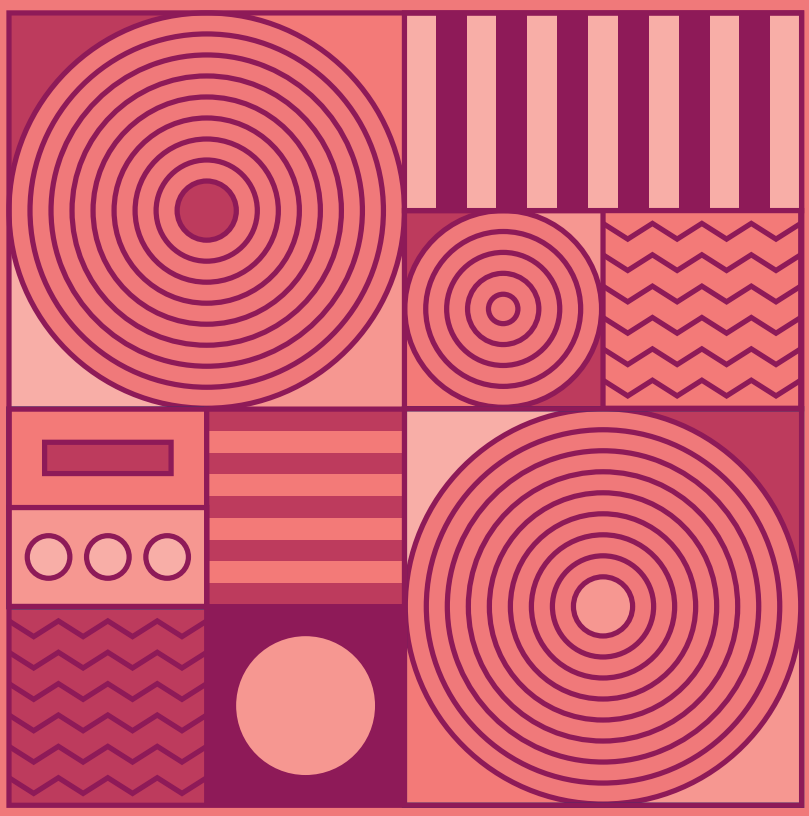


Surveillance of peaceful assemblies in the OSCE region

Human rights implications and strategies for independent monitoring



OSCE ODIHR

Surveillance of peaceful assemblies in the OSCE region: human rights implications and strategies for independent monitoring



Acknowledgements

The OSCE Office for Democratic Institutions and Human Rights (ODIHR) would like to thank all participants that gave their time, insights and expertise with such generosity, including members of the ODIHR peaceful assembly monitoring network. Acknowledgements are also due to Professor Pete Fussey who led the research and drafting of the report. Finally, ODIHR would like to thank Denis Shedov, Michael Hamilton and the Omega Research Foundation for their contribution to the report.

Surveillance of peaceful assemblies in the OSCE region: human rights implications and strategies for independent monitoring

Published by the OSCE Office for Democratic Institutions
and Human Rights (ODIHR)
Miodowa 10
00-251 Warsaw
Poland
www.odihr.osce.org

© OSCE/ODIHR 2026

All rights reserved.

The contents of this publication may be freely used and copied for educational and other non-commercial purposes, provided that any such reproduction is accompanied by an acknowledgement of the OSCE/ODIHR as the source.

ISBN: 978-92-9271-588-5

Designed by Filip Andronik



Contents

Glossary and acronyms 5

Foreword 6

Executive Summary 8

Surveillance and digital interference 8

Assembly monitoring and digital surveillance 8

Recommendations 8

Introduction 10

Methodology 11

1. The right to peaceful assembly: standards and monitoring in practice 12

The right to monitor assemblies 14

The purposes of assembly monitoring 15

2. Strategies for monitoring surveillance and human rights concerns surrounding assemblies 17

Direct observation 17

Pre-protest communication and stakeholder engagement 18

Monitoring surveillance in criminal justice procedures (especially trial and detention) 21

Monitoring administrative processes 22

Building strategic networks 24

Digital hygiene and cybersecurity 25

3. Technological expansion: the legitimate use of and justifications for assembly surveillance 27

Justifications for the surveillance of assemblies 28

Legislative and policy considerations 32

4. Digital tools observed in assemblies across the OSCE region 35

Remote biometric identification technologies 35

Digital infiltration 39

Open-source surveillance and social media patrolling 41

Communications and cellular monitoring 42

Aerial surveillance and drones 43

Data fusion and management 44
Enduring forms of surveillance 45
5. The impact of surveillance of assemblies on the right to peaceful assembly 47
Assemblies as surveillance opportunities and 'surveillance creep' 47
The banning and disruption of assemblies 48
Prosecution and detention 49
Retaliation and other coercive uses of surveillance data 50
6. Obstacles to monitoring surveillance at assemblies 51
The invisibility of technology and absence of transparency 51
Legislative and administrative blocks to scrutiny 53
Intimidation, violence and chilling effects 54
Knowledge gaps on technology and human rights 56
7. Recommendations and conclusions 58
Recommendations for participating States 58
Recommendations for international organizations 61

Glossary and acronyms

FOIA	Freedom of Information Act (shorthand for formal information disclosure requests)
FRT	Facial recognition technology
GC37	United Nations Human Rights Committee General Comment 37 on Article 21 of the ICCPR (Right of Peaceful Assembly)
GDPR	EU General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
ICE	US Immigration Customs Enforcement
IMSI	International Mobile Subscriber Identity (a form of communications surveillance)
ISP	Internet service provider
LFR	Live facial recognition
ODIHR	OSCE Office for Democratic Institutions and Human Rights
OIFR	Operator-initiated facial recognition
OSCE	Organization for Security and Co-operation in Europe
OSINT	Open-source intelligence
pSs	OSCE participating States
RFR	Retrospective facial recognition
SAR	Subject access request
VPN	Virtual private network

Foreword

This report documents the fraught contemporary environment in which the right of peaceful assembly is exercised — illuminating, in particular, how those who seek to protest increasingly become objects of surveillance. The report further underscores the critical role that protest monitors can play in helping to ensure that the right of peaceful assembly is effectively protected, including where surveillance is deployed.

For many years, the OSCE Office for Democratic Institutions and Human Rights (ODIHR) has led and supported efforts to strengthen peaceful assembly monitoring. The UN Human Rights Committee and the UN Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association have also emphasized the protections that international human rights law and standards afford to monitors and observers: they have the right to record law enforcement officials, even if a protest is declared unlawful or is dispersed, and they must be protected and facilitated in their work.

Members of the ODIHR peaceful assembly monitoring network have been at the forefront of these efforts. Network members are not only involved in monitoring the policing of assemblies, but — as this report demonstrates — also critically engage with questions of emerging practice, working to ensure that peaceful assembly monitoring as a methodology keeps pace with technological developments in policing, including facial recognition and geo-tracking capabilities.

The information that monitors gather can help contribute to an accurate record of events and support accountability. In this regard, courts too have a vital role to play in scrutinizing whether surveillance practices have a legal basis, and are necessary and proportionate in pursuit of a legitimate purpose. This scrutiny must extend not only to the deployment of surveillance tools but also to data storage, sharing, processing and analysis, including through the use of artificial intelligence.

