Research Program
on Digital Constitutionalism
Project Aristotle

United States

Country Report

December 2021

Authors

Avinash Topno, NLSIU Legal Services Clinic
Jwalika Balaji, NLSIU Legal Services Clinic
Mugdha Mohapatra, NLSIU Legal Services Clinic
Priya Chaudhari, NLSIU Legal Services Clinic

Institute
for Internet &
the Just Society

project
Aristotle

Research Program on Digital Constitutionalism **Project Aristotle**

United States

Country Report

Authors
Avinash Topno, NLSIU Legal Services Clinic
Jwalika Balaji, NLSIU Legal Services Clinic
Mugdha Mohapatra, NLSIU Legal Services Clinic
Priya Chaudhari, NLSIU Legal Services Clinic

December 2021

Inquiries may be directed to digitalgovdem@internetjustsociety.org

DOI: 10.5281/zenodo.5792102

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

Introducing Digital Constitutionalism

The creation of a 'digital society' due to the pervasive use of the internet has raised critical questions on how to navigate issues surrounding privacy, inequality and human rights. It is evident that the role of the government as a regulator and participant must be studied to anticipate and address the exercise of power in the digital age. With this aim in mind, through this report, an extensive analysis concerning the use of the internet, access to data and governance of the internet in the USA has been presented. This analysis is founded upon identifying best practices, relevant statutes/ guidelines and critiquing case law.

In the first section, the core tenets of digital Constitutionalism have been identified and their manifestations discussed. This provides relevant context for the issue of human rights and privacy discussed in the second and third section. In the fourth section, the concept of intermediary liability has been analysed in order to identify key actors and their role in the movement towards conceptualising digital Constitutionalism.

1. How can we define Digital Constitutionalism?

This section outlines the scope and definition of digital Constitutionalism and the philosophical foundations of this movement for political rights and governance in the context of internet usage.

Digital Constitutionalism is a loose term used to describe the relatively recent phenomenon brought forth by the rapid advancements in technology and its consequent interactions with the existence of modern Constitutionalism.[1] However, despite universal agreement on its usage as an umbrella term, the specific definition and scope of the term remains a matter of contention. Herein it should be noted that the agreement on the definition only extends to the matter that the same is used to refer to the matter of adapting constitutional interactions with the challenges of modern technology and not with respect to the scope and content of the term.

Digital Constitutionalism is a component of modern Constitutionalism. Modern Constitutionalism shares foundational values about the Constitution and overall aims which it shall strive to achieve, whereas digital Constitutionalism focuses specifically on the context of the advent of digital technology. This, within the context of the United States, the primary aims of digital Constitutionalism would be to ensure that values such as liberty, political equality etc are upheld and other such values as indicated through its conception of rights within the *Bill of Rights* and its various *Amendments* alongwith its interpretation by the Federal Supreme Court. However, the concept of digital Constitutionalism would also include the limitation of powers exercised by both private and public actors.[2]

Scholars such as Fitzgerald,[3] Berman[4] and Suzor[5] are of the opinion that digital Constitutionalism mainly intends to limit the private powers of big companies. Gasser, in his first work on this topic (2015),[6] proposed a conception of digital Constitutionalism as the limitation of public power, thus it would be maintaining the vision of traditional Constitutionalism relating to the State dimension. However, this viewpoint of Gasser was changed in his second version on this topic (2018),[7] in which he states that the efforts made by the digital Constitution may aim to limit the powers of both public authorities and private companies. Digital Constitutionalism is indeed a concept that refers to a specific context, the digital environment, where private actors emerge beside nation-States as potential infringers of fundamental rights. Such a peculiarity of the digital environment requires a dis-anchoring of the concept of Constitutionalism from the State.

[1]Lex Gill, Dennis Redeker and Urs Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' (2015) BCRP 15.
[2]Celeste E, 'Digital Constitutionalism: a New Systematic Theorisation' (2019) 33 IRL 76.
[3]Fitzgerald, Brian. 'Software as Discourse' (1999) ALJ 25.
[4]Berman PS, 'Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to 'Private' Regulation' (2000) 45 SSRN 54.
[5]Nicholas Suzor, 'Digital Constitutionalism and the role of the rule of law in the governance of virtual communities,' (2010) 14 QUT 45.
[6] Gill (n 1).
[7]Dennis Redeker, Lex Gill and Urs Gasser, 'Towards digital Constitutionalism? Mapping attempts to craft an Internet Bill of Rights' (2018) 80(4) ICG 302.

2. What factors can be considered important to ground Digital Constitutionalism in traditional constitutional concepts?

As per Edoardo Celeste, the value of digital Constitutionalism lies in that it has spurred constitutional law scholars to analyse the impact of digital technology on traditional Constitutionalism and reflect on whether these principles need to be maintained and adapted or done away with in light of the advent of an era of digital communities.[8]

The matter has resulted in the consideration of an internet Bill of Rights delineating the rights available to American citizens on privately owned platforms. Though the conception of the Bill of Rights is mostly centered around the matter of privacy, the Bill may also accommodate other rights such as freedom of speech, right to access etc. The concept is explored by Urs Gasser, an American scholar in relation to digital Constitutionalism as per whom the specific definition of digital Constitutionalism would be "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."[9] Gasser considers the digital Constitution as a complement to the written *Constitution*, with the similar major objective being to limit state power,[10] and subsequently in his 2018 paper, private power.[11] Therefore, he sees the ultimate end of digital Constitutionalism as a Bill of Internet rights.

Digital Constitution

3. What should be the core tenets of a Digital Constitution?

Given the complexities of delineating digital rights from ordinary constitutional rights, it is imperative to identify a set of core values or tenets based on both State and non-State dimensions while including both national and transnational dimensions.[12]

a. Universal Accessibility

The primary tenet of a digital Constitution would be to ensure that the ecosystem in which it exists and operates upon is universally accessible and affordable, as without access to such an ecosystem the value of a digital Constitution would be depreciated. It is noted that approximately 15% of the US Households have no access to the internet, which is a direct result of problems with affordability.[13] A digital Constitution should ensure that access to the ecosystem is free and unfettered and available to all those who may choose to access it without subject to discrimination of any kind[14]. Such a commitment to ensuring universal accessibility would also result in higher digital inclusion, ensuring the participation of individuals from a diverse background.[15]

b. Commitment to privacy and governance

In both national and international spheres, the right to privacy is valued dearly, with the United States under the *14th Amendment* of its *Federal Constitution*[16] while the international community under *Article 12* of the *UDHR*.[17] It is to be noted that the right to privacy includes under it various other rights such as data anonymity, protection surveillance etc.[18] Furthermore drawing upon the existence of a mixed governance structure of public and private actors, these acts must ensure the highest standards of data protection and ensure that the privacy policy of the digital ecosystem is lucid enough to be understood by all while being rigid enough to prevent it from being circumvented.

c. Commitment to Freedom of speech and privacy

[8]Celeste E, 'What Is Digital Constitutionalism?: Digital Society Blog' (2018) 28 *HIIG* 18 <https://www.hiig.de/en/what-is-digital-Constitutionalism/> accessed June 20, 2021.
[9] Gill (n 1).
[10]ibid.
[11] Gill (n 1).
[12]Gill (n 1).
[13]American Community Survey Reports, "Computer and Internet Use in the United States: 2018" (2021) 49 ACS 21. <https://www.brookings.edu/research/5-steps-to-get-the-internet-to-all-americans/> accessed June 18, 2021.
[14]Davies, Todd R., Digital Rights and Freedoms: A Framework for Surveying Users and Analyzing Policies (October 3, 2014). Luca Maria Aiello and Daniel McFarland (Editors), Proceedings of the 6th International Conference on Social Informatics, SocInfo 2014 (Barcelona, November 10-13) , Springer LNCS Series, 2014.
[15]OHCHR, "The Charter of Human Rights and Principles for the Internet".
[16]U.S. Constitution, 14th amendment.
[17]Universal Declaration of Human Rights, Article 12.
[18]Gill (n 1).

The digital ecosystem being one which resulted in greater interconnectivity and interaction is highly susceptible to instances of misuse of the universal right to freedom of speech and privacy, while simultaneously it is at the risk of excessively curbing free speech through unnecessary censorship, defamation etc.[19] Thus, a balance should be sought between the two to ensure that within a reasonable framework the right can be utilised by all.

d. Economic Rights and responsibilities

Considering the facilitation of interaction and the economic opportunities provided due to the creation and proliferation of the digital ecosystem, it becomes imperative for a digital Constitution to ensure that the economic rights and responsibilities arising out of such a situation are capable of being enjoyed by all without being subject discrimination.[20] The rights and responsibilities herein refer to matters such as proper handling of intellectual property, ensuring the economic activity taking place within the governed digital ecosystem promotes free and fair competition supporting innovation and accessibility of services etc.[21]

4. How can Digital Constitutionalism present a constitutional model for the people, by the people, and of the people?

With digital Constitutionalism adopting a formulation wherein the inherent values and aims it seeks to incorporate within the digital Constitution is derived from a mixture of both State and non-State dimensions while including both national and transnational dimensions, it would be quite feasible for the same to create a constitutional model which fits the phrase "for the people, by the people, and of the people."[22] This phrase, in particular, is of great significance in the context of the United States due to being part of the famous Gettysburg address and is considered to be important for the understanding of American Constitutionalism.

