especially useful when "exploited by trained analysts to ensure the intelligence produced is unbiased and free of prejudice, open-source material is no less important than protectively marked material..[25] This statement of OSINT being equal to other forms of intelligence is a recurring theme within official doctrine around OSINT; however, many of these reports also mention that it sometimes can have difficulty in being taken seriously.[26] In the UK, both law enforcement and the military have incorporated the use of open source intelligence (OSINT) into their daily operations. Both military and law enforcement officers may, when authorised, draw upon 'open source' data that a non-service civilian could not gain access to. Two such examples include; driver and vehicle registrations (DVLA databases) and financial data including credit ratings and banking providers.[27]

OSINT has merits of its own as a single intelligence source, particularly in the military domain it can also be used to validate information garnered from closed intelligence sources and as such may enable the protection of a closed source though obtaining the same information from an open one. OSINT can also be utilised as part of an 'all-source analysis' bringing further credibility to the intelligence as it has been verified through multiple sources. The UK government has also launched projects to improve current public perceptions of UK policing OSINT including Fundamental OSINT Research. The 2013-2014 Annual Report from the Chief Surveillance Commissioner has a section (Pages 20-21, Points 5.30-5.33) on using social networking sites as an investigation/surveillance tool. In *Locke v. Stuart and AXA Corporate Solutions*,[28] the insurers were able to show that motor accident claims were fraudulent by producing three large files of Facebook searches, concerning 28 account holders, which revealed links between many of those suspected to have been involved in a fraudulent series of road traffic claims in the Birkenhead area between 2006 and 2007. The judge endorsed the proper use of Facebook in such circumstances. Even in *Safetynet Security Ltd v. Coppage*,[29] the defendant was sued for breach of a non-solicitation covenant in his contract of employment during which the claimants attacked the defendant's credibility by referring to the fact that he had lied on his Facebook page, as they put it, "he claimed to be an ex-SAS officer and did not reveal that he was an ex-police officer when asserting his credentials in security." In the near future, it is expected that the use of OSINT within the military will only increase simply due to the amount of information being made available online, the ease with which it can be accessed, the relatively low-cost of obtaining it compared with other intelligence sources as well as counteracting the feeling of not being left behind, i.e., everyone else is doing it.[30]

In using OSINT for investigations both the military and the police have to tread a fine line around perception and how this impacts on the privacy of those who are under investigation. There are various other ethical considerations arising out of the use of OSINT including incorrect automated analysis as many OSINT-related cases involve cleaning, organising and analysing deluges of raw data.[31] No technology platform is infallible, and the resulting analysis could have harmful consequences if it is wrong. Moreover, the origin and intent of

---

[24] Wells D and Gibson H, 'OSINT from a UK Perspective: Considerations from the Law ...' (*Sheffield Hallam University Research Archive)* <http://shura.shu.ac.uk/17412/2/OSINT_EASS.pdf> accessed March 27 2021.

[25] ibid.

[26] Wells D and Gibson H, 'OSINT from a UK Perspective: Considerations from the Law ...' (*Sheffield Hallam University Research Archive)* <http://shura.shu.ac.uk/17412/2/OSINT_EASS.pdf> accessed March 27 2021.

[27] ibid.

[28] Locke v Stuart and AXA Corporate Solutions [2011 EWCH] 399 QB.

[29] Safetynet Security Ltd v Coppage [2013] EWCA Civ 1176.

[30] "UK Public Safety & Homeland Security Market - 2017-2022" (*Homeland Security Market Research*) <https://homelandsecurityresearch.com/reports/uk-public-safety-homeland-security-market/> accessed March 27 2021.

[31] Stephen Pritchard, OSINT: What is open source intelligence and how is it used? (*The Daily Swig* 19 November 2020) https://portswigger.net/daily-swig/osint-what-is-open-source-intelligence-and-how-is-it-used accessed November 8. 2021.

the intelligence can bias the data sample and create mislead analysis.[32] Furthermore, there is a blurring of lines between Human Intelligence (HUMINT) and OSINT (particularly when dealing with crowdsourcing intelligence). This concern would also be present when police or military extrapolate investigations and operations to third parties or outside experts.. As the *GDPR (General Data Protection Regulation)* comes into force this also raises concerns around the access and storage of personal data; although, there are exceptions around law enforcement. Further confusing the issue are the complications that will arise as the UK looks to leave the EU and implements its own legislation away from existing EU law. [33]

So far, OSINT has shown to be a potential technique for improving cyber intelligence, and digital forensics. The potential influence of this technique on society, owing to current technology and a huge number of open sources is yet to be fully realised. However, it is equally essential to serve the ethical considerations arising out of use of OSINT. Therefore, it can be fairly concluded that OSINT: the discipline of assembling and analysing publicly available information will have a bright role in the future if implemented with caution.

VII. An Integrative Digital Constitution To Cater To a Pluralistic Society and Pluralistic Enterprise

Constitutionalism speaks to the broad conviction that an institutional and normative framework for our common forms of political life can be supplied through a legal code. Pluralism offers a concept with an even wider referential scope.[34] Yet what all variants of pluralism have in common is an emphasis upon the existence of a multiplicity and diversity of sources of whatever is central to the particular plural domain in question, and upon the need to accommodate that multiplicity and diversity in terms that are not reducible to a set ranking or any other general ordering formula.[35] In the United Kingdom, 87% of people in the UK are White, and 13% belong to a Black, Asian, Mixed or Other ethnic group. In England and Wales, there are 18 ethnic groups recommended for use by the government when asking for someone's ethnicity.[36]

The enforcement of Digital Constitutionalism will always be contingent on the will of the state, and therefore, certain standards have to be established in order to limit the potential arbitrary use of the state's power. It will be difficult to impose values in the absence of standards to follow, especially in developing nations, where the state controls the public realm. The UK consists of a pluralist society. It is vital for this pluralistic society to cater to the interests of these different stakeholders. Digital Constitutionalism will have to find a balance between an integrative model, which draws upon and comprehensively presents standards for specific laws (e.g. antitrust, evidentiary standards and a pluralistic enterprise, which is in accordance with the pluralistic world we are living in. This would assure that a digital environment is inclusive, representative, and equitable.

VIII. Competition Laws of the United Kingdom and Their Role In Protecting The Global Market from Big Tech Dominance

Competition policy is integrated into the UK's general policy framework for regulation in several complex ways. The role of competition policy in regulatory reform is recognised in practice and in recent statements of principle. As regulatory reform stimulates structural change, vigorous enforcement is needed to preclude the possibility that private market abuses might reverse the benefits of reform.[37] The UK adopted explicit competition policy instruments over 50 years ago. The central institutions are the Department of Trade and Industry (DTI), the Director General of Fair Trading (OFT), and the Competition Commission (formerly the Monopolies and Mergers Commission). Enactment of the *Competition Act 1998* is the most visible sign of a credible emphasis on enforcement.[38] It adopts the "prohibition" approach to restrictive practices and abuse of dominance, while streamlining and strengthening the enforcement process. Yet, the UK's general reliance on sectoral specialization to apply competition policy is explained in part by the lack of strong competition policy tools at the time public monopolies became private ones. The report of the Digital Competition Expert Panel

---

[32] ibid.

[33] Wells D and Gibson H, "OSINT from a UK Perspective: Considerations from the Law …" (*Sheffield Hallam University Research Archive)* <http://shura.shu.ac.uk/17412/2/OSINT_EASS.pdf> accessed March 27 2021.

[34] Walker, Neil, Constitutionalism and Pluralism: A Conflicted Relationship? (2016) https://ssrn.com/abstract=2849038 accessed November 8 2021.

[35] ibid.

[36] Government of the United Kingdom, *Ethnicity Facts and Figures* <https://www.ethnicity-facts-figures.service.gov.uk/> accessed August 27 2021.

[37] OECD Reviews of Regulatory REFORM: United Kingdom 2002: Challenges at the Cutting Edge (2002) OECD Publishing https://www.oecd-ilibrary.org/governance/oecd-reviews-of-regulatory-reform-united-kingdom-2002_9789264199255-en accessed August 27 2021. .

[38] ibid.

(DCEP Report), led by Jason Furman, was released in March 2019. The DCEP Report offered a number of suggestions for reforms to the UK's competition regime in response to fundamental economic changes brought on by the expansion of digital marketplaces. In March 2020, the UK Government accepted the recommendations made by the DCEP Report and instructed the taskforce to "consider the practical application of the potential pro-competitive measures set out by the DCEP." Similarly, the Competition and Markets Authority (CMA) completed and published the findings of a market study on online platforms and digital advertising in July 2020. Following the CMA's four key recommendations following the online platforms and digital advertising market research, the UK Government stated its general approval of the CMA's four main recommendations, including the decision to construct a Digital Markets Unit (DMU) to be headquartered inside the CMA, in November 2020.[39] The UK government is planning on creating new rules, which would limit the power of tech giants like Google and Facebook. Reports state that these rules will be legislated in 2022.[40]

The practice and the range of variations on the institutional themes, display the UK's predisposition for particularly in institutional structures, for pragmatic adjustment rather than comprehensive design, as well as a general concern to diffuse power widely. Institutions and systems for ensuring consistency among the many regulators with concurrent, overlapping powers seem to be working, but the boundary between sectoral and general competition policy competence is still contested occasionally.

The citizens still don't regard competition to be an important issue. A recent survey of experienced observers in the UK reports that only 10% thought competition policy was important to the UK public; by comparison, in the US the figure was 83%.[41] The Blue Ribbon regulatory reform group, the Better Regulation Task Force, does not mention competition or market solutions in its "Five Principles of Good Regulation", which are preoccupied instead entirely with process issues such as transparency, accountability, proportionality, consistency, and targeting. But that relative lack of direct attention may simply result from lack of direct familiarity, as competition policy had not been at the top of the agenda before.[42]

To regulate big tech effectively, legislation will need to harmonise competing policy objectives, notably privacy and antitrust law, encouraging competition while also offering individuals sufficient protection in their interactions with digital markets.

IX. Role of Grassroot Judicial and Social Media Actors in the Digital Ecosystem

The rise of non-state actors has changed society, nationally and internationally, in ways that are increasingly recognised. In the digital ecosystem of the United States, different non-state actors like civil society organisations have played an important role in upholding digital freedom. For example: Stop Funding Hate, a UK grassroots activist campaign which gets people to ask brands to stop advertising in newspapers publishing racist and anti-migrant content. Organisations like Ford Foundation are working to ensure equal access to, and fair regulation of, digital technology that is designed to advance transparency, privacy, access to knowledge, and free expression for all people.[43] Another organisation, Privacy International, is examining the actions of governments, the organisation also researches, investigates and exposes the producing, selling and distribution of surveillance technology.[44] Social media platforms have revolutionised our ability to connect across historic social, political and geographic divides. A local organisation named Open Technology Fund (OTF) has announced an 'Internet Freedom Fund' Program to support projects and people working on open

[39] James Marshall & Thomas Reilly, UK CMA Published Recommendations for the Regulation of Digital Markets (*Covington Competition* 11 December 2020) https://www.covcompetition.com/2020/12/uk-cma-published-recommendations-for-the-regulation-of-digital-markets/ accessed November 8, 2021.

[40] Mark Scott, UK targets Big Tech with New Competition Rules (*Politico* 27 November 2020) https://www.politico.eu/article/uk-targets-big-tech-new-competition-rules/ accessed November 8 2021.

[41] Christian Ahlborn - William Leslie - Nayantara Ravichandran, UK's CMA seeks new regulatory regime to take on Google and Facebook (*Linklaters* 2020) https://www.linklaters.com/en/insights/blogs/linkingcompetition/2020/july/uks-cma-seeks-new-regulatory-regime-to-take-on-google-and-facebook accessed April 4 2021.

[42] ibid.

[43] "Technology and Society" (*Ford Foundation* 11 August 2021) <https://www.fordfoundation.org/work/challenging-inequality/technology-and-society/> accessed August 27 2021.

[44] Magee T, "Here Are the UK Ngos Fighting for Digital Rights, Data and Privacy" (*Computer world* February 3 2016) <https://www.computerworld.com/article/3557640/the-uk-ngos-fighting-for-digital-rights-data-and-privacy.html> accessed August 27 2021.

and accessible technology-focused projects that promote human rights, internet freedom, and open societies.[45]

Inter-judicial Cooperation has to be also noted. The Strasbourg Court has played a crucial role not only in protecting the aforementioned fundamental rights but also underlining the constitutional challenges coming from new technologies.[46] Moreover, in *Chambers v. DP*[47], the High Court of the United Kingdom held that users "are free to speak not what they ought to say, but what they feel."

X. Traditional Constitutionalism v. Digital Constitutionalism

Constitutionalism evolves constantly. Its underlying values, ideals, principles have changed over time. Digital Constitutionalism is an appealing concept to explain the recent emergence of constitutional counteractions against the challenges produced by digital technology.[48] The notion of constitutionalism emerged at the beginning of the 19th century as a response to absolute monarchy and popular despotism. The power of the government should be legitimated by the constitution, an expression of popular sovereignty, and should be bound by the constitution, which represents its ultimate limit. This normative vision of society championed by the original constitutionalism was subsequently enriched with other ideals.[49] As a result, it is argued that the conventional idea of constitutionalism has not been static for a long time. As a result, we may expect certain modifications when these values are reconfigured in the digital world, which is fundamentally dynamic. Therefore, the Digital Constitution must be adaptable to evolving technology, or it will become obsolete and unable to preserve the freedoms and rights it was designed to protect. [50]

A series of ongoing transformations in contemporary society are challenging existing constitutional law apparatuses. The changes prompted by the digital revolution in relation to ourselves, our relationships with other individuals and, ultimately, in the society at large ferment under a vault of constitutional norms that have been shaped for 'analogue' communities.[51] However, the constitutional ecosystem does not lie inert. Existing constitutional settings are being modified or integrated in a way that better addresses the transformations of the digital age. We are witnessing a new constitutional moment: a complex process of constitutionalization is currently under way.[52]

The increased power of states that, through the use of digital technology, have gained even more control over the lives of their citizens. The *Data Protection Act 2018* controls how your personal information is used by organisations, businesses or the government. The UK is about to become one of the world's foremost surveillance states, allowing its police and intelligence agencies to spy on its own people to a degree that is unprecedented for a democracy. The UN's privacy chief has called the situation "worse than scary." Edward Snowden says it is simply "the most extreme surveillance in the history of western democracy." The legislation in question is called the *Investigatory Powers Bill*. The bill will legalise the UK's global surveillance program, which scoops up communications data from around the world, but it will also introduce new domestic powers, including a government database that stores the web history of every citizen in the country. The UK spies will be empowered to hack individuals, internet infrastructure, and even whole towns — if the government deems it necessary.[53]

But also, the power of the new 'silicon giants,' potent multinational companies that, by managing digital products and services, de facto influence the way in which we enjoy our fundamental rights. A paradigmatic example is the progressive development of data protection law. An area of law that has profound

---

[45] "Internet Freedom Fund 2021" (Funds ForNGOs 18 March 2021) <https://www2.fundsforngos.org/latest-funds-for-ngos/internet-freedom-fund-2021/> accessed August 27 2021.

