Freedom of expression and the private sector in the digital age

ARTICLE 19's written comments

Introduction

The Internet has fundamentally changed the way in which people communicate and go about their daily lives. Whereas the printing press was the gateway to access to information for many centuries, the Internet has brought down those barriers. Anyone with a computer can now create and share content instantly on a scale never before imagined. At the same time, it would be impossible to exercise the right to receive and impart information and ideas online without a plethora of Internet intermediaries, from telecommunications providers to computer hardware and software manufacturers or companies providing hosting or search services. It is therefore fundamental to understand the role of these actors and services in facilitating the exercise of freedom of expression in order to determine the way in which they should be regulated. ARTICLE 19 thus welcomes the decision of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Special Rapporteur) to focus his report on the role of private sector.

In this submission, ARTICLE 19 seeks to assist the Special Rapporteur in identifying (1) the categories of actors in the digital sector whose activities implicate the freedom of opinion and expression; (2) the main legal issues raised for freedom of opinion and expression within the digital sector; and (3) the conceptual and normative work already done to develop corporate responsibility and human rights frameworks in these spaces, including governmental, inter-governmental, civil society, corporate and multi-stakeholder efforts. We have provided country specific information (Brazil) in Annex A.

1. Relevant actors in the private sector

At the outset, we note that there are various ways in which private actors in the digital sector can be categorised. For instance, the Internet is often represented as being made up of the following layers: physical infrastructure layer, the data-link layer, the network layer, the transport layer and the application layer. Another Internet model includes social, content and technical layers.[1]

[1] https://www.icann.org/en/system/files/files/report-23feb14-en.pdf

Freedom of expression advocates have traditionally been more concerned with what could be described as the content layer of the Internet and Internet access. For instance, in our *Internet Intermediaries, Dilemma of Liability* policy brief (2013), ARTICLE 19 distinguished between Internet Service Providers (ISPs), hosting providers, social media platforms and search engines.[2] Similarly, in his 2011 report, the Special Rapporteur Frank LaRue identified ISPs, search engines, blogging services, online communities and social media platforms. By contrast, the OECD also identified data processors, E-Commerce intermediaries, Internet payment systems and participative networking platforms as relevant Internet intermediaries.[3] The various types of Internet intermediaries were summarised in UNESCO's report *Fostering Freedom Online: the Role of Internet Intermediaries* (2014) with the following table:[4]

Table 1: categories and key examples of Internet intermediaries

OECD[42]	Special Rapporteur La Rue[43]	Article 19[44]	CDT[45]	Global Partners[46]
Internet access and service providers	Internet service providers (ISPs)	Internet service providers (ISPs)	Access providers/ISPs Network operators and mobile telecommunications providers	Physical layer: makes communications possible
				Connectivity & code: the language or protocols of the communication
Data processing and web hosting providers		Web hosting providers	Domain registrars and registries Website hosting companies	Applications: tools to navigate content
Internet search engines and portals	Search engines	Search engines	Internet search engines and portals	
E-commerce intermediaries			E-commerce platforms and online marketplaces	
Internet payment systems				
Participative networking platforms	Blogging services Online communities Social media platforms	Social media platforms	Online service providers In general, any website that hosts user-generated content or allows user-to-user communications	

These categories, however, do not account for the various private actors involved in maintaining the security of communication networks, hardware manufacturers, software developers, app developers and companies selling cybersecurity and intelligence systems - all of which play a role in facilitating, and sometimes chilling, the exercise of freedom of expression.

[2] See https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf , page 6
[3] OECD, T*he Economic and Social Role of Internet Intermediaries*, March 2010. p. 9, available at: www.oecd.org/internet/ieconomy/44949023.pdf
[4] See http://unesdoc.unesco.org/images/0023/002311/231162e.pdf at page 21.

More recently, there has been greater policy focus, particularly in Europe, on a new broad category of 'online platforms'. In particular, European regulators have proposed a new definition of 'online platforms' as "*an undertaking operating in two or (multi)-sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups. Certain platforms also quality as intermediary service providers*". However, it is unclear whether the new definition is designed for bringing in new regulation in this area instead of or in addition to the E-Commerce Directive (ECD). Interestingly, the ECD does not seek to categorise *actors* for regulatory purposes but rather focuses on the *function* at issue (mere conduit, caching, hosting). This seems sensible since many Internet companies offer various types of services, from search to video-sharing or social media, which may themselves correspond to different functions (e.g. mere conduit or hosting in the case of search).[5]

