**European Center for Not-for-Profit Law (ECNL) Stichting**

**Response to call for input from civil society organizations in connection with the report that is being prepared in accordance with Human Rights Council resolution 38/11 on “The promotion and protection of human rights in the context of peaceful protests”**

**Introduction**

The **European Center for Not-for-Profit Law (ECNL) Stichting** undertakes ongoing research to identify best practices, effects and impacts of legislation, factors of influence and other relevant information in the field of civil society law and related areas, such as the freedom of assembly. ECNL provides practical guidance and assistance to build domestic capacity for policy research and analysis related to an enabling environment for civil society.

In recent years ECNL has been monitoring, researching and gathering expertise on the impact of new technologies on fundamental rights which are at the center of its work that is, association, assembly and participation.

This Resolution 38/11 of the HRC, states that, “*although an assembly has generally been understood as a physical gathering of people, human rights protections, including for the rights to freedom of peaceful assembly, of expression and of association, may apply to analogous interactions taking place online*”, also, the UN Special Rapporteur on Assembly and Association, wrote in his recent report that “ *Technology serves both as a means to facilitate the exercise of the rights of assembly and association offline, and as virtual spaces where the rights themselves can be actively exercised*.” This follows on from what has been the approach of numerous documents both at the international[[1]](#footnote-1) but also regional level[[2]](#footnote-2), that the “*same right apply online as offline*”.

Based on its observations, ECNL would like to submit what follows:

***1) Laws, policies and programmes that have been developed to address the impact of new technologies, including information and communications, technology on human rights in the context of assemblies, including peaceful protests.***

A number of laws, policies and programmes of States have been developed that address the impact of new technologies on human rights. Some of these laws, policies and programmes have been positive, others less so.

**The Digital Divide**

In order to facilitate the exercise of the right to freedom of assembly online, States should work to close the so-called digital divide to provide ever increasing access to the Internet.

The 2030 Agenda for Sustainable Development includes a commitment to “significantly increase access to information and communications technology and strive to provide universal and affordable access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020” (target 9.C).[[3]](#footnote-3)

On a regional level, the European Court of Human Rights has stated in *obiter dicta;*

*“The Court cannot overlook the fact that in a number of Council of Europe and other international instruments the public-service value of the Internet and its importance for the enjoyment of a range of human rights has been recognised.* ***Internet access has increasingly been understood as a right****, and calls have been made to develop effective policies to attain universal access to the Internet and to overcome the “digital divide” (see paragraphs 23 to 25 above). The Court considers that these developments reflect the important role the Internet plays in people’s everyday lives.”[[4]](#footnote-4)*

Council of Europe documents also declare that “Member states should foster and encourage access for all to Internet communication and information services on a non-discriminatory basis at an affordable price”[[5]](#footnote-5) and highlight that fundamental nature of Internet access as a conduit for the exercise of human rights and freedoms – “Access to the Internet is an important means for you to exercise your rights and freedoms and to participate in democracy. You should therefore not be disconnected from the Internet against your will, except when it is decided by a court. In certain cases, contractual arrangements may also lead to discontinuation of service, but this should be a measure of last resort.”[[6]](#footnote-6)

At the level of the European Union, Internet access despite its transformative impact on the rights or citizens through allowing further participation, the focus is on the economic benefits and a systematization and completion of the Digital Single Market.[[7]](#footnote-7) Access to the Internet within the European Union is seen through the prism of economic rather that fundamental rights benefits. Furthermore, the policy focus has already seemed to turn to the “speed”[[8]](#footnote-8) at which the Internet is delivered rather than universal access to all parts of the European Union potentially leaving behind the issue of access, as such.[[9]](#footnote-9) This switch to concentrating on fast Internet as opposed to widely accessible Internet is not conducive to addressing the digital divide, *prima facie* potentially leaving already marginalized communities further behind.[[10]](#footnote-10)

At a national level, some (European Union Member) States have taken the leap to enshrine the right to the Internet in their domestic legal regimes, including Greece and Estonia.[[11]](#footnote-11)

The UN Special Rapporteur on Freedom of Assembly and Association has rightly stated in his most recent report on the topic that “In the digital age, the positive obligation to facilitate the exercise of the rights to freedom of peaceful assembly and of association includes efforts “to bridge the digital divides, including the gender digital divide, and to enhance the use of information and communications technology, in order to promote the full enjoyment of human rights for all”.

**Internet Intermediaries**

The obligation to protect requires that positive measures be taken to prevent actions by non-State actors, including businesses, that could unduly interfere with the rights to freedom of peaceful assembly and association.

An Internet intermediary,[[12]](#footnote-12) plays a critical role in the discussion of human rights exercised online in general but also the right to assembly in the specific, because it is the Internet intermediaries that are the go-betweens, the providers of the platform, that facilitate speech, protest, the assemblies whether they are wholly online or enabled by the Internet. Without intermediaries, online exercise of assemblies would not be possible. Nonetheless, these are private actors with private goals may sometimes benefit also from exemption from liability for the content of third parties, depending on the service provided even though they are the beneficiaries of the content they host.

