International Review of the Red Cross (2020), **102** (913), 181–198.
Digital technologies and war
doi:10.1017/S1816383121000047

IRRC

Freedom of assembly under attack: General and indiscriminate surveillance and interference with internet communications

Ilia Siatitsa*
Dr Ilia Siatitsa is a Programme Director and Legal Officer at Privacy International.

Abstract

Every day across the world, as people assemble, demonstrate and protest, their pictures, their messages, tweets and other personal information are amassed without adequate justification. Arguing that they do so in order to protect assemblies, governments deploy a wide array of measures, including facial recognition, fake mobile towers and internet shutdowns. These measures are primarily analyzed as interferences with the right to privacy and freedom of expression, but it is argued here that protest and other assembly surveillance should also be understood as an infringement of freedom of assembly. This is necessary not only to preserve the distinct nature of freedom of assembly that protects collective action, but also to allow for better regulation of surveillance and interference with internet communications during assemblies.

Keywords: freedom of assembly, protest, digital age, mass surveillance, interference, internet communications.

* Many thanks to Valentina Cadelo and Tomaso Falchetta for their input on the latest version of this article. The views expressed in this article reflect those of the author.

Introduction

The ability to assemble, dissent and protest peacefully is a key element in every society, democratic or otherwise.[1] In 2019 alone, there were more than 100 protests in numerous countries around the globe.[2] Digital technologies have to a certain degree enabled and facilitated these movements as they have been used to coordinate conversations, raise awareness, encourage participation and generate support.[3] At the same time, these same technologies and other means have been increasingly used to surveil and suppress such movements.

A peaceful assembly, including the right to protest,[4] is understood here as "a gathering of persons for a purpose such as expressing oneself, conveying a position on a particular issue or exchanging ideas".[5] The emphasis here is put on the collective exercise of an individual right irrespective of the means used to that end, whether social media is the main platform of expression or assembling physically.[6] The #MeToo movement is an example of the use of the online space to mobilize women's activities and whole populations on a global scale.[7] While the boundaries of when an online campaign is or becomes part of an assembly will depend on the particularities of each specific case, it is better to retain an inclusive approach at a definitional level.[8] Certain forms of expression online, including online protests, will also be protected by freedom of assembly, while others may primarily enjoy other human rights protections, such as freedom of expression.[9]

The close connection between surveillance and interference with internet communications and freedom of assembly has been highlighted in, *inter alia*, the 2020 report of the United Nations (UN) High Commissioner for Human Rights.

1 African Charter on Human and Peoples' Rights, 1520 UNTS 245, 27 June 1981 (ACHPR), Art. 11; American Convention on Human Rights, San José, 22 November 1969 (ACHR), Art. 15; International Covenant on Civil and Political Rights, 999 UNTS 171, 16 December 1966 (ICCPR), Art. 21; European Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by subsequent protocols), CETS No. 5, Rome, 4 November 1950 (ECHR), Art. 11; Universal Declaration of Human Rights, UNGA Res. 217A, 10 December 1948 (UDHR), Art. 20(1).

2 UN Office of the High Commissioner for Human Rights (UN Human Rights), "Press Briefing Note on Protests and Unrest around the World", 25 October 2019, available at: www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25204&LangID=E (all internet references were accessed in January 2021).

3 See, among many, Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, Yale University Press, New Haven, CT, 2017, p. 29.

4 "Protest" and "assembly" are used hereinafter almost interchangeably, though they do not have the exact same meaning. On freedom of assembly, see the sources cited in above note 1.

5 Human Rights Committee, General Comment No. 37, "Article 21: Right of Peaceful Assembly", UN Doc. CCPR/C/GC/37, 27 July 2020 (General Comment 37), para. 12.

6 While the physical gathering of persons used to be considered a key component of an assembly, in the digital age, there is an increasing consensus that assembly includes all forms of collective expression, even if occurring only in the digital/online space. See *ibid.*, para. 13; Clément Voule, *Rights to Freedom of Peaceful Assembly and of Association: Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*, UN Doc. A/HRC/41/41, 17 May 2019.

7 C. Voule, above note 6, para. 23.

8 See Michael Hamilton, "The Meaning and Scope of 'Assembly' in International Human Rights Law", *International and Comparative Law Quarterly*, Vol. 69, No. 3, 2020, p. 527.

9 See further below on the relationship between assembly and expression. See also *ibid.*, p. 528.

The report focused on the "impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests".[10] However, the accent has primarily been on how digital technologies are used to interfere with privacy and expression, which as a result negatively affects the right to assemble. There has been less analysis of direct interference with freedom of assembly itself.

It is argued here that there is further room to analyze how surveillance and other interferences with internet communications, carried out by governments, may directly infringe on people's freedom of peaceful assembly. This understanding not only enables us to preserve the distinct nature of freedom of assembly as a right that protects collective action, but also allows for better regulation of surveillance and internet communications interference in protests and other forms of assembly.[11]

In the following pages, the author provides a brief overview of common protest surveillance and interference with internet communications; outlines the close relationship between the right to privacy, freedom of expression and freedom of assembly; and provides a legal analysis on why some of those measures directly infringe on freedom of assembly.

Surveillance of peaceful assembly and interference with internet communications

People take over the streets and online spaces in order to assemble for a collective cause and to show solidarity, but also to criticize or protest against their government's policies and measures. State authorities have been responding with the deployment of technology-enabled surveillance, censorship and violent oppression. This article focuses on the first two.[12] Governments have been invoking their positive obligations to protect freedom of assembly, as well as their prerogative to limit protests in the name of public order and national security, as justifications to impose general and indiscriminate surveillance and interference with internet communications.[13]

10 See, among others, UN Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, including Peaceful Protests: Report of the United Nations High Commissioner for Human Rights*, UN Doc. A/HRC/44/24, 24 June 2020. But even earlier, see HRC Res. 15/21, "The Rights to Freedom of Peaceful Assembly and of Association", 30 September 2010; Maina Kiai and Jeff Vize, "Three Years after Tunisia: Thoughts and Perspectives on the Rights to Freedom of Assembly and Association from United Nations Special Rapporteur Maina Kiai", *Journal of Global Ethics*, Vol. 10, No. 1, 2014.