The involvement in the context of digital Constitutionalism would be at the stage of deciding what sort of values and aims should the conception of digital Constitutionalism carry in order to achieve a normative digital Constitution[23]. With respect to the Constitution governing the regulated individuals in a manner in which their rights and interests within the digital ecosystem are ensured, the matters would be very challenging. In this regard however, The Internet Corporation for Assigned Names and Numbers (ICANN)[24] and The Internet Governance Forum (IGF) can be utilised to formulate a global public policy based on the core tenets identified as above. The policy also takes into account having regional or country councils wherein the participation of the citizenry may be ensured thereby.

As noted by Jennifer Widner, main phases of drafting a Constitution or a constitutional model are namely drafting, consultation, deliberation, adoption, and ratification.[25] Therefore, by ensuring public consultation, public objections to certain clauses and public oversight of drafting, citizen participation can be ensured.

Representativeness of Online Platforms

5. How can online platforms be made more inclusive, representative, and equal?

The question now arises about the composition of the user group of the online platforms on which these rights are applicable. It is usually shown that despite many users which hail from or are part of marginalised groups on various social media platforms face discrimination which results in discouraged use of said online platforms.[26] On the other hand, there are individuals from minority groups who do want to be a part of these online platforms but are unable to do so due to lack of money, access etc. With respect to certain online platforms especially pertaining to governance, the key is to ensure proper representation for all communities.[27]

[19]ibid.
[20]Gill (n 1).
[21]Celeste (n 2).
[22]Abraham Lincoln, 16th U.S. President, *'Gettysburg Address'*.
[23]Gill (n 1).
[24]Klein H, 'ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy' (2002) 18 ISR 193.
[25]Widner J, 'Constitution Writing in Post-Conflict Settings: An Overview' (2008) 49 WMLR 351.
[26]Keum BTH and Miller MJ, 'Racism on the Internet: Conceptualization and Recommendations for Research' (2018) 8 PVR 782 <https://www.pewresearch.org/fact-tank/2017/07/25/1-in-4-black-americans-have-faced-online-harassment-because-of-their-race-or-ethnicity/> accessed June 20, 2021.
[27]Berg AC and others, 'Inclusivity in Online Platforms: Recruitment Strategies for Improving Participation of Diverse Sociodemographic Groups' (2020) 80 PAR 989, accessed 21 April 2021.

Furthermore, noting that the issues of discrimination against these users usually stems from personal data being readily available to other users without any safeguards,[28] it would be feasible to incorporate some form of anonymization. This should be done especially with regards to those online platforms which deal with e-commerce due to showing a tendency to be affected by offline biases thereby affecting the rights to equal economic opportunities. Further it is noted that the hiring policies of online platform based businesses and companies may also have algorithmic biases in their hiring processes.[29]

In addition to the above, it can be seen that various online platforms are not inclusive by design as in many cases, persons with disabilities cannot access them.[30] With regard to universal design principles and accessibility for people with disabilities, it is noted that much headway has been made with respect to ensuring the same as it noted that major online platforms such as Facebook[31], Twitter[32], and Linkedin[33] have been making efforts in ensuring that disabled individuals are able to utilise the platform as per normal.

Open Source Intelligence

6. What role should open-source intelligence (=OSINT: the discipline of assembling and analyzing publicly available information) play in the future of our society?

In the context of the United States public law, Open-Source Intelligence, generally referred to as OSINT, is defined as such intelligence that is produced from publicly available information. This information goes through the screening process of being collected, exploited and disseminated to a particular appropriate audience.[34] However, this definition does not necessarily restrict the application of any unclassified information to be used for being collected as information, as per NATO.[35] An important utility surrounding OSINT is with operational use towards improving the operational security of an organization.[36] Besides this, OSINT can also be utilised in various other general uses for a varying degree of importance, such as discovering any relevant information about an organization that is outside the reach of said organization in public platforms, collating information into useful and actionable intelligence, among other utilities.[37]

When the question comes in of how said Open-Source Intelligence affects our society, one does not need to look any further than its implementation in various fields of State-run activities. An acute example of the same can be with the Law Enforcement Agencies such as the police force of various states utilizing the OSINT tools to create the foundation of an 'intelligence-led policing';[38] easing up the process of gathering data regarding any contemporary forms of criminal activity.[39] To this extent, with the addition of stringent guidelines in place to avoid racial profiling, the utility of OSINT in LEA field seems to be promising and seemingly creates a safer space for law enforcement to be enacted and followed. However, when taking into consideration the readily available nature of OSINT tools such as the prime source for gathering OSINT information with the Harvester, the question we are begged to answer is rather 'to what extent do these OSINT tools have to go, for it to cross the border surrounding legality' i.e., to what extent does OSINT fall within the rules of digital Constitutionalism ? To that extent we need to look no further than the method which

[28] Koh V and others, 'Offline Biases in Online Platforms: a Study of Diversity and Homophily in Airbnb' (2019) 8 EPJ Data Science, accessed 21 April 2021.
[29]Dastin J, "Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women" (*Reuters*October 10, 2018) <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G> accessed June 20, 2021.
[30]Gleason C and others, "Future Research Directions for Accessible Social Media" [2020] ACM SIGACCESS Accessibility and Computing 1
[31]Al-Heeti A, "Facebook Boosts Accessibility with Scalable Font Sizes, Screen Reader Changes" (*CNET*July 30, 2020) <https://www.cnet.com/news/facebook-boosts-accessibility-with-scalable-font-sizes-screen-reader-changes/> accessed June 20, 2021.
[32]Brand D and Beykpour K, "Making Twitter More Accessible" (*Twitter*September 2, 2020) <https://blog.twitter.com/en_us/topics/company/2020/making-twitter-more-accessible> accessed June 20, 2021.
[33]Linkedin T (*Accessibility*) <https://www.linkedin.com/accessibility> accessed June 20, 2021.
[34]The National Defense Authorization Act for Fiscal Year 2006, s.931.
[35]NATO Terminology Database, <https://nso.nato.int/natoterm/content/nato/pages/home.html>, accessed March 31, 2021.
[36]Josh Fruhlinger, 'What is OPSEC? A process for protecting critical information.', (*CSO India*, 08 May 2019), <https://www.csoonline.com/article/3391566/what-is-opsec-a-process-for-protecting-critical-information.html>, accessed March 31, 2021.
[37]John Breeden II, Josh Fruhlinger, '8 top open-source intelligence tools', (*CSO India*, 15 September 2020), <https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html>, accessed March 31, 2021.
[38]Babak Akhgar, Douglas Wells, 'Critical success factors for OSINT driven situational awareness', (2018) 18 European Law Enforcement Research Bulletin,<https://core.ac.uk/download/pdf/161527778.pdf>, accessed March 31, 2021.
[39]Babak Akhgar, Open Source Intelligence Investigation: From Strategy to Implementation, (1st edn. Springer 2017) p.11-19.

threat actors can utilize to attack weaker points in a target network, exposing said vulnerability to further exploitations to achieve a wide array of nefarious end goals.[40] Threat actors in this particular context can generally be deemed as the individuals or entities that utilize these OSINT tools and sources to identify vulnerabilities within a system and exploit it for their own personal means.[41] Although this should also lead us to spotlight the fact that these very tools can be utilised to identify and investigate these threat actors themselves.[42]

However, in this scenario, the utilization of OSINT tools by the relevant bodies themselves to find the overlying digital vulnerabilities is a rather simplistic and straightforward way to ensure the same tools cannot be utilised to find such vulnerability in the first place.[43] In such scenarios, it thus becomes imperative for the management of digital Constitutionalism that digital frameworks of internet governance are implemented to the open-source OSINT tools, so that it may be able to assess and address issues that could possibly have trans-national consequences. In this regard, the context in which OSINT exists adjacent to digital Constitutionalism is in the form of a double-edged sword, as it can be purposefully utilised to formally exploit the publicly available sources of organizations to be a grasp on what particular strings of data can be utilised to form a credible threat to said organization.[44]

Competition Law and the Internet

7. How can competition and antitrust laws of different jurisdictions protect the global market from big-tech domination, and is there a need to?

The Federal Trade Commission has a concise list of the antitrust laws in the United States.

a. *The Sherman Act* outlaws "every contract, combination, or conspiracy in restraint of trade,"[45] and any "monopolization, attempted monopolization, or conspiracy or combination to monopolize."[46] The Supreme Court decided that the *Sherman Act* prohibits unreasonable restraints of trade, not all restraint of trade.[47]
b. *The Federal Trade Commission Act*[48] bans "unfair methods of competition" and "unfair or deceptive acts or practices."[49]
c. *The Clayton Act*[50] addresses specific competition law practices, like mergers and acquisitions, and directors who may control a host of companies. *The Clayton Act* forbids mergers and acquisitions where the effect "may be substantially to lessen competition, or to tend to create a monopoly."[51]

These laws are important to ensure that there is no big tech domination. House Democrats in the US prepared a comprehensive report in 2020 stating that the Big Tech powers — Amazon, Apple, Facebook and Google had exercised and abused their monopoly power.[52] They argued that these corporations had abused their dominant positions, by setting prices and laying down the rules for search, advertising, commerce, social networking and publishing. They made a case for changing the way antitrust rules operate in the country, to challenge the monopoly power of these big organizations. They proposed stronger reviews of big mergers and restoring competition by effectively breaking up the companies, emboldening the agencies that police market concentration and throwing up hurdles for the companies to acquire start-ups.