In Europe, the exemption of liability of Internet intermediaries derives from the European Union E-Commerce Directive,[[13]](#footnote-13) however the European Court of Justice[[14]](#footnote-14) has repeatedly interpreted this to apply only to those intermediaries “which are of a mere technical, automatic and passive nature”.[[15]](#footnote-15)

As an example, Germany has adopted a law which holds Internet intermediaries liable for the content posted by its users, which would place them nearly on par with “publishers” of news and newspapers.[[16]](#footnote-16) It is understandable that intermediaries might like to err on the side of caution and take down any content which is even mildly controversial (not to mention content which may “offend, shock or disturb”[[17]](#footnote-17), as many protest actions and messages do) for the simple reasons of avoiding litigation, bad reputation or advertising contracts.[[18]](#footnote-18) These do not seem good enough reasons to give Internet intermediaries the role of “gatekeepers” of the right to freedom of assembly online and the decision-making power on the proportionality and necessity of the interference therewith. The dangers of this kind of constitutional “contracting-out”, to the understanding of the demands of pluralism, tolerance and broadmindedness appear too great.

Furthermore, as the recent report of the Special Rapporteur on the promotion and protection of the freedom of opinion and expression notes, States may not use internet companies as tools to limit expression that they themselves would be precluded from limiting under international human rights law.[[19]](#footnote-19)

**Self Regulation by Internet Intermediaries**

Self-regulation (by ISP’s) continues to be a prevalent form of regulation in the online environment.[[20]](#footnote-20)

Unsurprisingly, regulations and even self-regulations, do not appear to be in the interest of Internet intermediaries and social media platforms.[[21]](#footnote-21) In one way it may said that they are increasingly receiving this role by States and through the increasing litigation against them domestically, laws such as that in Germany (described above) but also through case-law at the European regional level such as *Delfi[[22]](#footnote-22)*, where the intermediary was ordered to vamp up their content management system in order to ensure that hateful speech was not appearing on its platform. In another way, they have taken these content management steps to appease their clients and the advertising market. This prevailing self-regulatory approach, has significant impact on the right to peaceful assembly as it strikes at the core of the message of the assembly or protest, in case the content is taken down or blocked by the ISP and left to their internal decision making schemes and adjudication.[[23]](#footnote-23)

At the level of the European Union, a recent positive example of self-regulation is EU Code of Conduct on Countering Illegal Hate Speech Online[[24]](#footnote-24) which reflects the Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law 2008/913/JHA.[[25]](#footnote-25) Through this Code the companies assigned to themselves, amongst others, the responsibility to remove “illegal hate speech”, put in place “Community Standards”, and review valid notifications within 24 hours.

States should therefore ensure that self-regulation by ISP’s does not lead to a censorship of content. This also applies to assemblies expressing views that may ‘offend, shock or disturb’ the State or any sector of the population[[26]](#footnote-26) for as long as they do not incite violence[[27]](#footnote-27) – and that these ISPs do not interfere with the message sought to be conveyed by the expression and/or assembly, through catch-all algorithms or unwarranted take down of content (discussed below). On the other hand, ISPs may also be held accountable where they do not react to or remove content or expression which amounts to an incitement to violence or hate speech.[[28]](#footnote-28)

**Other laws and policies**

There is also a plethora of laws, policies and programmes that have an impact on the exercise of human rights online, some of these have a positive impact, others have a negative impact. These range from privacy laws, cyber-crime laws[[29]](#footnote-29), anti-terrorism and anti-extremism laws, fake news laws, surveillance laws, administrative and criminal codes among others.

For instance, approximately, 52 nations including France, Russia, Denmark, Singapore, Egypt, and Brazil have laws against fake news. Some of these laws could serve to limit dissent and encourage support for controversial government policies, while others will serve to preserve truth in media.[[30]](#footnote-30) Indeed, it can be easily seen how the content of the message conveyed by an assembly, which is at the core of the right, could be affected. Futhermore, as illustrated by the Special Rapporteur on Freedom of Peaceful Assembly and Association, in his recent report[[31]](#footnote-31), cybercrime laws, anti-terrorism laws, surveillance laws (in addition to ‘fake news’ laws and freedom of assembly laws) could impinge on the right to exercise freedom of assembly online.

Media laws are also used to curtail the space within which assembly and association may take place online. In Egypt last year, the government adopted a law requiring anyone with a social media account that has more than 5,000 followers to register with the country’s State media regulator.[[32]](#footnote-32)In Uganda, in early 2019, a social media tax was introduced which saw the plummeting of social media use by millions of users.[[33]](#footnote-33)

There is also a growing number of national strategies and programmes on Artificial Intelligence (discussed below).