11 The present article does not cover violent assemblies or situations described by the International Committee of the Red Cross as "other situations of violence". Nor does it cover situations of armed conflict (whether international or non-international) to which international humanitarian law applies.

12 The use of force to respond to peaceful protests is not covered by this article.

13 See analysis below in the third part of this article. States have a positive obligation to take reasonable and appropriate measures to facilitate, protect and enable lawful demonstrations to proceed peacefully. See, *inter alia*, HRC Res. 44/20, "The Promotion and Protection of Human Rights in the Context of Peaceful Protests", 17 July 2020, para. 4; HRC Res. 25/38, "The Promotion and Protection of Human Rights in the Context of Peaceful Protests", 28 March 2014, para. 4; HRC Res. 24/5, "The Rights to Freedom of Peaceful Assembly and of Association", 26 September 2013, preambular para. 8. See also

General and indiscriminate surveillance of peaceful assembly

Digital technologies have significantly expanded the capabilities of authorities to surveil assemblies, including protests. Technologies are used to monitor the planning and organization of protests, to conduct surveillance during protests and even to continue surveillance after protests. This information is obtained in bulk and indiscriminately from public and private spaces,[14] irrespective of whether the persons involved are suspected of committing a crime.[15]

"Safe and confidential communications play a key role in the planning and holding of peaceful protests",[16] and yet through the availability of data and tools to process it, public authorities are increasingly collecting and analyzing the personal information of those planning or organizing protests, as well as of protesters themselves, just for the mere fact of planning or participating in an assembly. Many of these surveillance methods are invisible to protesters and can be used without the knowledge, consent or participation of those surveilled.

Each new protest has been a testament to the fact that the list of tools used to surveil protests is only becoming longer. Online, authorities may monitor social media communications and collect all information posted in relation to the protest indiscriminately.[17] This includes accessing and collecting information from both public and private digital spaces. They even infiltrate private online groups by creating false accounts to monitor conversations, and impersonate protest organizers in order to influence discussions and planning and even arrest dissenters.[18] They may further request that user data be provided by social media platforms and mobile phone applications that track movement, including information on who has carried out an internet search about a protest and on

Pieter van Dijk, Fried van Hoof, Arjen van Rijn and Leo Zwaak (eds), *Theory and Practice of the European Convention on Human Rights*, 4th ed., Intersentia, Antwerp, 2006, pp. 836–837.

14 General Comment 37 underlines that the right to privacy may be infringed upon even when an assembly takes place in public: see General Comment 37, above note 5, para. 62. A similar approach has been followed by the European Court of Human Rights (ECtHR), which has recognized in its jurisprudence that individuals have a reasonable expectation of privacy, despite the fact that their actions might have taken place in public. See, among others, ECtHR, *Uzun v. Germany*, Appl. No. 35623/05 (Fifth Section), 2 September 2010, paras 48–53.

15 In this context, the concept of "a person of interest" in protests has been expanding to include also "influencers" of protests – a term which has been borrowed from marketing and which includes persons whose voice seems to attract attention and mobilize people. See Lina Dencik, Arne Hintz and Zoe Carey, "Prediction, Pre-Emption and Limits to Dissent: Social Media and Big Data Uses for Policing Protests in the United Kingdom", *New Media & Society*, Vol. 20, No. 4, 2018, p. 1445.

16 UN Human Rights, above note 10, para. 24; Human Rights Council, *Joint Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association and the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions on the Proper Management of Assemblies*, UN Doc. A/HRC/31/66, 4 February 2016, para. 75.

17 On the extent of intelligence that can be acquired by collecting, analyzing and combining information, see Privacy International, "Social Media Intelligence", 23 October 2018, available at: https://privacyinternational.org/explainer/55/social-media-intelligence. See also L. Dencik, A. Hintz and Z. Carey, above note 15.

18 They may also spread false information by impersonating organizers, or even directly endanger protesters by using, *inter alia*, a technique called "boxing" whereby they maliciously publish personal information in order to encourage physical harm to organizers and protesters. UN Human Rights, above note 10, para. 27.

discussions between the organizers or the protesters.[19] Finally, they use hacking techniques[20] either to infiltrate the social media accounts of organizers and protesters in order to get their contacts and private messages, or to infiltrate their devices by tricking them into, for example, downloading malicious software that gives the authorities unhindered access to contacts, messages, pictures, videos and all other personal information on their phones.[21]

General and indiscriminate surveillance intensifies during protests. Fake mobile phone towers, facial recognition software and sentiment analysis software[22] – and more recently, the deployment of military-grade drones reportedly equipped with some of these tools – are all used in concert to ensure that if authorities so decide, not a single person remains anonymous during a protest. For instance, interference with protesters' mobile phones is facilitated by a variety of devices impersonating mobile phone traffic towers that intercept and track all mobile phones in their vicinity. Such devices typically collect International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) data that are unique to each mobile phone and SIM card – this is where they get one of their names, IMSI catchers.[23] However, they can do more than that: once connected, some devices also have the capability to block or intercept data transmitted and received by mobile phones, including the content of calls, text messages and websites visited.[24] They can potentially indiscriminately capture the mobile activity of thousands of people.

Authorities do not necessarily need to monitor mobile phones to capture everyone that was at an assembly. It is becoming a regular practice for authorities to make audio-visual recordings of assembly participants and often combine it with facial recognition technology, in real time (live facial recognition) or at a

19 Council of Europe, *Report by the Committee of Experts on Cross-Border Flow of Internet Traffic and Internet Freedom on Freedom of Assembly and Association on the Internet*, 10 December 2015.

20 Hacking is understood here as an act or series of acts which interfere with a system, causing it to act in a manner unintended or unforeseen by the manufacturer, user or owner of that system. Hacking can present grave and unique threats to privacy and security. For further information, see Privacy International, "Hacking Necessary Safeguards", 2018, available at: https://privacyinternational.org/demand/government-hacking-safeguards.

21 Access Now, "OHCHR Call for Input: The Promotion and Protection of Human Rights in the Context of Peaceful Protests", 2019, available at: www.accessnow.org/cms/assets/uploads/2020/06/OHCHR-Call-for-Input-Use-of-ICTs-in-Protests-October-15.pdf.

22 "Sentiment analysis" is used here to describe technology that aims to analyze various data, such as language, text and biometric data, in order to deduce the emotions of individuals. The term is also applied to "voice of the customer" materials such as reviews and survey responses.