At the same time, there is growing unease in countries such as France with the dominance of American Internet companies in European markets. For instance, a French parliamentary Committee on European Affairs recently noted in its observations on the new draft law for a digital Republic that a new notion of 'online platforms' had emerged because the category of 'hosting services' no longer corresponded to the reality of what these platforms were offering.[6] In particular, they were no longer passive since they played an active role in referencing and indexing content, products and services.[7] The committee suggested that online platforms should therefore be regulated differently, which was what the new draft law sought to achieve.[8] Article 22 of the draft law no. 3318 for a digital Republic lays down a broad definition of online platforms as "*activities which consist in indexing or referencing content, goods or services offered or made available online by third parties, or connect, by electronic means, several parties with a view to selling goods, providing services, including for no remuneration, or exchanging or sharing goods or services*". Online platforms falling with this definition would be subject to transparency and loyalty obligations (Articles 22-24), though it remains unclear whether this would apply to algorithms used by companies to index content, goods and services.[9] Whilst this may be the text's ambition, it seems unlikely to materialise.[10] Be that as it may, it illustrates the importance of clear definitions and the need to identify the particular services or functions offered by private actors for the purposes of regulation.

In summary, ARTICLE 19 suggests that, for the purposes of freedom of expression, digital private actors can be divided into the following categories:

---

[5] See ARTICLE 19, *Dilemma of Liability,* cited above at page 6.

[6] See Mme Marietta Karamanli, rapporteure pour la Commission des Affaires Europeennes, Rapport d'information no. 3366 portant observations sur le projet de loi no. 3318 pour une République numérique, 16 December 2015: http://www.assemblee-nationale.fr/14/europe/rap-info/i3366.asp#P346_63622

[7] Ibid.

[8] Ibid.

[9] For more information, see here: http://www.assemblee-nationale.fr/14/projets/pl3318.asp

[10] Articles 22-24 provide for more specific transparency obligations in relation to paid for content/indexing, contractual relations or other capitalistic links between the referencing and the referenced organisation.

- **Actors providing essential services in order to gain access to the Internet:** these include internet access providers, network operators, internet exchange points, mobile telecommunications operators telecommunications providers, which enable Internet users to be connected. These actors may interfere with freedom of expression by blocking, filtering content or otherwise shutting down the Internet. It is also worth noting that actors who were traditionally associated with non-essential services such as Facebook (see below) are now seeking to move into Internet access raising net neutrality issues, for instance in India.

- **Actors providing essential services in order to gain access to information on the internet:** these include ICANN,[11] domain name registries and registrars, which generally enable a given location on the Internet to be found through the Domain Name System (DNS) and may interfere with the right to freedom of expression by refusing to register certain domain names. It also includes website hosting services which allow third parties to upload or post material, and search engines without which information would be nearly impossible to find. In general, hosting services and search engines may interfere with freedom of expression by taking down content or links in the absence of a court order on the basis and/or on the basis of their terms of service (see further below).

- **Actors who facilitate the sharing of information but are not essential to exercising the right to freedom of expression and information:** these include social media and video-sharing platforms such as Facebook, Twitter, LinkedIn, Youtube and many others. While these actors cannot be strictly speaking be said to be essential to accessing information online, they have become the medium of choice for sharing information online. For instance, while Internet users can easily get access to newspaper sites by entering their address in their browser, Internet users increasingly rely on Facebook or Twitter to read the news. For instance, Facebook recently entered into a contractual agreement with the New York Times to host its content.[12] Given Facebook's global reach and financial weight as an organisation with over 1 billion users, this potentially raises issues for media pluralism. Otherwise, social media platforms are generally considered as hosts and may therefore interfere with freedom of expression by taking content down without a court order or on the basis of their terms of service (see further below).

  Other actors in this category include e-commerce services offering or distributing content, such as books (Amazon) or apps (such as the Apple store or Google Play). In the case of the latter, the controls exercised by closed platforms can have a negative impact on the plurality of content available to users. Unlike social media platforms, these controls tend to be applied *ex ante* rather than *ex post,* i.e. following a complaint about the content at issue.

[11] For more information about ICANN and its impact on freedom of expression, see ARTICLE 19, ICANN's Corporate Responsibility to Respect Human Rights, Policy brief, February 2015: https://www.article19.org/data/files/medialibrary/37845/ICANN-PAPER-WEB.pdf

[12] http://www.nytimes.com/2015/05/13/technology/facebook-media-venture-to-include-nbc-buzzfeed-and-new-york-times.html?_r=0

Finally, other important actors in this category include advertisers and payment systems who can exercise significant influence over social media platforms, search engines, websites and content providers since they are a considerable source of revenue for them. For instance, Facebook reportedly changed its policy on content celebrating rape when, among other things, major advertisers, including Dove and American Express suspended their marketing campaign on the site.[13]

- **Actors producing content:** this includes newspapers and other copyright holders - whether individual authors or companies - without whom there would be no content to be shared. At the same time, these actors can interfere with freedom of expression by making abusive copyright complaints in circumstances where the material at issue should be protected as fair use. Nonetheless, it is also true that their activity now largely depends on search engines, social media and closed platforms in order for their activities to be financially sustainable.

