Monitoring Assemblies: Online Activities and Digital Technology

European Center for Not-for-Profit Law

#right2freeassembly

There is growing recognition of the centrality of the use of different social media platforms and other forms of digital technologies by people organising and participating in public assemblies as well as by state authorities in responding (both positively and negatively) to assemblies and protests. The UN General Comment 37 on the right of peaceful assembly for example notes (at para 10)[1]

> ***10.** The way in which assemblies are conducted and their context changes over time. This may in turn affect how they are approached by the authorities. For example, emerging communication technologies offer the opportunity to assemble either wholly or partly online and often play an integral role in organizing, participating in and monitoring physical gatherings, which means that interference with such communications can impede assemblies. While surveillance technologies can be used to detect threats of violence and thus to protect the public, they can also infringe on the right to privacy and other rights of participants and bystanders and have a chilling effect …*

This text acknowledges the role of digital technologies in enabling people to gather together online as a means of accessing the right to peaceful assembly, their use in organising and exercising the right to assembly in physical space, as well as their use by authorities who may see protests as a threat and whose responses may effectively serve to undermine the right.

While there are an increasing number of purely online assemblies, most assemblies still involve the physical gathering of people in public spaces and these necessarily involve the use of online and digital technologies in their planning, preparation and participation. The General Comment also usefully acknowledges (in para 33) that publicising a planned assembly and the activities involved in the organising of it are part of right to assemble and should not be unduly restricted:

> ***33.** Article 21 and its related rights do not only protect participants while and where an assembly is ongoing. Associated activities, conducted by an individual or by a group, outside the immediate context of the gathering but which are integral to making the exercise meaningful, are also covered. The obligations*

[1] https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx

Sweden Sverige

ICNL INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

Text by Neil Jarman, on behalf of the European Center for Not-for-Profit Law Stichting (ECNL) as part of the 'Monitoring the Right to Free Assembly' regional project.

The project is made possible by the International Center for Not-for-Profit Law (ICNL) through the Civic Space Initiative, financed by the Government of Sweden. The Government of Sweden does not necessarily share the opinions here within expressed. The author bears the sole responsibility for the content.

> *of States parties thus extend to actions such as participants' or organisers' mobilisation of resources; planning; dissemination of information about an upcoming event; preparation for and travelling to the event; communication between participants leading up to and during the assembly; broadcasting of or from the assembly; and leaving the assembly afterwards. These activities may, like participation in the assembly itself, be subjected to restrictions, but these must be narrowly drawn. Moreover, no one should be harassed or face other reprisals as a result of their presence at or affiliation to a peaceful assembly.*

This growing use of digital technologies as part of assemblies in public space in turn impacts on the monitoring of such assemblies (monitoring purely online assemblies presents different challenges which are not the focus of this briefing). Observers need to be aware of a varied range of activities that occur online and via social media platforms and which may take place before, during and after an assembly, and they need to be able to monitor such activities if they are to fully assess the extent to which the right to assembly is being facilitated or restricted.

Monitoring of digital activities will involve **being aware of a diverse range of potential platforms and technologies** that may be used, some of which are global (e.g. Facebook, Twitter, Instagram, YouTube, WhatsApp, Zoom, Skype, etc.), while others may be more localised or a specific response to a local context (e.g. Bridgefy and FireChat in Hong Kong[2]). It is also important to note that different usages and approaches that may be taken by the organisers, by participants, by opponents and by state actors, and that different platforms may be used in different ways in different contexts and countries.

This may require being aware of different usages of public social media (accessible to all) as well as forms of private or encrypted messaging; use of text based messaging as well as image recording and dissemination; and of the ever more diverse forms of surveillance technologies that are being employed by state actors.[3] **While public platforms may be readily accessible to monitors, private platforms or encrypted technologies will not normally be accessible.**

This short paper sets out some of the things that human rights activists will need to be aware of and look out when monitoring at assemblies.

Before an assembly

Organisers and Participants

Organising an assembly is increasingly occurring through use of social media channels and the ease by which people can be mobilised means that there may not be a readily identifiable formal organiser to approach for information. Monitors may therefore need to keep an eye on social media platforms to gather advanced information about an assembly.

In doing so monitors will need to document such things as: **which social media platforms are being used; do different types of groups favour specific platforms; are different platforms being used for organisational activities from those used for publicity or mobilisation; are any evident restrictions being imposed on usage?** Some of this will be readily accessible, but some information may only be evident through interviews with organisers and activists.

[2] https://hackernoon.com/why-firechat-was-used-in-hong-kong-and-is-successful-with-crowds-2874fd0925c3 and https://thenextweb.com/socialmedia/2019/09/03/how-hong-kong-protesters-are-embracing-offline-messaging-apps-to-avoid-being-snooped-on/

[3] https://www.eff.org/deeplinks/2020/06/how-identify-visible-and-invisible-surveillance-protests

Opponents of an assembly may also use social media to mobilise potential participants in counter protests.

Use of digital technologies by the police / authorities

The authorities in turn are increasingly using social media to gather information about planned or forthcoming assemblies. Information may legitimately be gathered through accessing forms of public social media but may also involve less evident forms of surveillance to gather data on plans and people involved. Some of this activity may be overt and well known, but some surveillance activities may only become evident after the event through information released as part of court cases, research or media reporting.

Different bodies may be involved in such activities, this may depend on which bodies have responsibility for facilitating assemblies, but these will include ministries, local government and the police.