***2) Effective uses of such technologies as enablers of the exercise of human rights, including peaceful protests(e.g how new technologies have facilitated the organization of assemblies including peaceful protests)***

It is without a doubt that technologies are the enablers of the exercise of the right to assembly when used by authorities to facilitate the exercise of this freedom. Examples have shown that the Internet and social media can be a forum for protest itself[[34]](#footnote-34) or a mobiliser of protest. Recently, in the mass protests in Barcelona, a new application for phones was developed in order to move the protest to certain key areas of the city. [[35]](#footnote-35) In Russia, chat bots assist protesters when they are stopped or arrested by the police during and assembly by providing essential legal aid.[[36]](#footnote-36)

Where there is good faith, new technologies can also be used by authorities to communicate and exchange key information with organisers and participants.[[37]](#footnote-37)

As the Special Rapporteur on Freedom of Peaceful Assembly and Association further describes in his recent report,[[38]](#footnote-38) individuals can now use online spaces to assemble in a virtually connected civil society, as exemplified by the #MeToo movement in the United States and analogous online movements in France, the Arab world, India, Ukraine, and Mexico. Groups have used Twitter, Facebook, and Skype to assemble online across the world, from Jordan (where women’s rights activists mounted a digital campaign with the hashtag #Article308 to push for abolition of a controversial provision of the penal code),[[39]](#footnote-39) to Vietnam (where efforts to build a cable car in a UNESCO World Heritage Site were stalled by activists who created a Facebook page that amassed over 33,000 likes),[[40]](#footnote-40) to Singapore (where an activist was fined for organizing a Skype video call featuring a Hong Kong democracy campaigner without applying for a police permit).[[41]](#footnote-41)

***3) The human rights challenges posed by interferences with the availability and use of such technologies in the context of assemblies, including peaceful protests (e.g. through network disruptions, blocking of internet services or restrictions on secure and confidential information).***

**Network disruptions, blocking of internet services, filtering and shut-down**

In addition to government sponsored trolling and cyberattacks,[[42]](#footnote-42) the gravest restriction on the exercise of the right to assembly online is government filtering or shutting down of the Internet all together. Some states have already legislated for this possibility, without any benchmarks or safeguards in place such as the necessity of a declaration of state of emergency or the formal derogation from ICCPR of ECHR rights or even at least a court order.[[43]](#footnote-43) Other States simply do so without enacting legislation and do so at targeted times, in particular elections, when political discourse, organization of assemblies and the activity of political parties is at its peak,[[44]](#footnote-44) again, leaving internet users without remedy.

Filtering or shut-down of the Internet, should only be resorted to by a State within the remit of an officially proclaimed state of emergency, where the state has officially derogated from the responsibility to respect, protect and fulfil non-absolute rights in the ICCPR. Even in the case of a state of emergency where no derogation documents have been submitted, the freedom of assembly should continue to be protected, respected and fulfilled. This is because, more often than not it is the coming together of persons to demonstrate their views, or the assistance of human rights, political, or humanitarian associations that is crucial in restoration of peace and order in times of emergency.

As an example, in Turkey, in November 2016, the monitoring network TurkeyBlocks detected restrictions on access to multiple social media services,[[45]](#footnote-45) Facebook, Twitter, YouTube and WhatsApp allegedly in response to detention of multiple leaders of the opposition party HDP, accompanied by raids of their headquarters in Ankara. The government confirmed that this was part of the “security measures” it had put in place. The measures apparently in fear of social media backlash and mobilisation for protest through social media in response to the jailing of the opposition. In the run up to the early presidential elections in Kazakhstan, 2019, the OSCE ODIHR long term observation mission found that, “legally prescribed sanctions,[[46]](#footnote-46) blocking of specific websites, and limited access to social networks on a daily basis, led to self-censorship and limited online political discourse.”[[47]](#footnote-47) Most recently, during the protests against austerity measures in Ecuador, protesters experienced disruption in mobile and telephony signals.[[48]](#footnote-48) However, in January 2019, in Zimbabwe, a Court ruled that the government had exceeded its powers by ordering an internet blackout during civilian protests, and instructed mobile operators to immediately and unconditionally resume all services.[[49]](#footnote-49)

States should therefore refrain from use of shut-down, kill switches or filtering as these amount to a dis-proportionate limitation on the right to freedom of assembly online. It has been said in the context of the freedom of expression[[50]](#footnote-50) and would equally apply to the freedom of assembly.[[51]](#footnote-51) Bearing in mind that the more general the ban, the less likely it is to really respond to a pressing social need[[52]](#footnote-52) for it to be introduced, even for the purposes of national security. It is considered that such a drastic measure would only be available to States under the extremely limited circumstances permitted based on official derogation, and here, the livelihood of the entire country (as opposed to one political group in power) would have to be at stake.

**Take-down and removal by ISPs and Algorithms**

The right to assemble online and the right to mobilise peaceful assembly through online means is to a degree also controlled by ISPs.