Moreover, as the report explores, independent monitoring can help identify instances in which information may have been gathered through surveillance. Monitors can help identify where such information surfaces in legal proceedings and then forensically back-trace where, and how, that information was obtained and used.

The acquisition and deployment of powerful surveillance technologies without adequate regulation or oversight significantly increases the risks to the exercise of human rights. These risks are particularly acute where surveillance technologies are used for predictive policing or profiling, including where the categorization of assemblies or their participants leads to preventive interventions targeting certain groups.

Surveillance also impacts how public space is perceived and how, or whether, people choose to be present within it, including for political, social or recreational ends. The proliferation of cameras and the use of geolocation technologies erodes individual expectations of privacy and creates a powerful chilling effect on the organization and mobilization of peaceful assemblies. Importantly, the effects of surveillance are generally experienced unevenly — impacting particularly those who are already marginalized or most at risk.

The increasing normalization of surveillance puts in jeopardy the effective exercise of the right of peaceful assembly, undermining the presumption of peacefulness of assemblies, while potentially overlooking the negative obligations of state authorities not to intervene. International human rights law requires authorities to respect and facilitate peaceful assemblies, and any surveillance measures that interfere with protected rights must have a sufficient legal basis and meet applicable requirements of necessity and proportionality. The indiscriminate mass surveillance of protesters can never be justified.

In short, surveillance technologies profoundly alter the environment in which protests take place, changing the way in which we understand the role of policing, the use of public space, and the exercise of the right to peacefully assemble.

The report bears testament to the human rights risks associated with surveillance, yet also shows how independent monitoring can contribute to transparency, accountability and the effective protection of the right of peaceful assembly. It is my hope that the report will inspire civil society actors to explore new methodologies for monitoring the policing of protest, and in so doing, to document the nature of surveillance practices, to identify and assess the chilling effects and to contribute to informed scrutiny of surveillance policies, procurement and deployment decisions.

Michael Hamilton
Co-Chair of ODIHR's Panel of Experts on
Freedom of Peaceful Assembly and Association

Executive Summary

Surveillance and digital interference

The rapid advance of digital technology and its growing deployment into protest policing has significant implications for the freedom of peaceful assembly. At the same time, new surveillance tools and practices have changed the nature of policing. These technologies offer law enforcement unprecedented potential to track, monitor and identify participants at assemblies. In short, despite their resemblance to existing tools, today's advanced surveillance technologies represent a step change in the ability, scope and scale of law enforcement capability. This report details how effective monitoring of surveillance tools is becoming increasingly challenging, and it demonstrates that the need to hold these powerful systems and their uses to account has never been more important.

Assembly monitoring and digital surveillance

Civil society organizations have developed a range of monitoring strategies to respond to this new surveillance landscape. Drawing on the first-hand experiences of assembly monitors, a survey of OSCE participating States (pSs) and other data sources, this report outlines the various strategies that have been developed to meet this challenge, including direct field observations, administrative procurement tracking, scrutiny of criminal justice proceedings and strategic network building. Significant obstacles to effective monitoring remain. These include the growing invisibility of modern surveillance, legislative ambiguity and instances of physical intimidation or even violence by police forces.

Recommendations

The report concludes with seven recommendations to support pSs and international organizations in supporting the work of assembly monitors and legal observers, developing public trust and confidence in pSs' use of these technologies, and promoting the facilitation of assembly. The recommendations are:

1. **Recognize and preserve the status of monitors.** International frameworks recognize the right to monitor assemblies freely, yet adherence is inconsistent across jurisdictions.

2. **Facilitate monitoring and ensure the safety of monitors and their equipment.** States should implement concrete measures to protect monitors from harassment, violence and equipment confiscation.

3. **Ensure transparency and develop meaningful democratic oversight of surveillance technologies and their use.** Effective monitoring requires public accountability, independent oversight bodies and transparency across the entire surveillance lifecycle.

4. **Adhere meaningfully to legal disclosure obligations.** States need better processes for transparent disclosure, avoiding blanket refusals based on operational secrecy.

5. **Foster constructive dialogue and the pursuit of de-escalation strategies.** Dedicated police liaison roles can improve communication with civil society, de-escalate conflict and increase safety and accountability.

6. **Establish consistent mechanisms to ensure that the deployment of surveillance at assemblies is aligned with established standards of international human rights law.** Aligning surveillance use with the establishment of an adequate and explicit legal basis, and ensuring necessity and proportionality claims are properly substantiated, would support the responsible and accountable use of these technologies.

7. **Establish a requirement to evidence public safety and national security justifications for surveillance.** States must properly evidence vague national security claims without compromising genuine operational confidentiality, exploring the possibilities that exist in this regard.

Introduction

The advance of digital technology has brought profound changes to the facilitation of assemblies. Driven by artificial intelligence (AI), advanced image analysis and automated data processing, today's surveillance tools offer unprecedented capability, scope and reach. These technologies are fundamentally changing the landscape of law enforcement and hold significant implications for the freedom of peaceful assembly. Authorities are now furnished with unparalleled capacities to trace, observe, recognize and connect individuals assembling in public or online. It has become easier to penetrate the most intimate spheres of life, extract increasingly fine details of an individual's activities and retain information indefinitely. Remote identification tools have subtly, yet significantly, altered police-citizen relationships, the dynamics of suspicion and the possibility of remaining anonymous in public. This growth has been driven further by diminishing barriers to the procurement and deployment of these technologies. Respectively, these include the continued cheapening of technological components alongside significant gaps and limitations in applicable regulatory frameworks. At the same time, advances in edge computing, interoperability and data harmonization have allowed seemingly unconnected devices to become co-opted into law enforcement tools. These include data derived from personal consumer electronics, vehicles and 'smart city' digital infrastructure designed for urban management.

The rapid growth in the scale and scope of today's surveillance technologies contrasts sharply with their declining visibility. Biometric surveillance tools now establish identities remotely. Social media monitoring is often invisible to those subjected to it. Increasingly, law enforcement data is processed at times and in places far from when and where it was collected. In some cases, images of assembly participants are analysed years later by technologies that did not exist at the time of capture, as the now routine use of retrospective facial recognition (RFR) demonstrates.

These developments underline the important role assembly monitors have in holding authorities and their use of such technologies to account. Yet monitoring these activities is undeniably difficult. This report draws on the first-hand experiences of legal observers and assembly monitors who routinely confront this challenge. Supplemented by analysis of other documentary sources and, separately, response data from a bespoke survey addressed to pSs, the report identifies the various strategies that have been developed to monitor the use of surveillance before, during and after assemblies. These include direct field observations, administrative procurement tracking, scrutiny of criminal justice proceedings and strategic network building. Significant obstacles to effective monitoring persist and include the growing invisibility of modern surveillance, legislative ambiguity, and instances of physical intimidation and violence by police forces. The report concludes with seven recommendations to support pSs and international organizations in supporting the work of assembly

monitors and legal observers, developing public trust and confidence in pSs' use of these technologies, and promoting the facilitation of the right to peaceful assembly.

Methodology

This report is grounded in empirical enquiry, using established social science and socio-legal research methods. Semi-structured interviews were conducted with 20 legal observers and assembly monitors operating in 16 OSCE pSs,[1] two of whom work in international non-governmental organizations (NGOs). Thirteen were male and seven were female. Further written responses from civil society organizations, operating in three different countries in the OSCE were also received. A survey was also sent to the delegations of all OSCE pSs, and ten responses were received.[2] Text-based document analysis of relevant legislation, legal rulings, public policy and civil society materials was also conducted. Country-specific examples illustrate practices and concerns reported to ODIHR or identified through the sources reviewed.