[46] Dominika Bychawska-Siniarska, Protecting the Right to Freedom of Expression under the European Convention On Human Rights- A handbook for legal practitioners, available at https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814 accessed March 24 2021.

[47] Chambers v. DPP (27 July 2012), High Court, [2012] EWHC 2157.

[48] Celeste E, "Digital Constitutionalism: A New Systematic Theorisation" (*Sutherland School of Law*, *University College Dublin*, *Dublin*, *Ireland*) <http://doras.dcu.ie/24697/1/E.%20Celeste_IRLCT_Digital%20Constitutionalism_AM.pdf> accessed March 12 2021.

[49] ibid.

[50] Kenny MacIver & Rae Ritchie. 'The importance of developing a digital constitution' (*Fujitsu*, November 2019) <https://www.i-cio.com/big-thinkers/andreas-ekstroem/item/the-importance-of-developing-a-digital-constitution> accessed March 28 2021.

[51] Celeste E, 'Digital Constitutionalism: How Fundamental Rights Are Turning Digital' (*Convoco!* 26 January 2021) <https://www.convoco.co.uk/digital-constitutionalism-how-fundamental-rights-are-turning-digital/> accessed March 27 2021.

[52] ibid.

[53] Vincent J, 'The UK Now Wields Unprecedented Surveillance Powers - Here's What It Means' (*The Verge* 23 November 2016) <https://www.theverge.com/2016/11/23/13718768/uk-surveillance-laws-explained-investigatory-powers-bill> accessed August 27 2021.

constitutional implications, as it is designed to limit the power of public and private actors to control our digital body, and in parallel aims to strengthen a series of positive rights of the individuals, such as their capability to freely develop their personality in the online world.

XI. Diverse National Frameworks vis-à-vis Global Digital Constitution

In the digital domain, national boundaries lose their significance. Therefore, the question arises how to create the necessary global rules and norms that govern the digital world. In recent years, we have witnessed the emergence of over 100 proposals for basic rights and principles. These initiatives share the goal of transposing the values of our analogue world to the virtual one. They are the products of state initiatives, international conferences, scientific projects, private forums and individual creativity.[54] Through this discourse, constitutional principles are evolving that may not be legally binding, but exhibit significant normative power to guide public debate and global governance.[55] Not only in the institutional perimeter of nation-states, but also beyond; on the international plane, in the private fiefs of multinational technology companies, within the civil society.[56]

The UK takes a fundamentally dualist view of international law. In other words, it sees domestic and international law as operating on different planes. International law has of course inspired the common law. The UK's international commitments are also the basis of much domestic legislation. But the reception of international law into domestic law depends upon its acceptance in one of two ways: either by Parliament through legislation or by the judges through the common law. This principle rests on the so-called dualist theory, which is based on the proposition that international law and domestic law operate in independent spheres. The prerogative power to make treaties depends on two related propositions. The first is that treaties between sovereign states have effect in international law and are not governed by the domestic law of any state. The second proposition is that, although they are binding on the United Kingdom in international law, treaties are not part of UK law and give rise to no legal rights or obligations in domestic law.[57]

Different states view digital freedom differently. It is a peculiarity of the internet that information uploaded is available globally (and therefore is ubiquitous) and thus is subject to a variety of international, national or supra-national rules, which can lead to different, if not contradictory treatment.[58] One example is the existence of different approaches to freedom of expression in the United Kingdom and the United States. Studying freedom of speech in the United Kingdom involves examining the ways in which parliamentary acts, and to a certain extent the common law, restrict free speech in such areas as obscenity, libel, government secrets, and press reporting of trials. While American free speech is not absolute, and governmental restrictions certainly exist in all of these areas, the study of freedom of speech in America proceeds from an importantly different angle.[59] In the United Kingdom, the courts have been more willing to grant injunctions against publications containing confidential governmental information when it is "in the national interest" to do so. In a recent high-profile case, British courts enjoined newspaper publication of the book, *Spycatcher*, the memoirs of a former British intelligence officer. The injunction was only dissolved after the publication of the book in the United States had destroyed the secrecy of its contents.[60]

However, the UK legal community has been at the forefront of the development and promotion of international law and international human rights law. The UN treaty framework – the UK is bound by many UN human rights treaties, including the *International Covenant on Civil and Political Rights (ICCPR)* and the *International Covenant on Economic, Social and Cultural Rights (ICESCR)* – exists to protect the rights of individuals at home and requires domestic law, policy and practice to respect minimum standards agreed on a global stage. This global legal framework plays an important part in justice's work in promoting respect for the rule of law and individual rights within our justice system. The UK justice system is not just important

---

[54] Celeste E, 'Digital Constitutionalism: How Fundamental Rights Are Turning Digital' (*Convoco!* 26 January 2021) <https://www.convoco.co.uk/digital-constitutionalism-how-fundamental-rights-are-turning-digital/> accessed March 27, 2021.

[55] ibid.

[56] Celeste E, 'Digital Constitutionalism: How Fundamental Rights Are Turning Digital' (*Convoco!* 26 January 2021) <https://www.convoco.co.uk/digital-constitutionalism-how-fundamental-rights-are-turning-digital/> accessed March 27 2021.

[57] ibid.

[58] Wolfgang Benedek and Matthias C. Kettemann, 'Freedom of Expression and the Internet', available at https://rm.coe.int/prems-167417-gbr-1201-freedom-of-expression-on-internet-web-16x24/1680984eae accessed on 24th March 2021.

[59] Shapiro SJ, 'Comparing Free Speech: United States v. United Kingdom' (*University of Baltimore Law Forum 1989*). <https://scholarworks.law.ubalt.edu/cgi/viewcontent.cgi?article=1516&context=lf> accessed March 22 2021.

[60] ibid.

domestically. As the birthplace of the common law, this country is often held up as a 'Gold Standard' for the way in which legal systems should operate the world over.
Global constitutionalization is likely to compensate for globalization-induced constitutionalist deficits on the national level, that a constitutionalist reading of international law can serve as a hermeneutic device, and that the constitutionalist vocabulary uncovers legitimacy deficits of international law and suggests remedies. global constitutionalism, therefore, has a much-needed critical potential.[61]

B. Human and Constitutionally Guaranteed Rights

I. Human and Constitutional Rights and Online Platforms

A. Right to Privacy

The *Human Rights Act 1998 (HRA)* of the UK, is based on, and "gives further effect" to, the rights and freedoms contained in the *European Convention on Human Rights (ECHR)*.[62] Of particular relevance is the right to respect for private and family life provided in Article 8 of the ECHR.[63] Given that the ECHR is not an EU institution, it is not affected by Brexit.[64]

The *Regulation of Investigatory Powers Act 2000 (RIPA)* does not ensure that interception and access to communications data is carried out in accordance with the standards of privacy in *Article 17 of the ICCPR*.[65] This is concerning because on several occasions, there have been issues with government surveillance in the UK.[66] For example, under the United Kingdom's Prevent Programme, Muslim children can be referred to the authorities for exercising their curiosity about Islamist extremism or speaking out on behalf of oppressed groups.[67] Thus, people's right to privacy does not attract the protection it deserves via digital surveillance regulation in the UK, which has a significant impact on human rights.

B. Freedom of Expression

The Freedom House, a US-based non-profit which issues a ranked, country-by-country assessment of online freedom, has consistently given the UK a fairly high internet freedom score. It recognises that UK users have substantial internet freedom with few major constraints on access or content.[68] Via *Article 10 of the European Convention*, the UK protects freedom of expression, including the right to hold opinions, and to receive and share ideas without government interference.[69]

The UK plans on introducing a new censorship regime for social media as expressed in a 2019 White paper,[70] currently encompassed in its draft *Online Safety Bill*.[71] Introduced in May 2021 and currently being considered

---

[61] Peters, Anne. 'The Merits of Global Constitutionalism.' (2009) 16 (2) Indiana Journal of Global Legal Studies <www.jstor.org/stable/10.2979/gls.2009.16.2.397> accessed August 22 2021.

[62] Human Rights Act 1998, preamble.

[63] European Convention on Human Rights, art 8.

[64] Frederick Cowell, 'The Brexit deal locks the UK into continued Strasbourg Human Rights court membership' (*LSE Blog*, 17 January 2021) <https://blogs.lse.ac.uk/brexit/2021/01/17/the-brexit-deal-locks-the-uk-into-continued-strasbourg-human-rights-court-membership/> accessed 7 April 2021.

[65] Privacy International, *The Right to Privacy in the United Kingdom* (2015) 1 <https://www.privacyinternational.org/sites/default/files/2017-12/PI%20submission%20UK.pdf>

[66] 'UK government claims power for broad, suspicionless hacking of computers and phones' (*Privacy International*, 18 March 2018) <https://privacyinternational.org/press-release/1350/uk-government-claims-power-broad-suspicionless-hacking-computers-and-phones>

[67] 'Briefing: Children's rights in the digital age' (*Child Rights International Network)* <https://home.crin.org/issues/digital-rights/childrens-right-digital-age>; Secretary of State for the Home Department, *Prevent Strategy* (2011) 18 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf>

[68] 'Freedom On the Internet 2020: United Kingdom', *Freedom House*, https://freedomhouse.org/country/united-kingdom/freedom-net/2020

[69] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222 (entered into force Sept. 3, 1953)

[70] HM Government, *Online Harms White Paper: Full Government Response to the consultation* (White paper, cp 354, 2020) 45 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf

[71] Draft Online Safety Bill, 2021https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

by a Parliamentary Joint Committee,[72] this bill cover 'user-to-user service' and 'search service,'[73] regulating vast areas of the internet.[74] The bill requires service providers to conduct 'illegal content risk assessments' which are tailored differently for children and adults,[75] to ultimately remove content and accounts deemed harmful. Within this classification, journalistic content receives more leeway as compared to expression by ordinary citizens.[76]

The bill requires service providers to take the lead on assessing and regulating content, which gives these entities a high level of control, making them the "gatekeepers" to freedom of speech in the UK.[77] The bill prescribes some factors to be considered in regulating content and major penalties for failing in this duty of care toward users,[78] but that is about the external interference in service providers regulation.[79] Moreover, the definitions and factors provided are loose and wide. For instance, the term 'content harmful to children' is defined as content which the "provider… has reasonable grounds to believe that the nature of the content is such that there is a material risk of the content having, or indirectly having, a significant adverse physical or psychological impact on a child."[80] The bill does not prescribe for an appeal or review mechanism for users to avail of with respect to service providers decision. Thus, the regulation under the bill is solely vested in the hands of service providers, with no mechanism to question the decision-making. It raised a big question as to how equipped private entities are to play judge and jury in regulating netizens' freedom of internet access and expression.

C. Right to Equality

The *Equality Act 2010* prohibits direct and indirect discrimination by private on the grounds of age (but only if an individual is 18 or over); disability; gender reassignment; pregnancy and maternity; race; religion or belief; sex; and sexual orientation.[81] An investigation by the Financial Times has revealed several shocking examples of how targeted advertising in the UK had resulted in discriminatory outcomes.[82] For instance, several companies have advertised for jobs only to a certain age group, while Facebook was found to be accepting housing advertisements discriminating by race, and advertisements aimed specifically at 'Jew haters'.[83]

Such discriminatory advertising is an example of a violation of the right to equal treatment in the digital ecosystem. It is also an example of the difficulties the UK faces in enforcing human rights in the digital space, a combination of poor government regulation, which ought to be stricter, and the nature of the internet itself.

II. Netizens in the UK

The *Section 124N of the UK Communications Act*, *2003* defines a subscriber in relation to an internet access service, to mean a person who (a) receives the service under an agreement between the person and the provider of the service; and (b) does not receive it as a communications provider.[84] Additionally, the same section defines an 'internet access service' to be one provided to a subscriber consisting entirely or mainly of the provision of access to the internet and includes the allocation of an IP address(es) to the subscriber to

---

[72] https://committees.parliament.uk/committee/534/draft-online-safety-bill-joint-committee/

[73] Draft Bill (n 72), Section 2

[74] Alex Hern, 'Internet crackdown raises fears for free speech in Britain' *The Guardian* (London, 11 April 2019) <https://www.theguardian.com/technology/2019/apr/08/online-laws-threaten-freedom-of-speech-of-millions-of-britons>

[75] Draft Bill (n 72), Section 7

[76] Draft Bill (n 72), Section 14

[77] Giacamo Lee, 'Why the Online Safety Bill fails, and what can make the internet safer' (*Pharmaceutical Technology*, 7 September 2021) < https://www.pharmaceutical-technology.com/features/why-the-online-safety-bill-fails-and-what-can-make-the-internet-safer/">

[78] Draft Bill (n 72), Sections 5-16

[79] Draft Bill (n 72), Section 85

[80] Draft Bill (n 72), Section 45

[81] The Equality Act 2010

[82] Joint Committee on Human Rights, *The Right to Privacy (Article 8) and the Digital Revolution* (2019, HC 122, HL 14) 17 https://publications.parliament.uk/pa/jt201919/jtselect/jtrights/122/122.pdf

[83] Joint Committee on Human Rights, *Oral evidence: The Right to Privacy (Article 8) and the Digital Revolution*, (HC 1810) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/the-right-to-privacy-article-8-and-the-digital-revolution/oral/103572.html>

[84] The UK Communications Act 2003, s 124N; Alexander Brown and Peter Broadhurst, 'In brief: telecoms regulation in United Kingdom' (*Lexology*, 14 June 2019) https://www.lexology.com/library/detail.aspx?g=f76f1dfe-cc2b-497b-baf9-10b5a2b2b322

enable that access.[85] Thus, any user of such internet provision would technically be enabled to be a netizen as per the UK law.