In the case of online assemblies, algorithms or a group of persons working for the Internet intermediary are the assessors of the content, -the so-called “human factor”[[53]](#footnote-53) as too is the ability to attract advertising.[[54]](#footnote-54) This combination of factors makes it difficult to see *prima* facie whether it secures the protection, respect and fulfilment of the right to freedom of assembly to the extent that we can say with ease: “same rights online as offline”. Studies and case-examples have already shown that the goals of commercial operators that are the Internet intermediaries, do not always coincide with the goals of activists using, for instance, social networks for expression, assembly and association.[[55]](#footnote-55)

What is more, the technology is ever-expanding, meaning that algorithms may now be used to “predict” when a protest will become violent, through the content of Twitter posts, uploaded by protesters[[56]](#footnote-56) potentially giving fair warning to authorities, but also instilling prejudice in the reaction to protests, by premature dispersal or heavy-handed reaction to single isolated incidents of violence.

**The Right to Privacy**

The same technology that can and is being used for the facilitation of assemblies, can also be used to persecute persons taking part in assemblies and protest actions. Such technologies include police video recordings[[57]](#footnote-57) and facial recognition tools, surveillance of the Internet portals and social media sites used by activists and identification of a person’s whereabouts through location tracking (to establish attendance at a demonstration or rally). It is only recently that some social media websites have started banning surveillance and tools capable of tracking protesters[[58]](#footnote-58) and some national or state level legislatures have begun to ban facial recognition tools in particular.[[59]](#footnote-59) The pertinent question here is therefore what kind of safeguards are needed to protect the fundamental rights of protesters to the exercise of freedom of assembly but also the right to privacy and family life.[[60]](#footnote-60) The problem in this case is rather that, an assembly is held in a public place and implies some form of public exposure. A reasonable expectation of privacy nonetheless does exist in this context, however it is not conclusive.[[61]](#footnote-61) Protesters are entitled to some level of privacy and anonymity at a protest (face masks, for instance have been to date an acceptable form of expression and may serve to preserve privacy of discriminated groups, in particularly oppressive regimes). Therefore, appearing at an assembly does not automatically mean for instance agreement to facial recognition tools being used to record presence, or to the recording of private conversations between protesters during the course of the assembly. Appearing in public, in other words, does not strip an individual of the entirety of right to privacy.

Yet, data collected on protesters by the authorities, been shown to be shared between agencies of the authorities. For example, recently in Manchester, United Kingdom, concerns have been raised about what appear to be “discriminatory” actions by a police force that has admitted passing information about disabled protesters to the Department for Work and Pensions (DWP). Police said that this information was passed to DWP so the department could “assess and then investigate and determine if criminal offences had occurred in relation to benefit claims”.[[62]](#footnote-62)

 ***The human rights challenges posed by the new technologies, including information and communications technology, in the context of assemblies, including peaceful protests (surveillance and monitoring tools by the authorities, including biometrics-based recognition technology to identify protestors).***

The use and abuse of surveillance tools has been an area of growing concern for human rights, since the technologies themselves appeared. Already in 2009, the UN Special Rapporteur on the Promotion and Protection of Fundamental Rights while Countering Terrorism, warned, in his 2009 report “The rights to freedom of association and assembly are also threatened by the use of surveillance. These freedoms often require private meetings and communications to allow people to organize in the face of Governments or other powerful actors. Expanded surveillance powers have sometimes led to a “function creep”, when police or intelligence agencies have labelled other groups as terrorists in order to allow the use of surveillance powers which were given only for the fight against terrorism.”[[63]](#footnote-63)

Ten years later, in May 2019, the UN Special Rapporteur on Freedom of Opinion and Expression, issued a special Report on “Surveillance and Human Rights”,[[64]](#footnote-64) which while focusses on the individual freedom of expression, calls for a moratorium on the sale of surveillance tools to States, until such time as adequate legal safeguards can be put in place. The Special Rapporteur expresses grave concerns at the uncontrolled nature of the surveillance tools industry, and granted that the freedom of expression in inextricably linked with the right to peaceful assembly, a consideration should be given to this report, in the context of assemblies, in general, as States should refrain from using surveillance tools to track (or less still, persecute) persons taking part in assemblies and protest actions. Instead, the surveillance industry appears to be expanding, with some States such as Israel, relaxing the rules on cyber weapons exports, despite their known uses by authoritarian governments to supress dissent [[65]](#footnote-65), regardless of this warning. Some States are also accelerating efforts to monitor social media to ‘predict’ protests, such as efforts to predict anti-Trump protests in the United States[[66]](#footnote-66), thus encroaching of the freedom of peaceful assembly, which includes protection of the right to ‘prepare and organise’ an assembly, under international law and creating a “chilling effect” and self-censorship on protesters.

There is growing attention to the potential impact of artificial intelligence (AI) on fundamental freedoms, including freedom of assembly, as discussed further below. Some governments, including China, Qatar, and Kuwait, have used AI systems to find and block disfavoured online content, including content supporting the #MeToo Movement or LGBTQIA rights.