---

[40]The Recorded Future Team, 'What is Open Source Intelligence and How is it used?' (2019) RF 437 <https://www.recordedfuture.com/open-source-intelligence-definition/>, accessed March 31, 2021.
[41]CIS, '*Cybersecurity spotlight- Cyber Threat Actors'*,<https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/>, accessed March 31, 2021.
[42]The PhishLabs Team, 'OSINT: Mapping Threat Actor Social Media Accounts', PhishLabs, 15.02.2021, <https://info.phishlabs.com/blog/osint-mapping-social-media-accounts-to-determine-risk>, accessed March 31, 2021.
[43]Safak Herdem, 'Open Source Intelligence (OSINT) and its Effect on Cybersecurity', IRGlobal, 20.12.2018, <https://www.irglobal.com/article/open-source-intelligence-osint-and-its-effect-on-cybersecurity-40ae/>, accessed 31.03.2021.
[44]Steven D Gibson, 'Open Source Intelligence: A Contemporary Intelligence Lifeline', (2007) CUP 23, p. 358.
[45]Sherman Antitrust Act of 1890, s. 1.
[46]Sherman Antitrust Act of 1890, s. 2.
[47]*Standard Oil v. United States* [1911] 221 U.S. 1.
[48]Federal Trade Commission Act of 1914.
[49]Federal Trade Commission Act of 1914, s. 45.
[50]Clayton Antitrust Act of 1914.
[51]Clayton Antitrust Act of 1914, s. 17.
[52]Cecilia Kang and David McCabe, 'House Lawmakers Condemn Big Tech's 'Monopoly Power' and Urge Their Breakups' (*New York Times*, Oct. 6, 2020) <https://www.nytimes.com/2020/10/06/technology/congress-big-tech-monopoly-power.html> accessed 21 April 2020.

The House report indicates the increasing aversion towards Silicon Valley's influence. The report will perhaps culminate into a proper law to govern tech giants and kick off antitrust complaints and investigations by the Justice Department, the Federal Trade Commission and four dozen state attorneys general.

8. 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)?

Scholars are divided about whether there needs to be application and modification of existing constitutional law principles to apply to online platforms.

Professor Richard Epstein states that constitutional principles have been sound at their inception, and that the issues are the same — free speech versus protecting rights of minorities. He does not seem to think that technology is disruptive and needs an overhaul or modification of existing constitutional law principles.[53] This is because he finds no difference between the online and offline application of these principles. Peter Suderman also argues that the way we must be proceeding is that people must take responsibility for their own social media production and consumption, instead of constantly looking to regulate others.[54] This would mean that Government agencies would also not step in to carry out the major functions of regulation. If this suggestion is to be accepted, it would essentially mean self-regulation. The USA can learn from the European Union, who in 1997, adopted a global *Charter* for internet regulation based on two ideas: industry self-regulation, and inter-state regulation.[55] For example, even though hate speech is generally protected by the *First Amendment*, social media platforms like twitter have user guidelines which would not allow hate speech to feature on their platform.[56] However, in addition to the industry regulating itself (for example, privacy policies on each website, guidelines for what constitutes hate speech on social media), users and consumers also have a burden to ensure that they fulfill their legal obligations. This regulatory approach would depend on good faith from both the industry as well as the consumers' ends.

On the other hand, Professor Ari Ezra Waldman defended the position that intervention is necessary to convert constitutional law principles to suit digital interactions. Waldman presented this position before the House of Representatives, stating that lawyers and other moderators are the ones who develop the rules and regulations for content moderations — which ensures that a just set of trained eyes are making and applying the rules.[57] The US Supreme Court in the case of *Reno v. ACLU* stated that the internet is a different medium for communication and sharing of information, as compared to the traditional mediums of newsprint, telephone etc.[58] Therefore, constitutional principles, such as the *First Amendment* rights, will have to be modified when applied to issues pertaining to the digital sphere. This is especially relevant in the current times because social media serves as an echo chamber and also allows for fast mobilization, which is often made use of by extremist groups and resulting in violence.[59] Therefore, the reach and the speed of information transmission in the internet as opposed to other traditional media would also require modification of constitutional principles applying to online interaction. Therefore, advocates of regulation emphasize the unique qualities of cyberspace and call for modification of traditional *First Amendment* and privacy rights.[60]

Whether the principles are static and traditionally applied or have to be fluid, depending on the situation, is not a question that can be answered with a unified voice. For example, such a novel right as the right to be forgotten (in terms of erasing one's data from information systems) does not have an equivalent right in our traditional law principles right now. Therefore, such claims which arise uniquely due to the nature of the digital transaction will require modification of old principles and rethinking how they ought to be applied.

---

[53]Richard Epstein, 'The Irrelevance of the First Amendment to the Modern Regulation of the Internet' (2014) 23(1) JAUCL 115.
[54]Peter Suderman, 'The Slippery Slope of Regulating Social Media' (*New York Times*, 11 September 2018) <https://www.nytimes.com/2018/09/11/opinion/theslippery-slope-of-regulating-social-media.html> accessed 21 April 2021.
[55]Matthew J Feeley, 'EU Internet Regulation Policy: The Rise of Self-Regulation' (1999) 22 BCCLR 159.
[56]Lauren E Beausoleil, 'Free, Hateful, and Posted: Rethinking First Amendment Protection of Hate Speech in a Social Media World' (2019) 60 BCLR 2101.
[57]Filtering Practices of Social Media Platforms: Hearing Before the H. Comm. on the Judiciary, (2018) 115 COG 2 <https ://docs.house.gov/meetings/JU/JUOO/20180426/108231/HHRG- 115-JUOOWstate-WaldmanA-20180426.pdf> accessed 15th Septmeber 2021.
[58]*Reno v. American Civil Liberties Union* [1997] 521 U.S. 844.
[59]Lauren E Beausoleil, 'Free, Hateful, and Posted: Rethinking First Amendment Protection of Hate Speech in a Social Media World' (2019) 60 BC L Rev 2101.
[60]ibid.

B. Human and Constitutionally Guaranteed Rights

Internet Users and Online Platforms

1. Which human and constitutionally guaranteed rights do online platforms affect, and how?

Part A of this report answers the 'how should the internet be governed' using the means of digital Constitutionalism. However, a more fundamental inquiry which this part undertakes is answering 'why should the internet be governed'. Part B of the report focuses on rights implicated in the usage and governance of the internet, against whom these rights need to be protected and how they may be protected

Online platforms affect a host of onstitutional and human rights such as freedom of speech and expression, right to privacy, right to equality and even larger concepts such as democracy and rule of law. The *First Amendment* to the *US Constitution* protects freedom of speech and expression. On online platforms, there may be a need to restrict freedom of speech, or alternatively, even protect freedom of speech and expression against other private parties.[61] In *Packingham v. North Carolina*, the Supreme Court remarked that the right to access online platforms must be made available to everyone, in order for them to exercise their right to freedom of speech and expression.[62] In *Turner Broad. Sys., Inc. v. FCC* the Supreme Court held that there is value in "ensur[ing] that private interests [do] not restrict, through physical control of a critical pathway of communication, the free flow of information and ideas."

The flipside of free speech is ensuring that there is no hate speech, defamation, obscenity, pornography, etc. There must be equal protections for those who are on the receiving end of abusive speech on online platforms. Several US litigations have confirmed that these are areas where speech can be restricted. Illegal action is not to be allowed, as per *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969); fighting words are not protected according to *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942); obscenity is not protecting according to *Miller v. California*, 413 U.S. 15, 23 (1973); child pornography is not protected according to *New York v. Ferber*, 458 U.S. 747, 764 (1982); and some forms of defamation are not allowed as per *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 279-80 (1964) and *Gertz v. Robert Welch*, Inc., 418 U.S. 323, 345-46 (1974). However, some of the *First Amendment* rights are dangerous to be allowed for social media, as the *First Amendment* protects and allows hate speech.[63]

Online platforms also affect the right to privacy. For example, user generated content — speech or sharing of any pictures on social media — could affect the privacy rights of the ones who are being talked about, or pictures could be uploaded without consent, thus violating such persons' privacy. Most constitutional privacy rights exist against the State and the Government agencies, but not against companies or individual persons. However, these privacy rights could be pitched against the *First Amendment* rights on social media, as the person uploading the text or pictures could simply claim freedom of speech or expression.[64] Except the *Californian Constitution*, the freedom of speech and expression laws do not often directly recognize privacy implications.[65] The Courts still uphold the right to privacy in cases involving such speech and expression and a legal jurisprudence has evolved through these judgements.[66]