Also of relevance is *Directive 2000/31/EC of the European Parliament* on certain legal aspects of information society services. *Article 2(d) of the Directive* defines 'recipient of the service' to be any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking such as: information or making it accessible.[86] While this is limited to users of information services, which is considerably narrower than general users of the internet, it adds on to the idea of the UK legal understanding of users of the internet and its services.

III. Bad Actors and Netizens

Bad actors are not those who just violate the terms of conditions governing digital relationships but those who breach the ethical obligations it "owned" to them and the terms of informed consent. For example, in 2018, UK-based Cambridge Analytica came under fire for acquiring private Facebook data of tens of millions of users to sell psychological profiles of American voters to political campaigns.[87] This is a clear classification of the firm as a "bad actor".

Bad actors could also be small-scale criminals, hacktivists, companies and state entities. For example, as per *Section 127 of the UK Communications Act*, *2003*, making improper use of public electronic communications networks by sending messages that are grossly offensive or of an indecent, obscene or menacing character is a criminal offence.[88] Similarly, *Section 1(2A)(a) of the Malicious Communications Act*, *1988* makes the offence of sending electronic communications with intent to cause distress or anxiety a criminal offence.[89] Thus, the law makes netizens liable by virtue of recognising their 'netizenship', so as to speak.

Thus, netizens can be bad actors and the line between the good and the bad is definitely a sticky one. More importantly, bad actors should be considered netizens; else the accountability factor may not really come into play. Netizens are bound by legal and ethical obligations to one another, and it is a breach of such obligations that characterise a bad actor. To draw a rather simplistic parallel, when a citizen of a country breaches its laws, he does not lose citizenship, rather it is his citizenship that makes him accountable in that country.

IV. Minorities' Rights in Digital Ecosystems

There exists a fairly significant digital divide when examining minorities' access to as well as their rights on the internet.[90] Some minority needs identified in the UK and solutions to meet the same could be:

A. Health Information Seeking for Women and Racial Minorities

Access to internet and digital skills is not universal and evidence shows that marginalised ethnic groups have worse internet access.[91] This has wide ranging impacts, especially in the current context of a pandemic, including higher likelihood of isolation and being less able to access important public health guidance.[92] People from Black, Asian and minority ethnic (BAME) communities are more likely to face digital exclusion which further compounds social isolation and poor mental health as we increasingly rely on technology for social connection.[93]

B. Countering Hate Speech Against Minorities

Hateful content online is a growing problem in the UK which can pollute civic discourse and exacerbate social divisions. In general, there are two paths that can be identified to counter such content- the legal path and the technological one.

---

[85] ibid; Practical Law Media & Telecoms, 'Telecoms: a quick guide' https://uk.practicallaw.thomsonreuters.com/9-503-2464?transitionType=Default&contextData=(sc.Default)&firstPage=true

[86] ibid art 2(d)

[87] Nicholas Confessore, 'Cambridge Analytica and Facebook: The Scandal and the Fallout So Far' (*New York Times*, 4 April 2018) <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>

[88] cf Communications Act (n 84), s 127.

[89] Malicious Communications Act 1988, s 1(2A)(a)

[90] Minority rights group international, *Minority and Indigenous Trends 2020: Focus on technology* 18 (2020) https://www.ohchr.org/Documents/Issues/Racism/SR/RaceBordersDigitalTechnologies/Minority%20Rights%20Group%20International.pdf

[91] Angela Chen, 'Marginalized ethnic groups have poorer internet access even in the same country' *TheVerge* (8 September 2016) https://www.theverge.com/2016/9/8/12854476/internet-access-marginalized-ethnic-groups-digital-divide

[92] S Germain, and A Yong, 'COVID-19 Highlighting Inequalities in Access to Healthcare in England: A Case Study of Ethnic Minority and Migrant Women' (2020) 28 Fem Leg Stud 301–310

[93] 'AREA 1: HEALTH INEQUALITIES' (*Charity So White*) https://charitysowhite.org/covid19-health-inequalities

Legally, the UK does outlaw hate speech, specifically that which incites racial hatred.[94] *Section 4 of the Public Order Act 1986* makes it an offence for a person to use "threatening, abusive or insulting words or behaviour that causes, or is likely to cause, another person harassment, alarm or distress."[95] *Section 127 of the Communications Act 2003* makes it illegal to send a message via a public electronic communications network that is considered grossly offensive, or of an indecent, obscene or menacing character. Additionally, in a recent 2020 consultation paper, the UK government has made a number of proposals for reform of hate crime laws, including adding sex or gender as a protected characteristics under the law.[96]

Regarding the latter path, the Alan Turing Institute is working on a project to develop tools for automatically identifying and categorising hateful content.[97] The project involves using advanced computational methods, including supervised machine learning, stochastic modelling and natural language processing, to detect and analyse hate speech. In 2020, the project successfully tackled how to detect east-Asian prejudice on social media, which can now be used to moderate such harmful content.[98]

C. Sophisticated Surveillance Systems Designed to Profile Ethnic and Religious Minorities

Following the 2011 London riots, the Metropolitan Police launched the Gangs Matrix program, a system utilising AI and machine learning to compile a database of gang members. It has been criticised by an Amnesty UK Report as "a racially discriminatory system," finding 35 per cent of those on the matrix to have no priors or police intelligence linking them to gang violence. [99] Sharing certain YouTube videos of grime or drill music, meanwhile, is considered a key indicator of gang affiliation. According to a 2019 Freedom of Information Request obtained by WIRED, some 80 per cent are listed as 'African Caribbean,' with a further 12 per cent from other ethnic minority groups, while only the remaining 8 per cent are listed as 'white European'.[100] Since its inception, the database has listed around 7,000 people, and once someone is on this Matrix, finding out why or getting their name removed can be extremely difficult.

One way to go about securing rights of ethnic minorities in this regard is to strengthen privacy laws. Thankfully, several hundred names were removed from the Matrix in early 2020 to correct ethnic bias and violations of data protection.[101]

D. Diverse Set of Stakeholders Designing and Building AI

Big data is the driving force behind the growth of AI, which is why it is very important to have a diverse set of stakeholders designing and building them'.[102] Unfortunately, as noted in a 2019 study by the AI Now Institute, "there is a diversity crisis in the AI sector across gender and race," with no public data even available for trans or other gender minorities.[103] This lack of diversity is common across the whole science, technology, engineering and mathematics (STEM) field in general, but even more so at universities where the lack of diversity in STEM faculties can arguably be said to impact minority students choosing the field as a career path.

To counter this, the *Athena SWAN Charter* was promoted by the British Equality Challenge Unit in 2005 to promote the inclusion of women in science, technology, engineering, math and medicine (STEMM). The charter now also recognises work in the fields of arts, humanities, social sciences, business and law.[104]

V. Digital Age of Consent

[94] 'Hate speech vs. free speech: the UK laws' *The Week* (12 February 2020) https://www.theweek.co.uk/97552/hate-speech-vs-free-speech-the-uk-laws

[95] Public Order Act 1986, s 4

[96] Law Commission, *Hate crime laws Consultation paper* (Law Com Consultation paper No 250, 2020) 254

[97] 'Hate speech: measures and counter-measures' (*The Alan Turing* Institute) https://www.turing.ac.uk/research/research-projects/hate-speech-measures-and-counter-measures

[98] Bertie Vidgen, Austin Botelho, David Broniatowski et al, 'Detecting East Asian Prejudice on Social Media' (2020) Association for Computational Linguistics https://arxiv.org/pdf/2005.03909.pdf

[99] Met Police using 'racially discriminatory' Gangs Matrix database (*Amnesty International UK*, 9 May 2019) https://www.amnesty.org.uk/press-releases/met-police-using-racially-discriminatory-gangs-matrix-database.

[100] Yeung P, 'The grim reality of life under Gangs Matrix, London's controversial predictive policing tool', *Wired* (2 April 2019).

[101] ibid.

[102] Cf MRGI Report (n 90), at 34.

[103] Startz, D., 'Why is minority representation lagging among STEM faculty? It could be the money' (Brookings, 2017)

[104] CIPPEC, Gender Economic Equality: Bridging the Gender Digital Gap (2018) 12

In the UK, the first legislation brought into force on the issue of the digital age of consent for a child was the European Union's *General Data Protection Regulations (GDPR)* of 2016. [105] The UK brought the GDPR into effect through its national legislation titled the *Data Protection Act 2018 (DPA)*.[106] The UK chose to avail of the option it was given to lower the age of consent from 16, and has opted for the minimum age of 13 years.[107]

A. Factors to Determine this Age

The UK does not have a specific legislation dedicated to the rights of its children but it has ratified the *United Nations Convention on the Rights of the Child (UNCRC)*, which means that it guarantees to its citizens all the rights under the same.[108] Certain rights provided under the *UNCRC* that come into play while considering the digital age of consent for children are: *Article 16* — The right to privacy and the right to not be subjected to unlawful attacks on his or her honour and reputation;[109]*Article 28* — The right of access to information and the right to education; *Article 19* — The right to be safeguarded from all forms of physical or mental violence, injury or abuse, or exploitation;[110]*Articles 13 and 14* — The right to freedom of expression and thought. [111]

B. Rationale Behind the Age Arrived at by the UK

The rationale used by the UK in determining children's rights in regard to web-related services is to "ensure that children have the best possible access to online services whilst minimising data collection and use, by default."[112] It attempts to do so in its recent *Code of Practice for Online Service (Code of 2020)*, prepared under *Section 123 of the DPA 2018*.[113]

The UK government notes that it places particular emphasis on protecting children, particularly their freedom of expression online.[114] One of their priority considerations while making law on data protection is the harmful content and activity affecting children, such as pornography or violent content.[115] Thus, it is by balancing the various rights guaranteed to its children with the harms they face on the internet that the UK has established a higher level of protection for children than for adults. Thus, while the UK remains to keep its digital age of consent at 13 years, it has put in several safeguards applicable on the providers' end which ensure the privacy of its children. Safeguards in this context include obligations on companies to consult with parents and children on risks of exposure to harmful content, undertake assessments of data processing on grounds of necessity and proportionality, risk assessments of data processing with respect to their impact on children, etc. While the *Code of 2020* is more a set of guiding principles, non-compliance will attract assessment notices, warnings, reprimands, enforcement notices and penalty notices (administrative fines). For serious breaches of the data protection principles, fines of up to €20 million (£17.5 million when the *UK GDPR* comes into effect) or 4% of your annual worldwide turnover, whichever is higher, can be imposed.[116] Additionally, the *2021 Bill* also incorporates certain risk assessment measures specifically for children and content that is likely to be accessed by children. However, since the *Code* came into effect only in September 2021, the real effects of regulation are yet to be seen.

---

[105] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[106] Data Protection Act 2018

[107] ibid, s 9(a); Aaron Walawalkar, "Completely Inappropriate': Raise Age Of Digital Consent To 16, MPs Say' (*Each Other*, 5 November 2019) https://eachother.org.uk/raise-age-of-digital-consent/#:~:text=The%20GDPR%20contains%20specific%20protections,the%20UK%20has%20done%20this

[108] United Nations Convention on the Rights of the Child.

[109]Livingstone, 'Reframing media effects in terms of children's rights in the digital age' (2016) 10(1) Journal of Children and Media 5

[110] Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, *Children's data and privacy online; Growing up in a digital age-An evidence review* (2018) 12 https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf

[111] 'Briefing: Children's rights in the digital age' (*CRIN*) https://home.crin.org/issues/digital-rights/childrens-right-digital-age

[112] Information Commissioners Office, 'Age appropriate design: a code of practice for online services' (2020), 5 https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf

[113] Cf DPA (n 106), s 123

[114] HM Government, *Online Harms White Paper: Full Government Response to the consultation* (White paper, cp 354, 2020) 45 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf

[115] ibid 36.

[116] Cf Code (n 112), 12.

VI. Public Order in the Digital Space

In terms of the digital space, public order could refer to the free exercise of individuals' right to information and expression, as guaranteed by *Article 10 of the European Convention*, without violating the personal rights of others such as violating privacy, insinuating racism etc.[117]

The UK is usually hesitant to impose by itself measures to regulate public order in the online world.[118] However, as will be discussed subsequently, the UK has imposed internet shutdowns in the past to quell potential public disorder.[119]

VII. Internet Shutdowns and the Power of States

In the history of the UK, there has been a single state-imposed internet shutdown which occurred on the 17th of April 2019.[120] This is a prime example of the UK allowing for situations of disorder in the offline world to influence the definition and management of public order online when there has been a question of public safety and order involved.

The British Transport Police shut down the fixed-line Wi-Fi on London's Tube network as provided by Virgin Media, the underground transportation system, during a protest by climate change activists Extinction Rebellion.[121]

Rationale Adopted

The rationale adopted by the UK Government was that it was in the interest of safety and was based on intelligence that Extinction Rebellion protesters intended to cause disruption to the Tube service. Thus, the move was required to "prevent and deter serious disruption" by climate change protesters.[122] In fact, this rationale of imposing internet shutdown as "precautionary measures" and to ensure for "public safety" rank as the second and third most-popular justifications adopted by governments to explain their decision to cut off the internet in 2019.[123]

Checks on State Power

In the UK there are two pieces of legislation which give the government power to order the suspension of the internet — the *Civil Contingencies Act* and the *2003 Communications Act*.[124] In this regard, in 2011 a representative of the Department for Culture, Media and Sport said that it would have to be a very serious threat for these shutdown powers to be used, such as major cyberattack. Additionally, the representative noted that the powers are subject to review and if it was used inappropriately there could be an appeal to the competitions appeal tribunal. Also, any decision to use them would have to comply with public law and the *Human Rights Act*.[125]

Thus, the chances of such a shutdown happening in the UK do seem remote, partly because these powers can be used only in times of emergency to protect the public and safeguard national security and partly because consensus governance would act as a check to any nefarious individual ambitions.[126] Therefore, probably owing to the fail-safes in place, an internet shutdown in the UK is possible but not preferred by the government itself. However, the 2019 shutdown didn't seem to meet the threshold of seriousness as conveyed in the laws and executive statements, which could indicate a shift in attitude of the UK government to the use of internet shutdowns for public safety.