1 Armenia, Belarus, Bosnia and Herzegovina, Finland, France, Georgia, Kazakhstan, Moldova, Poland, the Russian Federation, Serbia, Spain, Türkiye, the United Kingdom, Ukraine and the United States.

2 Responses were received from representatives of Andorra, Germany, Liechtenstein, Lithuania, Serbia, Slovenia, Spain, Sweden, Switzerland and Türkiye.

1. The right to peaceful assembly: standards and monitoring in practice

The freedom of peaceful assembly is a foundational element of democratic societies and a prerequisite for the full realization of civil, political, economic, social and cultural rights. The foundational articulation of the right, and its universality, is codified in Article 20(1) of the Universal Declaration of Human Rights.[3] This principle acquired binding international legal status through the International Covenant on Civil and Political Rights (ICCPR) in 1966.[4] The normative scope of this right encompasses a wide range of activities, including stationary protests, moving marches, sit-ins, strikes and, more recently, online and other digitally-enabled gatherings. States' obligations extend significantly beyond non-interference with assemblies. They involve positive obligations to facilitate assemblies, protect participants and ensure the safety of third-party monitors. International standards also recognize how obstacles to participation in assemblies are not experienced equally and are highly conditioned by intersectional forms of discrimination and disadvantage. For example, the United Nations General Comment No. 37 on Article 21 (Right of peaceful assembly) (GC37)[5] requires states to pay particular attention to "race, colour, ethnicity, age, sex, language, property, religion or belief, political or other opinion, national or social origin, birth, minority, indigenous or other status, disability, sexual orientation or gender identity, or other status".[6] It places further obligations to:

> "Ensure the equal and effective facilitation and protection of the right of peaceful assembly of individuals who are members of groups that are or have been subjected to discrimination, or that may face particular challenges in participating in assemblies. Moreover, States have a duty to protect participants from all forms of discriminatory abuse and attacks".[7]

Unless compelling and verifiable evidence exists to assert the contrary, states also have an obligation to presume assemblies are peaceful in nature. Moreover, the presence of

3 Universal Declaration of Human Rights, United Nations, 10 December 1948.

4 International Covenant on Civil and Political Rights (ICCPR), United Nations, General Assembly resolution 2200A (XXI), 16 December 1966, Article 21.

5 General Comment No. 37 on Article 21 (Right of peaceful assembly), (GC37) UN Human Rights Committee, CCPR/C/GC/37, 17 September 2020. It is an authoritative interpretation of Article 21 of the ICCPR, clarifying the scope of the right of peaceful assembly and the obligations of States Parties in this regard.

6 *Ibid.*, para. 25.

7 *Ibid.*, para. 25.

non-peaceful, violent or disruptive elements within an assembly does not justify the designation of an entire assembly as such.[8] This distinction is important when considering the role of surveillance at assemblies. Also important is the principle that the disruption of ordinary life is an inherent feature of collective mobilization and, therefore, cannot provide an automatic justification for state interference, intensified surveillance or the dispersal of an assembly.[9]

These universal instruments establish an international standard for freedom of assembly. Several regional and intergovernmental organizations provide specific statutory frameworks and judicial mechanisms in this area. Relevant here are initiatives by the OSCE Office for Democratic Institutions and Human Rights (ODIHR) and, given the geographic spread of OSCE pSs, those of the Council of Europe.

The OSCE provides a framework for the protection of peaceful assembly across its 57 pSs. The framework is grounded in the 1990 Copenhagen Document and reinforced by other declarations, including the 1989 Vienna Document, the 1990 Charter of Paris for a New Europe, the 1999 Istanbul Summit Declaration and the 2008 Helsinki Ministerial Declaration.[10]

To operationalize these standards, in 2020, ODIHR and the Council of Europe's Venice Commission[11] jointly published the *Guidelines on Freedom of Peaceful Assembly*, which contain guidance for law enforcement on how to align domestic law and policy with international human rights standards.[12] The *Guidelines* are built around several principles and obligations to inform how pSs should facilitate assemblies. These include:

- Establishing a presumption in favour of assemblies;
- The positive obligation to facilitate them;
- Principles of legality and proportionality to govern any restrictions placed on gatherings;
- The promotion of equality and non-discrimination;

8 *Ibid.*, para. 27.

9 Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests, (A/HRC/55/60), Report of the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, 31 January 2024, developed with OHCHR and UNODC pursuant to Human Rights Council resolution 50/21.

10 Respectively, Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE (Copenhagen Document), CSCE/OSCE, Copenhagen, 29 June 1990; Charter of Paris for a New Europe, CSCE, Paris, 21 November 1990; Istanbul Document, OSCE, Istanbul, 19 November 1999; and Ministerial Declaration on the occasion of the 60th anniversary of the Universal Declaration of Human Rights, OSCE, Helsinki, 8 December 2008.

11 The Venice Commission is also known as the Council of Europe's European Commission for Democracy through Law.

12 Guidelines on freedom of peaceful assembly (3rd edition), Venice Commission and OSCE/ODIHR, 8 July 2019.

- Prohibiting the conflation of notification with authorization;
- Availability of remedies; and
- The development of rights-respecting legal definitions of terms such as 'peaceful' and 'assemblies'.

The right to monitor assemblies

The right to monitor assemblies is recognized in several international instruments. For example, GC37 sets out the importance of, and requirement for, protecting assembly monitors as follows:

> "The role of journalists, human rights defenders, election monitors and others involved in monitoring or reporting on assemblies is of particular importance for the full enjoyment of the right of peaceful assembly (…). They may not be prohibited from, or unduly limited in, exercising these functions, including with respect to monitoring the actions of law enforcement officials. They must not face reprisals or other harassment, and their equipment must not be confiscated or damaged. Even if an assembly is declared unlawful or is dispersed, that does not terminate the right to monitor."[13]

In their inaugural report in 2012, the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai, also noted how assembly monitoring is both a "valuable contribution to the effective enjoyment of the right to peaceful assembly" and that the presence of monitors not only brings accountability, but also "can deter human rights violations".[14] Assembly monitoring also interconnects with the enjoyment of several other rights, notably the general human right to receive and impart information, which exists as a corollary of the right to freedom of expression enshrined in the 1989 Vienna Document and the 1990 Copenhagen Document.[15] Assembly monitors are non-participant, third-party individuals or groups. Their objective is to observe, record and document the actions and activities taking place at public assemblies. ODIHR has actively monitored public assemblies across the OSCE region since 2011 and produces touchstone guidance for assembly monitoring.[16]

13 UN, General Comment No. 37 on Article 21, para. 30; see also para. 74.

14 UN Special Rapporteur, Model Protocol.

15 CSCE, Copenhagen Document; Concluding Document of the Third Follow-up Meeting (Vienna Document), CSCE, Vienna, 19 January 1989.