The character of the digital ecosystem has given rise to a situation where acts of free expression impinge upon the expression of others. This has led to the dissemination of fraudulent information and propaganda that affect the right to self-expression, silencing voices, and marginalising minorities.[67]

2. Who can be defined as a netizen? Who can be classified as a 'bad actor', and can 'bad actors' be netizens ?

A netizen is defined as a person who uses the internet.[68] It is a combination of the words 'net' and 'citizen'. Bad actors are those who attack information systems to compromise cyber-security. They are cyber-criminals,

[61] *Bronner v. Duggan* [2017] 249 DCC 27.
[62] 198 L. Ed. 2d 273.
[63] *Matal v. Tam* [2017] 1764 SCT 1744.
[64] Lothar Determann, 'Social Media Privacy: A Dozen Myths and Facts' (2012) 7 STLR 1.
[65] California Constitution, a.1.
[66] Suzanne Nossel and Viktorya Vilk, 'Protecting Free Expression, Access to Diverse Information and Democratic Engagement Online: Conceptual and Practical Challenges' (2017) GICW 45 <https://www.cigionline.org/sites/default/files/documents/Stanford%20Special%20Report%20web.pdf> accessed 25th September 2021.
[67] ibid; *Protecting Free Expression, Diversity and Civic Engagement in the Global Digital Ecosystem* (Special Report, Centre for International Governance Innovation 2018).
[68] 'Netizen' (*Cambridge Dictionary)* < https://dictionary.cambridge.org/dictionary/english/netizen> accessed 21 April 2021.

who could engage in practices like hacking, data theft, etc. Netizens can be cyber-criminals, because people could use the internet for malpractices, and to commit crimes against information systems as well.

There are some laws in the USA which criminalize those who attack information systems. The rationale for these is based on concerns of privacy and protection from fraud. The *Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030* is a cyber-security law, which protects federal and bank computers, and other computers connected to the internet. It shields information systems from trespass, threats, damage, espionage, and from being used as instruments of fraud. The *Cybersecurity Act of 2015* allows private parties to monitor their information systems to protect themselves from invasions.[69] This indicates that a model focused upon private protection as opposed to government intervention has been adopted.

Safeguarding the Digital Ecosystem: Minority Rights Protection and Consent

3. 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 ?

The digital age of consent in the USA has been set at 13 based on the *Children's Online Privacy Protection Act (COPPA).*[70] This *Act* requires websites to post a privacy policy when it collects information from children below the age of 12, notify parents, get parental consent, allow parents to review and delete information, maintain confidentiality etc.[71] This legislation is founded in the rights of a child to privacy, preservation of identity, the right to free speech which also includes the right to receive information, the right to reputation and the State's recognition of a parent's duties towards a child.

Public Order

4. 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?

"Public order by definition is the prevalence of public interest over the interests of the individuals. By public order we mean a harmonious society, a situation without social troubles. Public order is considered a distinct kind of restriction."[72]

One can adopt a maximalist or minimalist approach in regulating as per public order based on this definition. According to the maximalist approach any attack that can be carried out against public order via dissemination of information through the internet should be regulated. However, this goes against the liberal foundations of a democratic society that values individual liberties. A minimalist approach is thus desirable as it clearly recognises public order as the protection of national security or the security of persons or goods which is clearly distinct from the protection of the government. A clear distinction must also exist between imminent danger and controversial political opinions.[73]

In the American context, in response to the growing instances of online hate speech and the use of online communications to organise riots, it is considered desirable to have a comprehensive law on hate speech. However, any such law must be compatible with the *First Amendment* right to free spee ch and expression.[74]

Internet shutdowns, called 'network disconnections' occur when telecommunications companies either block or throttle internet applications, text messaging, or phone traffic. In the United States the *Standard Operating Procedure 303* codifies "a shutdown and restoration process for use by commercial and private wireless networks during national crises." This was approved by the NCS in 2006. Subsequently this was deployed in San Francisco after an officer in San Francisco killed a homeless man. Most recently, in 2016, the US Supreme Court denied a petition to observe the *SOP 303*. Thus it is evident that internet shutdowns are considered legally acceptable to regulate the flow of information because of expansive interpretation of the

[69]Jeff Kosseff, 'Defining Cybersecurity law' (2018) 103 ILR 985.
[70]Children's Online Privacy Protection Act of 1998, s.13.
[71]Children's Online Privacy Protection Act, 2000.
[72]Lean o Hasmeen, 'Stylianos Garipis, Internet and public order In: Cyber Identities: Canadian and European Presence in Cyberspace' (1999) UOP <https://books.openedition.org/uop/1374?lang=en> accessed 23rd September 2021.
[73]ibid.
[74]Richard Stengel, 'Why America needs a hate speech law', (*The Washington Post* October 29 2019).

existing laws. However, a further examination into the normative basis of such shut downs shows that internet shutdowns cannot be justified because they have little to no bearing on the desired outcome.[75]

C. Privacy, Information Security, and Personal Data

Personal and Non-Personal Data

1. How do we define personal and non-personal data?

In this section of the report, the legislations having an impact on privacy and information security have been analysed. This begins with an analysis of the definition of personal and non-personal data. In the ambit of personal data protection, systems such as end-to-end encryption and traceability and their importance have been highlighted. A critique of the validity of compliance with such laws during a crisis or the use of such information by intelligence agencies has been presented. Based on this, guiding principles that can be relied upon in such circumstances have been highlighted.

As there is no plenary data protection regulator in the USA, the legal definition of personal data in the USA differs from legislation to legislation. However the scope of authority of The Federal Trade Commission is very broad and defines personal data as information that is linked or reasonably linkable to a specific individual including IP addresses and device identifiers.[76]This definition was last updated in 2016 and does not reflect the changes taking place. On the other hand, the recently formed *California Consumer Privacy Act* takes a step in the right direction by defining personal information in a more comprehensive and specific manner. It defines personal information as any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular household or consumer. Further it specifically includes, names, contact information, alias, government IDs, contact information, and so on, if such information is linkable with a particular consumer or household.[77]

The lack of a federal level statute which comprehensively defines personal data negatively impacts any meaningful effort towards data protection and thus there is a need for a holistic, comprehensive and federal definition of the same. When it comes to non-personal data, there has been a lack of legal definitions in the USA.

2. What should be the ethical, economic, and social considerations when regulating non-personal data?

The question at hand is whether there is a need to regulate non-personal data and if so, what should be the considerations while doing so. To begin with, the reality of mixed datasets containing both personal and non-personal data, as well as the unavoidable overlap between the two, precludes a clear delineation. This raises the question of whether or not there is such a thing as completely non-personal data. Perhaps this is possible when data refers to non-human, non-personal data, but when data comes from an individual, the difference is murky, especially given the limitations of anonymization.

Second, because of the well-documented issue of the possibility of reidentification of anonymised data, the difference given is at best hazy. Re-identification from datasets that include coarse credit card metadata has been shown by computer scientists. Another study used movie preferences to re-identify people, indicating that “an adversary who knows a little bit about some subscriber can easily identify her record if it is contained in the dataset, or, at the very least, identify a small collection of records that include the subscriber's record.” As our ability to analyze and arrange data has increased, legal scholars have argued that the failure of anonymity and the development of re-identification techniques “lifts the curtain that has clouded privacy arguments for far too long.”

There are certain economic considerations to be kept in mind too. Data in today’s day and age is an undeniable asset. The acquiring of data depends on having a certain infrastructure and user-base in place which creates a vicious cycle where one who possesses data gets a greater capacity to gather more. It creates entry barriers in the market and creates an oligopoly in the market. This level of power to a handful of corporations has negative connotations for the consumers as well as the competitors.

---

[75]‘FAQ On Internet Shutdowns’ (*Internet Freedom Foundation*) <https://internetfreedom.in/shutdowns-faq/#:~:text=There%20has%20been%20zero%20evidence,we've%20had%20the%20Internet.> accessed 29 June 2021.
[76]‘Definitions In United States - DLA Piper Global Data Protection Laws Of The World’ (*Dlapiperdataprotection.com*, 2021) <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=US> accessed 30 June 2021.
[77]California Consumer Privacy Act 2018.

End-to-end Encryption

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?