23 IMSI catchers are known by a multitude of different names, including cell site simulators, cell grabbers, mobile device identifiers and man-in-the-middle devices, or by their specific brand names, such as StingRay or DRTbox. Jennifer Valentino-DeVries, "How 'Stingray' Devices Work", *Wall Street Journal*, 21 September 2011, available at: https://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/.

24 See Christopher Soghoian and Stephanie K. Pell, "Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy", *Harvard Journal of Law & Technology*, Vol. 28, No. 1, 2014; Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani and Edgar Weippl, "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers", *Proceedings of the 30th Annual Computer Security Applications Conference*, ACM Press, 2014, available at: http://dl.acm.org/citation.cfm?doid=2664243.2664272.

later point.[25] In the process, the authorities may indiscriminately collect images of everyone at a protest. The technology allows the comparison of the digital representation of a face captured in a digital image with other images in a database to determine whether a given passer-by was a person of interest.[26]

Additionally, some authorities have also been reported to be using military-grade surveillance equipment that could have been equipped with IMSI catchers, facial recognition cameras and other tools to monitor protestors.[27] Other reported technology deployed during assemblies or protests includes automated number plate recognition software, credit card monitoring, mobile phone extraction technology used during stop and search or remotely,[28] sentiment recognition software, body-worn cameras, data from telecommunications providers, and cloud analytics. These are all used in concert to surveil protests, along with a series of aggregation tools that can combine data from all these sources into one record.

Interference with internet communications in peaceful assemblies

On top of these surveillance measures, other tactics used by authorities to interfere with assemblies (before, during and after) include filtering of content related to protests; blocking of websites or platforms used to plan, organize and mobilize protests; closing accounts that belong to organizers, activists or journalists; and shutting down of the Internet and communications networks.

Internet shutdowns describe complete shutdowns of telecommunications and mobile services and internet traffic.[29] These are measures that intend to prevent or disrupt access to or dissemination of information online.[30] Shutdowns may affect an entire country or multiple countries, specific regions, towns, or

25 "Facial recognition technology" is used here to describe any system that has been built to analyze images of individuals for the purpose of identifying them. Such systems can scan distinct, specific facial features, such as face shape, to create a detailed biometric map of a face. UN Human Rights, above note 10, para. 30.

26 The images in a watch list may come from a range of sources and do not just include images of people suspected of criminal wrongdoing. Shaun Walker, "Face Recognition App Taking Russia by Storm May Bring End to Public Anonymity", *The Guardian*, 17 May 2016, available at: www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte. One company, called Clearview AI, trained its facial recognition system by using images found on people's social media profiles, without their consent. The Clearview AI facial recognition tool enabled police to link protesters to their respective social media accounts, making it harder for protesters to remain anonymous. Harmon Leon, "This Controversial Company Is Selling Your Social Media Photos to Law Enforcement", *The Observer*, 2 November 2020, available at: https://observer.com/2020/02/clearview-ai-social-media-photos-law-enforcement/.

27 Such technology combines data from mobile phones, license plate readers and real-time arrest records. In aggregate, this data makes it faster and easier for police to track and arrest suspects.

28 See Privacy International, "Mobile Phone Extraction", available at: https://privacyinternational.org/sites/default/files/2019-02/Explainers-MPE.pdf.

29 Also known as kill switches, network shutdowns or blackouts. See Access Now, "#KeepItOn: The Problem", available at: www.accessnow.org/keepiton/#problem. See also HRC Res. 32/13, "The Promotion, Protection and Enjoyment of Human Rights on the Internet", 1 July 2016.

30 David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HRC/35/22, 30 March 2017, para. 8, n. 6.

specific areas or neighbourhoods. Their duration varies from a couple of hours to months.[31] Internet shutdowns are becoming almost a common practice in times of public unrest and protests.[32] They "involve measures to intentionally prevent or disrupt access to or dissemination of information online in violation of human rights law".[33] At least sixty-five internet shutdowns reportedly took place during protests in 2019.[34]

Additionally, governments have been blocking, throttling or rendering effectively unusable entire websites, social platforms (such as Facebook and Twitter) and mobile applications (such as WhatsApp and Telegram).[35] Another more refined way of blocking and filtering information that the population receives is by blocking keywords or web pages.[36] Occasionally, authorities have been demanding that social platforms block specific users' accounts, claiming that they contain illegal content. This is a common practice targeting key figures of peaceful assemblies and associations in the making.

Other reported reactions include the removal of content related to protests and introducing new legislation that obliges intermediaries (telecommunications companies and service providers) to comply with such requests during protests or otherwise holding them accountable for these protests.[37] All these measures indicate that governments feel entitled to block digital means of communication in an era when they are often the only means of communication available to people.[38]

In addition to the above, governments are gradually introducing legal frameworks that criminalize uses of internet communications technologies, setting indirect barriers to the organization of and participation in assemblies. Increasingly, users of social media and other platforms used to organize protests have been targeted, arrested, prosecuted and even convicted exclusively for their online activities.[39] For instance, in certain States, a number of administrative and

31 Human Rights Committee, *Concluding Observations on the Fifth Periodic Report of Cameroon*, UN Doc. CCPR/C/CMR/CO/5, 30 November 2017, para. 41.
32 D. Kaye, above note 30, para. 8, n. 6, and para. 11. See also HRC Res. 32/13, above note 29, para. 10.
33 D. Kaye, above note 30, para. 8.
34 Access Now, *Targeted, Cut Off, and Left in the Dark: The #KeepItOn Report on Internet Shutdowns in 2019*, 2019, available at: www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf.
35 The UN High Commissioner for Human Rights recently reported that "[b]locking of entire websites of human rights organizations and political opposition parties has become increasingly common in many parts of the world, including in countries of the Middle East and North Africa region". UN Human Rights, above note 10, para. 23.
36 Sanja Kelly, Sarah Cook and Mai Truong (eds), *Freedom on the Net 2012: A Global Assessment of Internet and Digital Media*, Freedom House, 2012, pp. 164–176, available at: https://freedomhouse.org/sites/default/files/resources/FOTN%202012%20-%20Full%20Report_0.pdf.
37 Article 19, *The Right to Protest Principles: Background Paper*, 2016, p. 33, available at: www.article19.org/data/files/medialibrary/38581/Protest-Background-paper-Final-April-2016.pdf.
38 Disruption of protests through misinformation and attempts at disruptions of large-scale and public mobilization using the internet have been openly admitted by some States. Gayathry Venkiteswaran, *Freedom of Assembly and Association Online in India, Malaysia and Pakistan: Trends, Challenges and Recommendations*, APC IMPACT, 2016, p. 41, available at: www.apc.org/sites/default/files/FOAA_online_IndiaMalaysiaPakistan.pdf.
39 Victims of such arrests include journalists, human rights defenders (often the "faces" of protests) and other civilians – anyone that organizes, participates or reports on protests. Article 19, above note 37, pp. 33–34.