- **Actors who protect and/or interfere with the right to privacy and therefore have an impact on the exercise of freedom of expression:** on the one hand, there are computer or other hardware manufacturers, some software developers, companies providing data storage or cloud services and cybersecurity firms, who are essential for providing network security and therefore protect privacy as a pre-condition to the exercise of freedom of expression. On the other hand, many of these actors, data gatherers, data processors and surveillance firms can interfere with privacy and therefore have a chilling effect on the exercise of freedom of expression. These various groups can also influence the development of technical standards, including Internet Protocols, in ways which may both positively or negatively impact both freedom of expression and the right to privacy in fora such as the IETF, ISO, IEEE, W3C and the ITU.

2. Key legal and policy issues

At the outset, we note that a number of major Internet actors have now existed for well over 10 years.[14] Unsurprisingly, therefore, a number of laws and policy issues were adopted in the nineties and beginning of the naughties in order to deal with the new challenges raised by these new actors, including e.g. intermediary liability.[15] In other words, some of the policy issues faced by policy-makers today are not new.

At the same time, the size and market value today of Internet companies, such as Google or Facebook, is such that they arguably exercise an influence over people's daily lives and exercise of freedom of expression that goes beyond that of sovereign countries. Some services, such as

[13] http://www.telegraph.co.uk/women/womens-life/10086454/How-three-women-took-on-sexist-Facebook-and-won.html

[14] E.g. Yahoo was founded in 1995, Google in 1998 and Facebook is already 11 years old. Meanwhile, other Internet giants such as online retailer Amazon have been in existence for over 20 years and Apple Inc. for 40 years.

[15] Ee.g. Digital Millennium Copyright Act 1998 in the US, E-Commerce Directive 2000 in the EU and encryption issues (the 'Crypto Wars') in the US, the Regulatory Investigatory Powers Act 2000 in the UK.

Internet access and search, have arguably become basic utilities, since most individuals would not be able to access employment or health services without Internet access and without search services, information would be nigh impossible to find.

Meanwhile, recent legal and policy developments, particularly coming from the European Union, signal a changing tide in the values and regulatory approach that have long underpinned the Internet. Whereas Internet companies primarily developed in the US driven by its liberal approach to commerce (self-regulation) and the First Amendment, the EU has increasingly taken on a leadership role in championing data protection law and stricter regulatory models in the digital space. These competing visions for the Internet are not purely driven by human rights concerns for the protection of freedom of expression or the right to privacy or personal data protection, however. At stake is the hegemony (and arguably monopoly) of US companies in the ICT sector and the ability of other countries to compete in a globalised world.[16]

Nonetheless, the question remains whether policy models that were designed over 20 years ago are still fit for purpose in light of those changes.

In this section, we merely highlight the key issues that arise in relation to the following areas: (1) content regulation by private actors & intermediary liability; (2) the protection of the right to privacy as a prerequisite for the exercise of freedom of expression (3) the intersection between data protection and freedom of expression. In doing so, we also flag key legal and policy concerns raised by government regulation of the ICT sector, that would negatively affect freedom of opinion and expression. Other freedom of expression issues arising in the context of Internet access (such as affordability, universal access etc.) are not addressed here but should be the subject of further study.

Content-regulation by the private sector & intermediary liability

Given our mandate, ARTICLE 19's primary concerns lies with the various ways in which expression is regulated and access to content restricted online, whether by governments or private actors.

With hundreds of millions of users, private companies have come to exercise exceptional influence over individuals' exercise of their right to freedom of expression. In particular, we consider that the following issues should be highlighted:

- ***Lack of transparency and accountability*** in relation to content removals and/or the application of filters under Terms of Service leading to inconsistency and/or bias;
- ***Lack of procedural safeguards and access to an effective remedy*** when legitimate content is wrongfully removed or filtered, including imbalance of powers, unfair contract terms and restrictions on access to justice forcing users to abandon legal complaints;
- ***Failure to respect free expression standards*** *(as provided under international law)* ***in Terms of Service***, turning some of these quasi-public spaces into much more sanitized environments, where freedom of expression is not limited by principles of necessity and proportionality but rather by propriety;

[16] See e.g. Rapport d'information no. 3366 portant observations sur le projet de loi no. 3318 pour une République numérique, 16 December 2015 cited above at fn 6.