The safeguards to avoid an internet shutdown do exist in the UK. To start with, the *Communications Act* only allows the Secretary of State (SoS) to order the Office of Communications (OFCOM) to suspend an internet

---

[117] Cf ECHR (n 63), art 10.

[118] TJ McIntyre, 'Internet Censorship in the United Kingdom: National Schemes and European Norms' in Lilian Edwards (ed), *Law, Policy and the Internet* 2 (Hart Publishing, 2018)

[119] Berhan Tay, *Targeted, Cut Off, And Left In The Dark: The #KeepItOn report on internet shutdowns in 2019* (Access Now, 2019) 9 https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

[120] Joe Tidy & Becky Dale, 'What happens when the internet vanishes?' *BBC News* (25 February 2020) https://www.bbc.com/news/technology-51620158

[121] cf Tay (n 119) 9.

[122] Vincent, J., 'UK police shut off Wi-Fi in London Tube stations to deter climate protesters' *The Verge* (17 April 2019) https://www.theverge.com/2019/4/17/18411820/london-undergroundtube-wi-fi-down-shut-off-protests-extinction-rebellion

[123] Joseph Johnson, 'Official government justifications for internet shutdowns worldwide 2019' (*statista*, 19 March 2019) https://www.statista.com/statistics/1096316/government-justifications-for-internet-shutdowns/

[124] Nick Harding, 'Could The UK Government Shut Down The Web?' *Independent* (8 March 2011) https://www.independent.co.uk/life-style/gadgets-and-tech/features/could-uk-government-shut-down-web-2235116.html

[125] ibid

[126] ibid.

provider's (or any communication services provider) provision of communication services.[127] Such an order can only be made on three grounds — national security, public health and public safety.[128] Upon OFCOM giving such direction, the provider has an opportunity to (a) make representation about the effect of this suspension and (b) propose steps to remedy the situation,[129] and the direction can accordingly be modified by OFCOM[130] or revoked by the SoS.[131] The SoS's order and the OFCOM's decision can be appealed before the Competition Appeal Tribunal by any person affected by the decision or the order.[132]

What can be strengthened is pre-decision accountability. The SoS should be legally required to justify its order as to how it satisfies the grounds in *Section 132*. Moreover, the government should compensate the customers who are inconvenienced

VIII. SMCs in the UK

The UK has always sought to impose a self-regulatory mechanism for the digital space. Since the mid-1990s the government has developed distinctive patterns of regulation — targeting intermediaries, using the bully pulpit to promote 'voluntary' self-regulation, and promoting automated censorship tools such as web blocking. [133] Unfortunately, social media companies do not operate transparently as moderators and decision-making remains opaque and erratic.[134]

Need for Better Social Media Regulation

The *White Paper*, and the *2021 Bill*, proposes to regulate 'legal but harmful' content, which means that protected speech could be removed at scale from social media platforms, undermining free speech rights in the UK. The plans could also result in social media companies using automated tools to proactively monitor what people say on their networks, through fear of penalties or fines. [135]

It is against this background that the UK government has been urged to explore alternatives that would reward companies for demonstrating higher standards of conduct and to consider independent multi-stakeholder models, such as Social Media Councils (SMCs), which would allow public debate and independent oversight of key issues in content moderation.[136]

Solution Model — Integrating SMCs into the UK Legal Infrastructure

The UK already has in place the Equality and Human Rights Commission (EHRC), an independent statutory body for the protection of human rights which proactively undertakes investigations of its own into practices violating human rights. [137] An SMC-like body for widespread digital rights regulation could be set up under the aegis of the EHRC. Just like an SMC, such a council would bring together industry, media, academics, and human rights experts, including civil society organisations that represent the UK public and particularly vulnerable and marginalised groups.[138] The diversity would be a great addition given that it is marginalised groups who face a more severe backlash in terms of digital rights being violated (surveillance, discrimination, etc.). Moreover, given the freedom of censorship granted to social media and other communication intermediaries via the *2021 Bill*, such a regulatory body would instill much accountability to the process. It would provide an appeal forum, which the *2021 Bill* does not envision, and ensure that private companies do not arbitrarily exercise powers of censorship.

---

[127] cf Communications Act (n 84), Section 132(1)

[128] ibid.

[129] cf Communications Act (n 84), Section 132(7)

[130] cf Communications Act (n 84), Section 132(8)

[131] cf Communications Act (n 84), Section 132(9)

[132] Section 192; The Competition Appeal Tribunal (Amendment and Communications Act Appeals) Rules 2004

[133] Ben Wagner, *Global Free Expression – Governing the Boundaries of Internet Content*, *Law*, *Governance and Technology Series* (Cham, 2016) ch 4

[134] Sonia Sangiovanni, 'Social Media Councils' (*Institute for Internet and the Just Society*, 19 December 2020) https://www.internetjustsociety.org/social-media-councils; Kyle Langvardt, 'Regulating Online Content Moderation' (2018) 106 The Georgetown Law Journal 1355

[135] 'UK: Online harms proposals are significant threat to free speech' (*Article 19*, 1 July 2019) https://www.article19.org/resources/uk-online-harms-proposals-are-significant-threat-to-free-speech/

[136] Ibid.

[137] 'Regional Human Rights Bodie's (*Human Rights Commissions)* http://www.humanrightscomm ission.ky/regional-human-rights-bodies#:~:text=The%20UK%20Equality%20and%20Human,rights%20of%20everyone%20in%20Britain.

[138] 'UK: ARTICLE 19 response to leaked reports on online harms white paper' (*Article 19*, 5 April 2019) https://www.article19.org/resources/uk-article-19-response-to-leaked-reports-on-online-harms-white-paper/

C. Intermediary Regulation

I. Online Harms

The internet is an integral part of everyday life for so many people. Nearly nine in ten UK adults and 99% of 12 to 15-year-olds are online.[139] On 15 December 2020, the UK government published its full response to the *Online Harms White Paper (OHWP)* consultation,[140] a proposal to regulate a wide range of harms caused by user-generated content, which sets out final proposals for the new regulatory regime.[141] The *Online Harms paper* has been re-casted by the UK government as the *Draft Online Safety Bill* published in May 2021[142] and a Joint Select Committee has been appointed to consider the same and will report back by 10 December after which the government will look at the report and see if any changes are required. After this the bill will be formally introduced to parliament to begin its journey into law.

Clause 45(3) of the draft Bill defines harmful content as having a "significant adverse physical or psychological impact on a child of ordinary sensibilities."

The types of online harm covered are also wide-ranging. They are split into three categories: harms with a clear definition (such as terrorist content, child sexual exploitation, hate crime and incitement of violence); harms with a less clear definition (such as cyberbullying, coercive behavior, intimidation and disinformation); and underage exposure to legal content.[143] The proposals cover content that is legal but nonetheless harmful. The list of harms is not fixed and will be updated from time-to-time, allowing it to change as technology advances, new harms emerge and expectations develop.[144]

One of the main criticisms is that there is no definition of the term 'online harms' in the bill. A non-exhaustive list is included in the *OHWP* of what constitutes harm, and there are references to 'illegal' and 'unacceptable' content throughout, covering not only content and speech which is illegal (such as child sexual abuse imagery and terrorist propaganda), but content and speech which is legal, but 'harmful'.[145] This is highly problematic in regard to the human rights law criteria that guide restrictions on freedom of expression.

II. Social Media Regulation and Liability

Community guidelines are a set of rules created by each social media platform to ensure a standard of behaviour expected on the platform to create a safe environment for users to interact and have fun.[146]

In the United Kingdom, *the Code of Practice for providers of online social media platforms* offers guidance to providers of social media platforms on appropriate actions they should take to prevent bullying, insulting, intimidating and humiliating behaviours on their sites.[147] This code does not affect how illegal or unlawful content or conduct is dealt with.[148]

In a consultation survey, it was felt that the draft Code of Practice/community guidelines are usually too detailed and prescriptive.[149] Consultation with civil society and disabled people demonstrated an accessibility

---

[139] 'Adults' Media Use and Attitudes Report' (*Ofcom*, 25 April 2018) <https://www.ofcom.org.uk/__data/assets/pdf_file/0011/113222/Adults-Media-Use-and-Attitudes-Report-2018.pdf> accessed 13 Nov 2021

[140] O Dowden and P Patel, *Online Harms White Paper: Full government response to the consultation* (*GOV.UK*, Command Paper No. 354, December 2020) <https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response> accessed 8 April 2021 [hereinafter "RESPONSE"]

[141] 'Online harms: the regulation of internet content' (*Taylor Wessing*, October 2019) <https://www.taylorwessing.com/download/article-online-harms.html> accessed 8 April 2021 [hereinafter "TAYLOR WESSING"]

[142] Minister of State for Digital and Culture, *Draft Online Safety Bill* (Department of Digital, Culture, Media and Sport 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf> accessed 14 Nov 2021

[143] TAYLOR WESSING (n 141)

[144] ibid.

[145] 'Content regulation – what's the (online) harm?' (*EDRi*, 9 October 2019) <https://edri.org/our-work/content-regulation-whats-the-online-harm/> accessed 8 April 2021

[146] 'Understanding community guidelines: Advice for Parents & Cares' (*Internet Matters*) <https://www.internetmatters.org/connecting-safely-online/advice-for-parents/tackling-the-hard-stuff-on-social-media-to-support-young-people/understanding-community-guidelines/> accessed 8 April 2021

[147] Department for Digital, Culture, Media & Sport, 'Code of Practice for providers of online social media platforms' (*GOV.UK*, 8 April 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793324/Code_of_Practice_for_providers_of_online_social_media_platforms.d.pdf> accessed 8 April 2021 [hereinafter "PRACTICE CODE"]

[148] ibid.

[149] ibid.

issue with reporting processes on social media platforms. Additionally, a number of charities flagged a need for better and efficient notification processes.[150] In another survey, it was mentioned that the fact that online platforms apply their own standards makes them "biased by definition".[151] Thus, for proper and efficient drafting of community guidelines the following suggestions may be pertinent:

- Online platforms should implement clear, accessible, and specific terms of service, which should be available in all languages in which the services are offered;
- Online platforms should inform users when a moderation decision is made on their content and they should include adequate information on what triggered the decision, the specific rule that has been infringed, how the content moderation guidelines were interpreted, the actions that will be taken, and clear instructions for an appeal;
- Users should have a possibility to effectively appeal from the platform's decision; and
- Online platforms should be obliged to regularly publish transparency reports.[152]

For effective dissemination of community guidelines, civil society organisations and NGOs could contribute to the fight against illegal and harmful online content. They can develop media literacy, citizenship and democracy education actions as well as initiatives to develop critical thinking skills.

In the UK, the *Online Safety Bill* puts forward ambitious plans for a new system of accountability and oversight for tech companies, moving far beyond self-regulation. A new regulatory framework for online safety will make clear companies' responsibilities to keep UK users, particularly children, safer online with the most robust action to counter illegal content and activity.

The regulator, *OFCOM*, will have the power to require annual transparency reports from companies in scope, outlining the prevalence of harmful content on their platforms and what countermeasures they are taking to address these.[153] These reports will be published online by the regulator, so that users can make informed decisions about internet use. The regulator will have a range of enforcement powers (see *Clause 83 and 84 of the Bill*) including[154]:

- Issuing civil fines for proven failures in clearly defined circumstances.
- Serving a notice to a company.
- Requiring additional information from the company regarding the alleged breach.
- Publishing public notices about the proven failure of the company to comply with standards.
- Disruption of business activities.
- ISP blocking.
- Senior management liability.

The Joint Committee of the bill has been organising sessions with the tech companies to assess their approach to online safety and how they may be affected by the draft legislation.[155]

The OFCOM currently sets its own standards, with the objectives those standards should meet agreed by parliament, and the government is not allowed to direct OFCOM to target particular kinds of content.

However, the *draft Online Safety Bill* changes that and gives the Secretary of State "relatively unconstrained powers" to:

- Set strategic priorities which OFCOM must take into account
- Set priority content in relation to each of the safety duties
- Direct OFCOM to make amendments to their codes to reflect government policy
- Give guidance to OFCOM on the exercise of their functions and powers

---

[150] ibid.

[151] Alexandre de Streel et al., 'Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform' (*Policy Department for Economic, Scientific and Quality of Life Policies*, June 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf> accessed 8 April 2021

[152] ibid.

[153] HM Government, Department for Digital, Cultural, Media & Sport, 'Online Harms White Paper' (*Crown*, April 2019) 10-11 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf> accessed 8 April 2021 [hereinafter "OHWP"]

[154] ibid. at 62, 63

[155] Joint Committee on the draft Online Safety Bill, *Facebook, twitter, Google and TikTok to give evidence on the draft Online Safety Bill* (U.K. Parliament 2021) <https://committees.parliament.uk/committee/534/draft-online-safety-bill-joint-committee/news/158230/facebook-twitter-google-and-tiktok-to-give-evidence-on-the-draft-online-safety-bill/> accessed 14 Nov 2021

Carnegie Trust has said that the government "has not explained why the Secretary of State needs these powers" and proposed that they be "amended to create a more conventional balance between democratic oversight and regulatory independence."[156]

In the UK, the liability of internet intermediaries has been a key question in information technology law for nearly two decades. The *e-Commerce Directive*, adopted in 2000 by the European Union, sets up an Internal Market framework for online services.[157] *Articles 12-14 of the e-Commerce Directive* set out the limited liability exemptions, also referred to as the safe harbors, which contain the conditions under which certain intermediary service providers are exempted from liability for third party content.[158] The *e-Commerce Directive* does not provide a definition for intermediary service providers[159]; rather it provides for specific types of activities to be conditionally exempted from liability, specifically:

- Mere conduit;
- Caching; and
- Hosting.