legislative measures have been taken to target non-violent involvement with protests,[40] with laws that include online acts expressly or implicitly. An example of the latter is the prohibition of the use of social media for the organization of protests in Brazil.[41] Implicitly, the inclusion of broad terms in some laws allows the authorities to target organizers for disturbing public order, incitement to disturb public order, terrorism, or threats to national security.[42] In parallel, there is also an increasing tendency to criminalize activities that could fall under the protection of freedom of assembly, such as certain forms of electronic civic disobedience.[43]

The right to privacy, freedom of expression and freedom of assembly

The impact of general and indiscriminate protest surveillance and interference with internet communications that facilitate the planning and organization of protests has been increasingly considered in recent years. As the UN High Commissioner for Human Rights has concluded, "the use of [new] technologies to surveil or crack down on protesters can lead to human rights violations, including infringement of the right to peaceful assembly".[44] This development is welcome, as often concerns regarding surveillance of assemblies and protests have been primarily identified as infringements of the right to privacy[45] or freedom of expression.[46]

The European Court of Human Rights (ECtHR) has found, for instance, that the retention of data of a peace movement activist who had never been convicted of any offence, concerning a peaceful protest, had been shown to be neither generally necessary nor necessary for the purposes of a particular inquiry. It was therefore a violation of his right to privacy.[47] Also, in a judgment of 25 June 2020, the Economic Community of West African States (ECOWAS) Community Court of Justice ruled that the September 2017 internet shutdown

40 *Ibid*., p. 33.
41 *Ibid*., p. 33.
42 For instance, the Spanish Criminal Code was amended to include a provision criminalizing distribution or public dissemination, through any means, of messages inciting the commission of any crime of disturbance of the peace. Nils Muižnieks, *Report by Nils Muižnieks, Commissioner for Human Rights of the Council of Europe, Following His Visit to Spain from 3 to 7 June 2013*, CommDH(2013)18, 2013, para. 130. See also Council of Europe, above note 19, p. 14.
43 Article 19, above note 37, pp. 25–26; Alex Comninos, *Freedom of Peaceful Assembly and Freedom of Association and the Internet*, APC Issue Paper, 2012, p. 7, available at: www.apc.org/sites/default/files/cyr_english_alex_comninos_pdf.pdf.
44 UN Human Rights, above note 10.
45 UDHR, Art. 12; ACHR, Art. 11; ICCPR, Art. 17; ECHR, Art. 8.
46 UDHR, Art. 19. See also ACHPR, Art. 9; ACHR, Art. 13; ICCPR, Art. 19; ECHR, Art. 10.
47 ECtHR, *Catt v. The United Kingdom*, Appl. No. 43514/15, Judgment (First Section), 24 January 2019. In another case, the Court stated that "Article 10 [freedom of expression] is to be regarded as a *lex generalis* in relation to Article 11 [freedom of assembly], *a lex specialis*, so that it is unnecessary to take it into consideration separately". ECtHR, *Ezelin v. France*, Appl. No. 11800/85, Judgment, 26 April 1991, para. 35.

ordered by the Togolese government during protests was illegal and an affront to the applicants' right to freedom of expression.[48]

Undoubtedly, the three rights of assembly, expression and privacy converge to a great degree when it comes to assemblies, and the lines between them inevitably blur. It is a long-standing principle of the administration of justice that a court often will not examine violations of closely linked rights once it has found a violation of one. This is not unique to freedom of assembly – the ECtHR, for example, has repeatedly declared that it was not necessary to examine whether there had been a violation under another right.[49] There are also cases where the Court found a violation of freedom of assembly and declared that it was unnecessary to examine whether there had been a violation of freedom of expression. Nonetheless, these cases relate to instances where protesters were arrested before, during or immediately after a protest or where the State banned a protest from taking place or unjustifiably restricted the organization of an assembly.[50]

At the UN level, freedom of assembly has been increasingly added next to privacy and freedom of expression when considering the impact of surveillance and interference with internet communications on human rights, precisely in order to underline specific concerns that are raised by the surveillance of peaceful assemblies.[51] There are also resolutions, reports and other documents focusing on freedom of assembly in the digital age that underline the impact of surveillance on assembly.[52]

However, it is maintained here that despite the increasing attention given to freedom of assembly, international and regional bodies (judicial, quasi-judicial, political and independent experts) have not fully explored and captured the full extent to which general and indiscriminate surveillance and interference with internet communications – before, during and after – directly interfere with and potentially infringe on freedom of assembly.

For instance, when examining the impact of assembly surveillance, the UN Human Rights Committee's General Comment 37 focuses on the right to privacy. It states:

> The mere fact that a particular assembly takes place in public *does not mean that participants' privacy cannot be violated*. The right to privacy may be infringed, for example, by facial recognition and other technologies that can identify individual participants in a crowd.[53]

48 Community Court of Justice of ECOWAS, *Amnesty International Togo and Others v. The Togolese Republic*, Judgment, 25 June 2020. Similarly, in December 2012, the ECtHR ruled unanimously that the blanket blocking of entire platforms, in this case the hosting service Google Sites, violates freedom of expression provisions in Article 10 of the ECHR. ECtHR, *Ahmet Yıldırım v. Turkey*, Appl. No. 3111/10, Judgment (Second Section), 18 December 2012, paras 66–68.

49 ECtHR, *Ezelin*, above note 47.

50 See, among others, ECtHR, *Öllinger v. Austria*, Appl. No. 76900/01, Judgment (First Section), 29 June 2006, paras 52–53.