16 Handbook on Monitoring Freedom of Peaceful Assembly (Second Edition), OSCE/ODIHR, 11 December 2020.

The purposes of assembly monitoring

Assembly monitoring pursues several strategic, legal and protective purposes. These activities, and their success, are also contingent on many factors. These include specific political contexts, the positioning and capacity of organizations and the activities of law enforcement agencies and individuals. Interviews with assembly monitors active in different jurisdictions highlighted the following categories of objectives:

Documenting police conduct and ensuring accountability

A common rationale for monitoring across many regions is to observe and document police behaviour. Specifically, this focuses on scrutinizing the use of force and illegal arrests, and verifying if police actions are necessary and proportionate. A core focus for monitoring also involves documenting discrimination and intersectional harms, including discriminatory stop-and-search practices and online harassment directed against gender equality and LGBTI advocacy. Observations are conducted in order to facilitate the initiation of litigation and lodging of formal complaints, and for public communication and reporting strategies, through which monitors and organizations aim to hold law enforcement accountable.

Monitoring discriminatory and intersectional restrictions on the right to freedom of peaceful assembly

Monitoring takes place to identify differential and potentially discriminatory restrictions on assemblies. This issue is additionally relevant to restrictions justified on the basis of protecting 'morals'[17] or 'public safety' (for example, through the reported politically motivated or inappropriate application of 'hate speech' restrictions).

Monitoring surveillance technologies and digital coercion

This form of monitoring documents the use and impact of policing technologies and emphasizes visible forms, such as on-street surveillance cameras and biometric identification technologies, including facial recognition, as well as more remote technologies such as spyware and cyber patrolling.

Legal defence and strategic litigation

Assembly monitoring gathers evidence as a foundation for litigation. Organizations use findings to defend individual protesters against extra-procedural uses of force and other violations, or to pursue systemic changes through strategic litigation or judicial review. This rationale has been used particularly by legal observers operating in the United States (US), the United Kingdom (UK) and the Russian Federation.[18]

17 UN, GC37, para. 46.

18 Interview 8; Interview 9; Interview 11.

Assessing international standards alignment and influencing legislation

Assembly monitoring also involves tracking legislative processes to highlight legal initiatives that may contravene the freedom of peaceful assembly. For example, in Bosnia and Herzegovina, monitoring is used to assess whether new human rights-compliant legislation is implemented in practice, as well as to examine the alignment of domestic laws with international standards.[19] In Kazakhstan, monitors evaluated police behaviour in relation to "international standards (…) OSCE/ODIHR guidelines (…) [and] UN Human Rights Committee General Comment 37. We're making analysis of [domestic] law... to look at how legislation meets international standards".[20, 21]

Correcting public narratives and raising awareness

Assembly monitoring supports the publication of findings to notify (and mobilize) the public about abuses and to inform them of their rights. Material acquired through first-hand monitoring is frequently used to challenge or verify public statements or narratives issued by law enforcement agencies and aims to promote the accurate documentation of events.[22]

Establishing deterrence and promoting solidarity

Some monitors stressed that monitoring often serves a vital end in itself, as the physical presence of independent observers acts as a deterrent to excessive use of force. The physical presence of monitors can also be a way to express solidarity with participants.[23]

19 Interview 4.

20 Interview 7.

21 The most commonly cited international guidance documents and handbooks were the OSCE/ODIHR Handbook on Monitoring Freedom of Peaceful Assembly; The Right to Monitor Assemblies in the OSCE Region: Experiences from the Field, OSCE/ODIHR, 7 October 2024; Guide on Law Enforcement Equipment Most Commonly Used in the Policing of Assemblies, OSCE/ODIHR, 2 July 2021; and Guidelines on The Right to Freedom of Peaceful Assembly, Amnesty International, 27 November 2024.

22 Interview 14.

23 Interview 9.

2. Strategies for monitoring surveillance and human rights concerns surrounding assemblies

The assembly monitors interviewed for this report highlighted the wide range of strategies they deploy when attempting to monitor the use of surveillance technologies at protests. These have been organized into six categories.

Direct observation

Most obvious was the direct monitoring of technologies being deployed at assemblies.[24] At its most fundamental level, this activity involved expected strategies of "taking notes, videos, photos [and] collecting this evidence of tools we detect".[25] Furthermore, in a variation of this approach, "taking photos of them taking photos, videos of them taking videos (…) from as many angles as possible".[26] This interviewee offered a concrete example:

> "In June 2024, (…) when they used stun grenades, the police were saying that [these] were used because of the violent crowd. Fortunately, we had several angles of the videos. We just proved (…) there was absolutely no violence. (…). They deliberately threw the stun grenades directly into [groups of] unarmed protesters and journalists (….)."

Another successful strategy involved looking beyond the specific devices and tools to document who the police were monitoring:

> "You can observe concretely, in terms of [how] you can see them focusing on a particular incident, or you can see them following a particular individual. And that individualization, I think, is maybe one of the most significant things."[27]

24 Sometimes referred to as 'sousveillance'.

25 Interview 6.

26 Interview 1.

27 Interview 9.

This form of monitoring was often a standalone activity. For example, direct monitoring served as an initial, first-hand verification of practices, which could also inform further requests for accountability or future complaints.[28]

Monitoring covered both the existence and application of technology; often to understand whether such use breached regulations. For example, aspirations for European Union (EU) membership in Bosnia and Herzegovina led to the consideration of how policing practices could be adapted and aligned to international data protection standards. Assembly monitoring strategies were key to understanding these processes:

> "As an example, we had the draft law in one of the cantons [governing] police operations [at protests]. This provided for the police to use recording equipment. But it had no further qualification for what purposes; [if it was] for investigation purposes, or for maintaining public order, or any other clear justification (…). [We learned of] the [inconsistent] awareness about data protection law, [how it is] aligned with the GDPR, and the higher accountability for protecting personal data."[29]

Remote and online monitoring often involved accessing and analysing open-source intelligence (OSINT). This included social media monitoring, watching live streams, cross-checking media reports and verifying information via other online sources. These techniques were more prominent in situations where physical presence was unsafe or inaccessible, when monitors were exiled or when organizations were under-resourced.

Pre-protest communication and stakeholder engagement

Several assembly monitors emphasized the advantages of proactive communication with law enforcement agencies and, separately, with protest organizers. Some reported extremely positive encounters of this nature. For example, in Ukraine, monitors highlighted how dialogue with all sides of an assembly helped to protect monitors and secure access to critical information.[30] Others highlighted how such interactions were useful for establishing independent observer status at events and cultivating a recognized presence with law enforcement in advance. In these cases, it also reduced the vulnerability of monitors

28 Interview 10.

29 Interview 4.

30 Interview 17.

to police use of force, "so they treat us the same way, don't assault us or confiscate our equipment".[31]

Across the OSCE, monitoring strategies are shaped by the prospect of police violence. Monitor safety was also an important consideration, for example, when counter-demonstrations occurred, as in one case of a "far right counter-demonstration, [when] police [attempted] to separate them and prevent clashes".[32] In this and other respects, establishing a distinctive and separate presence was considered essential with regard to relations with protesters. This was important to mitigate suspicions if filming the crowd, when:

> "[Neither] the police nor the protestors are your friends. [Protesters] also wonder what you're doing there; why you're recording (…). So, there is some pedagogy required, some explanation to do beforehand with the protestors or the leader of the protests."[33]

Another aspect concerns the shifting relationships between police and monitors. In many cases, monitors maintained relationships with individuals rather than institutions. Individuals within organizations regularly changed roles, leading to challenges in maintaining consistent relations. In other respects, internal restructuring and refocused priorities within police organizations inhibited dialogue. For example:

> "We can't choose who we meet if we ask for a meeting (…), [and] last year, this unit force disbanded (…), the person in charge of this unit left the police force and gave critical comments on the police tendencies to [avoid such] preventive work."[34]

This also highlights the importance of law enforcement organizations establishing single point of contact roles, such as those that exist in other areas of policing.[35] These posts would remain even if individuals move on. Added to this, the tone of relationships varied and were particularly sensitive to shifts in political climate. For example:

31 Interview 14.

32 Interview 6.

33 Interview 14.

34 Interview 6. Also expressed in Interview 5.

35 For example, EUROPOL has established 'Single Point of Contact' designations for key liaison roles related to the reacquisition of communications data. These roles remain regardless of individual career paths. This idea could be adapted for the purposes discussed here.