- ***Circumvention of the rule of law*** with corporate actors complying, whether or not voluntarily, with government requests to take down, filter or block content or services, resulting in users being deprived an opportunity to challenge the legality of content restrictions;[17] this is compounded by the lack of transparency in relation to the way in which private companies may be amending their Terms of Service to comply with national legislation and ease the removal of content;
- ***Lack of transparency and neutrality*** in the way in which information is presented (e.g. search results, news feeds on Facebook);
- ***The potentially negative impact on pluralism of partnerships*** between internet intermediaries (e.g. Facebook, Google News) and content industries such as newspapers or between Internet and telecommunications companies such as in the debate on net neutrality.

In light of the above, the question arises whether private actors, in particular Internet companies should be subject to greater regulation beyond intermediary liability principles. In our view, there are several reasons why State regulation would be problematic:

- A cornerstone of freedom of expression online is the principle of intermediaries' immunity from liability for third-party content. This principle has been a powerful driver of innovation in the digital sectors, enabling freedom of expression to flourish; and has been recognised in the May 2011 report of the Special Rapporteur,[18] in the 2011 Joint Declaration on Freedom of Expression and the Internet[19] and the Manila Principles on Intermediary Liability (2015).[20] It should therefore not be abandoned in favour of strict forms of liability or the imposition of a duty of care on Internet companies that would not only have a chilling effect on freedom of expression but would also interfere with the right to privacy.[21]

- Regulation ultimately gives greater censorship powers to the state, ultimately chilling free expression. In particular, by putting the state in charge of regulating what constitutes permissible expression, minority viewpoints are highly likely to be significantly undermined.

- Regulation involving the administration of a content obligations code by a regulator would force companies to adopt the same community standards which would likely limit the diversity of platforms and content available.

- The independence of regulatory authorities could be threatened by corporations that have diverse ways of buying influence.

---

[17] See EDRi, *Human Rights and Privatised Law Enforcement*, 25 February 2014
[18] A/HRC/17/27, paras. 74-77, available here: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[19] http://www.osce.org/fom/78309?download=true
[20] https://www.manilaprinciples.org/
[21] See for instance, case comment on the decision of the Grand Chamber of the European Court of Human Rights in the *Delfi v Estonia* case (2015): https://inforrm.wordpress.com/2015/10/06/case-law-strasbourg-delfi-as-v-estonia-strasbourg-undermines-freedom-of-expression-gabrielle-guillemin/#comments

- In any event, measures such as requiring social media platforms to register or obtain a licence from a regulator would be incompatible with international standards on freedom of expression. Similarly, sanctions powers involving the blocking of entire platforms or hefty fines for failure to comply with domestic law requirements would in and of themselves constitute a disproportionate restriction on freedom of expression.

At the same time, we recognise that the dominant position of certain Internet actors, such as Google or Facebook raises issues for pluralism, diversity of content and visibility of such diversity. Accordingly, imposing certain transparency obligations on them may be appropriate, particularly as regards paid-for content, promoted links etc. More research would have to be carried into the role of consumer law and lessons learnt from consumer groups in this area. In addition, further research should be carried into the role of competition law, data portability and interoperability of standards as a potential solution to the dominance of certain platforms, network effects and their impact on pluralism. Finally, the potential role of must-carry obligations could be explored as a solution for the promotion of diversity of content.

Protection of privacy as a prerequisite for the exercise of FOE

Many of the issues concerning the intersection between the rights to freedom of expression and privacy have already been explored by the UN Special Rapporteur in his 2015 June report on encryption and anonymity but still deserve to be mentioned.[22]

- **Mass surveillance and export controls:** Among the most significant challenges to the protection of freedom of expression online concerns the mass surveillance of online communications by certain states and related issues of data retention laws, which require various private actors to retain the communications records of their customers or users. Among other things, there is a concern that private companies are required to handover user data upon request from intelligence and law enforcement agencies in the absence of a court order. Moreover, they may be generally criminally liable for disclosing the fact that a request has been made and are prohibited from notifying the individuals concerns. In other words, both surveillance and data retention laws tend to offer insufficient safeguards for the protection of freedom of expression and privacy. This is compounded by the general lack of strong regulation of controls over the export of surveillance technology to countries which routinely flaunt human rights and target activists (see e.g. Brazil).