51 See, *inter alia*, HRC Res. 42/15, "The Right to Privacy in the Digital Age", 26 September 2019, preambular para. 30.

52 See, *inter alia*, General Comment 37, above note 5; UNGA Res. 73/179, "The Right to Privacy in the Digital Age", 17 December 2018; HRC Res. 44/20, above note 13; C. Voule, above note 6; UN Human Rights, above note 10.

53 General Comment 37, above note 5, para. 62 (emphasis added).

The in-depth consideration of the impact of surveillance and interference with internet communications on assemblies is key both for ensuring that the distinct nature of freedom of assembly is preserved, and for the better regulation, implementation and enforcement of surveillance measures around protests.

Freedom of assembly incorporates the right of every individual to hold opinions without interference, an element that also describes freedom of expression.[54] However, assembly also encompasses a social component, the sense of acting to pursue a common interest or purpose. It protects the collective nature of protests brought together by a common aim.[55] When freedom of assembly is attacked, the societal network that is united under the specific aim is damaged.[56] As such, freedom of assembly helps to develop and strengthen democratic societies.[57] In equal measure, while surveillance may be primarily an interference with the right to privacy, such interference often provides a gateway to violations of other rights, including freedom of assembly.[58] A violation of the right to privacy, more often than not, is not an end in itself; it rather offers the means for infringing on other rights.[59] In that sense, it often becomes the enabler for infringing on, among others, freedom of assembly.

Mass surveillance and interference with internet communications as an infringement of freedom of assembly

Direct interference with freedom of assembly

Many of the surveillance and internet communications interference measures referred to above can be used to directly interfere with the exercise of freedom of assembly. For example, as mentioned above, so-called IMSI catchers can be used to monitor and intercept ingoing and outgoing communications, but can also edit

54 This *lex specialis* nature is mentioned in ECtHR, *Ezelin*, above note 47.

55 The Human Rights Committee found the right to freedom of assembly to be irrelevant if one is acting alone. Human Rights Committee, *Patrick Coleman v. Australia*, Communication No. 1157/2003, UN Doc. CCPR/C/87/D/1157/2003, Views, 10 August 2006, para. 6.4.

56 One of the distinctive criteria noted by the ECtHR is that in the exercise of the right to freedom of assembly the participants would be seeking not only to express their opinion, but to do so together with others. See, among others, ECtHR, *Navalnyy v. Russia*, Appl. Nos 29580/12 and 4 others, Judgment (Grand Chamber), 17 February 2004, para. 101. See also M. Hamilton, above note 8, pp. 525–526, 534–535.

57 As the ECtHR has underlined, "the participation of citizens in the democratic process is to a large extent achieved through belonging to associations in which they may integrate with each other and pursue common objectives collectively". ECtHR, *Gorzelik and Others v. Poland*, Appl. No. 44158/98, Judgment (Grand Chamber), 17 February 2004, para. 92. See also HRC Res. 38/11, "The Promotion and Protection of Human Rights in the Context of Peaceful Protests", 16 July 2018, p. 11.

58 Most recently, UNGA Res. 73/179, above note 52, para. 9; HRC Res. 42/15, above note 51, preambular para. 12.

59 "[I]n the digital age, technical solutions to secure and to protect the confidentiality of digital communications, which may include measures for encryption, pseudonymization and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression *and to freedom of peaceful assembly* and association." UNGA Res. 73/179, above note 52, preambular para. 26 (emphasis added).

or reroute mobile communications, as well as block service. Governments may use an IMSI catcher to send a message to mobile phones in the area as a way of intimidating protesters or manipulating them into disbanding or conducting some other activity. Similarly, internet shutdowns or placing restrictions on secure and confidential communications may constitute a direct interference with freedom of assembly insofar as they represent an attempt by the government to prevent a protest from being organized or disperse an already ongoing protest. These actions directly hinder the ability of individuals to attend a gathering, to communicate with one another and to organize further.[60]

Freedom of assembly is indeed a qualified right and may be restricted when necessary in a democratic society for a legitimate aim – in the interests of national security, public safety etc.[61] However, as the Human Rights Committee has repeatedly underlined, it may only be limited under strict conditions.[62] Restrictions can be imposed only if prescribed by law and necessary and proportionate in the circumstances, but more often than not these interferences are not even prescribed by law. For instance, in many countries there is no legal framework regulating the use of mass surveillance tools, such as IMSI catchers, and often protesters will not even be aware of their presence during a protest.[63]

Additionally, restrictions to freedom of assembly need to be specific and necessary to achieve a specific legitimate aim;[64] there needs to be a rational connection between the measure and the prescribed aim, meaning that a measure cannot be based on an abstract aspiration that it might facilitate the aim.[65] However, it is arguably impossible to find such a link when imposing general and indiscriminate surveillance measures,[66] or indeed to justify such mass interferences in any circumstances. When protests turn violent or in other situations of violence, certain targeted surveillance and investigatory measures may be taken, but generalized measures against an abstract threat cannot tilt the balance. For instance, governments often claim that internet shutdowns are

60 See Privacy International, *Submission to the Office of the United Nations High Commissioner for Human Rights on the Promotion and Protection of Human Rights in the Context of Peaceful Protests*, October 2019, available at: https://tinyurl.com/2tcqlbn8.

61 ICCPR, Art. 21; ECHR, Art. 11(2).

62 See, among others, Human Rights Committee, *Zinaida Shumilina et al. v. Belarus*, Communication No. 2142/2012, Views, 28 July 2017; Human Rights Committee, *Pavel Levinov v. Belarus*, Communication No. 2082/2011, Views, 14 July 2016.

63 Privacy International, "IMSI Catchers: Facilitating Indiscriminate Surveillance of Protesters", 19 June 2020, available at: https://privacyinternational.org/news-analysis/3948/imsi-catchers-facilitating-indiscriminate-surveillance-protesters.

64 "Such attempts to interfere with the freedom of expression unlawfully pursue an illegitimate objective of undermining the right to peaceful protest". David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HRC/29/32, 22 May 2015, para. 53.