> "In practice, I think the police are quite approachable (...). But, in general, I think the trend is moving more and more to the stricter side. And we have seen it in demonstrations as well. For instance, when we look at climate demonstrations by Extinction Rebellion a few years ago, they could be having a street blocked for an hour (…), and the police would negotiate (….). They don't now (…). They are more focused on prohibiting, or getting rid of the [assembly]."[36]

These experiences also reflect a deeper concern affecting similar dialogues between protest organizers and law enforcement agencies — the way the 'notification of' an assembly can become conflated with 'permission for' an assembly.[37]

Assembly monitors noted how, when holding such dialogue, technological and legal literacy conferred several advantages:

> "In 2021, for example, there was an issue with illegal recording. [The] police are supposed to announce it [in advance]. We went public with that. And the police [subsequently] started announcing the recordings. So, they listened to us and changed their practices."[38]

In the UK, monitors considered that technical and legal knowledge helped gain insight when confronted by evasive responses to specific questions:

> "And [we are] able to see what's being concealed by the absence of response on key technical aspects [of surveillance]. So, we asked them quite technical questions [so] that they've answered everything. Literally, like everything. But the only answer [was this]. It really wasn't anything controversial (…). When there are things they are hiding, they don't answer. They label it as a secret or something like that."[39]

36 Interview 6.

37 UN Special Rapporteur, Model Protocol. For a critique of how notification can also be used to legitimize restrictions on the right to peaceful assembly, see Michael Hamilton, "(Un)Governing Assembly: A Manifesto for Voluntary Notification" in Tabatha Abu El-Haj, Michael Hamilton, Thomas Probert and Sharath Srinivasan (eds), *The Oxford Handbook of Peaceful Assembly*, (Oxford: Oxford University Press, 2024).

38 Interview 5.

39 Interview 9.

Monitoring surveillance in criminal justice procedures (especially trial and detention)

Because many surveillance practices are invisible on the streets, they may only become detectable in post-protest bureaucracy, for example, in judicial and administrative processes. Accordingly, monitors highlighted the value of examining judicial and criminal justice processes, particularly with respect to indictment and evidence presentation that may reveal distinct surveillance practices. This also became a valuable approach in contexts where public protests were heavily restricted. Associated strategies included documenting detentions, monitoring criminal court proceedings, recording disclosures from prosecuting bodies and accessing legal case files. For example, an account of surveillance monitoring in the Russian Federation highlighted: "In terms of surveillance, what we do now is get info from court systems and other work of lawyers. This is quite effective, because we can see how the bureaucracy works."[40] A particularly effective strategy involved tracking responses to minor transgressions.[41]

Similarly, one legal observer focused on Georgia noted how, ["Upon observing evidence presented to court,] recordings [have revealed the use of] face recognition camera recording and [how it] has [been a] very important force in finding people and in their conviction"[42] following protests. This technique was also used to monitor other forms of surveillance. For example, in Türkiye, monitors noted:

> "WhatsApp and other types of communication tools, we now understand that these are also being surveilled. Because the content of the dialogue of those apps is included in court documents (…), we're collecting all this information from the indictments, so we can have a proactive monitoring strategy."[43]

Consistent with other accounts, technical literacy within civil society groups has proved advantageous for uncovering undeclared forms of surveillance. For example, assembly monitors reported how numerical data stamped into video surveillance footage indicated a high likelihood that the images had been analysed with facial recognition technology.[44] Court documents were also used to identify legal loopholes and likely extra-procedural uses of surveillance. For example, a common concern over the covert use of surveillance technologies was that of 'parallel construction'. In its simplest form, this involves the illegal

40 Interview 8.

41 Interview 1.

42 Interview 15.

43 Interview 3.

44 Interview 8. For example, video footage often includes text-based data such as time and date stamps. Additional numerical data added to video can reveal the types of technology used.

— and therefore inadmissible — use of surveillance to generate investigative leads. Once suspicion is established, more conventional means are used to gather evidence that would be admissible in legal proceedings. The account below highlights how court observations were used to compensate for the absence of meaningful surveillance oversight. In this case, surveillance footage was the only evidence offered in the court:

> "[We attend court to discover] how procedures are presented (…); how they [the authorities] identified that person. When we applied to the Data Protection Service, we wanted our questions answered. We haven't had any answer. Our lawyers tried to address the courts and ask the judge to scrutinize the legality of [this surveillance] evidence; whether the person who analysed the images had the authorization to do so; whether the grounds on which they got the authorization was legal. The issue of obtaining evidence when it comes to administrative offences is not well regulated, [but] the courts refuse to take [due process] into consideration. They basically just take a recording for what it is, and don't really consider how [the footage] was obtained, or whether it was legal or proportionate."[45]

In this case, the approval of warrants requesting footage within highly specific time frames revealed extra-procedural uses of surveillance. "It is also curious that (…) the letters [requesting footage] (…) had very specific times, like, hours and minutes. [This] indicated that they were, from the very start, targeting a certain person [who] would appear at that very specific time on camera, even before 'seeing' the footage."[46]

Monitoring administrative processes

Many assembly monitors reported the benefits of analysing administrative processes for the procurement and use of surveillance technologies. Examination of tender processes and documentation were considered valuable. Other practices involved, "look[ing] at everything from manufacturing, trade and through to use (…). Looking for journalistic articles on incidents and then following through to see if there are investigations and prosecutions etc.".[47]

In Georgia, scrutinizing tender documentation revealed that police had purchased cameras with facial- and emotion-recognition capabilities: "[We] tracked down the model and number

45 Interview 15.

46 Interview 15.

47 Interview 16.

of the cameras. [We] basically saw that the online description of the model included face-recognition and emotion-recognition capabilities."[48] Monitors active in Serbia felt that limited state compliance with disclosure obligations required a change in strategy. Here, a decision was made to depoliticize the request with questions about technical details:

> "In the past, tenders were quite transparent, to the point we could search them online (...). Things have really worsened since then, and it depends on what type of questions we ask. Do we ask them general questions about the use of force at protests, the number of people up here, etc.? They answer, and their information is quite perfunctory. But when (…) we asked them technical questions, (…) they've answered everything, literally, like everything, but [only perhaps] because [there] really wasn't anything controversial about it."[49]