Facial recognition technology is particularly worrisome to the right to freedom of peaceful assembly[[67]](#footnote-67) and the right to privacy (discussed above in the section on ‘the right to privacy’), as recently demonstrated by the protests in Hong Kong.[[68]](#footnote-68) This technology is being used not only to quash and silence dissent, but is also being used in other areas of decision making by the States concerning individuals. The biases contained in facial recognition technology are already well known and just how open to abuse the technology is, assisting State efforts to profile individuals, or indeed, groups of individuals[[69]](#footnote-69) such as the Uyghur Muslims in China.[[70]](#footnote-70)

While a number of countries are in the process of developing national strategies on AI, these strategies too rarely consider key human rights issues. At the local level, however, some municipalities, including New York City, Santa Clara, and Seattle, have adopted ordinances that include civic oversight when systems based on AI are deployed.[[71]](#footnote-71)

Furthermore, States authorities regularly request social media platforms for information on the online activity of persons and groups, for example, Facebook received 322,923 such requests in 2018 alone.[[72]](#footnote-72) In this regard, ISPs should also respect and protect the privacy of users and should not be compelled by the State to divulge information thereon without a court order. This in addition to the (as already described in the section on privacy above) surveillance systems which allow for the exchange of data between agencies of the State authorities.[[73]](#footnote-73)

1. Prior to this resolution: UN GA resolution of 27 June 2016 on the Promotion, protection and enjoyment of human rights on the Internet”, A/HRC/32/L.20, par 1, as well as; UN HRC Resolution 20.8 of 5 July 2012 and 26/13 of 26 June 2014 on the promotion and protection of human rights on the Internet, HRC resolutions 12/6 of 2 October 2009 on freedom of opinion and expression HRC resolution 28/16 of 24 March 2015 on the right to privacy in the digital age, GA resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014 on the right to privacy in the digital age and 70/184 of 22 December 2015 on the information and communications technologies for development, amongst others [↑](#footnote-ref-1)
2. Council of Europe: Recommendation of the Committee of Ministers to member States on Internet freedom of 13 April 2016, Recommendation CM/Rec(2016)5 and The Guidelines on Freedom of Association and Assembly of the African Commission on Human and Peoples’ Rights (African Commission) stipulate that “the right to assembly may be exercised in a number of ways, including through demonstrations, protests, meetings, processions, rallies, sit-ins, and funerals, through the use of online platforms, or in any other way people choose.” <https://www.achpr.org/legalinstruments/detail?id=5> [↑](#footnote-ref-2)
3. Transforming Our World: The 2030 Agenda for Sustainable Development, A/RES/70/1. [↑](#footnote-ref-3)
4. *Kalda v Estonia* (Application no. 17429/10) Judgment of the European Court of Human Rights, of 19 January 2016 par 52 [↑](#footnote-ref-4)
5. Principle 4: Removal of barriers to the participation of individuals in the information society, Declaration on freedom of communication on the Internet adopted on 28 May 2003, at the 840th meeting of the Ministers’ Deputies, the Committee of Ministers of the Council of Europe. [↑](#footnote-ref-5)
6. Recommendation [CM/Rec(2014)6](https://search.coe.int/cm/Pages/result_details.aspx?Reference=CM/Rec(2014)6) of the Committee of Ministers to member States on a Guide to human rights for Internet users [↑](#footnote-ref-6)
7. L Jasmontaite and Paul de Hert, “*Access to the Internet in the EU: A Policy Priority?* A Fundamental, a Human Right or a Concern for eGovernment?” in B Wagner, M C Ketteman, K Veith, “*Research Handbook on Human Rights and Digital Technology”*, Edward Elgar Publishing, 2019 page, 157 [↑](#footnote-ref-7)
8. Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)
*Official Journal L 108 , 24/04/2002 P. 0051 – 0077,* Par 8 which states as follows “[…] Connections to the public telephone network at a fixed location should be capable of supporting speech and data communications at rates sufficient for access to online services such as those provided via the public Internet. The **speed of Internet access** experienced by a given user may depend on a number of factors including the provider(s) of Internet connectivity as well as the given application for which a connection is being used. […] Currently available voice band modems typically offer a data rate of 56 kbit/s and employ automatic data rate adaptation to cater for variable line quality, with the result that the achieved data rate may be lower than 56 kbit/s. Flexibility is required on the one hand to allow Member States to take measures where necessary **to ensure that connections are capable of supporting such a data rate**, […] Member States should be able to require **the connection to be brought up to the level enjoyed by the majority of subscribers** so that it supports data rates sufficient for access to the Internet.” [↑](#footnote-ref-8)
9. L Jasmontaite and Paul de Hert, “Access to the Internet in the EU: A Policy Priority? A Fundamental, a Human Right or a Concern for eGovernment?” in B Wagner, M C Ketteman, K Veith, “Research Handbook on Human Rights and Digital Technology”, Edward Elgar Publishing, 2019 page, 162 [↑](#footnote-ref-9)
10. By 2017, the share of EU-28 households with Internet access had risen to 87 %, some 32 percentage points higher than in 2007 and broadband Internet access was used by 85 % of the households in the EU-28 in 2017, approximately double the share recorded in 2007 (42 %).