The exemptions in the *e-Commerce Directive* have a horizontal scope, covering all types of illegal content (e.g. infringements of copyright, defamation, etc.) as well as both civil and criminal liability.[160] Thus, under the current liability regime, which is derived from the EU's *e-Commerce Directive*, platforms are protected from legal liability for any illegal content they 'host' (rather than create) until they have either actual knowledge of it or are aware of facts or circumstances from which it would have been apparent that it was unlawful, and have failed to act 'expeditiously' to remove or disable access to it.[161]

The UK having now cut its direct ties with EU law, is in a difficult situation as to the intermediary liability protections in *Articles 12 to 15*. Until recently, the government's policy has been of status quo as mentioned in its 2019 "eCommerce Directive guidance for businesses if there's no Brexit deal" stating that following the UK's exit from the EU in a no deal scenario, the government will minimize disruption. Therefore the UK's policy approach will continue to align with the provisions contained in the directive, including those on liability of intermediary service providers and general monitoring.[162] Consistently with that, in October 2020 the government published post-transition guidance, stating that it "has no current plans to change the UK's intermediary liability regime or its approach to prohibition on general monitoring requirements".[163] Thus, until the bill is passed as legislation in the UK Parliament, the status quo remains.

III. Parameters to Define Problematic User-generated Content

The bill seeks to tightly circumscribe user-generated content — so tightly that only a small number of internet giants will be able to profitably publish user-generated content.[164] The independent regulator, as proposed by the bill, will set out how operators can comply with the duty of care in Codes of Practice (although operators can adopt their own practices). *Code of Practice for providers of online social media platforms*[165] which references

---

[156] William Perrin et al., 'Secretary of State's Powers and the draft Online Safety Bill' (Carnegie Trust 2021) <https://www.carnegieuktrust.org.uk/blog-posts/secretary-of-states-powers-and-the-draft-online-safety-bill/> accessed 14 Nov 2021

[157] European Commission, 'E-commerce Directive' <https://ec.europa.eu/digital-single-market/en/e-commerce-directive> accessed 8 April 2021

[158] Clive Gringas and Claire Walker, 'E-commerce Directive: extending the limits of liability' (*Thomson Reuters*, 27 June 2005) <https://uk.practicallaw.thomsonreuters.com/8-200-9542?transitionType=Default&contextData=(sc.Default)&firstPage=true> accessed 8 April 2021 [hereinafter "REUTERS"]

[159] Ecem Yildirim, 'A Critical Analysis of the Intermediary Liability Regime Imposed by Different Regulations' (*Turkish Law Blog*, 26 January 2020) <https://turkishlawblog.com/read/article/194/a-critical-analysis-of-the-intermediary-liability-regime-imposed-by-different-regulations/> accessed 8 April 2021 [hereinafter "TURKISH LB"]

[160] Graham Smith, 'Corrosion-proofing the UK's intermediary liability protections' (*Cyberleagle*, 7 February 2021) <https://www.cyberleagle.com/2021/02/corrosion-proofing-uks-intermediary.html> accessed 8 April 2021 [hereinafter "CYBERLEAGLE"]

[161] OHWP (n 153)

[162] Ted Shaprio, 'Government publishes guidance on the E-commerce Directive (2000/31/EC) in the event of a "no deal" EU exit' (*Wiggin*, 14 January 2019) <https://www.wiggin.co.uk/insight/government-publishes-guidance-on-the-e-commerce-directive-2000-31-ec-in-the-event-of-a-no-deal-eu-exit/> accessed 8 April 2021

[163] Department for Digital, Culture, Media & Sport, 'The eCommerce Directive after the transition period' (*GOV.UK*, 16 October 2020) <https://web.archive.org/web/20201016105650/https:/www.gov.uk/guidance/the-ecommerce-directive-after-the-transition-period> accessed 8 April 2021

[164] Eric Goldman, 'The U.K. Online Harms White Paper and the Internet's Cable-ized Future' (2020) OSTLJ <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3438530> accessed 8 April 2021 [hereinafter "GOLDMAN"]

[165] PRACTICE CODE (n 147)

the *OHWP* has already been issued, setting out appropriate actions to prevent bullying, insulting, intimidating and humiliating behaviours. For certain tightly defined categories of illegal content – terrorist activity, child sexual exploitation and abuse, hate crime and serious violence – online operators will have an obligation to proactively monitor and filter content.[166] Apart from these parameters set in by the *Online Harms White Paper*, other parameters can be untrustworthy product reviews, copyright violations, offensive or inappropriate content, privacy violation and defamation.

There haven't been many objections to this particular section of the bill as parameters are quite comprehensive and have been sufficiently explained. Additionally, there is very little scope of ambiguity in the said parameters.

IV. The Need to Moderate 'Fake News'

The extent of untrustworthy information on social media is concerning, and recent events have certainly put social media under question. In the EU, 13 percent of consumers say they stay up to date on European politics via social media, with the figure rising to 16 percent regarding domestic politics.[167] Of all the content in these platforms, those that are extremist, fake and populist are found to often garner high "interaction" numbers. A recent study from the University of Oxford's Computational Propaganda Project has found evidence of organised social media manipulation campaigns in 48 countries in 2018.[168]

Printed media like newspapers and journals build relationships with their readers based on reputation. They establish this reputation by carefully checking information before publishing it. On social media, however, there are no editors, which allows all kinds of content to spread without control.[169] Facebook, for example, took down 40 million misleading posts in March 2020 alone, and another 50 million the following month.[170] For its part, Twitter challenged more than 1.5 million accounts from mid to end March.[171] Because of the above reasons, it becomes imperative for online platforms to moderate fake news or disinformation campaigns.

These concerns have been well set out in the wide-ranging inquiry led by the Digital, Culture, Media and Sport (DCMS) Select Committee report on fake news and disinformation, published on 18 February 2019.[172] The *Online Harms White Paper* has benefited greatly from this analysis and takes forward a number of the recommendations. The *Draft Online Safety Bill* establishes an Advisory Committee on Disinformation and Misinformation through *Clause 98*, whose function is to provide advice to OFCOM of how providers of regulated service in case of disinformation or misinformation present on such services or may be encountered via search results. An independent regulator will be appointed with the power to issue substantial fines for social media platforms and their senior members. At present, the National Security Communications Unit is tasked to combat disinformation campaigns by state actors and others during elections.[173]

One of the major technological challenges in disinformation is the continued development of AI systems. AI techniques can be used to target and manipulate individual voters, with highly sophisticated micro-targeting based on individual psychology.[174] Currently, social media companies have adopted two approaches to fight misinformation. The first one is to block such content outright. For example, Pinterest bans anti-vaccination

---

[166] TAYLOR WESSING (n 141)

[167] European Commission, 'Public Opinion: Standard Eurobarometer 86' (December 2016) <https://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2137> accessed 8 April 2021

[168] Samantha Bradshaw and Philip Howard, 'Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation' (13 August 2018) <https://comprop.oii.ox.ac.uk/research/cybertroops2018/> accessed 8 April 2021

[169] Karina Shyrokykh, 'Fake news on social media: Whose responsibility is it?' (*Ericsson Blog*, 5 November 2018) <https://www.ericsson.com/en/blog/2018/11/fake-news-on-social-media-whose-responsibility-is-it> accessed 8 April 2021

[170] IANS, 'Facebook flagged 50 million misleading COVID-19 posts in April' (*IndiaTV News*, 13 May 2020) <https://www.indiatvnews.com/technology/news-facebook-flagged-50-million-misleading-covid-19-posts-in-april-616897> accessed 8 April 2021

[171] Vijaya and Matt Derella, 'An update on our continuity strategy during COVID-19' (*Twitter*, 1 April 2020) <https://blog.twitter.com/en_us/topics/company/2020/An-update-on-our-continuity-strategy-during-COVID-19.html> accessed 8 April 2021

[172] Digital, Culture, Media and Sports Committee, 'Disinformation and 'fake news': Final Report' (*House of Commons*, 14 February 2019) <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf> accessed 8 April 2021

[173] BBC News, 'Government Announces Anti-Fake News Unit' (*BBC News*, 23 January 2018) <https://www.bbc.com/news/uk-politics-42791218> accessed 8 April 2021

[174] Katarina Kertysova, 'Artificial Intelligence and Disinformation' [2018] SHR 29(1-4) 55-81 <https://www.researchgate.net/publication/338042476_Artificial_Intelligence_and_Disinformation> accessed 8 April 2021

content[175] and Facebook bans white supremacist content.[176] The other is to provide alternative information alongside the content with fake information so that the users are exposed to the truth and correct information.[177] Thus, moderation of fake news on online platforms becomes the need of the hour in the digital world.

V. Balancing Fundamental Rights and Safe Harbour Provisions

Our personal data is now tightly interwoven with the way we view content online.[178] From targeted ads to search patterns to social media to news to political content, what tech companies know about us defines what they show us. In order for regulation to properly tackle these issues separately, and the massive inequalities and harms they cause when combined, regulators need to be able to cut across issues and make real changes in the way online platforms work. And for this, we need to stop seeing privacy and online content as two separate issues.[179]

The *e-Commerce Directive*, adopted in 2000 by the European Union, sets up an Internal Market framework for online services.[180] *Articles 12-14 of the e-Commerce Directive* set out the limited liability exemptions, also referred to as the safe harbors, which contain the conditions under which certain intermediary service providers are exempted from liability for third party content.[181] The *e-Commerce Directive* does not provide a definition for intermediary service providers[182]; rather it provides for specific types of activities to be conditionally exempted from liability, specifically:

- Mere conduit;
- Caching; and
- Hosting.

Only when a service falls under one of the specific activities can it be exempted from liability. The safe harbors do not prevent intermediaries from taking measures against the infringement of third-party rights, either through injunctions or duties of care, as was set out in case law and various legal instruments.[183] In the current age of social media where all our personal data can be found online and a simple post or tweet has the ability to have unimaginable consequences, this legislation falls short on many accounts, including to safeguard an individual's right on the internet.

Further, a study titled *Digital Society: Regulating Privacy and Content Online* published in September 2020,[184] led by Dr. Garfield Benjamin, found a strong case for more integrated regulation across existing policy recommendations and in the public view. There is widespread support for greater regulation of the use of personal data online (73%), fake news online (75%) and hate speech online (71%).[185] Trust in platforms is low, and people want greater action by platforms and government, with 67% of people surveyed showing support for regulating online privacy and content with the same set of laws and oversight bodies.

---

[175] Mark Wilson, 'The tech giant fighting anti-vaxxers isn't Twitter or Facebook. It's Pinterest' (*Fast Company*, 26 February 2019) <https://www.fastcompany.com/90310970/the-tech-giant-fighting-anti-vaxxers-isnt-twitter-or-facebook-its-pinterest> accessed 8 April 2021

[176] David Ingram and Ben Collins, 'Facebook bans white nationalism from platform after pressure from civil rights groups' (*NBC News*, 27 March 2019) <https://www.nbcnews.com/tech/tech-news/facebook-bans-white-nationalism-after-pressure-civil-rights-groups-n987991?cid=sm_npd_nn_tw_ma> accessed 8 April 2021

[177] Niam Yaraghi, 'How should social media platforms combat misinformation and hate speech' (*Brookings*, 9 April 2019) <https://www.brookings.edu/blog/techtank/2019/04/09/how-should-social-media-platforms-combat-misinformation-and-hate-speech/> accessed 8 April 2021

[178] Garfield Benjamin, 'Gaps in UK regulation of online platforms make it difficult to tackle systemic issues – here are some ways we can fix this' (*LSE*, 23 September 2020) <https://blogs.lse.ac.uk/medialse/2020/09/23/gaps-in-uk-regulation-of-online-platforms-make-it-difficult-to-tackle-systemic-issues-here-are-some-ways-we-can-fix-this/> accessed 8 April 2021

[179] ibid.

[180] European Commission, 'E-commerce Directive' <https://ec.europa.eu/digital-single-market/en/e-commerce-directive> accessed 8 April 2021

[181] REUTERS (n 158)

[182] TURKISH LB (n 159)

[183] Joris Van Hoboken, Joao Pedro Quintais, Joost Poort and Nico Van Eijk, Hosting intermediary services and illegal content online (Directorate-General for Communications Networks, Content and Technology (European Commission) 2018) <https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en> accessed on 9 March 2021

[184] Garfield Benjamin, Regulating Privacy and Content Online (Digital Society 2020) <https://digitalcultu.re/policy/digitalsociety/> accessed on 28 March 2021

[185] ibid.

This report proposes several steps to enable more effective and comprehensive regulation of online platforms, including:

1. Regulate privacy, data and content online together: By establishing an Office for Digital Society as a formal mouthpiece to bring relevant existing regulators together;
2. Build regulation on principles linked to rights: By placing equity, diversity, dignity and justice at the centre of policy;
3. Provide a platform for representation: by involving affected communities in policy and regulation;
4. Give regulators meaningful powers and the resources to exercise them: By ensuring the necessary funding, expertise and ability to effect change.[186]

By taking these steps, and working more closely across government, academia, industry and communities, we can empower regulation and citizens to make a more equitable, inclusive and just digital society for everyone and a fine balance can be achieved. The current bill takes care of point 1st, 2nd and 4th, as discussed above, but falls short on point 3rd, something which must be catered to by the joint committee.

VI. Transitioning from a Post-hoc, Harm-prevention Lens to a Proactive Approach Towards Understanding and Regulating Technology in the Global Intermediary Ecosystem

The ever-increasing phenomena of online infringement activities is taking the platform to a position of being monitored constantly and proactively. *Articles 12 to 14 of e-Commerce Directive* provide limitations on the liability of conduits, caches and hosts for unlawful user information. *Article 15*[187] prohibits EU member states from imposing general monitoring obligations on those intermediaries. The government's commitment to *Articles 12 to 15* though seems to have been faltering as is evident in the bill. With nothing said in the *UK-EU Trade and Co-Operation Agreement* about online intermediary liability, there appears to be nothing to prevent the government — should it wish to depart from its previous policy — from legislating in future contrary to *Articles 12 to 15* — subject always to the possibility of a legal objection on fundamental rights grounds.[188]

There was a detectable drift away from the overt commitment to *Article 15* with the publication of the government's *Full Consultation Response* to the *Online Harms White Paper*.[189] The response strayed into proposing proactive monitoring obligations that could not readily be reconciled with that policy. That drift was also evident in the simultaneously published *Interim Voluntary Codes of Practice on Terrorism*, *and Online Child Sexual Exploitation and Abuse*,[190] which are in effect a template for obligations likely to be imposed under the future *Online Safety Bill*. The *Full Response* was silent on the apparent conflict with *Article 15*.[191]

EDRi and Access Now have long emphasised the risk that privatised law enforcement and heavy reliance on automated content filters pose to human rights online. In this vein, multiple civil society organisations, including EDRi members (for example Article 19[192] and Index on Censorship[193]), have warned against the alarming measures the British approach contains. To avoid liability, the envisaged duty of care, combined with heavy fines, create incentives for platform companies to block online content even if its illegality is doubtful. The regulatory approach proposed by the UK *Online Harms White Paper* will actually coerce companies into adopting content filtering measures that will ultimately result in the general monitoring of all information being shared on online platforms, which to an extent is good unless it starts illegitimate restrictions on freedom of expression or, in other words, online censorship. A rather helpful mechanism can be the use of AI to identify proper checks and balances in online censorship and also seeing that content on online media be properly judged without any bias or predetermined ideology. This would, of course, be followed up by the human resource team of the company. But this too has certain drawbacks which are discussed in the next section.