Legal observers also used administrative processes to expose how police bypass warrant requirements by purchasing location data from third-party brokers (e.g., 'Webloc' in the US). Most observers reported using longstanding disclosure tools such as freedom of information (FOIA) requests and subject access requests (SAR) for these purposes. Others highlighted repeated frustrations with disclosure processes such as FOIA and SAR requests,[50] citing a range of concerns, including the absence of responses, excessive redactions, blanket rejections on the grounds of public security and the absence of appeals or oversight mechanisms. (See Section 6)

Nevertheless, monitors highlighted that accurately targeting and focusing such requests was critical for improving the likelihood of successful disclosure applications. This included considering the level of governance (e.g., local, state, national bodies) or doing groundwork to identify the best-placed recipient for requests. For example:

> "Under our records laws, if a federal agency enters into a contract with a local or state agency that is now part of that state or local agency's normal operations, you have access to that, even though a federal entity is involved. So, if I'm trying to get information on immigration, I don't have to go through ICE. I don't have to send [them] an FOIA [request]. I can send it to my local or state agency."[51]

48 Interview 15.

49 Interview 5.

50 Interview 4, among others.

51 Interview 11.

Others again emphasized the value of technical knowledge and specific detail. In cases of global providers or multinational uses of a specific technology, another strategy involved using FOIA requests in jurisdictions with stronger accountability mechanisms.[52] Others highlighted how a repository of questions that police refuse to answer may have value for advocacy. As one monitor suggested: "Whenever there is some corruption, they basically hide it under the way of secrecy."[53] (See Section 6)

Building strategic networks

Organizations rely heavily on media partners to support their monitoring activities. The following account is representative of a general sentiment, where journalists offer a dual supportive function. They assist in accessing information, and they can amplify specific issues to wider audiences: "When there are issues at protests, the media has been a good ally in getting information out (…). You can put together a press release and pretty much rely on certain types of agencies or reporters, or like the AP [Associated Press], to get the information out to the masses."[54] Others commented on how their work became more effective as public interest grew in their specific area of advocacy. This also highlights the value and importance of effective collaboration with journalists.

Monitoring was also enhanced through building networks with other activists, both regionally and internationally. The ability to build coalitions around different capabilities, skills and capacities was seen as particularly effective.[55] Such coalitions also allowed organizations to collect verified, first-hand data about surveillance. This enhanced their ability to focus observation activities more effectively on specific issues, locations and contexts. Here, coalitions help to "collect cases of mass surveillance (…); help us to better adapt our observation mechanisms to the realities and the needs on the ground" and allows organizations to "demand explanations from the responsible governments and police forces, as well as to take legal action or file complaints if necessary".[56] Coalition building was consistently highlighted as vital for exiled observers and other activists.[57]

In addition to better awareness and effective resource mobilization, coalitions are also useful for other areas of mutual support. These include pooling digital hygiene capabilities (see below) and mutual psychological support.[58]

52 Interview 5; Interview 6; Interview 11.

53 Interview 5.

54 Interview 11; also Interview 8.

55 Interview 10.

56 Interview 10.

57 Interview 8.

58 Interview 14.

Other monitoring organizations enhanced their capacity through alliances with legal aid providers. For example, these bodies:

> "Actually go to court and help people, and look through the materials (…) and [fulfil a] kind of watchdog [function]. [This] knowledge, paired with actual groundwork in court, litigation, seeing the materials and [so on], reinforces itself and helps us (…) [when] we don't really have the information to [develop] definitive conclusions, but at least have to know what kind of concerns and questions to have."[59]

Interviewees also noted that collaboration with external oversight bodies and regulators, where possible and appropriate, could be valuable. This collaboration worked in a similar way to that with journalists, with respect to identifying key issues and amplifying advocacy efforts.

Digital hygiene and cybersecurity

The stakes for digital hygiene are high. Several organizations stressed how "cyber security is the number one thing".[60] This applies to individuals and entire organizations, as well as wider networks, including donors and beneficiaries, "because donors often have much more sensitive information than intermediaries".[61] Cybersecurity is seen as a collective endeavour and a basic requirement to function. This is particularly relevant for civil society actors working across jurisdictions:

> "Everybody who works with Belarus or repressive contexts like this, on all sides, should have a high enough level of cyber security and awareness of the context that we're working with. So, you cannot be demanding people in Belarus you're working with to send you [information] on secure channels (…), because (…) when your phone is physically taken by the police, if you didn't have a self-delete function, the fact that you're encrypted (…) doesn't mean you're insulated from the people who physically take your phone and make you unlock it [to reveal] your encrypted messages."[62]

59 Interview 15.

60 Interview 12.

61 Interview 12.

62 Interview 12.

The inability to be certain about the level of compromise across multinational networks elevates the necessity for "cyber security, on all ends, for all actors".[63] Breaches of cybersecurity can have devastating consequences for activists. For example, one observer highlighted:

> "(…) prosecutions like the Belarusian Hajun case (…) [involving a] chatbot, where people sent information about the movement of Russian equipment, Russian troops in Belarus and so on. Helping to document the war that's not talked about very openly. Because of [infiltration of] the Telegram boards (…), people were identified. And now more than 100 people[64] are defendants in the case (…), and a lot of them are already in prison. And more will be in prison, because they were de-anonymized by a hack. So that's the biggest threat (…). Of course, [cybersecurity is] the priority."[65]

63 Interview 12.

64 175 confirmed defendants according to One year of mass persecution for reporting Russian military movements, Viasna, 6 February 2026.

65 Interview 12.

3. Technological expansion: the legitimate use of and justifications for assembly surveillance

International human rights law acknowledges that the right to freedom of peaceful assembly is not absolute. According to Article 21 of the ICCPR, states hold the authority to place restrictions under strict conditions and in the interests of "national security or public safety, public order (*ordre public*), the protection of public health or morals or the protection of the rights and freedoms of others".[66] GC37 dictates that this list of five grounds is "exhaustive".[67] Moreover, the legal threshold for any modification of the right is high and, as stated in Article 21 of the ICCPR, any restrictions must be "in conformity with the law and which are necessary in a democratic society". These parameters for limitations essentially follow the requirement to satisfy a cumulative, rigorous, three-part test for any restrictions. They are elaborated by the 1984 ICCPR 'Siracusa Principles' and in jurisprudence across the OSCE region.[68] Variations exist but, essentially, this involves:

- **Prescribed by law:** Limitations must be formally codified in domestic law, be non-arbitrary and contain adequate rights safeguards. Vague and poorly formulated provisions that grant significant discretion to law enforcement typically fall short of this test.
- **Legitimate aim:** Limitations must service one of the grounds listed in Article 21 of the ICCPR — i.e., the protection of national security, public safety, public order, public health or morals, or the protection of the rights and freedoms of others.
- **Necessary in a democratic society:** To satisfy the necessity test, limitation measures need to be proportionate to the legitimate aim pursued.