- **Weak data protection laws and policies:** Data collection is not just an issue in the context of mass surveillance however. The nature of communications online is that they are recorded and therefore traceable. They can enable the identification of individuals behind handles or devices. To the extent that the vast amount of data collected about individuals enables certain actors to predict their behaviour and choices, it also has an impact on the way in which people seek and receive information. In this sense, the compatibility of the privacy policies of search engines like Google or social media platforms like Facebook with international standards on data protection are relevant to freedom of expression. In practice, however, difficult issues of compliance with various

[22] A/HRC/29/32

- and sometimes competing - domestic laws on data protection arise. Overall, more can be done to strengthen data protection frameworks and enable individuals to claim their rights. The EU is taking the lead in this area with the recent adoption of the General Data Protection Regulation ('GDPR').

- **Promoting strong encryption standards and privacy by design**: While many Internet companies have privacy policies which significantly interfere with the right to personal data protection, they tend to adopt strong technical standards for the protection of the confidentiality of their customers' communications (e.g. end-to-end encryption). Technical standards are generally developed on a self-regulatory basis in fora such as the W3C, IETF and ISO. This is an area that governments should not seek to regulate as it would likely lead to weaker security standards (backdoors) and would facilitate covert surveillance. Nonetheless, it is important to continue advocating for strong encryption standards and promote privacy by design.

- **Anonymity**: underlying the concerns outlined above is the need for strong legal protection for anonymity. In the absence of a requirement to protect anonymity, companies should be encouraged to adopt anonymity-friendly policies. Encouragingly, Facebook recently relaxed its anonymity policy in certain limited circumstances. More needs to be done, however, as anonymity is essential for individuals to express themselves freely online.

Intersection between data protection and freedom of expression: 'the right to be forgotten'

An increasing matter of concern for freedom of expression in the digital sector concerns the growing role of data protection law as a means to restrict access to information, which is legitimately in the public domain under the banner of 'right to be forgotten' ('RTBF').[23] In this sense, whilst strong data protection laws are generally to be welcomed and promoted, it is vital that they include strong safeguards for the protection of freedom of expression.

ARTICLE 19 is especially concerned that following recent developments on the 'right to be forgotten' in the EU: (1) companies are increasingly *required* to determine whether information ought to remain in the public domain on private companies rather than judges; (2) there is no remedy for content providers to challenge a decision to erase links to their content. Indeed, one of the striking features of data protection law is that it protects the right to personal data protection by directly imposing obligations on both public and private actors. There is no such equivalent for freedom of expression; (3) a number of countries, including Russia and Brazil, are seeking to replicate the CJEU/EU position on the 'right to be forgotten' without any of the limited safeguards available under EU law.[24]

[23] See also, for instance, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland,* no. 931/13, 21 July 2015, which has been referred to the Grand Chamber. The case concerns the extent to which news organisations may be prevented from re-using and re-publishing public information under data protection law (here tax records, which under Finnish law, is public information).

[24] https://www.article19.org/resources.php/resource/38099/en/legal-analysis:-russia's-right-to-be-forgotten

3. Corporate responsibility and human rights

In this section, ARTICLE 19 merely identifies existing conceptual and normative work on corporate responsibility and human rights frameworks, including governmental, inter-governmental, civil society, corporate and multi-stakeholder efforts, as request by the Special Rapporteur.

International human rights framework

Under international human rights law, states are not only required to refrain from interfering with human rights but also to take positive measures to protect those rights. For instance, the European Court of Human Rights has found that, in certain circumstances, States had *positive obligations* under Article 10 to protect the right to freedom of expression, including from interferences by private actors.[25] The concept of positive obligations is also well-established under Article 8 (right to private life) jurisprudence.[26] Indeed, data protection law is an example of legislation that imposes obligations on both public and private actors to protect personal data, i.e. the right to privacy. The concept of positive obligations could therefore be explored in the context of legislation that would impose certain transparency requirements on companies, if deemed appropriate. Similarly, it could be used in relation to access to a remedy for violations of free expression rights by private actors, though further research would be needed to draw the contours of what such remedies or procedural safeguards might look like. Any such positive obligations should also comply with the requirements of necessity and proportionality.

UN work on Business and Human Rights:

The UN has done a considerable amount of work on Business and Human Rights. The landmark standard-setting document in this area is the **UN Guiding Principles on Business and Human Rights** (also known as "the Ruggie Principles").

The Ruggie Principles have generally been well received and led to the adoption of a number of corporate social responsibility ('CSR') policies in a large number of companies. In this sense, it has generally led to better understanding, protection and promotion of human rights in the business sector. At the same time, concerns remain that companies may adopt Ruggie Principle-compliant policies to protect their reputation, whilst engaging in practices which seriously threaten human rights (e.g. Hacking Team). Meanwhile, some UN Member States, including the UK, seek to promote the adoption of **National Action Plans** that seek to implement the Ruggie Principles at national level.