---

[186] Garfield Benjamin (n 184)

[187] Graham Smith, 'Time to speak up for Article 15' (*Cyberleagle*, 21 May 2017) <https://www.cyberleagle.com/2017/05/time-to-speak-up-for-article-15.html> accessed 8 April 2021

[188] CYBERLEAGLE (n 160)

[189] RESPONSE (n 140)

[190] Home Office, Department for Digital, Culture, Media & Sport, 'Online harms: interim codes of practice' (*GOV.UK*, 15 December 2020) < https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice> accessed 8 April 2021

[191] CYBERLEAGLE (n 160)

[192] 'Response to the Consultations on the White Paper on Online Harms' (*Article 19*, June 2019) <https://www.article19.org/wp-content/uploads/2019/07/White-Paper-Online-Harms-A19-response-1-July-19-FINAL.pdf> accessed 8 April 2021

[193] Index on Censorship, 'The UK Government's online harms white paper: implications for freedom of expression' (*Index on Censorship*, 3 June 2019) <https://www.indexoncensorship.org/2019/06/the-uk-governments-online-harms-white-paper-implications-for-freedom-of-expression/> accessed 8 April 2021

VII. Moderation Fallibility and Guidelines

AI can be beneficial in the automatic detection of content, or automatically fact checking articles. But developments in AI also make it possible to generate fake content (text, audio and video) which is difficult to detect by humans and algorithms — known as 'deepfakes'.[194] As a result, it is becoming even easier to create and disseminate false content and narratives. A combination of personal data collection, AI-based algorithms and false or misleading information could be used to manipulate the public with unprecedented effectiveness.[195]

Critical conversations about algorithmic moderation systems often emphasise the technical challenges that these systems face now and in the future. In particular, there is outsized concern about overblocking: it is commonly (and correctly) pointed out that it is very difficult for predictive classifiers to make difficult, contextual decisions on slippery concepts like 'hate speech,' and that automated systems at scale are likely to make hundreds, if not thousands, of incorrect decisions on a daily basis.[196]

The UK already enjoys high standards of data protection law, which were updated in 2018 with the introduction of the *General Data Protection Regulation (GDPR)* and the *Data Protection Act 2018*. Key protections for online harms involving personal data, among others, include a power to inspect algorithms in situ, to understand their use of personal data and whether this leads to bias or other detriment.[197]

The *Draft Online Safety Bill* also empowers, through *Clause 49 & 50*, regulator to require annual transparency reports from companies in scope, outlining the prevalence of harmful content on their platforms and what countermeasures they are taking to address these to ensure that companies proactively report on both emerging and known harms.

Where necessary, to establish that companies are adequately fulfilling the duty of care, the regulator will have the power to request explanations about the way algorithms operate. The regulator may, for example, require companies to demonstrate how algorithms select content for children, and to provide the means for testing the operation of these algorithms. In determining where such explanations will be appropriate and what form they should take, the regulator will, as per *Clause 101 of the Bill*, work closely with the Centre for Data Ethics and Innovation, the expert body that has been set up to advise the government on the regulation of data, including algorithmic tools.

VIII. Governance of User-generated Content

User-generated content on online platforms refers to anything on the web which is not made by a brand but by the users of the platform. It could be anything such as photos, videos, reviews or posts.[198] Online platforms, big and small, rely on terms of service/terms of use or community standards/guidelines to regulate and user behaviour and base their illegal content online moderation practices.[199] These terms and standards/guidelines do not necessarily reflect a specific legal system. However, as they are designed to prevent harm, online platforms' policies do overlap in several instances with local law.

Due to the increasing pressure from platform users and regulators to do more to stop the spread of illegal and harmful user-generated content, online platforms have progressively tightened their rules with regard to all types of content, including hate speech and material implicated in incitement to violence.[200] Critically, however, the process platforms use to implement their self-imposed rules has remained for the most part opaque. In fact, of the actors involved in internet governance, private actors disclose the least amount of information about how their regulatory mechanisms are formulated or enforced.[201]

In the United Kingdom, *the Code of Practice for providers of online social media platforms* offers guidance to providers of social media platforms on appropriate actions they should take to prevent bullying, insulting,

---

[194] OHWP (n 153) at 26

[195] OHWP (n 153) at 27

[196] Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance' (2020) 7 (1) BIG DATA AND SOCIETY <https://journals.sagepub.com/doi/full/10.1177/2053951719897945>

[197] OHWP (n 153) at 35

[198] Megan Marrs, 'UGC 101: A Guide to User-Generated Content Marketing' (*WordStream*, 05 March 2020) < https://www.wordstream.com/blog/ws/2014/04/28/user-generated-content> accessed on 30th March 2021.

[199] POLICY DEPARTMENT FOR ECONOMIC, SCIENTIFIC AND QUALITY OF LIFE POLICIES (n 151)

[200] 'Facebook. (n.d.). Community Standards. Part III, Objectionable Content' (*Facebook Inc.*) <https:// www.facebook.com/communitystandards/objectionable_content>

[201] "Freedom of Expression" in *Ranking Digital Rights* (Corporate Accountability Index 2019) <https://rankingdigitalrights.org/index2019/report/freedom-of-expression/>

intimidating and humiliating behaviours on their sites. This code of practice/community guideline does not affect how illegal or unlawful content or conduct is dealt with.[202]

However, in the UK there is no mechanism to hold companies to account when they fail to tackle these breaches. As highlighted in the *White Paper*, the UK government believes that voluntary efforts have not led to adequate or consistent steps to protect British citizens online and users' own experiences confirm a sense of vulnerability online.[203] Thus, to solve the situation the bill sets up an independent regulator. The regulator will expect companies to make clear how they are fulfilling their statutory duty of care and ensure that relevant terms and conditions are sufficiently clear and accessible, including to children and other vulnerable users. The regulator will assess how effectively these terms are enforced as part of any regulatory action. The author feels that in the past the companies could easily absolve themselves from any liability for a user-generated content and thus overlooked the self-imposed rules. With the *Online Safety Bill*, which probably will turn into legislation soon, a fine balance can be achieved between community guidelines, public policy domestic contexts, and international human rights.

IX. Online Advertisement Standards

The internet advertising industry has grown very strongly as online media consumption has increased and advertisers have allocated more budget to online.[204] The UK internet advertising expenditure increased from £3,508m in 2008 to £11,553m in 2017, a compound annual growth rate of 14%.[205] In 2017, internet advertising overtook all other forms of advertising (television, press, radio, cinema and outdoor) combined, to reach 52% share of total advertising spending.[206]

Online advertising plays a crucial role in the digital economy, with many free digital services, such as search engines or social networks, funded by advertising revenues. The online advertising ecosystem is highly complex, with much of the advertising space online bought through automated processes, and the velocity with which adverts are created and displayed is far higher than offline.[207]

The growth and complexity of the online advertising market has generated policy and regulatory debate in the UK and overseas. This debate has included consideration of a number of potential harms to consumers, firms and wider society that could arise as a result of the structure and operation of the sector. The potential harms can be thought of in terms of three broad categories:

- Individual harms, referring to potential impacts on individual firms and consumers[208];
- Societal harms, referring to practices which may be detrimental to society as a whole[209]; and
- Economic harms, referring to potential harms that may arise from lack of competition or inefficiencies within the sector.[210]

Individual harms may include digital advertising fraud, brand risk (when a legitimate display ad appears next to inappropriate content), and inappropriate advertising (display advertising creative that is offensive, explicit, discriminatory, etc).[211] Societal harms may include non-transparent political advertising, which may be used by anonymous actors to influence elections and referendums in the UK. In the UK, political advertising on non-broadcast media is not regulated outside of election periods; during election periods, UK electoral law sets limits on the amount that can be spent on campaign activity – including online advertising.[212] Economic harms may include product bundling and exclusivity, lack of transparency in programmatic display, differential treatment, leveraging, control of web browsers, etc.

As of now, the current regulatory framework includes:

---

[202] ibid.

[203] OHWP (n 153) at 41

[204] Stephen Adshead et al., 'Online Advertising in the UK' (*Department for Digital, Culture, Media & Sport*, January 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777996/Plum_DCMS_Online_Advertising_in_the_UK.pdf> accessed 8 April 2021 [hereinafter "OAUK"]

[205] IAB, *Full Year 2017 Digital Adspend Results* (*PwC Digital Adspend Study* 2017) <https://www.iabuk.com/adspend/full-year-2017-digital-adspend-results> accessed 8 April 2021.

[206] ibid.

[207] ibid.

[208] OAUK (n 104) at 17

[209] OAUK (n 104) at 18

[210] OAUK (n 104) at 17

[211] OAUK (n 104) at 17

[212] OAUK (n 104) at 18

- The Electoral Commission's oversight of the activity of political parties, and other campaigners, including activity on social media through *The Political Parties, Elections and Referendums Act 2000 (PPERA).*
- The revised *EU Audiovisual Media Services Directive*, which introduces new high-level requirements for video sharing platforms such as YouTube to protect minors from harmful content, protect the general public from illegal content and content that incites violence and/or hatred.

In 2018, the Information Commissioner's Office (ICO) conducted an investigation into data analytics and micro targeting of political advertising online. The report, *Democracy Disrupted?*, highlighted the risks of personal data being abused in digital campaigning and made a number of recommendations to improve transparency and data protection compliance.[213] The ICO has also commenced a broader examination of the use of personal data in adtech. Further, the *Online Harms White Paper* noted the recent developments in the digital world and with an aim to improve the transparency of digital advertising, announced that Digital, Culture, Media and Sport (DCMS) will conduct a review of how online advertising is regulated in the UK.[214] Although the *Online Safety Bill*, through *Clause 9*, outlines a requirement for platforms to remove 'priority illegal content,' this requirement only governs user-generated content, meaning that there's nothing to stop threat actors using advertising on these platforms as a means to defraud people. This is one of the major drawbacks of the bill which falls short of regulating online advertising frauds. This could prove to be another window for the potential harms to consumers and society at large.

D. Privacy, Information Security, and Personal Data

I. Differentiating Personal and Non-Personal Data

On 31st December, 2020, the United Kingdom seceded from the membership of the European Union. Post-Brexit, the UK enacted two pieces of legislation: the *Data Protection Act 2018*[215] *(DPA)* and *General Data Protection Regulation* [216] *(UK GDPR)*. Both of the legislations were enacted with the scope of regulating the usage of 'personal data'.[217]

Personal data being the primary subject matter of both the legislation is defined under the *Article 4(1) of the UK GDPR* as: "Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[218]

DPA defined 'personal data' in similar lines under *Section 3(2)* as: "Any information relating to an identified or identifiable living individual."[219]

The *UK GDPR* was enacted with the intent to provide an equivalent protection as that provided by *EU GDPR*.[220] The similarity in many aspects to EU GDPR was to allow free flow of data between EU and the UK even when the UK is treated as a third country.[221] Owing to such origin and similarity, assistance of the jurisprudence on definition of 'personal data' available under *EU GDPR* has been taken to supplement the definition of 'personal data' under the regulatory framework of UK data law.

Article 4(1) of the UK GDPR when read in the light of the scheme of *EU GDPR* has four primary elements: (1) any information, (2) relating to, (3) identified or identifiable, and (4) natural person.

---

[213] Information Commissioner's Office, 'Democracy disrupted? Personal information and political influence' (*ICO*, 11 July 2018) <https://ico.org.uk/media/ action-weve-taken/2259369/democracy-disrupted-110718.pdf> accessed 8 April 2021

[214] OHWP (n 153) at 32

[215] Data Protection Act 2018.

[216] UK General Data Protection Regulation 2018.

[217] Data Protection Act, 2018, s 1(1); UKGDPR, Article 1.

[218] UKGDPR, Article 4(1).

[219]Data Protection Act 2018, s 3(2).

[220] ICO refers to UKDPR as 'Frozen GDPR' as it is supposed to be adoption of the exact version of EU GDPR as present on 31st December 2020.Information Commissioner's Office, 'Information Rights after the end of the transition period' (ICO, 2020) <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/transition-period-faqs/#:~:text=From%201%20January%202021%2C%20the,anywhere%20else%20in%20the%20world> accessed 8 April 2021; Data Protection Bill 2018, cl 3(3)(b); LokkeMoerel and Ronan Tigner, 'Data Protection Implications of "Brexit"' (2016) 2(3) EDPL 381-383, 382.

[221] 'EU Transfers of Data to UK Post Brexit: The GDPR Perspective' (2017) 1 Int'l J Data Protection Officer, Privacy Officer & Privacy Couns 8.

The interpretation of these four elements under the *EU GDPR* is provided in *Article 29 Working Party* as follows:[222]

S No.	Article 4(1) UK GDPR Element	Meaning as per Article 29 Working Party
(1)	*Any Information*	Under *Article 29 Working Party* it is clarified that the wordings call for a wide interpretation.[223] The nature of information can be objective, i.e., pertaining to a substance in one's blood or subjective, like assessments made by insurance companies, banks etc. [224]
(2)	*Relating to*	The information must relate to an individual.[225]
(3)	*Identified or Identifiable*	An individual can be considered identified or identifiable when that individual can be distinguished from all other members of the group.[226]
(4)	*Natural Person*	The individuals being identified or identifiable are supposed to be living individuals in principle.[227]

Article 29 Working Party further defines 'personal data' by including information touching the individual's private and family life is not limited to such a sphere in the strictest sense; it also includes information regarding whatever type of activity is undertaken by the individual, like that concerning working relations or the economic or social behaviour of the individual.[228]

Recital 26 of EU GDPR established a risk-based approach to determine the nature of data (personal or non-personal data).[229]The recital clarifies when there exists a reasonable likelihood of identification then the data is considered to be personal data. Whereas in contrary scenarios, the data is construed to be of non-personal nature.[230]

When data in its raw form or through subsequent processing produces information that relates to facets of the private life of a natural person, then the same can be construed as personal data. When data through processing results in information, but there is no way to establish its linkage to a natural person,then the given data can be construed as non-personal data.