An end-to-end encryption system is one where only the sender and the recipient of certain information can access it.[78] This system is secured by creating a public-private key pair, i.e., two keys for encrypting every piece of information. Public keys are used to lock a message or a piece of information and are widely disseminated, whereas private keys are used to unlock a piece of information and are only known to the owner, thus denying access to the data to all third parties like governments, hackers and even the tech companies themselves. Although not wholly fool proof[79], this encryption system ensures a high level of security of data and is thus employed in a whole range of tech products, including those of major tech giants like Facebook[80] and Apple.[81]

Law Enforcement Agencies and, subsequently, governments worldwide have been calling for tech companies to create backdoors in their encryption systems,[82] to provide the State with access to the content earlier protected by End-to-End encryption. The reason cited for this demand is mitigating risks posed to public safety. The instances of online harm are evermore real and varied as the world becomes increasingly interconnected as social media penetration reaches unprecedented heights.[83] The National Center For Missing and Exploited Children received 16.9 million reports of children being exploited online in 2019 alone;[84] a massive majority of these reports came from Facebook, a company that employs end-to-end encryption systems in their products. The use of the internet and social media to help bolster activities related to terrorism is a cause for worry as recognised by the United Nations.[85]

In the USA, Law Enforcement Agencies and the Justice Department's persistent demand has resulted in the introduction of multiple *Anti-Encryption bills* in the senate,[86] though none of them has yet successfully been passed as laws[87] as they often create a major uproar within the citizenry with prominent cyber-experts criticizing them. Governmental Agencies' long-standing demand of weakening encryption systems stems from a fear of not having access to information in encrypted channels. The *United States Federal Stored Communications Act (SCA)* provides for access to the user data held by US-based technology companies. The information obtainable through this framework ranges from basic subscriber records, which may include: name, length of service, credit card information, and so on to stored content, which may include messages, images, videos, and location information.[88]

Given the existing legal framework for providing user data to law enforcement agencies, one might question the government's need for a backdoor into end-to-end encryption systems. However, it must be noted that these laws apply only to the data stored on the server, and in end-to-end encryption, data is rarely stored on the server, and even when it is, it is in an unreadable form, thus serving no real purpose to the law enforcement agencies.

---

[78]'End-To-End Encryption And How It Works | Preveil' (*PreVeil*) <https://www.preveil.com/blog/end-to-end-encryption/> accessed 15 March 2021.

[79] 'End-To-End Encryption Isn't Enough Security For 'Real People' (*The Conversation*, 2017) <https://theconversation.com/end-to-end-encryption-isnt-enough-security-for-real-people-82054> accessed 16 March 2021.

[80] Nandita Mathur, 'Facebook Messenger Joins Whatsapp In End-To-End Encryption' (*Livemint*) <https://www.livemint.com/Consumer/llIJ9Est0ZZIYfmvRSsTZP/Facebook-Messenger-joins-WhatsApp-in-endtoend-encryption.html> accessed 15 March 2021.

[81]Take That, FBI: Apple Goes All In On Encryption (*the Guardian*, 2016) <https://www.theguardian.com/technology/2016/jun/15/apple-fbi-file-encryption-wwdc> accessed 15 March 2021.

[82]Department of Justice, 'International Statement: End-To-End Encryption And Public Safety' (2020), <https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety/> accessed 15 March 2021.

[83]'Demographics Of Social Media Users And Adoption In The United States' (2019) PRCIST <https://www.pewresearch.org/internet/fact-sheet/social-media/> accessed 15 March 2021.

[84]National Center for Missing and Exploited Children (2019) <https://www.missingkids.org/content/dam/missingkids/gethelp/2019-reports-by-esp.pdf> accessed 15 Mar 2021.

[85]'The Use Of Internet For Terrorist Purposes' (2021) UNDC <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> accessed 15 March 2021.

[86]'EARN IT Act, 2020, s. 3398.

[87] ibid.

[88]'H.R.4943 - 115Th Congress (2017-2018): CLOUD Act' (2021) CC <https://www.congress.gov/bill/115th-congress/house-bill/4943> accessed 15 March 2021.

The critics of this 'backdoor encryption' oppose regulations aimed at weakening the end-to-end encryption systems for various reasons. Tech experts oppose the proposal of backdoor encryption as creating a backdoor to end-to-end encryption amounts to breaking it; the creation of a backdoor corrupts the encryption system's entire structural integrity as backdoors open up the possibility of this access falling into the hands of malevolent third parties. The U.S. House Encryption Working Group observed "any encryption which weakens the encryption works against the national interest".[89]

The creation of a backdoor ensures an ability to decrypt which opens up billions of users to a potential breach of privacy by companies already under fire for collecting and commercializing extensive user data. This ability to decrypt can and will incentivize authoritarian governments worldwide to abuse this newfound source of comprehensive information on its citizens, thus violating their rights to freedom of opinion and expression, a right recognised by the United Nations in its report.[90]

Regulatory Sandbox

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?

Governments of major countries like the UK, India, Australia, or Canada have enacted data protection or privacy statutes. However, the USA is yet to have a sweeping federal data protection law that covers all states and guarantees uniform protection of privacy to all citizens regardless of their location. Despite the lack of a sweeping legislation, other laws enable the US government to hold tech-companies liable. The US government has time and again fined tech companies like Facebook,[91] Uber,[92] and Paypal[93] under the *FTC Act 1914*, for engaging in "unfair or deceptive" practices regarding their self-declared privacy and data protection policy. Consider the following scenario: If a tech-company like Facebook engages in any action which goes against its privacy policy, the US government can fine it under *FTC Act 1914*. Suppose a company does not have a privacy policy, then there lies no cause of action under *FTC Act 1914*. Essentially, tech-companies are the one setting the rules for themselves, as long as the rules concern data protection.

The absence of a federal law on data protection means that the US government could hypothetically roll out a Contract Tracing/Exposure Notification App with the legal hurdles being compliance with the various state privacy laws, the most prominent ones of which only apply to commercial services.[94] The services rolled out would require the mobile phone devices to collect particular forms of data regularly, and the opacity of these systems could spell out potential misuse of data by device manufacturers.

Intelligence Agency

5. According to which principles and regulations should intelligence agencies operate online?

Three primary pieces of legislation which govern the surveillance activities of intelligence agencies in the USA are as follows:

a. The *Foreign Intelligence Surveillance Act*[95] lays down the procedures for the surveillance of foreign powers that include US citizens and permanent citizens suspected of terrorist activities. It requires judicial intervention, but only in US citizens' cases, and after 72 hours, the surveillance starts.

---

[89]'Encryption Working Group Year-End Report' (2016) EWC <https://info.publicintelligence.net/US-HouseEncryptionWorkingGroup-2016.pdf> accessed 15 March 2021.

[90]'Report Of The Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression' (2017) UNHRC <https://www.undocs.org/A/HRC/35/22> accessed 15 March 2021.

[91]'FTC Imposes $5 Billion Penalty And Sweeping New Privacy Restrictions On Facebook' (2019) FTC<https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions> accessed 17 March 2021.

[92]'Uber Agrees To Expanded Settlement With FTC Related To Privacy, Security Claims' (2018) FTC <https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security> accessed 17 March 2021.

[93]'Paypal Settles FTC Charges That Venmo Failed To Disclose Information To Consumers About The Ability To Transfer Funds And Privacy Settings; Violated Gramm-Leach-Bliley Act' (2018) FTC <https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information> accessed 17 March 2021.

[94]Ccpa-info.com <https://ccpa-info.com/wp-content/uploads/2019/09/bclp-practical-guide-to-the-ccpa.pdf> accessed 17 March 2021.

[95] Foreign Intelligence Surveillance Act, 1978.

Section 702 of *FISA* provides for surveillance of non-Americans outside the country but many US citizens find themselves in surveillance programs by the FBI and NSA. This *Section* requires periodic reauthorization by congress and is currently in effect till 2023.[96]

b. The *Patriot Act* was rushed into law shortly after the 9/11 attacks, covering a range of issues of the security of the state, including surveillance. It increased the scope of surveillance under US law and empowered any district judge to issue a warrant for terrorism investigations.

The most problematic provisions of the act are:

i. Sneak-peek warrants allowed law enforcement agencies to break and enter premises after obtaining a warrant without informing the owner.
ii. Roving wiretaps removes the need of a warrant if the suspect throws away his phones or changes his address while including casual contacts of the suspect in surveillance. Critics argue that these wiretaps violate the *Particularity Clause* of the *4th Amendment*[97]
iii. Legitimizing surveillance of a 'lone wolf' who has no connections with terrorist organizations.

c. *The Freedom Act* reauthorised most of the *Patriot Act* provisions, including roving wiretaps and lone wolf, but it also provided some limits concerning bulk interception and required agencies to request data on particular users instead of maintaining a whole bulk database.

The US Foreign Intelligence Surveillance Court is a federal court set up to issue warrants and oversees law enforcement surveillance. The NSA and FBI's requests are made, most of which are kept secret, leading to questions on the said court's transparency and accountability. The advancement of end-to-end encryption systems that deny access to data to even the companies themselves has prompted Intelligence agencies to demand new laws[98] that would mandate creating a backdoor in End-to-End encryption systems. The analysis of the current legal regime shows a rather robust surveillance framework with relatively little effective oversight.

SUGGESTED GUIDING PRINCIPLES

a. DATA MINIMALISATION

Article 5(1)(c) of the *General Data Protection Regulation* of the EU states that "Personal Data shall be adequate, relevant and limited to what is necessary for the purposes for which they are processed." There needs to be an effort that focuses on minimizing data collection to the bare essentials; mass surveillance should not be allowed solely due to claims of better pattern spotting by the agencies. Massive data collection would hamper the right to privacy which in turn will negatively impact the freedom of expression. The present system allows for massive data collection with little real restraint in the form of the US FIS court.

b. ACCOUNTABILITY

Intelligence Agencies shall be held accountable for the limited data they collect for law enforcement purposes. A mechanism that aims to redress the wrongful harms or losses suffered by people due to surveillance operations by agencies online, needs to be present.

c. TRANSPARENCY

Intelligence Agencies shall aim to remain transparent in their surveillance programs. There should be complete transparency about the criteria that can get a person under surveillance, the spectrum, and the extent of the data collected.