In addition to the above, a **UN working group** is currently seeking to establish a *treaty* that would be directly binding on corporate actors. Whilst such an initiative would have the advantage of being legal enforceable against companies, the adoption of such a treaty is likely to be slow at best and likely to draw resistance from private actors. Without companies' support, the treaty would be ineffective. At the same time, it is worth mentioning that similar treaties already exist in the form of Bilateral Investment Treaties (BITs), though they tend to advantage

[25] *Dink v Turkey*, nos. 2668/07, 6102/08, 30079/08, 14 September 2010.
[26] See e.g. *K.U. v. Finland*, no. 2872/02, §§ 45-49, ECHR 2008

corporate actors by, among other things, allowing them to opt for international arbitration mechanisms to resolve disputes with States. Nonetheless, it might be worth exploring how such treaties could be applied to the ICT sector and whether there would be a reasonable prospect of success that such treaties would achieve a high standard of protection for the right to freedom of expression.

Finally, a number of UN fora and working groups deserve mention. The **UN Forum on Business & Human Rights** is "a space for representatives and practitioners from civil society, business, government, international organizations and affected stakeholders to take stock of challenges and discuss ways to move forward on putting into practice the Guiding Principles on Business and Human Rights – a global standard for preventing and addressing adverse impacts on human rights linked to business activity". Furthermore, the **Working Group on Business & Human Rights** seeks to address the issue of human rights and transnational corporations and other business enterprises. In particular, it seeks to promote the Ruggie Principles and coordinates initiatives between various stakeholders on business & human rights. As such it guides the work of the UN Forum on Human Rights and Business.

Government-led & multistakeholder self-regulatory initiatives

The UN is not the only organisation working on business and human rights. The **EU** recently produced an ICT Sector Guide to the Implementation of the UN Guiding Principles on Business and Human Rights.[27] The report has generally been well-received but questions remain as to the implementation of its recommendations.

Meanwhile, a number of multi-stakeholder initiatives seek to promote the adoption of strong free expression and privacy standards by Internet companies and telecommunications service providers. These include the **Global Network Initiative**[28] and the **Telecommunications Industry Dialogue**.[29] Whilst these self-regulatory initiatives have generally had a positive impact on the behaviour of private actors in the ICT sector, these efforts are sometimes hampered by companies' inability to disclose information publicly for legal or policy reasons, raising issues of transparency and company accountability.[30] Moreover, given the purely self-regulatory nature of these initiatives, their ultimate effectiveness may be questioned: in particular, only those companies which sign on to these initiatives or principles undertake to follow what are ultimately only best practices rather than binding requirements.

A more recent initiative is the **Ranking Digital Rights Corporate Accountability Index** ('RDR'). RDR is based on publicly available information and has shone light on the lack of transparency surrounding companies' content restrictions based on their own terms and conditions. RDR can be seen as complementary to initiatives such as GNI. Whilst GNI may be able to achieve positive outcomes by working with companies on individual cases requiring the utmost confidentiality, it would usually not be in a position to publicise such successes. By contrast, RDR can hold companies to account by reference to what companies say they do as against the RDR indicators

[27] http://www.shiftproject.org/publication/european-commission-ict-sector-guide
[28] https://www.globalnetworkinitiative.org/
[29] http://www.telecomindustrydialogue.org/about/
[30] http://bhr.stern.nyu.edu/blogs/why-were-leaving-the-gni

but it cannot account for the positive work done by companies, which remains confidential for security reasons.

Finally, also worth noting is **EFF**'s recent onlinecensorship.org initiative,[31] which allows individuals to report cases where their content has been removed or account suspended on the basis of Terms of Service.

Conclusion

The role of private actors in the digital space raises many legal and policy issues. In our view, the UN Special mandate on freedom of expression should begin his work in this area by focusing on Internet companies (social media platforms, search engines) and telecommunications operators in separate thematic reports. Each report should highlight the key legal and policy issues that arise for freedom of expression in respect of each category of Internet intermediary, with recommendations for both states and companies.

[31] https://onlinecensorship.org/

ANNEX A - Outline of key actors and concerns in Brazil

1. Actors in the ICT sector whose activities implicate the freedom of opinion and expression

Search engines and data processors

The main engines and data processors in Brazil are disclosed by the top 10 used websites and by the top downloaded apps in the country. They are Google (with Youtube), Facebook, Bing and Live.com (with Microsoft Mail, OneDrive and Office), Yahoo, Twitter, two news websites that usually have account systems (UOL and Globo.com) and Mercado Livre, an e-commerce website. The most significant apps side include WhatsApp, Instagram, Facebook, Youtube, Twitter, Skype, Netflix, Waze, Snapchat, Spotify, Linkedin and often internet banking apps. It is safe to say that all of those process data in Brazil at least at a minimum level - all of which may have an impact on freedom of expression.