Digital technologies may be used to facilitating the right to assembly, and monitors will need to consider **if the authorities accept forms of digital notification for physical assemblies. Do they make notifications accessible to the public? And do they make any restrictions that they impose accessible to the public?**

Digital technology usage may also act as a constraining or chill factor, for example through the use of social media to express concerns or warn about risks or disruption to daily routines. Monitors should consider **whether any communications by the authorities is likely to encourage people to participate or rather serve as a chill factor?**

During the assembly

Organisers and Participants

Different platforms may be used by organisers and participants to record and document events. These may include ongoing calls for participants, livestreaming of activities, report on incidents and police actions. **Monitors should aim to document which platforms are being used in different assemblies: are different groups using different platforms for different activities? Is use of social media being impeded or restricted? If so how?**

People are also innovating and adapting apps and social media usage in response to developing and evolving protests contexts, for example in Hong Kong protest participants developed an app to enable them to monitor police movements[4] , while in the USA they utilised a community safety app for the same purpose.[5] Monitors should ask: **is there evidence of new or innovative uses of social media or digital platforms? If so, how are they used and how do the authorities respond?**

Use of digital technologies by the police / authorities

In parallel with the use of digital technologies by civil society, there is also a diverse use of forms of surveillance and information gathering by the authorities during assemblies. Some of this may be more visible, such as different forms of digital cameras, body worn cameras, drones, helicopters, CCTV and hand held devices, and forms of facial recognition technologies,[6] while the process of monitoring use of social media platforms may be less evident at the time.[7]

[4] https://www.washingtonpost.com/world/asia_pacific/apple-pulls-police-tracking-app-used-by-hong-kong-protesters/2019/10/10/4aad5ebe-eb14-11e9-a329-7378fbfa1b63_story.html

[5] https://www.vox.com/recode/2020/6/3/21278558/protest-apps-signal-citizen-twitter-instagram-george-floyd

[6] https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database?CMP=Share_iOSApp_Other

[7] https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/

UN General Comment has noted that rights to privacy still exist even though a person is participating in an assembly in a public place:

> *62. 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. The same applies to the monitoring of social media to glean information about participation in peaceful assemblies. Independent and transparent scrutiny and oversight must be exercised over the decision to collect personal information and data of those engaged in peaceful assemblies and over its sharing or retention, with a view to ensuring the compatibility of such actions with the Covenant.*

Monitors should therefore aim to document and record the different forms of image and data gathering technologies that are being deployed by the authorities.[8] These may include technologies used to capture data on mobile phones in the vicinity of protests, which wasnoted in Ukraine in 2014[9] but which have since become more widely used[10] as well as more evident image capturing devices.

Documenting use of such technologies is important in ensuring that the authorities have and adhere to publicly available guidelines regulating their use and that such usage is consistent with international standards on privacy.[11]

Monitors should also be aware of the potential for the blocking or limiting of internet connectivity during an assembly which can serve to limit communication and prevent livestreaming of activities more generally in the vicinity of an assembly or even more widely. Such extreme responses to the mobilisation in assemblies have been more widely documented in recent years.[12]

Safety and Privacy of Monitors

The authorities may also attempt to seize data from journalists, human rights monitors and others who have been present at an assembly, and which highlights an increasing awareness of the need for additional forms of personal safety and digital privacy while attending and observing at assemblies.

A number of guides have recently been produced by organisations such as Amnesty International,[1] the Electronic Frontier Foundation[2] and others[3] that provide advice and guidance on improving safety and maintaining digital privacy while involved in protests or activities related to the right to peaceful assembly.

[1] https://citizenevidence.org/2020/06/03/protecting-protester-privacy-against-police-surveillance/

[2] https://ssd.eff.org/en/module/attending-protest

[3] https://www.vice.com/en_uk/article/gv59jb/guide-protect-digital-privacy-during-protest; https://www.pogo.org/analysis/2020/10/how-to-respond-to-risk-of-surveillance-while-protesting/; https://www.wired.com/story/how-to-protest-safely-surveillance-digital-privacy/

[8] https://www.popularmechanics.com/technology/security/a32851975/police-surveillance-tools-protest-guide/ and https://www.eff.org/deeplinks/2020/06/how-identify-visible-and-invisible-surveillance-protests

[9] https://www.washingtonpost.com/news/the-switch/wp/2014/01/21/ukraines-1984-moment-government-using-cellphones-to-track-protesters/

[10] https://www.eff.org/deeplinks/2020/06/quick-and-dirty-guide-cell-phone-surveillance-protests

[11] UN General Comment 37 para 94

[12] https://freedomhouse.org/report/freedom-net/2019/crisis-social-media and https://netblocks.org/

After the Assembly

General Comment 37 noted that the right to assemble includes activities that take place before and after the actual physical assembly, and although people may have dispersed diverse forms of activities related to the assembly, the activities of the various key actors may continue.

Organisers and Participants

Post-assembly activities by organisers and participants may include reporting on the actions of the authorities, publicising information about people who have been detained or arrested, and encouraging people to participate in further assemblies and related activities.

It may also involve trying to hold the authorities to account for their actions and raising questions about the use of surveillance data: **how are surveillance images used and stored? For how long? And what does local law say about image use and retention?**

Assembly monitors may also raise questions about any restrictions on internet access during protests and ask **how the authorities justify such disruptions to internet connectivity.**

Use of digital technologies by the police / authorities

The authorities may in turn **continue the surveillance of social media and/or online hosting platforms; use platforms to disseminate a narrative about what happened and why;** and publicise people they are seeking for activities that occurred during an assembly among other things.