Jeremy Bentham's panopticon described a cost-effective 18th-century prison model, consisting of a single, concealed watchtower capable of monitoring the inmates without them knowing if they were being monitored or not.[99] This system's success can be attributed to the collective psychology of fear of being constantly monitored.[100] Similarly, Michel Foucault uses the term 'panopticism' to define modern "disciplinary societies,"

---

[96]'Statement By The Press Secretary On The FISA Amendments Reauthorization Act Of 2017 | The White House' (*The White House*, 2018) <https://web.archive.org/web/20201111100755/https://www.whitehouse.gov/briefings-statements/statement-press-secretary-fisa-amendments-reauthorization-act-2017/> accessed 20 April 2021.
[97]Legal Information Institute, Fourth Amendment.
[98]EARN IT Act Of 2020, s.3398 <https://www.govtrack.us/congress/bills/116/s3398> accessed 15 March 2021; 'Lawful Access To Encrypted Data Act (2020 - S. 4051)' (*GovTrack.us*, 2020) <https://www.govtrack.us/congress/bills/116/s4051> accessed 15 March 2021.
[99]ibid.
[100]ibid.

which use the fear of the ability to surveil an individual to create an atmosphere of effective control.[101] The creation of this modern disciplinary state should not be aided, and strict requirements of transparency should be imposed upon intelligence agencies so that the ill effects on free speech are minimised as much as possible. A transparency requirement would force the agencies to provide clearer rationale for their demands of personal data.

D. Intermediary Regulation

Online Harms and Netizens

1. How do we define online harms?

This section offers a descriptive and analytical overview of the USA's legal, social and political position of intermediary regulations of the USA, covering issues such as community guidelines and problematic user-generated content, sponsored content, online harm, and accountability and transparency of online platforms.

Section 230 of *the Communications Decency Act* states that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider",[102] which absolves intermediary platforms from liability of content posted by their users. Before creating a regulatory framework or community guidelines to deal with online harms, there needs to be recognition and a clear definition of what constitutes online harm.[103] The online harms can be broadly divided into three categories,[104] the categories being :

- **a.** Harms with a clear definition: universally accepted harms with relatively easier indicators such as like child sexual exploitation, terrorism content, cyberstalking, etc.
- **b.** Harms with a less clear definition: The components and indicators of these harms are relatively harder to spot, such as disinformation, cyberbullying, advocacy of self-harm, etc.
- **c.** Underage Exposure to legal content.

2. How should community guidelines for online platforms be drafted, disseminated, and enforced? 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?

The interpretation and applicability of community guidelines in controlling the discourse online brings the ever-present dilemma that whether decisions of such public importance should be left with the government or whether free speech must be protected at all costs. Mark Zuckerberg in the wake of criticism against Facebook in influencing the 2016 US Presidential Elections, said that the platform is capable of managing its growing base and mentioned how Facebook is shifting its approach from "connecting people" to "building social infrastructure".[105] This approach finds its roots in the well-established American legal metaphor of 'marketplace of ideas'. Articulated by Justice Oliver Wendell Holmes in *Abrams v. United States*, 1919, "the best test of truth is the power of the thought to get itself accepted in the competition of the market". This position of Facebook, as Nieborg and Helmond write, imply "that the solution to Facebook is simply more Facebook".[106]

The ideas of *First Amendment* jurisprudence and the marketplace of ideas metaphor are echoed in the community guidelines of online platforms.[107] The applicability of this metaphor is legally backed by *Section 230* of the *Communications Decency Act (CDA)* which states "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information

[101]ibid.
[102]Communications Decency Act (CDA) of 1996, S 230.
[103]'Online Harms White Paper' (*GOV.UK*) <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper#the-harms-in-scope> accessed 17 March 2021.
[104]ibid.
[105]Facebook, Building global community, 2017, <https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/> accessed 12 March 2021.
[106]Nieborg, D. B., & Helmond, 'The political economy of Facebook's platformization in the mobile ecosystem: Facebook Messenger as a platform instance' (2019) MCS 41(2), p.199.
[107]Ammori, M, 'The "new" New York Times: Free speech lawyering in the age of Google and Twitter' (2014) HLR 127(8), 2259–2295. <https://harvardlawreview.org/2014/06/the-new-new-york-times-free-speech-lawyering-in-the-age-of-google-and-twitter/> accessed 8 April 2021

content provider".[108] By absolving the online platforms of accountability, the law promotes the marketplace of ideas metaphor by encouraging dispute resolution by the way of "more speech" rather than "speech suppression".

However, the departure from this metaphor is where the problem of ambiguity lies. Twitter mentions in its community guidelines, "we prohibit behavior that crosses the line into abuse."[109] The definition of the 'line' leaves a major room for ambiguity and puts immense power in the hands of unelected tech executives.[110] It is also argued that in the garb of restricting harmful content, online platforms protect its "worst offenders of hate speech, harassment, and abuse." Governments are also jumping in to misuse the gaps in these guidelines to further their ideology and 'direct' the tech-giants to take down their content. As David Kaye, a former UN special rapporteur on free expression writes, "Authoritarian governments are taking cues from the loose regulatory talk among democracies."[111]

The solution to all of the aforementioned problems lie in harmonised action between the government and the online platforms. Community guidelines can be drafted, disseminated and enforced in a better way by the way of following suggestions:

- **a.** When it comes to drafting the community guidelines, the current space for vagueness must be replaced with thorough established principles of human rights to set standards on free speech and requires restrictions to be relevant and proportionate.
- **b.** The lack of availability of detailed data in the public sphere could promote underhand practices as was evident in the case of Cambridge Analytica. Just like listed companies open up their accounts, online giants should also make their data available for audit for further public scrutiny.
- **c.** As proposed by the human rights organisation 'Article 19', the cases of content-moderation must be open to review by a representative non-statutory board and independent non-governmental 'social media councils.'[112] These councils will serve as transparent, accountable, independent and participatory bodies allowing democratic debate over content moderation. Facebook took the initiative in this matter by creating an independent oversight body.[113] However, there were concerns regarding the little or no power granted to the body.

3. Should online platforms be immune from liability from third-party, user generated content [refer to intermediary liability laws]?

The US law does not treat data intermediaries as publishers of the information.[114] Other than for few acts such as 'obscenity' and child pornography,[115] The internet is protected by the *First Amendment* which bars the government from directly censoring it.

Several scholars have raised concerns over the unchecked powers that the online platforms enjoy because of *Section 230*.[116] Blanket immunity granted to these platforms eliminates any will to voluntarily work to minimize harm and such immunity "can foster irresponsibility."[117] Unchecked immunity to these platforms can eliminate deterrence. As Citron notes, ordinary citizens will have to bear the consequences of such immunity as the resources employed in fighting their case against hate speech online will be hefty.[118]Conversely, to avoid liability, online platforms might excessively curtain speech, leading to a more significant challenge of

[108] 47 U.S.C. § 230, 1996.
[109]'The Twitter Rules: Safety, Privacy, Authenticity, And More' (*Help.twitter.com*, 2021) <https://help.twitter.com/en/rules-and-policies/twitterrules#:~:text=Hateful%20conduct%3A%20You%20may%20not,%2C%20disability%2C%20or%20serious%20disease.> accessed 15 June 2021.
[110] Crawford K., & Gillespie T, 'What is a flag for? Social media reporting tools and the vocabulary of complaint' (2016) NMS 18(3) 410–428.
[111]'Social Media'S Struggle With Self-Censorship' (*The Economist*, 24 October 2020) <https://www.economist.com/briefing/2020/10/22/social-medias-struggle-with-self-censorship> accessed 8 March 2021.
[112]'The Social Media Councils: Consultation Paper' <https://www.article19.org/wp-content/uploads/2019/06/A19-SMC-Consultation-paper-2019-v05.pdf> accessed 15 June 2021.
[113]'Facebook Will Create An Independent Oversight Group To Review Content Moderation Appeals' (*The Verge*, 2021) <https://www.theverge.com/2018/11/15/18097219/facebook-independent-oversight-supreme-court-content-moderation> accessed 1 April 2021.
[114]Communications Decency Act of 1996, s 230.
[115] ibid.
[116]Jack Goldsmith & Tim Wu, Who Controls the Internet? 2006; James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors, 1997, 66 U. CIN. L. REV. 177.
[117]Mark A. Lemley, Rationalizing Internet Safe Harbors, 2007, 6 J. TELECOMM. & HIGH TECH. L. 101, 112-13.
[118]Danielle Keats Citron, Cyber Civil Rights, 2009, 89 B.U. L. REV. 61, 115–25.

limitation of free speech. However, a middle ground can be achieved by striking a standard of liability as noted by the Supreme Court in *New York Times Co. v. Sullivan*.[119] Countries such as Canada, Germany, and the UK value free speech and do not grant blanket immunity to online platforms.[120]

Online platforms can take a major step in this direction to ensure 'traceable anonymity.'[121] In the event of any unlawful behaviour, the anonymous account can be taken down by the permission of a court order, and action can be initiated against them. This action rules out the possibility of over-deterrence or under-deterrence. As Citron suggests, these complaints must "include proof that the claims would survive a motion for summary judgment".[122] As noted by Justice Scalia, "because anonymity makes lying easier, the identification of speakers can significantly deter the spreading of false rumors and allow us to locate and punish the source of such rumors."[123] Improvements in screening technology will also help the social media giants to minimise problematic content online. Alternative Dispute Resolution in such matters can be promoted to reduce the burden of complainants of going through formal litigation.