It is also important to point out that a huge amount of Brazil's traffic is heavily concentrated around these actors, mostly Facebook and Google, and is often shaped by behavioral data that directs users to its "relevant" interests. Companies direct users to what they believe are their interests. This in turn may be an issue freedom of expression and access to information as individuals tend to prefer receiving information that they agree with instead of information that might go against their views and beliefs. That is exactly what social media and search engines tend to do when they are showing relevant content to their users, which is probably similar to its closest friends and so on. This undermines our society's ability to engage in debate and of interacting with people and content that might oppose them. This is especially problematic when we think that social media communication and discussions are usually straightforward, synthetical and aim to polemicize.

Social media

A 2014 research showed that Facebook was still the most accessed social media in Brazil with 61,74%, against 28,97% from YouTube.[32] Twitter comes right after, followed by Yahoo Answers Brazil, Instagram, Badoo and Ask.fm. Brazil is the second world's top user of social media:[33] in 2012, Brazil became the second country with the largest number of people accessing Twitter, in 2013 Brazil was the second biggest Facebook user and in 2014 the second on Youtube.

If social media gives voice for low income people, on the other hand, it brings new forms of censorship. A recent case illustrates how Brazilian culture clashed with Facebook's policies. In 2015, the Ministry of Culture of Brazil decided to legally sue Facebook after a picture of a couple of *botocudos* Indians was censored by the social network. The photo, taken in 1909 by Walter Garbe, was posted on institutional ministry page and removed with a warning that, by the terms and conditions, the photo had been blocked.

---

[32] http://economia.uol.com.br/noticias/valor-online/2014/07/28/facebook-e-lider-mas-perde-participacao-entre-redes-sociais-no-brasil.htm

[33] http://www.tecmundo.com.br/brasil/63192-brasil-segundo-maior-pais-acessar-redes-sociais.htm

Free Basics in Brazil

Brazil is alsoone of the targets of Facebook's Internet.org, now called Free Basics, menacing the Marco Civil's Net Neutrality provisions. Its implementation is imminent even with civil society's pressure against the government to clearly state that the project would break the law. It is also directly related to the regulations implementing the Marco Civil, which is open to public consultation again and very close to its end. However, the government signaled that eventual "exceptions" related to economical issues and business models would have to be assessed by Anatel, the telecommunications regulator in Brazil. Unfortunately, Anatel is historically aligned with these companies.

News media

Several major news websites from newspapers in Brazil, such as Folha de São Paulo, Valor Econômico and Estado de São Paulo, have been adopting content blocking to promote the paid signature of its services. However, few other websites and tools are widespread in order to avoid the blocking.

Internet Service Providers (ISPs)

As a matter principle, providers are not liable for the actions of their users under Brazilian laws. However some exceptions have been included in the Marco Civil. Warranties and exceptions to the liability of internet service providers are set mainly in Art. 19 of the Marco Civil. In any event, providers may be held liable for failure to comply with a court order ordering the removal of specific content. Moreover, they are required to keep data logs for six months and may be asked to keep it for longer if determined by a court.

Telecommunications providers

Before the adoption of the Marco Civil da Internet, and for a long time, net neutrality has dominated public policy debates as a result of heavy lobbying by telecommunications companies. At present, there there is still a lack of regulation over the technical issues and essential requirements for the provision of services and applications in the net neutrality debate. In particular, there is no definition of what it means damage to the user; definitions of agreements by level of service. Moreover, zero rating and discriminatory blocking issues remain unsettled. There is pressure from telecommunications providers in order to allow zero-rating practices, which are said to be merely economical issues.

Surveillance and cybersecurity firms

Brazilian law enforcement and investigation bodies created a large demand of technology that was rapidly fulfilled, creating a national market for digital tapping technologies. However, there is currently no regulation of surveillance technology exports. The increasing need for tapping by the police and by the Brazilian Public Ministry has caught the attention of neighboring countries. Companies like *Dígitro*, from the state of Santa Catarina, started exporting Brazilian technology similar to the software Guardian. This was made public in Uruguay, where the government refused to provide information regarding the purchase of the tool.[34] In addition, the

[34] http://www.dw.com/en/surveillance-and-human-rights-in-the-digital-age/a-18399282

technology has been used by the Uruguayan police without the existence of a clear regulation of this practice in that country.

2. Legal and policy issues concerning the ICT sector

Regulation of content

Companies and services on the Brazilian web tend to reproduce the Terms of Service of the biggest actors in the ICTs sector, even though not every ICT actor has ostensibly the capacity to rapidly react to every kind of content. Marco Civil, however, has mechanisms to enforce these kinds of reactions from possible victims of actions that are harmful to others, such as revenge porn, as it is stated on the Art. 21 of the Law and classified as "intimacy violation". This article provides for an urgent procedure to deal with these kinds of violations.