Also relevant is how this three-part test also applies to limitations of other rights through the deployment of surveillance technologies. For example, directed surveillance operations inevitably breach the right to privacy of targeted individuals. Such infringements of the right would therefore only be permissible subject to the above test. This is one of many reasons why the 'nothing to hide, nothing to fear' argument holds no legal substance. Typically for surveillance, considerations of necessity also emphasize the possibility of using less intrusive means to pursue the same legitimate aim and focus on the time-limited nature of such restrictions. Also germane to this discussion as assemblies evolve, is that the same surveillance tool may 'creep' from one purpose to

66 UN, ICCPR, Article 21.

67 UN, GC37, para. 41.

68 Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR, American Association for the International Commission of Jurists, April 1985.

another, for example, from 'public safety' to 'public order'. Under the process outlined above, such changes would require a separate justification under the three-part test.[69]

Justifications for the surveillance of assemblies

States and law enforcement agencies justify the uses of such surveillance tools on several strategic, tactical and operational grounds. These include:

Facilitation of assemblies

In their responses to the survey, pSs consistently highlighted the role of surveillance technology for facilitating protest. The most cited specific purpose in this regard was for the maintenance of 'public safety'.[70] While some did not make an explicit link between how a particular measure would fulfil any defined purpose, the perception that these tools were valuable for public safety was consistent. For some, this related to an apparent belief in the inherent value of technology:

> "Police officers responsible for security during demonstrations carry individual video surveillance cameras that they can activate at any moment if they need to intervene or engage with individuals within the demonstration. Additionally, when necessary, a drone camera (unmanned aerial vehicle operated by remote control) may also be used, operated by agents specialized in its use."[71]

Others claimed further benefits existed for assembly participants. "These tools allow activists to take control of their narrative; connect with global audiences."[72] Where detail was offered, the 'public safety' arguments can be broken down into several purposes. One was in monitoring crowd density and supervising access to, and egress from, assembly sites:

69 This is elaborated in OHCHR Report 2023, United Nations, 30 May 2024.

70 It is important to restate that this survey of pSs yielded a small sample size. No claims are, or could be, made over how generalizable these accounts are for other pSs' practices.

71 Survey response from Andorra.

72 Survey response from The Public Order Bureau of the Police Department under the Ministry of Interior and Human Rights Department, Ministry of Foreign Affairs, Republic of Lithuania (hereafter 'Lithuania').

> "The necessary security measures are being taken to ensure the safety of the crowd and to enable them to enter the venue [in a] more orderly [way] for the peaceful protest and action/event to be organized, as notified to the relevant civil authorities."[73]

Other pSs emphasized the protection of participants from violence and disorder, as in the case of drone use in Sweden where: "The police may use UAS [Unmanned Aerial Surveillance] for real-time monitoring of demonstrations and other protests to monitor crowds, to detect risks, such as potential clashes or violence, allowing for early intervention [and to] ensure safety."[74] Some highlighted the use of technologies more generally for communication and crowd direction: "Loudspeaker vans or loudspeaker backpacks, for example, can be used to inform and guide participants in order to help the police ensure that an assembly runs smoothly."[75] Representatives from Lithuania widened this framing, stating: "The technologies are used to facilitate, organize and amplify peaceful protests by enabling rapid communication, co-ordinating logistics, documenting events and mobilizing supporters."[76]

'Situational awareness' and crowd control

Typical examples of these justifications for surveillance include the use of drones and other cameras to gain a wider picture of an assembly (situational awareness), in order to assess matters such as crowd density and the deployment of finite police assets. In Ukraine, for example, the same law enforcement officers routinely rotated through civic, military and humanitarian roles. Online and offline surveillance tools were claimed to be a way of managing scarce police resources.[77]

Public surveillance operations are routinely justified in terms of public safety. Advanced surveillance measures undertaken for public-safety purposes may nevertheless interfere with protected rights and therefore require an appropriate legal basis and safeguards. Given the remote, and often less visible, nature of such technologies, adequate transparency concerning their purpose and use is particularly important to mitigating potential chilling effects for assembly participants.[78] Meaningful dialogue between surveillance users, organizers and participants can further contribute to transparency and public confidence.

---

73 Survey response from Türkiye.

74 Survey response from Department of Justice, Sweden (hereafter 'Sweden').

75 Survey response from Permanent Mission of the Federal Republic of Germany to the OSCE (hereafter 'Germany').

76 Survey response from Lithuania.

77 Interview 17.

78 See Section 6 and for elaboration on this theme, Gina Romero, Pete Fussey and Daragh Murray, "Pushed into the Shadows": Evidencing Digital Surveillance Chilling Effects and the Erosion of the Rights to Freedom of Assembly and of Association, UN Human Rights Council, 13 May 2026.

A further risk associated with the public safety justification is the potential for surveillance creep. Investigative and other law enforcement surveillance activities should be distinct from monitoring crowds for public safety purposes. Assembly monitors routinely experienced instances where crowd-safety justifications were reportedly used to enact more directed and intrusive surveillance. For this reason, general and undefined public safety justifications are often inadequate as a general authorization for surveillance practices.

Pre-emptive targeting and investigation

In the context of facilitating peaceful assemblies, law enforcement agencies commonly justify surveillance operations in terms of 'policing need' and the targeting of violent or disruptive elements. Security and law enforcement agencies routinely actively monitor online spaces for these purposes. Several challenges exist here. For example, the covert nature of such operations brings a heightened risk of surveillance creep. From an accountability perspective, such activities are seldom available for external scrutiny, and the auditability of police decision-making is difficult to secure. Added to this, the police intelligence used to underpin such operations is rarely available for scrutiny by outsiders and oversight bodies.[79]

Retrospective identification and prosecution

The use of surveillance for the retrospective identification and prosecution of those committing violence, criminal damage or other criminal offences during assemblies is a complex legal area. One crucial factor is the timing of when surveillance is actioned. For example, conducting surveillance as a pre-emptive and precautionary measure, 'in case' criminal offences take place would require a high threshold of justification to satisfy the necessity in a democratic-society test. This would include the need for a properly substantiated reasoning to support the deployment in relation to a specific policing purpose.[80] Actioning surveillance while an offence is unfolding would change this dynamic. As above, this justification is highly susceptible to surveillance creep.

Specificity and clarity of purpose is also important to protect against surveillance creep. Assemblies are dynamic events and regularly change in size and character as they progress. At the same time, modern surveillance tools are designed to be adaptable. For example, drones may offer wide-angle coverage to help monitor crowd densities, yet they can also be used to focus on particular individuals for investigative purposes. However, repurposing a surveillance tool during the course of an assembly — in this example, switching from crowd safety to investigation — would constitute a distinct law-enforcement

79 Daragh Murray, Pete Fussey, Lorna McGregor and Maurice Sunkin, (2021), Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective, *Journal of National Security Law and Policy*, 11(3), pp. 743-770.