65 Aharon Barak, "Rational Connection", in *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, pp. 303–316.

66 "General and indiscriminate surveillance measures" here describes systems or technologies that collect, analyze and/or generate data on large numbers of people instead of limiting surveillance to individuals about which there is reasonable suspicion of wrongdoing. See, for instance, Court of Justice of the European Union, *Tele2 Sverige AB v. Post- och telestyrelsen (C-203/15) and Secretary of State for the Home Department v. Tom Watson ao (C-698/15)*, Judgment, 21 December 2016.

necessary for public safety when a peaceful protest is about to turn violent, but such kill switches "may well exacerbate, rather than curtail, tensions";[67] they can stress the gathered crowds, who are no longer able to be informed about what is happening around them.[68] In addition, internet shutdowns affect not only the assemblers but also those who are living in, working in and passing through the area where the assembly takes place.

Following a blockage of Twitter and YouTube, the Commissioner for Human Rights of the Council of Europe underlined that although illegal content could be blocked, applying this measure to entire platforms was a disproportionate response. Accordingly, he requested that such blockages should be lifted.[69] The UN Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association has emphasized that shutdowns and the blocking of entire websites constitute an extreme and disproportionate measure that cannot be justified in any circumstances.[70] He has also called for the prohibition of indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly, in both physical and digital spaces.[71]

Certainty of surveillance amounts to an infringement of freedom of assembly

The certainty of surveillance and interference with communications technologies, particularly due to the general and indiscriminate nature of such measures, arguably infringes on the obligation not to interfere with protests as such, irrespective of whether the information collected is used to further directly interfere with the organization of an assembly, as argued above.

Undoubtedly, when attending a public assembly there may be a reasonable expectation that individuals might be identified, either because police conduct an investigation or because their face appears in a newspaper photograph. However, current surveillance of assemblies, particularly protests, has gone far beyond the expectation of some degree of publicity.[72] It is now becoming a certainty that protesters could be identified through the data collected by the authorities when

67 "Silencing Opposition Is 'Not the Solution', UN Rights Chief Says as Internet Blackout Looms in DR Congo", *UN News*, 17 December 2016, available at: https://news.un.org/en/story/2016/12/548052-silencing-opposition-not-solution-un-rights-chief-says-internet-blackout-looms.

68 On the contrary, the Special Rapporteur has underlined that the Internet may be used to mitigate public safety concerns and help restore public order. For instance, internet communications are key to disseminating accurate information during a crisis. D. Kaye, above note 64, para. 14.

69 *Annual Activity Report 2013 to the Parliamentary Assembly of the Council of Europe: Report of the Thirteenth Sitting*, AS (2014) CR 13, 8 April 2014.

70 UN Human Rights, above note 10, para. 22.

71 Surveillance of protesters should only be conducted on a targeted basis, and only when there is reasonable suspicion that the targets are engaging in or planning to engage in serious criminal offences, based on principles of necessity and proportionality and with judicial supervision. C. Voule, above note 6, para. 57.

72 While the notion of "reasonable expectation of privacy" is found in US law, the jurisprudence of the ECtHR, among others, also seems to recognize the concept, albeit not with an identical understanding. See, for example, John Ip, "The Legality of 'Suspicionless' Stop and Search Powers under the European Convention on Human Rights", *Human Rights Law Review*, Vol. 17, No. 3, 2017.

it is processed and analyzed. As such, the general and indiscriminate surveillance of protests amounts to an unjustified interference not only with the right to privacy but also with the right to peacefully assemble, and in turn violates freedom of assembly.

For instance, the regular audio-visual recording of protests in combination with facial recognition technology requires the collection and processing of facial images of all persons captured by the camera (irrespective of whether the authorities use facial recognition in real time or at a later stage). The permanent record that can be created by these recordings could allow authorities, if they so decide, to identify all those that participated in a protest even at a later time.[73] The UN High Commissioner for Human Rights has recommended that States "[n]ever use facial recognition technology to identify those peacefully participating in an assembly".[74]

Similarly, identity catchers, such as IMSI catchers, can capture the call activity of thousands of people indiscriminately. These are interferences on a mass scale.[75] Additionally, the aggregation of information acquired from different means and methods of surveillance before, during and after protests gives police forces the power to de-anonymize and identify everyone involved in the protest, irrespective of whether they are suspected of having committed a crime.[76] At the same time, the duration of the consequence of surveillance has also radically changed, as there is little indication of how long law enforcement and other agencies involved in protest surveillance will be keeping a record of the collected data.[77]

Inherent to freedom of assembly is the ability to participate in a protest without retribution. Anonymity plays a key role for safe and confidential communications in the planning and holding of protests, as well as for

73 General Comment 37 reiterates that "[t]he wearing of face-coverings or other disguises by assembly participants, such as hoods or masks, or taking other steps to participate anonymously may form part of the expressive element of a peaceful assembly, serve to counter reprisals, or to protect privacy, including in the context of new surveillance technologies". General Comment 37, above note 5, para. 60. Depending on how facial recognition technology develops, it could interfere with this possibility. A company has already claimed to be in the process of developing technology that even bypasses masks. Khari Johnson, "Facial Recognition Is No Match for Face Masks, but Things Are Changing Fast", *VentureBeat*, 8 April 2020, available at: https://venturebeat.com/2020/04/08/facial-recognition-is-no-match-for-face-masks-but-things-are-changing-fast/.

74 UN Human Rights, above note 10, para 53(h).

75 The 2020 Annual Report of the UN High Commissioner for Human Rights confirmed as much, even though it didn't go as far as concluding that blanket measures as such amount to a violation of freedom of assembly. UN Human Rights, above note 10. See also HRC Res. 44/20, above note 13, para. 26.

76 Before a protest, if a person uses social media to support or register with the protest, the police will collect this information; during a protest, if a person takes their mobile phone with them, which most would do, they may be surveilled by drones and IMSI catchers, or if they do not take their mobile, they may be surveilled by facial recognition technology, stop and search of passers-by or the use of a credit card or travel card; and finally, organizers and other "persons of interest" (not suspected of having committed a crime) are often kept under surveillance long after the protest.