Acquiescence of corporate actors with government mandates or requests to take downcontent or services

This matter is strictly regulated by Marco Civil, since there is a process created to allow that most of the requests pass through judicial scrutiny, unless, as stated in Art. 21, the content is admittedly sensistive and violates one's intimacy. Despite that, Art. 19 of the Law describes the process. Content centralizers and consequently those that receive most requests, such as Facebook, Google and Twitter, usually fight back when they believe that the defence of a case will be good to their image if it reflects its policies, even though these cases are more concentrated on data requests.

Cooperating with government surveillance

Internet services, such as Social Media and Search Engines, usually affirm that they are not comfortable cooperating with government surveillance. This started happening since the Snowden leaks, that revealed that some of them used to cooperate with the NSA. However, after that, mostly because of the effects on their image related to user's security, they have been publicly stating that they stand by users to protect their data against the courts and some are even going towards the idea of privacy by design and encryption of communications by default in order to avoid having the data and being the target of government requests.There have been several court orders in Brazil related to the request of user information by the police and other law enforcement agencies. However, even knowing that Marco Civil regulates what can be demanded and how it can be demanded, a number of cases show that the authorities still try to abuse their powers by demanding more data than is strictly necessary. Cases show that companies are not complying with these practices and public declarations show that they have been standing behind the idea of cryptography to defend users data from governments.[35] This is in contrast to internet access providers, who have not resisted the authorities' abusive wiretapping demands.

The liability of intermediaries

Under Article 18 of the Marco Civil, intermediaries are not liable for users' content. It has exceptions as stated above and the law seems to be respected by the courts since its approval.

[35] http://tecnologia.ig.com.br/2015-12-01/whatsapp-e-facebook-defendem-uso-da-criptografia-para-seguranca-dos-usuarios.html

The security and privacy policies and technologies adopted by private actors, such as encryption
As mentioned above, private actors tend to avoid problems with courts by encrypting most of users communication data. This is well illustrated by the recent WhatsApp Messenger case. In late 2015, a court ordered that Whatsapp must be blocked after Facebook failed to comply with an order for data about three users for the purposes of an investigation into criminal gangs. Millions of people in the country were denied access to the service as a result. Facebook - main shareholder of WhatsApp since February 2014 – claimed that it could not comply with the order against WhatsApp because they are independent operations. WhatsApp also claimed afterwards that it did not have the requested data, because the exchanged messages are stored temporarily on servers, only until they are delivered to the recipient. Then, according to the company, they are deleted.[36] The service also claims that "WhatsApp communication between your phone and our server is encrypted".[37]

Moreover, these companies' storage of user data also seems effective since there have been no recent cases of massive leaks by the major actors, besides the notable case of Ashley Madison.

Net Neutrality
Net neutrality was the core issue in dispute over the Marco Civil debate and approval. Even though it is in the final text, internet access providers didn't want to be affected by it and lobbyied aggressively against the concept. However, there is still a lot of discussion related to it, since the interpretations of the text by the same companies and civil society seem to differ. The zero-rating issue also gained a heavy weight defender, since Facebook started pushing for its Internet.org/FreeBasics program.There is still discussion amongst it since the Marco Civil regulation has not been finished yet, and it is supposed to cover the issue. Civil society and other actors defend that the existing text is enough to display that traffic discrimination is abolished by Marco Civil, however the companies insist that the law does not, and should not, touch on "economic" regulatory issues. With this situation still on standby, FreeBasics is still not massively implemented, but advances, and the telecommunications companies still discriminate data in order to offer zero-rated mobile plans to WhatsApp, Facebook and Twitter to smartphone internet users.

3. **Relevant human rights principles or obligations of the private ICT sector**

The human rights section of the outcome document from NetMundial has the affirmative statement that "Human rights are universal as reflected in the Universal Declaration of Human Rights and that should underpin Internet governance principles." It also reaffirms that "Rights that people have offline must also be protected online, in accordance with international human rights legal obligations." With NetMundial, all stakeholders, including the private sector now endorsed it. It is also important to mention the rights of persons with disabilities to enjoy full access to online resources, which means that the private sector also has to create mechanisms to include this public. It is also stated that some areas of the private sector should engage more

[36] http://blogs.estadao.com.br/link/especialistas-questionam-bloqueio-do-whatsapp/
[37] https://www.whatsapp.com/faq/en/general/21864047

with other stakeholders involved with cybersecurity, for example, network operators and software developers.