Source: Eurostat: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital\_economy\_and\_society\_statistics\_-\_households\_and\_individuals [↑](#footnote-ref-10)
11. Article 5A par 2 of the Constitution of Greece, states that *“2. All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19.*” In force 1975, as amended 2008. <https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf> (official English translation, last accessed May 13, 2019), and ; Paragraph 5 of the Telecommunication Act of Estonian Republic, Estonia Riikogu Daatu, # 56, 2000, which stipulates that Internet services must be universally available to all subscribers regardless of their geographical location and at a uniform price and article by C Woodard “*Estonia, where being wired is a Human Right*”, The Christian Science Monitor, 1 July 2003, <https://www.csmonitor.com/2003/0701/p07s01-woeu.html> last accessed 13 May, 2019 [↑](#footnote-ref-11)
12. Council of Europe Convention on Cybercrime Budapest, 23.XI.2001, ETS No 185, Article 1 (c) “service providers” as “(i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.” According to the Manila Principles on Intermediary Liability (developed within the IT sector) “Internet Intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to host, transmit and index content, products and services originated by third parties on the Internet or provide Internet based services to third parties”. <https://www.manilaprinciples.org/principles> (last visited: 16 February 2017) [↑](#footnote-ref-12)
13. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') *Official Journal L 178 , 17/07/2000 P. 0001 –* 0016 states in Recital (9) that “The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression” Whereas, Article (4) provides the actual exemption “Article 12

"Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; and

(c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.” [↑](#footnote-ref-13)
14. L’oreal SA and others v. Ebay International A.G. and others,Case C‑324/09, Judgment of the Court (Grand Chamber) of 12 July 2011, par 119 where the provider has confined itself “*to a merely technical and automatic processing of data*” and par 123 where the exemption is relevant as “*applying to the operator of an online marketplace where that operator has not played an active role allowing it to have knowledge or control of the data stored”* [↑](#footnote-ref-14)
15. Coche, E “Privatized enforcement and the right to freedom of expression in a world