77 The ECtHR in the *Catt* case referred to Principle 2 of Recommendation R(87)15 that regulates the use of personal data in the police sector, which states that "the collection of data on individuals solely on the basis that they belong to particular movements or organisations which are not prescribed by law should be prohibited unless absolutely necessary or for the purposes of a particular inquiry". ECtHR, *Catt*, above note 47, para. 124. See also ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, Appl. No. 7124/09, Judgment (Second Section), 6 June 2006, para 107.

participating in protests.[78] Individuals rely on the anonymity of the crowd to protect themselves against retribution, particularly in contexts where any form of dissent is suppressed.[79] This is no longer an option, however, as people's mere participation in a protest today promises the erosion of their privacy, particularly as the cumulative use of these surveillance systems and methods guarantees that the information of individual protesters will be captured by at least one of them, leading to the individual's potential identification. It is argued here that the inevitability of surveillance, as such, becomes a barrier to the organization of and participation in assemblies, including protests, and thus constitutes an unjustified interference that infringes on freedom of assembly.

Infringement of the obligation to facilitate assemblies

General and indiscriminate assembly surveillance and interference with internet communications violate the positive obligations of States to facilitate assemblies and protect assemblers, as well as their positive obligation to take precautionary measures to prevent violations and abuses of the different rights at stake.

States need to secure the effective enjoyment of freedom of assembly.[80] Therefore, they have a positive obligation to take reasonable and appropriate measures to facilitate, protect and enable lawful demonstrations to proceed peacefully.[81] Undoubtedly, in order to fulfil these obligations, they have to take certain measures – for instance, redirecting traffic or providing security.[82] However, the need to adopt such measures is not without limits. The measures must never impair the essence of the right and cannot serve as a justification for measures that violate freedom of assembly, among other rights.[83]

If the network that enables the organization and holding of assemblies is shut down before a demonstration takes place, such a measure directly violates the positive obligation of States to facilitate the exercise of freedom of assembly. Associated activities that happen online in advance of an assembly are equally protected under freedom of assembly.[84] As the ECtHR has repeatedly underlined, "a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it".[85]

78 See the sources cited in above note 16.
79 General Comment 37, above note 5, para. 60.
80 ECtHR, *Kudrevičius and Others v. Lithuania*, Appl. No. 37553/05, Judgment (Grand Chamber), 15 October 2015, para. 158; ECtHR, *Djavit An v. Turkey*, Appl. No. 20652/92, Judgment (Third Section), 20 February 2003, para. 57.
81 See, *inter alia*, HRC Res. 44/20, above note 13, para. 4; HRC Res. 25/38, above note 13, para. 4; HRC Res. 24/5, above note 13, preambular para. 8. See also P. van Dijk *et al.*, above note 13, pp. 836–837.
82 ECtHR, *Oya Ataman v. Turkey*, Appl. No. 74552/01, Judgment (Second Section), 5 December 2006, para. 39.
83 Human Rights Committee, General Comment No. 31, "The Nature of the General Legal Obligation Imposed on States Parties to the Covenant", UN Doc. CCPR/C/21/Rev.1/Add.13, 26 May 2004 (General Comment 31), para. 6.
84 General Comment 37, above note 5, para. 34.
85 See, *inter alia*, in relation to privacy-related cases, ECtHR, *Big Brother Watch and Others v. the United Kingdom*, Appl. Nos 58170/13, 62322/14, 24960/15, Judgment (First Section, pending referral to the

Undermining the privacy of communications as such infringes on freedom of assembly, because the capacity to use communications technologies securely and privately is vital to the organization and conduct of assemblies.[86] Therefore, any general and indiscriminate surveillance or internet communications interference, including blocking internet connectivity or monitoring social media and other online communications, should also be understood as a violation of the obligation of States to facilitate assemblies.[87]

Infringement of the obligation to ensure a legal framework that safeguards freedom of assembly

Mass surveillance and interference with internet communications infringe on the positive obligation of States to promote an enabling environment for the exercise of the right to peaceful assembly.

Part of this obligation is the overarching obligation to ensure that there is an appropriate, accessible and foreseeable legal and institutional framework that regulates the exercise of freedom of assembly.[88] The legal framework must clearly set out the duties and responsibilities of all those acting in an official capacity – including private companies contracted to provide security – involved in managing assemblies in accordance with international standards, including who can surveil protests or interfere with new technologies, and when they can do so.[89] For instance, the use of IMSI catchers without any framework or of military-grade predator drones, or interference with internet communications by intercepting, redirecting or blocking the use of specific platforms or pages, should all be also understood as *ipso facto* violations of freedom of assembly.[90]

More often than not nowadays, police are deploying surveillance measures and interfering with communications technologies without necessarily abiding by a specific legal framework, either because such a framework does not exist or because the existing one is interpreted too broadly. The absence of a legal framework regulating the use of new technologies for surveillance or interference before, during and after protests, or the existence of one that gives very broad and excessive powers to authorities, should be understood as a direct violation of the obligation to safeguard the exercise of freedom of assembly.

Grand Chamber), 13 September 2018, para. 308; ECtHR, *Roman Zakharov v. Russia*, Appl. No. 47143/06, Judgment (Grand Chamber), 4 December 2015, para. 232.

86 The UN Human Rights Council has underlined that "the possibility of using communications technology securely and privately … is important for the organization and conduct of assemblies". HRC Res. 44/20, above note 13, preambular para. 22. See also the sources cited in above note 16.

87 *Inter alia*, the Human Rights Council reiterated "the importance for all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries". HRC Res. 24/5, above note 13, preambular para. 8.

88 General Comment 37, above note 5, para. 28; see also the obligation to facilitate protests at para. 24.

89 *Ibid*., para. 28.

90 See above on IMSI catchers.

Violation of the obligation to respect freedom of assembly

General and indiscriminate surveillance and interference with internet communications violate the obligation to respect freedom of assembly, due to the chilling effect that their use causes.

As part of the obligation to respect freedom of assembly, States have a negative obligation to refrain from actions that will undermine the enjoyment of this right.[91] General and indiscriminate surveillance and interference with internet communications have the capacity to "chill" the exercise of freedom of assembly, as the monitoring and recording of participants at an assembly may prevent them from joining.[92] In the *Big Brother Watch* case, the ECtHR accepted that any perceived interference with the confidentiality of communications without any limitations may result in a "chilling effect" – that is, a self-restraint – on the lawful exercise of a right, particularly freedom of expression; hence it found a violation of Article 10 of the European Convention on Human Rights.[93] The inevitability of surveillance (see above) should thus be understood as a violation of the obligation to respect freedom of assembly, and not only as an interference with freedom of assembly.