The Intermediary Platforms in the USA are currently primarily regulated by two crucial pieces of legislations: *Section 230* of *the Communication Decency Act*[124] and *Section 512 of Digital Millennium Copyright Act (DMCA).*[125] *Section 230* of *CDA* provides any 'interactive computer service' provider or user with broad liability from user-generated or third-party content by not treating them as the publisher of the content and absolving them of the liability to screen or remove any content they deem offensive. In the recent case of *Viacom Int'l Inc. v. YouTube, Inc*.[126], the US districts and Second Circuit Courts held that in order to hold an intermediary liable for copyright infringement, the copyright owner has the onus to prove that the intermediary platform had specific knowledge of infringement activities exerted 'substantial influence' on the infringing activities of the users.

There are two arguments to explain this almost unchecked immunity given to intermediaries. The first is that the lack of immunity would result in a chilling effect and cause a knee-jerk reactionary system that would severely limit Free Speech in a rather arbitrary manner. The other argument against holding intermediaries liable comes from an economic perspective. Holding intermediaries liable for user-generated content would require them to employ oversight systems, either automated or human-controlled, which require substantial revenue.[127] An Internet Association report suggests that a weakened Intermediary Liability protection would cost 4.25 million jobs and nearly half a trillion dollars in a decade.[128]

Section 230 should not immunize platforms for ratification, republication, or amplification of unlawful speech. As one participant noted, "freedom of speech is not freedom of reach."[129]The question is how to define re-publication where algorithms and technology could be seen as 're-publishing' or 'amplifying' almost all speech on the service. While there may be a way to distinguish where a platform actively promotes speech on the basis of its substance (e.g., featured story of the day or sponsored content), this distinction should be carefully considered and defined.

In light of this, well-calibrated modification of *CDA 230* may go a long way in helping to give the public and civil society a fighting chance by encouraging platforms to stabilize and balance the marketplaces of ideas they own and operate. Of particular importance is the reduction or elimination of techniques of distribution that, regardless of the truth or falsity of the messages channelled through them, erode trust in public discourse and

---

[119]New York Times Co. v. Sullivan, 376 U.S. 254, 279-83 (1964).

[120]Thomas J. Webb, Note, Verbal Poison-Criminalizing Hate Speech: A Comparative Analysis and a Proposal for the American System, 2011, 50 WASHBURN L.J. 445, 446; Michael L. Rustad & Thomas H. Koenig, Harmonizing Cybertort Law for Europe and America, 2005, 5 JHTL. 13, 47-49.

[121] Luis von Ahn and others, 'Selectively Traceable Anonymity' <https://www.petsymposium.org/2006/preproc/preproc_12.pdf> accessed 16 June 2021.

[122]Danielle Keats Citron, Cyber Civil Rights, 2009, 89 B.U. L. REV. 61, p. 123.

[123]*McIntyre v. Ohio Election Comm'n*, 514 U.S. 334, 382 (1995).

[124]'47 U.S. Code § 230 - Protection For Private Blocking And Screening Of Offensive Material' (*LII / Legal Information Institute*) <https://www.law.cornell.edu/uscode/text/47/230> accessed 24 March 2021.

[125]'17 U.S. Code § 512 - Limitations On Liability Relating To Material Online' (*LII / Legal Information Institute*, 2021) <https://www.law.cornell.edu/uscode/text/17/512> accessed 24 March 2021.

[126] *Viacom Int'l Inc v YouTube Inc* [2013] Southern District Court of New York (Southern District Court of New York).

[127]Christopher Hooton, 'Measuring The U.S. Internet Sector: 2019 • Internet Association' (*Internet Association*, 2019) <https://internetassociation.org/publications/measuring-us-internet-sector-2019/> accessed 24th March 2021.

[128]Christian Dippon (*Internet Association.org*, 2017) <https://internetassociation.org/wp-content/uploads/2017/06/Economic-Value-of-Internet-Intermediaries-the-Role-of-Liability-Protections.pdf> accessed 24 March 2021.

[129]'Read Sacha Baron Cohen's Scathing Attack On Facebook In Full: 'Greatest Propaganda Machine In History' (*The Guardian*, 22 November 2019) <https://www.theguardian.com/technology/2019/nov/22/sacha-baron-cohen-facebook-propaganda> accessed 16 June 2021.

democratic processes. Fine-tuning the bounds of *CDA 230* represents one step in realizing and revitalizing this original vision.

4. What should the parameters to define problematic user-generated content be?

Individuals and collaborative groups can now create and share content on a very large scale that previously could have only been undertaken by book publishers, recording companies and studios. As the volume of content increases, so too do its problems. Problematic User Generated Content (UGC) can majorly occur in three forms. Individual textual, audio, image, video, and multimedia productions are distributed online through software platforms such as blogs, Twitter, Youtube, etc. Second, software modifications or applications that individuals write. Third, formal or informal groups that collaboratively produce and distribute UGC, including open source software (OSS) etc. The following are some of the legal issues relating to UGC:

- **a.** Copyright Infringement: Businesses that use user-generated content run the risk of infringement by publishing submissions from fans that use protected photos.
- **b.** Privacy Rights: If a photographer posts an image under a royalty-free license, a company might be tempted to reasonably conclude that they have all the verification and approval needed to use it for commercial purposes, which may not be true.
- **c.** Ownership and Licensure Matters / Intellectual Property: The issue of whether a brand name violates copyright law by sharing user-generated content is a major consideration.
- **d.** Revenue Generation or 'Monetization': Users who freely submit content may not want companies to use their material for ad campaigns and thus earn revenue from the same.
- **e.** Hate Speech and Harassment: The issue of intermediary liability arises with UGC.
- **f.** Inaccurate Statements: Often, users publish inaccurate declarations about a company's rivals. For example, a company rival can create an ad campaign or a contest to publish inaccurate declarations about their rivals.

There are various laws to deal with the UGC, the *1998 Digital Millennium Copyright Act (DMCA), General Data Protection Regulation (GDPR)* and the *California Consumer Privacy ACT (CGPA).* But there should be a proper policy framework that must ensure user's privacy (and anonymity if desired) in creating and posting collaborative UGC.[130] A forward-thinking policy framework will require balancing several factors that will take into account the changing nature and context of the digital environment. First, the ability to access, utilize, re-purpose and distribute existing source materials in a transformative manner is a fundamental prerequisite to optimal creation and use of UGC.[131] Second, copyright and licensing laws that facilitate the creation and protection of UGC must also allow the production of UGC from other source material. Third, care must be taken not to do further damage to the fragile UGC environment through the enactment of overly restrictive digital locks provisions. Fourth, the policy framework must also ensure users' privacy (and anonymity if desired) in creating and posting collaborative UGC and sufficient mechanisms to determine authorship in some specific circumstances. Finally, the expansion of patentable subject matter to include software-based business methods must not encumber OSS production and apps, given that software is already protected by copyright.[132]

5. 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.]

The internet has always been imagined as a forum for democratizing public spaces by allowing more people to participate and transforming how people communicate and conduct business. However, the rapid adoption of internet-based technology has provided both opportunities and challenges that require immediate and strategic resolution.

Online platforms are given protection from bearing liability for the Content posted by the users. Safe harbour is given to the digital media under *Section 230* of the *Communication Decency Act*.[133] This *Section*

[130]Cristina Newsberry, 'A marketer's guide to using user-generated content on social media' (2019) HB <https://blog.hootsuite.com/user-generated-content-ugc/> accessed 13th April 2021.
[131]ibid.
[132]ibid.
[133]Communication Decency Act 1996, s 230.

protects companies operating on the internet from liability for any content their user may post. An example of Facebook can illustrate it; the user will be held liable for Facebook's legal action. This ensures that the company is not the publisher of the Content. Tech companies can freely moderate the Content of users posted on the platform because of the protection given under *Section 230*. It allows platforms to set the content standard and remove the Content if not followed properly.