confronted with terrorism propaganda online”. Internet Policy Review, 7(4), 2018, [↑](#footnote-ref-15)
16. Network Enforcement Act of Germany, Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken of 1 September 2017 (Federal Law Gazette I, p. 3352 ff. In force from 1 October 2017) [↑](#footnote-ref-16)
17. *Handyside v United Kingdom* Judgment EcHR (Application no. [5493/72](https://hudoc.echr.coe.int/eng#{%22appno%22:[%225493/72%22]})), Judgment of 7 September 1976, par 49 [↑](#footnote-ref-17)
18. https://www.theguardian.com/commentisfree/2019/oct/15/facebook-elizabeth-warren-regulation [↑](#footnote-ref-18)
19. A/74/48050, para. 29. [↑](#footnote-ref-19)
20. C Angelopoulos, et.al “*Study of Fundamental Rights Limitations for Online Enforcement through Self-regulation”* Institute for Information Law (IViR) Faculty of Law University of Amsterdam, 2015 [↑](#footnote-ref-20)
21. “*Actions by governments that restrict access to Facebook or our other products in their countries, or that otherwise impair our ability to sell advertising in their countries, could substantially harm our business and financial results”*. Facebook Inc., Annual Report Pursuant to Section 13 Or 15(D) of The Securities Exchange Act Of 1934, For the fiscal year ended December 31, 2018. [↑](#footnote-ref-21)
22. *Delfi AS v Estonia* Application No.64569/09, Judgment of the European Court of Human Rights of 16 June 2015 [↑](#footnote-ref-22)
23. <https://www.theverge.com/2019/9/17/20870827/facebook-supreme-court-mark-zuckerberg-content-moderation-charter> [↑](#footnote-ref-23)
24. Code of Conduct on Countering Illegal Hate Speech Online (2016), adopted by Twitter, Facebook, Microsoft and YouTube. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/countering-illegal-hate-speech-online\_en#theeucodeofconduct [↑](#footnote-ref-24)
25. https://eur-lex.europa.eu/legal-content/ [↑](#footnote-ref-25)
26. *Handyside v. The United Kingdom* (*The United Kingdom*, Application no. 5493/72, 7 December 1976, para. 49. [↑](#footnote-ref-26)
27. See *Delfi AS v. Estonia* Application No 64569/09, 16 June 2015; *Smajić v. Bosnia and Herzegovina*, Application No 48657/16, January 2018. [↑](#footnote-ref-27)
28. *Ibid. (Delfi AS v. Estonia* Application No 64569/09, 16 June 2015; *Smajić v. Bosnia and Herzegovina*, Application No 48657/16, January 2018.) [↑](#footnote-ref-28)
29. See for instance the case of Tanzania: https://slate.com/technology/2015/10/tanzania-s-terrible-cybercrimes-act-used-to-arrest-opposition-leaders.html [↑](#footnote-ref-29)
30. T J. Gordon, M Todorova “Future Studies and Counterfactual Analysis”, Springer, 2019 [↑](#footnote-ref-30)
31. A/HRC/41/41, 17 May 2019 paras 33-37 [↑](#footnote-ref-31)
32. https://www.bbc.com/news/world-middle-east-44858547 [↑](#footnote-ref-32)
33. https://www.theguardian.com/global-development/2019/feb/27/millions-of-ugandans-quit-internet-after-introduction-of-social-media-tax-free-speech [↑](#footnote-ref-33)
34. https://gizmodo.com/apple-and-blizzard-slammed-over-china-censorship-by-top-1839172675 [↑](#footnote-ref-34)
35. https://techcrunch.com/2019/10/17/catalan-separatists-have-tooled-up-with-a-decentralized-app-for-civil-disobedience/ [↑](#footnote-ref-35)
36. https://globalvoices.org/2018/09/25/chat-bot-lets-russians-detained-at-protests-request-legal-assistance/ [↑](#footnote-ref-36)
37. For example OSCE ODIHR Report Monitoring of Freedom of Peaceful Assembly in Selected OSCE Participating States (May 2017–June 2018) ; Par 187 states that in Quebec, Canada, *“Police services from the so-called Integrated Security Unit (formed for the purposes of the facilitation of the G7 Summit) shared information on* ***social media*** *before the planned protests and formed partnerships with conventional media to ensure that relevant messages could be conveyed*” and par 346 stating that “ *The Integrated Security Unit in Canada supported the work of journalists by holding information and technical briefings, establishing special telephone lines and* ***social media accounts*** *to facilitate media inquiries and granting accreditation to provide access to designated Summit sites”* https://www.osce.org/odihr/430793?download=true [↑](#footnote-ref-37)
38. A/HRC/41/41, 17 May 2019 para. 23 [↑](#footnote-ref-38)
39. Freedom House, Freedom on the Net 2018, <https://freedomhouse.org/report/freedom-net/2018/jordan>. [↑](#footnote-ref-39)
40. Freedom House, Freedom on the Net 2018, <https://freedomhouse.org/report/freedom-net/2018/vietnam>. [↑](#footnote-ref-40)
41. “Singaporean fined over Skype forum with Hong Kong activist,” The Jakarta Post, 21 February 2019, <https://www.thejakartapost.com/seasia/2019/02/21/singaporean-fined-over-skype-forum-with-hong-kong-activist.html>. [↑](#footnote-ref-41)
42. See: Report of the Special Rapporteur on the rights to freedom of assembly and of association, Advanced Edited Version, Human Rights Council 44th session 24 June- 12 July 2019 Agenda Item 3. Report of 17 May, 2019 A/HRC/41/41, par 43-48 [↑](#footnote-ref-42)
43. The Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai, Addendum Mission to Kazakhstan, 16 June 2015, A/HRC/29/25/Add2, par 57 states: “*For the same reasons, the Special Rapporteur is concerned at amendments to the Law on Communications, adopted in April 2014, which grants the Prosecutor’s Office the power to suspend the operation of a network, including the Internet, without a court order”.* [↑](#footnote-ref-43)
44. “In almost half of the countries where Internet freedom declined, the reductions were related to elections”. Source: Freedom House: Freedom on the Net, Report of 2018 https://freedomhouse.org/sites/default/files/FOTN\_2018\_Final%20Booklet\_11\_1\_2018.pdf [↑](#footnote-ref-44)
45. Editorial, *“Facebook, Twitter, YouTube and WhatApp shutdown in Turkey”* <https://turkeyblocks.org/2016/11/04/social-media-shutdown-turkey/> 4 November, 2016 [↑](#footnote-ref-45)
46. Defamation remains a criminal offence in Kazakhstan. [↑](#footnote-ref-46)
47. OSCE ODIHR International Election Observation Mission, Republic of Kazakhstan, Early Presidential Election, 9 June 2019 Statement of Preliminary Findings and Conclusions, page 2. [↑](#footnote-ref-47)