The present framework of personal data protection allows legal processing under certain considerations enlisted under *Section 8 of Data Protection Act 2018*. One of such criteria is processing of personal data that assists an activity that supports or promotes democratic engagement. Such exception carved into *Section 8 of Data Protection Act*, provides an ambit for political micro-targeting (PMT) which has led to a loophole for allowing political micro-targeting practices of varied demography in the UK a distinct possibility.[231]

PMT as a practice refers to an extreme form of audience segmentation made possible by combining multiple datasets for predictive analysis.[232] This technique is used by political actors to target voters with highly personalised messages. The overall practice has been considered a vector of disinformation.[233] The individuals whose personal data are being processed should be informed about the data processing, its circumstances,

---

[222] Article 29 Data Protection Working Party, Opinion 04/2007 on the Concept of Personal Data ((WP 136) 01248/07/EN).

[223]ibid 6.

[224]ibid 6.

[225]ibid 7.

[226]ibid 12.

[227]ibid 22.

[228] ibid 6.

[229] General Data Protection Regulation (EU) 2015/679 Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive) [2016] L 100000, Recital 26.

[230]Michele Finck and Frank Pallas, 'They who must not be identified - Distinguishing personal from non-personal data under the GDPR' (2020) International Data Privacy Law 10(1) 11, 14.

[231]Investigation into the use of data analytics in political campaigning: a report to Parliament, ICO, 6 November 2018, p6.

[232] Cristina Blasi Casagran*et al*, Reactions on the murky legal Practices of Political from GDPR perspective, International Data Privacy Law, p1.

[233] Kate Jones, 'Online Disinformation and Political Discourse Applying a Human Rights Framework'
(Chatham House The Royal Institute of International Affairs, 2019) 7; Judit Bayer and others, 'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States' (European Parliament, 2019) 122; Susan Morgan, 'Fake news, disinformation, manipulation and online tactics to undermine democracy' (2018) 3(1) Journal of Cyber Policy 39, 42.

character and scope, including through transparent data privacy policies. In order to prevent the arbitrary use of personal information, the processing of personal data should be based on the free, specific, informed and unambiguous consent of the individuals concerned, or another legitimate basis laid down in law.[234]

The EU as a body being party to *Convention 108+* in its data protection has also imbibed the concept of free and informed consent in *EU General Data Protection Regulation*,[235] under which strict requirements are placed on information that must be provided to data subjects such as the purpose and legal basis for processing and collecting data. *Article 29 Working Party* clarifies that 'consent' under *GDPR* is presupposed to be understood along with the principle of transparency and thus the data subjects must be capable of exculpating the scope and consequences of the processing; so that the data subject is not surprised by the way in which their data has been used.[236]In *Planet49 case* it was clarified by CJEU that failing to collect consent via a 'clear affirmative action' by the users could lead to a breach of the *GDPR*.[237] For instance, according to the court, it would appear impossible in practice to determine objectively whether users had actually given their consent by not deselecting a pre-ticked checkbox that is required for continuing their primary activity on the website visited.[238]

Right to privacy is an intrinsic right of an individual recognised under *Article 17 of ICCPR*. This right calls for a positive obligation on the state to protect privacy from all forms of attack.[239] This protection extends to protection against private parties.[240]In present times data of political opinions are considered to be an intrinsic part of the private sphere of an individual by *Convention 108+*.[241] Such sensitive data requisites additional safeguards to be provided to prevent reidentification of an individual. As disclosure of identity may lead to unwarranted discrimination and risks.

II. Ethical, Economic and Social Considerations When Regulating Non-Personal Data

At present, the primary focus of the UK government has been in safeguarding individual rights of privacy and not much has been pondered upon in the context of non-personal data. The *UK GDPR* at present has been implemented to crease out and provide a robust framework of personal data from UK to EU and vice versa.

However, it is posited that the market definition in the present context is data-driven and thereby certain economic considerations need to be taken into consideration when regulating flow of non-personal data. Digital information is unlike any previous resource; it is extracted, refined, valued, bought and sold in different ways. It changes the rules for markets and it demands new approaches from regulators.[242] As advancements of technology have taken leaps and bounds, increasing value of data has resulted in consumer data becoming the core of many business models.[243]

Thus, many a time, acquisitions made by companies now are also based on the consideration of acquisition of unique datasets of anonymised data falling under the ambit of non-personal data. Such acquisitions of data have two-fold benefit: firstly, it makes the data available on present consumers even more rounded and complete assisting the business in fulfilling the consumer's need with more accuracy; secondly, on account of data-driven network effect acquisition results in acquiring new potential customers.[244] When acquisition and

---

[234] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Article 5(2); Malabo Convention, Article 13(1); Madrid resolution, principle 12; The right to privacy in the digital ageA/HRC/39/29; Antoinette Rouvroy, Bureau of The Consultative Committee of The Convention for The Protection Of Individuals With Regard To Automatic Processing Of Personal Data [Ets 108], "Of Data And Men" Fundamental Rights And Freedoms In A World Of Big Data, p 22

[235] GDPR, Art 6(1); GDPR, Art 7; GDPR, Art 13; GDPR, Art 14

[236]Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) wp260rev.01

[237]C673/17 Planet49 GmbH [2019] ECLI:EU:C:2019:801, ¶ 61

[238] ibid, ¶55

[239]Manfred Nowak, U.N. Covenant on Civil and Political Rights: CCPR commentary (2005) 379

[240] ICCPR, Article 17(2).

[241] Modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Article 6.

[242] The Economist, Fuel of the Future: Data Is Giving Rise to a New Economy <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy> accessed on 25th April, 2021.

[243] Addressing the Tax Challenges of the Digital Economy <https://read.oecd-ilibrary.org/taxation/addressing-the-tax-challenges-of-the-digital-economy/the-digital-economy-new-business-models-and-key-features_9789264218789-7-en#page1> accessed on 28 August, 2021 ;Anoop George & Shreya Bambulkar, , A Need to Relook the Merger Control in the Digital Economy – An Analysis, NLIU Trilegal Summit on Corporate and Commercial Laws (2019) 4.

[244] United National Commission on Trade and Development, 'Competition issues in the digital economy' UNCTAD TD/B/C.I/CLP/54 <https://unctad.org/system/files/official-document/ciclpd54_en.pdf> accessed 23 April 2021.

mergers are motivated by the two factors mentioned above the mergers and acquisitions in business terminology are termed as 'data driven mergers'.[245]

Many a time, such kinds of mergers and acquisitions fly under the radar of competition authorities as such mergers are motivated by acquisition of data unlike the conventional consideration of physical assets or turnovers might not be the motivating factors. So many times such acquisitions are effectuated during the nascent stage of a company or start-up which shows potential of amassing more and more consumer data. For instance, Instagram was acquired for a billion dollars when it had a mere 12 employees and no source of revenue.[246] However, in the present times, the understanding of such competition concerns has become mainstream as data is now a source of market power.

Such free flow of unregulated data at present has resulted in internet giants, who by owing to the dearth of their economic resources hinder start-ups operating in their shadows. Thus, such startups fail to achieve their potential to disrupt the market. Albert Wenger, a venture capitalist from the United States, commented on 'Kill Zones' as "areas not worth operating or investing in, since defeat is guaranteed."[247] These 'kill zones' are further enhanced as the giants adopt methods to mimic the practices of the small companies by incorporating the features of the small entities in their applications. Especially in the digital markets, the shadow of giants disincentivises the smaller companies to excel because they know that one day these giants are going to take over their companies, "killing" their efforts of establishing their enterprise. It is an established practice of these giants to target companies that are at a nascent stage and neutralising them via acquisitions.

Thus, in context of this, it is suggested that regulations on usage of non-personal data must have a competition law perspective attached to it. The UK can rely on the European Consumer Organisation (BEUC) that the EU merger regulation needs to be changed on some of its jurisdictional and procedural characteristics, on this account BEUC had recommended: "The EU Merger Regulation should include in its rules on jurisdiction two additional criteria based on the value of transfer and, in case of two-sided markets, on the number of consumers affected by the operation. This would allow DG Competition to consider mergers between companies that do not reach the turnover thresholds but nevertheless have the potential to disrupt competition due to the number of consumers that will be aggregated by the purchasing company."[248]

As data driven mergers are of higher value during transactions. For instance, the acquisition of Skype[249] by Microsoft for $8.5 billion or the $19 billion acquisition deal by Facebook to acquire WhatsApp in 2014.[250]Putting forth a transactional threshold in regards acquisition of companies of such internet giants, who are motivated in their acquisition by non-personal datasets will assist start-ups with innovative technologies present in the local markets to flourish.

III. Viability of Backdoor and Traceability to End-To-End Encryption Practices ('E2EE' Practices)

The E2EE is a method used for drawing modular boundaries around communication subsystems and defines a firm interface between it and the rest of the system.[251] E2EE ensures that only one person communicating and the person being communicated with can read or listen to what is sent, and nobody else in between. In simple terms, E2EE practices operate on a concept of a lock and special key, the messages being communicated are secured with a lock, and only the sender's and recipient's device have the special key needed to unlock and read them.[252]

---

[245]United National Commission on Trade and Development, 'Competition issues in the digital economy' UNCTAD TD/B/C.I/CLP/54 <https://unctad.org/system/files/official-document/ciclpd54_en.pdf> accessed 23 April 2021.

[246]Autorité de la concurrence &Bundeskartellamt, 'Competition Law and Data' 11 <https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2> accessed 22 May 2021

[247]Asher Schecter, 'Google and Facebook's 'Kill Zone': 'We've Taken the Focus Off of Reward- ing Genius and Innovation to Rewarding Capital and Scale', (Promarket, 25 May, 2018)

[248] European Consumer Organisation, EU Merger Control: BEUC's Comments On Jurisdictional Thresholds, European Union, (2 May 2021, 10:40 PM), <http://ec.europa.eu/competition/consultations/2016_merger_control/european_consumer_organisation_contribution_en.pdf>. accessed 24 April 2021

[249]COMP /M. 6281, Microsoft/Skype, 7 October 2011.

[250]COMP/M. 7217, Facebook/WhatsApp, 3 October 2014.

[251] J.H. Saltzer, D.P. Reed & D.D. Clark, End-to-End Arguments in System Design, 2 ACM TRANSACTIONS ON COMPUTER Sys. 277 (1984)

[252] End-to-End Encryption, WHATsApp, https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption.

E2EE provides a secure space to users; however, such practices are inimical towards investigations conducted by law enforcement agencies. Since E2EE practices prevent traceability from the intermediary service providers.[253] One of the solutions explored was the presence of a key that can assist in accessing information through the back door.

A backdoor entry as a solution is not prudent primarily due to three reasons: First, a backdoor entry results in devolving from the best practices now being used to make the internet more secure. For instance, the usage of temporary encryption keys which self-destructs immediately after usage, making stealing of such encryption keys virtually impossible. Second, building in an access back route for exceptional cases will increase system complexity. It needs to be understood that as such backdoors are a new feature, interaction of such new features can subsequently result in new vulnerabilities to culminate in the security framework. Third, if an attacker gains access to the key to the backdoor, he will privy to all the information present in the given framework.[254] Additionally, there exists space for jurisdictional complexity as such laws may compel corporations to divulge information which are present in different jurisdictions altogether.

The former Prime Minister of the UK, David Cameroon, launched a 'UK encryption ban' to ban all messaging apps offering E2EE service whilst not providing the UK security services access to them.[255] This deliberation in the UK led to creation of the *Investigatory Powers Act, 2016 (IP Act).*[256]

The aim of *IP Act* is to consolidate the UK's patchwork of surveillance laws and provide a transparent, legally grounded legitimacy to interception of communication to prevent serious crimes.[257] The *IP Act* initially was challenged for violating the *Human Rights Act, 1998* incorporated under the aegis of the *European Convention on Human Rights*. However, the High Court reviewed the act and held that the *IP Act* was not incompatible with the *Human Rights Act*. The formation of the Investigatory Powers Commission, an independent body responsible for preventing abuse guarantees that there are safeguards to prevent potential abuse of the act.[258] However, internationally the *Watson case* which found that the scope of the UK's data retention laws was too wide and incompatible with European Union law.[259] While at the time of enacting the *IP Act* in 2016, the government maintains that the *IP Act* is compatible with the *ECHR*[260], the UK government following the *Watson case* made changes to the *IP Act* and introduced the *Data Retention and Acquisition Regulations 2018*. These regulations increased the threshold for accessing communications data only for the purposes of serious crimes defined as offences which are capable of being sentenced to imprisonment for a term of 12 months or more and requires that authorities consult an independent Investigatory Powers Commissioner before requesting data. The regulations also included a loophole where rapid approval can be made internally without independent approval but with a three-day expiry and with subsequent review by the independent body.

While there is no panacea for the challenges of modern technology in crime, the powers of investigative agencies cannot be absolutist. The ideal is to enable solutions that provide for responsible law enforcement backdoor access to encrypted data with the assistance of service providers without undermining user privacy or security. This requires principled collaboration and compromise.

A general perusal of *IP Act* evinces that it achieves the end goal through incorporation of the following principles such as:

- Interception of data based on the basis of legitimacy and proportionality. Under the *IP Act*, the Secretary of State and an independent judge must both sign a warrant when the interception powers are particularly intrusive.[261]
- Assistance and collaboration of service providers with law enforcement agencies for saving public resources and understanding the product and services better.[262]

---

[253] "Hacker Lexicon: What Is End-to-End Encryption?",*WIRED*, *https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/*

[254] Harold Abelson *et al* Keys under doormats: mandating insecurity by requiring government access to all data and communications (2015) 1(1) Journal of Cybersecurity 69, 70

[255] ibid 71

[256] Investigatory Powers Act 2016

[257] S McKay, *Blackstone's Guide to the Investigatory Powers Act 2016* (Oxford, OUP, 2017)

[258] Carey, Scott (27 April 2018). "The Snoopers' Charter: Everything you need to know about the Investigatory Powers Act". *Computerworld UK*. IDG UK

[259] Tele2 Sverige AB v Post- ochtelestyrelsen and Secretary of State for the Home Department v. Watson (C 203/15; C-698/15).