In the vision of the binaries, safety and privacy are two sides of the same coin. It is essential to provide citizens with the right to free speech and privacy to ensure online security and national security. It has been demonstrated that creating an overarching exception to safe harbour protections to protect the safety of online platforms is counterproductive. It leads to making the internet unsafe for children, women and people from marginalised communities[134] The online platform should not be shielded from the responsibility when they knowingly allow Content on their platform that promote and facilitate violence. Hate speech needs to be condemned and people should be accountable for their words. Citizen's rights to free speech should be protected as it is crucial for democracy. But the speech accompanying violence should not be protected. Technological changes allow people to find each other easily and unite, making it easier to incite violence and hatred. Algorithms are designed to increase polarization and incite violence.[135]

Due to safe harbour protection online platforms are protected from the accountability for hate speeches and the misinformation propagated on their platform. The online platform can moderate the Content on the platform. The issues here are inconsistent enforcement of the platform's policy, which must be noted and addressed.[136]

a. GUIDELINES AND THE APPLICATION OF ALGORITHMS

An important but still relatively under-examined feature of the rapidly evolving content moderation ecosystem is the use of technologies grouped under the generic term 'artificial intelligence' (AI). Amidst significant technical advances in machine learning, automated tools are not only being increasingly deployed to fill essential moderation functions, but are actively heralded as the force that will somehow save moderation from its existential problems. As government pressure on significant technology companies builds, both companies and legislators seem to hope that technical solutions to complex content governance puzzles can be found. Incidents like Christchurch clearly show that automated moderation systems have become necessary to manage growing public expectations for increased platform responsibility, safety and security; however, as has been repeatedly pointed out by civil society groups, these systems remain opaque, unaccountable and poorly understood.[137]

The most obvious deficiency of automated content moderation is the greater risk of false positives and negatives: an educational video about breastfeeding may be mislabelled as pornography. Simultaneously, weaponised disinformation may be promoted in the same way as a news article from a reputable source. As platforms come to terms with their global footprints, they respond however they can, from rolling out new features and interventions to harmful squash content to complying with formal or informal demands from states.[138] Existing arrangements raise questions about how the speech of the many is lost inside a large scale and complex system where it can be difficult to be sensitive to culture, language and context. If platforms prioritize certain users, what happens when the influential few engage in behaviour that qualifies as hate speech or incitement? While over-moderation and censorship are an issue, platforms that decide to leave up

[134]Daniel Kardefelt-Winther, Emma Day, Gabrielle Berman, Sabine K. Witting, and Anjan Bose, 'Encryption, Privacy and Children's Right to Protection from Harm' (2020) UNICEF <https://www.unicefirc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf> accessed 14th April 2021.

[135]Karen Hao, 'Nearly half of the Twitter accounts pushing to reopen Americans maybe bots' (*MIT Review* 21 May 2020) <https://www.technologyreview.com/2020/05/21/1002105/covid-bot-twitter-accounts-push-to-reopen-america/> accessed 14th April 2021.

[136]Ariana Tobin, Madeleine Varner and Julia Angwin, 'Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up' (*ProRebulica* December 9, 2017) <https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes> accessed 14th April 2021.

[137]Tarleton Gillespie and Patricia Aufderheide, 'Expanding the debate about content moderation: scholarly research agendas for the coming policy debates' 2020 IPR 9(4) <https://policyreview.info/articles/analysis/expanding-debate-about-content-moderation-scholarly-research-agendas-coming-policy> accessed 13th April 2021.

[138]Joyti Panday, 'Exploring the problems of content moderation on social media' 2020 IJR <https://www.internetgovernance.org/2020/12/23/exploring-the-problems-of-content-moderation-on-social-media/> accessed 14th April 2021.

are as important.[139] Platform's failure to take action against content that violates their policies or community standards has been the cause of recent content moderation controversies. We increasingly see these play out in the regulatory context and platforms being hauled up in front of committees to explain the political bias in their decision making and being threatened with changes to the intermediary liability regimes.

b. COMMUNITY GUIDELINES ROLE IN GOVERNANCE OF UGC

Community guidelines are a basic set of rules produced by social media and other online platforms to ensure nothing harmful, hateful or detrimental to anyone should be posted on these platforms. The problem arises when these platforms have to control the user-generated Content in large social media spaces such as Instagram, Facebook and Twitter etc. because of the diversity on these platforms. It is never easy to take into consideration each and everyone's values and sentiments and also at the same respect everyone's freedom of speech and expressions. On a general level, these community guidelines by these platforms try to ensure public safety and safeguard public values. They require all the users to post their Content within the sphere of law, therefore they also prohibit posting nudity as they do not consider it appropriate for a diverse audience.[140]

In an ideal scenario, these community guidelines, public policy in the domestic contexts and International human Rights should be overlapping with each other. Only when the three of them are in concurrence can ensure that these platforms remain a safe space and inclusive of all. International Human rights, as under the *Universal Declaration of Human rights (UDHR)*, includes fundamental civil, political, economic, social and cultural rights that all humans should enjoy without fail.[141] If there is a conflict between the community guidelines, public policy and international human rights, international human rights should prevail in case of conflict between these three.

Political Advertising

6. 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?

A political advertisement is a form of campaigning that allows politicians to communicate their message to voters and sway public opinion directly through advertisements and online campaigns.[142] The impact of these advertisements was seen in the 2016 elections.[143] It was disclosed that the Russian government spent $100,000 on the Facebook advertisement to affect the US election.[144]

In political advertisement, lying is legal as political ads are considered political speech protected under *First Amendment Law*.[145] The government has more power to punish or censor commercial speech, but it has little ability to control political advertisements. The logic behind this is that voters have a right to uncensored information from candidates, which they can analyse before voting. For the 2020 US presidential election Facebook announced its strategy to tackle disinformation on the site ahead of the 2020 presidential election, which included flagging Content from state-sponsored media outlets and marking news reports contested by third-party fact-checkers as "false information".[146] At the same time, Google stated that it would not opt for

[139]Jennifer Cobbe, 'Algorithmic censorship by Social Platforms: Power and Resistance' (2020) Springer < https://link.springer.com/article/10.1007/s13347-020-00429-0> accessed 15th April 2021.

[140] Instagram Community Guidelines, *Facebook*, <https://www.facebook.com/help/instagram/477434105621119/> accessed 15th April, 2021.

[141] International Human Rights law, *United Nations human Rights*, 'Office of the high commissioner for human rights" <https://www.ohchr.org/en/professionalinterest/pages/internationallaw.aspx> accessed 16th April 2021.

[142]Lata Nott, 'Political Advertsiment on Social media platform' (2020) ABA 45(3) <https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/voting-in-2020/political-advertising-on-social-media-platforms/> accessed 15th April 2021.

[143]Erika Franklin Fowler, Travis N. Ridout and Michael M. Franz, 'Political Advertising in 2016: The Presidential Election as Outlier?' (2017) TF 14(4) < https://www.degruyter.com/document/doi/10.1515/for-2016-0040/html> accessed 15th April 2021.

[144] Scott Shane and Vindu Goel , 'Fake Russian Facebook Accounts Bought $100,000 in Political Ads' (September 7, 2017) < https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html> accessed 15th April 2021.

[145]John Stewart Fleming, 'Renewing the Chase: The First Amendment, Campaign Advertisements, and the Goal of an Informed Citizenry' (2017) ILJ 87(2) <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3015&context=ilj> accessed 15th April 2021.

[146]Facebook Business, 'Our commitment to security' (2020) <https://www.facebook.com/business/news/our-commitment-to-safety> accessed 15th April 2020.

a different approach for political advertisement.[147] It can be seen that while Facebook has made an exception for speech in political advertising in its rules, Google's ban on misinformation in political ads echoes the basic principles of libel law, enabling victims to claim compensatory damages for false claims of truth against them but not for opinions or insinuations. This ensures that advertisements which are not overtly false are permitted, leaving voters to decide which insinuations to accept and which to ignore. Therefore, Advertisement policies of online platforms adhere to specific standards to reduce the spread of false information and protect the democracy of the country.

The policymakers should draft the policies related to political advertisements on the online platform. Along these lines, Ravel, Woolley, and Sridharan recommend that digital platforms "consult with civil rights groups on an ongoing basis and incorporate findings into product development."[148] Policymakers could find ways to incentivize such partnerships or involve civic and civil society feedback, resulting in more open digital environments that are less susceptible to political exploitation. The degree to which such interventions will override the dominant design imperative of communications networks to maximize private profits will significantly affect the progress of attempts to implement democratic accountability.

Conclusion

Through this report it is apparent that the issues arising in the digital world are rooted in the realities and inequalities of the offline world. It is no longer sufficient to say that there exists a distinction between the 'real world' and 'digital world'. Hence, existing conceptions of governance are proving to be inadequate.

Digital Constitutionalism must rest on a strong foundation of inclusivity, diversity and minimal intervention by the government. Human rights and constitutional rights must be conceptualised keeping in mind public participation and consultation. Privacy issues can be addressed through informed consent, clarity on data use and accountability for violators. Finally, intermediary liability must balance the need for freedom of intermediaries with the need to prevent harm in and through digital spaces.

Thus, the legal, policy-based and technical developments highlighted in this report provide a framework to conceptualise the problems, the need for solutions and how such solutions can be implemented.

[147]Lata Nott, 'Political Advertisement on Social media platform' (2020) ABA 45(3) <https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/voting-in-2020/political-advertising-on-social-media-platforms/> accessed 15th April 2021.

[148]Matthew Crain and Anthony Nadler, 'Political Manipulation and Internet Advertising Infrastructure' (2019) 9 (5) <https://www.jstor.org/stable/pdf/10.5325/jinfopoli.9.2019.0370.pdf> accessed 16th April 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 analyzing 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