48. https://www.accessnow.org/disrupciones-de-internet-en-ecuador-como-ocurrieron-y-como-eludirlas/ [↑](#footnote-ref-48)
49. https://www.reuters.com/article/us-zimbabwe-politics/zimbabwe-court-says-internet-shutdown-during-protests-was-illegal-idUSKCN1PF11M [↑](#footnote-ref-49)
50. Please see: Joint Declaration on Freedom of Expression and responses to conflict situations
The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, of 4 May, 2015, in which provision 4 c. states as follows: “*Filtering of content on the Internet, using communications ‘kill switches’ (i.e. shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures which can never be justified under human rights law”* [↑](#footnote-ref-50)
51. The draft General Comment Number 37 on Article 21 of the ICCPR states in draft par 38 *“In the digital age, many of these associated activities happen online or rely upon digital services. Such activities are also protected under article 21. States parties should, for example, refrain from unduly blocking Internet connectivity in relation to demonstrations. The same applies to geo-targeted or technology-specific interference or hindering of connectivity.*” [↑](#footnote-ref-51)
52. Van Dijk, Van Hoof , Van Rijn et.al.,(eds) *“Theory and Practice of the European Convention on Human Rights”* Fourth Edition, Intersentia, 2006, page 824 and C Grabenwarter, “European Convention on Human Rights Commentary”, C.H Beck, Hart, Nomos, Helbing Lichtenhan Verlag, pg 823 [↑](#footnote-ref-52)
53. Ibid [↑](#footnote-ref-53)
54. S Hill,. “Empire and the megamachine: comparing two controversies over social media content” *Internet Policy Review*, *8*(1), 2019 [↑](#footnote-ref-54)
55. W L Youmans, J C York, *“Social Media and the Activist Toolkit: User Agreements, Corporate Interests and the Information Infrastructure of Modern Social Movements”*, Journal of Communication 62(2012) at 316 “Firms focus primarily on increasing users, avoiding negative public relations, seeking access to new markets, and protecting other larger classes of non-activist users. These privatized goals of platform owners and developers can conflict with their use as tools for civil society and popular mobilization.” [↑](#footnote-ref-55)
56. <https://www.rt.com/news/428277-algorithm-protest-twitter-violent/> [↑](#footnote-ref-56)
57. An example of arrests based on police filming of protesters can be seen in the case of the Kurdish protests in Turkey in 2008 (where amongst others, minors were filmed throwing rocks at police and arrested) which have been decided on by the ECtHR recently. Please see *Gülcü v Turkey,*  Application No 17526/10, Judgment of 19 January 2016, para 6: “According to a report prepared by four police officers on 21 July 2008 following the examination of video footage of the demonstration recorded by the police…” [↑](#footnote-ref-57)
58. M Moon, *“Facebook bans known protest-tracking tool for law enforcement”* 19 January, 2017 <https://www.engadget.com/2017/01/19/facebook-bans-known-protest-tracking-tool/> and BBC Technology *“Facebook data can no longer be used by developers to create surveillance tools, the social network has said.”* March 14, 2017 <http://www.bbc.com/news/technology-39266003> and Reuters *“Facebook bans developers from using its data like location for surveillance and tracking tools*” 14 March 2017, <http://tech.firstpost.com/news-analysis/facebook-bans-developers-from-using-its-data-like-location-for-surveillance-and-tracking-tools-366745.html> all articles last accessed: 21 March, 2017 [↑](#footnote-ref-58)
59. M O’Brian and J Har *“San Francisco May Become the First City to Ban The Use of Facial Recognition Technology”* , 13 May, 2019 <http://time.com/5588098/san-francisco-facial-recognition-technology-ban/> and <https://www.economist.com/science-and-technology/2019/08/15/as-face-recognition-technology-spreads-so-do-ideas-for-subverting-it> [↑](#footnote-ref-59)
60. Article 8 ECHR, Article 17 ICCPR, Article 7 CFREU [↑](#footnote-ref-60)
61. *P.G and J.H. v. United Kingdo*m, (Application no. 44787/98), 25 September 2001, para. 57 [↑](#footnote-ref-61)
62. <https://www.disabilitynewsservice.com/concerns-grow-over-police-force-that-shares-info-on-protesters-with-dwp/> and https://www.theguardian.com/politics/2019/aug/07/innocent-people-caught-up-in-uk-welfare-state-surveillance-system [↑](#footnote-ref-62)
63. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin 28 December, 2009, U.N. A/HRC/13/37, par 36. [↑](#footnote-ref-63)
64. Report of the Special Rapporteur on Freedom of Opinion and Expression, A/HRC/41/35, 28 May, 2019 [↑](#footnote-ref-64)
65. https://www.channelnewsasia.com/news/business/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-11833272 [↑](#footnote-ref-65)
66. <https://www.vice.com/en_us/article/7x3g4x/pentagon-wants-to-predict-anti-trump-protests-using-social-media-surveillance> and <https://www.projectcensored.org/pentagon-aims-to-surveil-social-media-to-predict-anti-trump-protests/?doing_wp_cron=1571392462.3039820194244384765625> [↑](#footnote-ref-66)
67. https://qz.com/1721321/chinas-new-weapon-of-choice-is-facial-recognition-technology/ [↑](#footnote-ref-67)
68. https://www.dezeen.com/2019/10/09/facial-recognition-hong-kong-threat/ [↑](#footnote-ref-68)
69. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [↑](#footnote-ref-69)
70. https://www.forbes.com/sites/zakdoffman/2019/05/03/china-new-data-breach-exposes-facial-recognition-and-ethnicity-tracking-in-beijing/#bfd0e2534a75 [↑](#footnote-ref-70)
71. Zach Lampell & Lily Liu, “How can AI amplify civic freedoms?”, OpenGlobal Rights, 18 December 2018, *available at* <https://www.openglobalrights.org/how-can-AI-amplify-civic-freedoms/> [↑](#footnote-ref-71)
72. Please see: <https://transparency.facebook.com/government-data-requests/country/> , where information is disaggregated by country, nature of request, and for the US the legal basis for the request (subpoena, court order, etc.) [↑](#footnote-ref-72)
73. <https://www.disabilitynewsservice.com/concerns-grow-over-police-force-that-shares-info-on-protesters-with-dwp/> and <https://www.theguardian.com/politics/2019/aug/07/innocent-people-caught-up-in-uk-welfare-state-surveillance-system> [↑](#footnote-ref-73)