[260] Home Office, 'Investigatory Powers Bill European Convention On Human Rights Memorandum' (2015) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473763/European_Convention_on_Human_Rights_Memorandum.pdf accessed 4 April 2021

[261] Investigatory Powers Act 2016, S. 2(4)(c)(i)

[262] Saving resources through collaboration: Investigatory Powers Act 2016, s. 78- 80

- Exceptional interception of communication solutions should not fundamentally change the level of trust a user needs to have in a service provider or device manufacturer.[263]
- Governments should not have unfettered access to user data[264] and should maintain transparency about interceptions and access.[265]

A government with unfettered access to private communication resembles an Orwellian dystopian surveillance state. Hence, the balance between monitoring of individual information and maintaining privacy rights needs to be proportional. However, whether the *IP Act* upholds the principles of right to privacy has come under scrutiny of the international community and the *European Commission for Human Rights (ECHR)*.[266]As one of the first western countries to introduce a surveillance regime, the UK has to balance accessing an individual's information who is a threat to national security with the information of all individuals that can be accessed with backdoor encryption methods. The IP law is in direct contract to data protection and privacy laws, and though deterring terrorism is a valid justification, it should not fall into the trap of an Orwellian surveillance state incompatible with the *European Convention on Human Rights*.

IV. Tackling Crises Through Regulatory Sandboxes

COVID-19 has altered the way we function, communicate and think, affecting almost every part of our culture, environment, and mental wellbeing. This historic incident has also had a significant effect on our perceptions of privacy and the value we place on the security of our personal records. The pandemic has forced us to reconcile privacy with health and security, as it has put other human rights into context that we would never have welcomed seeing limited by state policies before.[267]

The right to privacy and the right to data security are universal rights. However, in the past, states of emergency, security interests, and extraordinary situations have permitted restrictive approaches on human rights such as privacy. Crises such as COVID-19 has been described by the Director-General of the World Health Organisation (WHO) as "a danger to every nation, poor and rich," a rare occurrence that has prompted nations around the globe to impose emergency measures.[268]

Limitations on the exercising of the rights and freedoms recognised by the *Charter* can be imposed only if they actually fulfil purposes of general interest recognised by the Union, according to *Article 52(1) of the Charter of Fundamental Rights of the European Union*.[269] Specifically concerning right to privacy, *Article 8(2) of the ECHR* enumerates the legitimate aims that may justify an infringement upon the right to privacy, being "in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protections of the rights and freedoms of others."[270]

The *EU GDPR* further adds to this. *Recital 4* states that data privacy must always be weighed against other human rights and treated in relation to its role in society.[271] Furthermore, *Article 23(1) EU GDPR* requires member states to limit data principal rights and the data security standards specified in *Article 5 EU GDPR* if they do so by legislation that preserves the spirit of the very same fundamental human rights. These prohibitions should serve to protect, along with other aspects, "essential interests of general public concern, including fiscal, budgetary, and taxation matters, public welfare, and social security," so that they are reflected in essential and equitable steps in a democratic country.[272]

---

[263] Investigatory Powers Act 2016, s.3

[264] Investigatory Powers Act 2016, S. 12

[265]David Anderson QC, 'The Investigatory Powers Act 2016 – an exercise in democracy'(David Anderson QC, 3 December 2016) < http://www.daqc.co.uk> accessed 4 April 2021

[266] Privacy International, 'Mass Surveillance' https://www.privacyinternational.org/node/52

[267]Emanuelle Ventrella, 'Privacy in emergency circumstances: data protection and the COVID-19 pandemic' (2020) ERA Forum 21, 379–393 <https://doi.org/10.1007/s12027-020-00629-3> accessed 4 April 2021

[268] WHO Director-General's opening remarks at the media briefing on COVID-19 < https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-world-health-assembly > accessed on 28 August 2021

[269] Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02

[270] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5

[271] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation [2016] OJ 2016 L 119/1

[272] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation [2016] OJ 2016 L 119/1

UK's data protection authority, ICO, provided official guidelines in wide ranging topics providing a framework for compliance of data protection and privacy law during the pandemic.[273] The philosophy of the European Data Protection Board (EDPB) has been that for an efficient response to the crisis, a subject should not have to forgo their fundamental rights: both can be achieved and moreover data protection principles would play an important role in fighting the virus. European data protection laws allow for responsible use of personal data for health management purposes while also ensuring that individual rights and freedoms are not eroded in the process. This philosophy allowed contract tracing of COVID-19 cases without erosion of *Articles 6 and 9 of the ePrivacy Directive* and the general scheme of the *EU GDPR*.[274]

In the face of crises, under certain qualifications, a legal basis for processing data by private or public entities in the interest of personal safety to public interest is required. However, the leeway on suitable legal bases for handling personal data in times of crisis need to be established to prevent discriminatory practices.

A sandbox refers to an environment where a product or service is tested in a controlled manner with relaxed regulatory norms. In the UK, the ICO formed a regulatory sandbox and collaborated with NHS Digital to develop a country-wide central consent mechanism where individuals can consent to share their health data to provide for contact tracing, research, vaccine trials etc.[275] It had similar data-sharing projects aimed at protecting the vulnerable from cybercrimes.[276] The *GDPR* in its guidelines following the COVID-19's impact on data protection specified that an informed valid consent is necessary to collect an individual's personal data, making such data sharing voluntary in nature provides a valid legal basis.[277]

The justification for regulatory sandboxes is that in the uncertainty of innovation and its impact on data protection of the data principal, a sandbox provides the government an opportunity to ensure that the digital change takes place in a way that enables benefits but also minimises the risks. In the case of data protection, it involves enabling data-driven innovation while ensuring responsible use of data and protection of individual's rights and interests. Hence, in the time of crisis where in a short period of time, innovative technology needs to be used keeping in mind data protection considerations, a regulatory sandbox is an important tool to achieve the same.

V. Principles and Regulations for Intelligence Agencies Operating Online

The broad principles of fairness and transparency must be the governing principle on the basis of which the intelligence agencies operate. The *DPA Act* inculcates these two principles to a great extent to govern the framework under which Intelligence agencies [278]operate. On perusal of the *DPA Act*, it can be found processing of data by the intelligence agencies is mandated to follow *Schedule IX and Schedule X*.[279]

Furthermore, intelligence agencies need to be regulated, their access to personal data and processing of such personal data must be limited to the extent required and must not derogate the universal right to privacy of an individual. The scheme of *DPA Act* does inculcate the facet of proportionality. For instance, under *Section 88*, *DPA Act* it is specified that data should be relevant, adequate but not excessive for the purpose for which it is processed. The *DPA Act* ensures that processing of personal data shall be for the purpose for which it was obtained and the purpose shall be explicit and legitimate[280] and that retention of the data is strictly kept only for the duration when it is necessary for the intended purpose.[281]

However, under *Section 87*, data collected by intelligence agencies for one purpose is allowed to be used for another purpose if such usage is allowed under law and proportionate in nature. Such alternative usages can lead to a bulk surveillance practice and thereby requiring independent officials within the organisations who are tasked with scrutinising all surveillance requests to ensure the action is necessary and proportionate and

---

[273] ICO Regulatory Approach <https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf> accessed 28 August 2021

[274] Guidelines 04/2020 of 21 April 2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak [2020]

[275] ICO's call for views on building a sandbox: summary of responses and ICO comment, < https://ico.org.uk/media/about-the-ico/consultations/2260322/201811-sandbox-call-for-views-analysis.pdf> accessed August 28, 2021

[276]Sandbox Beta Phase Discussion Paper, UK Information Commissioner's Office (ICO, January 2019) <https://ico.org.uk/media/2614219/sandbox-discussion-paper-20190130.pdf> accessed August 28, 2021

[277] Guidelines 05/2020 of 4 May 2020 on consent under Regulation 2016/679 [2020]

[278] Data Protection Act 2018 s. 82(2) defines Intelligence services as: (a)the Security Service; (b)the Secret Intelligence Service;(c)the Government Communications Headquarters.

[279] Data Protection Act 2018, s 86 sch IX, X

[280] Data Protection Act 2018, s 87

[281] Data Protection Act 2018, s 90

that no less intrusive means can be adopted to achieve the same ends. These authorizations are available for scrutiny by the judiciary.[282] The intelligence agencies are bound by strict norms contained in *Part IV*. These norms allow intelligence communities to deal with paramount threats particularly stemming from terrorism. Such threats coming under the ambit have reasonably been restricted in the UK and are congruent with the international practices.

Conclusion

Human rights in the UK's digital ecosystem seems to be fairly well-guaranteed. The state recognizes that human rights deserve to be protected, and have taken or are taking measures to do so in the digital context. The state does, however, need to be more proactive about these protections and have more stringent enforcement of basic human right laws for violations in the digital ecosystem. It should adopt the path of creating a balance where it puts reasonable restrictions on the actions of private parties and also protects their digital freedom.

In this authors' opinion, an SCM like body is a much-needed addition to the UK regulatory space. While the UK has laws in place, these laws need to be applied and regulated to ensure they are enforced, and to do so a dedicated body is required. While the state does not ordinarily overreach its regulatory powers in the digital ecosystem, there have been some instances which could have been avoided if there was a regulatory and redressal mechanism for such violations.

With a comprehensive *Online Harms White Paper* and the initial response of the government to the same, the UK has responded to the situation, and traced the evolution of an identifiable strategy for the control of online content by placing certain obligations upon internet intermediaries. While there is certainly room for improvement in the UK strategy for dealing with intermediaries as regards third party-provided content as have been highlighted in this report, it remains to be seen just how effective the current approach may prove in practice.

[282] 'MI5's Law and Governance' (*Mi5 Security Services*) <www.mi5.gov.uk/law-and-governance> accessed 28 August 2021

ANNEXURE

Questionnaire | Project Aristotle

a. Digital Constitutionalism and Internet Governance

1. What factors can be considered important to ground Digital Constitutionalism in traditional constitutional concepts?
2. How can we define Digital Constitutionalism?
3. What should be the core tenets of a Digital Constitution?
4. How can Digital Constitutionalism present a constitutional model for the people, by the people, and of the people?
5. How can online platforms be made more inclusive, representative, and equal?
6. What role should open-source intelligence (=OSINT: the discipline of assembling and analysing publicly available information) play in the future of our society?
7. Should the Digital Constitution be an integrative model, which draws upon and comprehensively presents standards for specific laws (e.g. antitrust, evidentiary standards etc.) as opposed to grounding ideals? If so, how should it fulfil the responsibilities of a pluralistic enterprise such as this as well as the specific needs of a pluralistic global society?
8. How can competition and antitrust laws of different jurisdictions protect the global market from big-tech domination, and is there a need to?
9. What is the role of regional/grassroots actors as well as inter-judicial cooperation/coordination in the digital ecosystem? Which other mechanism(s) might be more helpful?
10. Can the Digital Constitution present an anchor for the governance of the virtual world similar to a traditional constitutional model or will it always be in flux? Is there a need for constitutional innovation, and if so, in which areas (e.g. the right to be forgotten as a novel right)?
11. How is it possible to harmonise diverse national frameworks in order to achieve a global Digital Constitution?

b. Human and Constitutionally Guaranteed Rights:

1. Which human and constitutionally guaranteed rights do online platforms affect, and how?
2. Who can be defined as a netizen?
3. Who can be classified as a 'bad actor', and can 'bad actors' be netizens?
4. How can we embed within the digital ecosystem approaches which are responsive to the needs of minorities (e.g. ethnic minorities, racial minorities, gender minorities, religious minorities)?
5. How should the digital age of consent be arrived at and what should it be? In pursuance of which child rights should such an age be identified?
6. How should public order be defined for the digital space? Should situations of disorder in the offline world influence the definition and management of public order online, and if so why and when?
7. Should the state be allowed to impose internet shutdowns, slowdowns and communication throttles? What socio-legal rationale could be adopted by states in order to do so?
8. Could the Social Media Councils (SCMs) model, as introduced by Article 19, be reinterpreted on a larger scale, with the purpose of monitoring human rights, within the context of Digital Constitutionalism?

c. Privacy, Information Security, and Personal Data:

1. How do we define personal and non-personal data?
2. What should be the ethical, economic, and social considerations when regulating non-personal data?
3. Should there be a backdoor to end-to-end encryption/Should traceability be enabled to prevent and mitigate instances of online harms? What would the benefits and detriments of the same be?
4. How important is compliance with complex/technical/lengthy data protection and privacy statutes in events of crises (e.g. such as during pandemics, where time is essential)? In that regard, is there a need to provide regulatory sandboxes, and if so what could be the grounding philosophy to shape the rules of control for such ecosystems?
5. According to which principles and regulations should intelligence agencies operate online?

d. Intermediary Regulation:

1. How do we define online harms?
2. How should community guidelines for online platforms be drafted, disseminated, and enforced?
3. To what legal standards of accountability and transparency should online platforms be held, and in what capacity? Can you suggest any mechanisms (judicial, or otherwise) which might be capable of ensuring such a check on the functioning of these platforms?
4. Should online platforms be immune from liability from third-party, user generated content [refer to intermediary liability laws]?
5. What should the parameters to define problematic user-generated content be?
6. Should online platforms moderate 'fake news', and if so, why?
7. Should safe-harbour protections be offered to online platforms, given that the grant of such a protection will come at the cost of fundamental rights (e.g. privacy) of citizens? If affirmative, how should this balance be achieved? [Read with Questions in Part B.]
8. How does the global intermediary ecosystem shift from a post-hoc, harm-prevention lens to a proactive approach towards understanding and regulating technology?
9. Do the guidelines/policies of online platforms account for fallibility of the algorithm and the human content moderators, and if so, to what extent?
10. What role should community guidelines drafted by online platforms play in the governance of user-generated content? How should the terrain of conflict between community guidelines, public policy domestic contexts, and international human rights be negotiated upon?
11. Should the advertisement policies and sponsored content of online platforms adhere to certain standards (e.g. of whether they interfere with the political opinions and elections in a democracy)? If so, who should frame these policies, and who should be the final arbiter?

Institute
for Internet &
the Just Society