Also, these newer forms of government surveillance, where practices (such as employing facial recognition technologies) lack foreseeability and transparency, exacerbate the negative impact on the exercise of freedom of assembly.[94] As warned by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, "even a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect without careful and public documentation of its use, and known checks and balances to prevent its misuse".[95]

91 Among others, see ECtHR, *Plattform "Ärzte für das Leben" v. Austria*, Appl. No. 10126/82, Judgment, 21 June 1988.

92 Human Rights Council, above note 16, para. 76.

93 ECtHR, *Big Brother Watch*, above note 85, para. 495. See also Bart van der Sloot, "Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities", in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, p. 422.

94 In the context of secret surveillance, the ECtHR has found it "unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation". ECtHR, *Klass and Others v. Germany*, Appl. No. 5029/71, Judgment (Plenary), 6 September 1978, para. 36. In the context of freedom of expression, Special Rapporteur David Kaye has noted that "[u]nnecessary and disproportionate surveillance may undermine security online and access to information and ideas. Surveillance may create a chilling effect on the online expression of ordinary citizens, who may self-censor for fear of being constantly tracked. Surveillance exerts a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, members of certain political parties, civil society, human rights defenders, professionals such as journalists, lawyers and trade unionists, victims of violence and abuse, and children." David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HRC/32/38, 11 May 2016, para. 57.

95 Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HRC/23/40, 17 April 2013, para. 52.

Attacking the essence of freedom of assembly

Finally, general and indiscriminate surveillance and interference with internet communications undermine the essence of freedom of assembly.

Human rights instruments that guarantee freedom of assembly permit certain interferences with this right, so long as those interferences abide by certain strictly interpreted principles, including legality, necessity and proportionality, to the extent that they do not undermine the essence or core of this right. As the Human Rights Committee has emphasized, "[i]n no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right".[96]

This obligation is embedded in the core provisions of each human rights instrument, which guarantee that nothing in their provisions may be interpreted as implying that a State or other entity can engage in any act that will lead to the destruction of any of the rights of freedom set forth therein, including freedom of assembly.[97] The ECtHR, on a case relating to measures restricting assembly, held

> that notification, and even authorisation procedures, for a public event *do not in general encroach upon the essence of the right* [of freedom of assembly], *as long as the purpose of regulating the assembly is to allow the authorities to take reasonable and appropriate measures in order to guarantee its smooth conduct*.[98]

It went on to add, though, that "the enforcement of such rules cannot become an end in itself".[99]

In another case, the Court has noted

> that the very essence of the right to freedom of peaceful assembly would be impaired, if the State was not to prohibit a demonstration but was then to impose sanctions on its participants, even one at the lower end of the scale of penalties, for the mere fact of attending it, without committing anything reprehensible, as happened in the applicant's case.[100]

In other words, what this reasoning suggests is that blanket surveillance and other interferences that dissuade individuals from participating in assemblies could be regarded as adversely affecting the essence of freedom of assembly.

96 General Comment 31, above note 83, para. 6. In a different context, the ECtHR has also observed that there exists "the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it". ECtHR, *Zakharov*, above note 86, para. 232. UN Human Rights has similarly observed that "any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights". UN Human Rights, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, UN Doc. A/HRC/27/37, 30 June 2014, para. 23.

97 ICCPR, Art. 2; ECHR, Art. 17; UDHR, Art. 30.

98 ECtHR, *Navalnyy*, above note 56, para. 100 (emphasis added).

99 *Ibid.*, para. 100.

100 The Court therefore concluded that the interference with the applicant's right to freedom of peaceful assembly was not "necessary in a democratic society". ECtHR, *Galstyan v. Armenia*, Appl. No. 26986/03, Judgment (Third Section), 15 November 2007, para. 117; see also ECtHR, *Ashughyan v. Armenia*, Appl. No. 33268/03, Judgment (Third Section), para. 93.

The restrictions imposed upon this right should not unacceptably weaken the protection afforded by it. Freedom of assembly guarantees the right to collectively and peacefully meet, demonstrate or protest without retribution. Read together with the arguments provided in the previous sections, we can conclude that the erosion of participants' anonymity, the inevitability of surveillance, and blanket interference with people's communications for the mere fact of having participated in a gathering adversely affect the essence of freedom of assembly.

Conclusion

New forms of control through the use of surveillance, as well as interference with internet communications, have been increasingly deployed by States to control assemblies, including general and indiscriminate surveillance, internet shutdowns, and the blocking of social media platforms, web pages and mobile applications. Undoubtedly, the new digital reality requires governments to adapt and use the tools at their disposal to assist them in ensuring the safe and free administration of assemblies and movements. However, there has always been one condition – they should always safeguard the enjoyment of human rights in the process.

The use of any such measures should comply with the legal requirements not only of the right to privacy and freedom of expression, but also of the right to freedom of assembly. General and indiscriminate surveillance and blanket interferences with internet communications amount to a direct infringement of the right to freedom of assembly on multiple grounds, and as such should not be used in the context of assemblies – if at all, though that is a separate conversation.[101] General and indiscriminate surveillance and interference with internet communications infringe on freedom of assembly when they are used for direct, unjustified interference with assemblies; they render surveillance inevitable, instead of a possibility; they violate the obligation to facilitate assemblies and the obligation to have a legal framework that facilitates assemblies, as well as the obligation to respect freedom of assembly; and, last but not least, they attack the essence of the right.

Undoubtedly, some of these acts can be and have on occasion been understood as violations of the right to privacy and/or freedom of expression. However, examining their impact on other rights allows for more effective protection of the core values that each protects. This separate legal analysis is needed not only to preserve the distinct nature of freedom of assembly that protects collective action, but also to allow for better regulation of surveillance and interference with internet communications in assemblies, demonstrations and protests. Freedom of assembly is only the beginning – other human rights and their distinct nature stand in line, including freedom of religion and belief and the right to participate in public affairs.

101 See arguments brought forward by Big Brother Watch, Privacy International, Amnesty international and seven other organizations in *Big Brother Watch and Others v. UK*, pending before the Grand Chamber of the ECtHR at the time of writing. ECtHR, *Big Brother Watch*, above note 85.