80 For default non-recording, see Corporate Policy Service Instruction on Unmanned Aircraft Systems, Police Service for Northern Ireland SI0221, 19 May 2021, p. 7.

aim and would need to be separately justified, and comply with the applicable necessity, proportionality and authorization requirements. Without a clear and separate surveillance-authorization procedure for a distinct, specified and evidenced law enforcement need, protests risk becoming opportunities for state surveillance. This is particularly important when considering surveillance activities as an 'ecosystem' (rather than as distinct practices and tools) and the accompanying risk of creep, alongside the obstacles to purpose limitation and overly broad necessity justifications. Several pSs highlighted the existence of law and policy designed to acknowledge the distinction between law enforcement aims. For example, the Lithuanian and Spanish governments reported, respectively, as follows:

> "There are specific legal and procedural processes [in place] in order to separate surveillance used to separate [sic] [monitor] protest from surveillance used for other policing purposes, such as criminal investigations or intelligence gathering. The separation is not symbolic — it is built into legislation, data-handling rules, authorization thresholds and oversight mechanisms."[81]

> "This shift in focus, from the purely administrative aim of ensuring proper conduct at the assembly, to that of an investigation, occurs when evidence arises during the event of a criminal offence (…). From that moment on, the relevant provisions of the Criminal Procedure Law have to be considered."[82]

Other pSs detailed how surveillance deployments had multiple public safety and law enforcement aims from the outset. The Swedish Department of Justice stated:

> "The purpose of the police's camera surveillance at demonstrations and other protests is to maintain public order and security, but also to prevent, deter or detect criminal activity in the area and to enable the investigation or prosecution of crimes afterwards. Video material that the police have collected from protests can later be used for a preliminary investigation if it is deemed necessary to prevent, detect or investigate a crime."[83]

81 Survey response from Lithuania.

82 Survey response from *Dirección General de Política Exterior*, Spain (hereafter 'Spain'), (informal translation).

83 Survey response from Sweden.

Rapidly escalating situations may require law enforcement officers to make rapid operational decisions, in real-time, about when to transfer between these public safety and coercive, non-consensual and investigative uses of surveillance. However, in most cases, these decision chains lie largely within the policing agencies and are subject to little external scrutiny or friction.

Legislative and policy considerations

Surveillance does not operate in a vacuum. It is facilitated, shaped and enhanced by the legal and policy frameworks that surround it.

The specificity of legal frameworks

Several pSs pointed to a range of statutes, legislative instruments, case law and other apparatus that enable and govern the use of surveillance at assemblies. In several cases, these included a blend of domestic and international law. This was most explicit in EU Member States given the establishment of key European legislation in this area, including the General Data Protection Regulation (GDPR),[84] the EU Law Enforcement Directive governing data handling[85] and the EU Artificial Intelligence Act (EU AI Act).[86] Some legal structures are rooted in specific domestic contexts, for example, in the constitutional changes following a transition towards democracy.

A common debate in this area concerns the speed of technological innovation compared to the ability to develop law and policy. This means that cutting-edge surveillance measures will often outpace regulation. If surveillance technologies are deployed when they are first brought to market, they risk operating in an ambiguous regulatory space. Another debate surrounds the level of specificity with which regulatory measures should be focused.[87] The concerns took many forms and were raised consistently by assembly monitors. These included concerns about the absence of an explicit legal basis sufficient to safeguard rights; ambiguity over necessity and proportionality; blanket authorizations; and excessive discretion over deployments. Other concerns centred on the existence of 'symbolic' legislation introduced without meaningful compliance mechanisms to accompany it.

84 European Data Protection Regulation, Regulation (EU) 2016/679, applicable as of 25 May 2018.

85 Directive (EU) 2016/680 (EU Law Enforcement Directive), 27 April 2016.

86 The EU Artificial Intelligence Act, (the AI Act), European Union, 12 July 2024. Prominent in the participating State survey responses from Spain and Lithuania.

87 For example, if too broad, they lack the specificity to address particular technologies. If too defined, they risk becoming outdated alongside designated technologies. In other respects, monitors reported how, in some jurisdictions, some new laws (e.g., the 2024 biometric surveillance law in Armenia), ostensibly positioned to regulate surveillance, grant significant latitude to authorize future surveillance technologies (Interview 1).

A permissive/amplifying environment for surveillance

Certain legal and policy measures may also amplify individuals' susceptibility to identification through surveillance technologies, as well as raising health-related concerns for some.[88] For example, many countries, such as Denmark, France, Georgia, Germany, the UK and the US, have pursued legislation that prohibits mask wearing or other face coverings at assemblies. Likewise, many states require mandatory SIM and/or device IMEI registration, backed by government-issued identification documents.[89] This significantly enhances the ability of states to link identities with mobile communications data.

Surveillance oversight and its effectiveness

Points of friction and adequate safeguards, in the form of independent and empowered oversight bodies, are crucial to ensuring compliance with international human rights law. Some pSs, including Sweden and the UK, have legislated to establish specific oversight roles for surveillance that is used at assemblies.[90] In other pSs, such as Switzerland, provision is made at the local level to enable public scrutiny of police surveillance activities.[91] Many have focused their regulatory efforts around data protection. This, it is argued, is both inadequate to cover the range of potential harms arising from advanced surveillance technologies and is explicitly focused on rights to privacy rather than the right to freedom of assembly.[92] Another concern involves reported instances in which data-protection mechanisms or procedures may impede civil-society efforts to scrutinize alleged abuses or malpractice.[93]

Related to this are questions of when oversight occurs. Surveillance oversight typically addresses authorization procedures and, therefore, focuses on the commencement of operations. Less frequent are interventions that occur during such operations. For example, inspections of live activities are rare. Equally, oversight and scrutiny of operations after they have concluded is also less common. Some pSs emphasized the existence of post-event initiatives in their survey responses.[94] However, these interventions typically relied on individuals to seek remedy through judicial processes. Assembly monitors in several countries also raised concerns over the unresponsive nature of oversight bodies

88 Interview 14.

89 Examples include Belgium, France, Spain, Tajikistan and Uzbekistan.

90 Respectively, these are the Swedish Camera Surveillance Act (survey response from Sweden) and the Biometrics and Surveillance Camera Commissioner in England and Wales. Notable about the latter is, at the time of writing, the absence of any regulatory power assigned to the role.

91 Survey response from the Specialist Advisor in the General Secretariat of the Conference of Cantonal Police Commanders of Switzerland (KKPKS) Switzerland (hereafter Switzerland).

92 For example, survey response from Serbia; Pete Fussey and Daragh Murray, *Facial Recognition Surveillance*, (Oxford: Oxford University Press, 2025).

93 Interview 12.

94 Articulated in most detail in the survey response from Lithuania, although responses from Serbia, Spain and Switzerland highlighted the possibilities for public accountability following surveillance operations.

to complaints and their failure to act in response to evident abuses. Others complained of excessive deference to states and, in extreme cases, of regulatory capture.[95] This includes the absence of friction being applied by regulators, failure to "question the police arguments at all"[96] and failure to scrutinize the intelligence case underpinning decisions to deploy surveillance.[97]

'Administrative ramping'

Assembly monitors from several countries highlighted how states increasingly bypass the higher evidentiary thresholds and procedural safeguards of criminal courts by pursuing protest-related actions via low-level 'administrative' offences. Surveillance technologies are increasingly central to the investigation and prosecution of these minor infractions. Examples include the use of intrusive facial recognition surveillance against littering[98] or to prosecute for obstructing a highway.[99, 100] There is also significant use of administrative systems to establish a first offence. Subsequent, minor infractions then become classified as repeat offences, and the 'offender' is brought into the criminal system, drawing more severe penalties. Such 'administrative ramping' can give authorities a pretext to deploy further surveillance against 'offenders'.

95 Interview 5.

96 Interview 14.

97 The inability to scrutinize the intelligence used to support requests for intrusive surveillance measures is a problem affecting surveillance oversight in many countries. See Daragh Murray and Pete Fussey, Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data, *Israel Law Review*, 52 (1), 18 February 2019, pp. 31-60. The existence and veracity of police intelligence is often taken on trust, and it is in this sense that police intelligence marks the boundary of accountability for external regulators.

98 Interview 1.

99 Interview 5; Interview 15.

100 See also *Glukhin v. Russia*, Application No. 11519/20, ECtHR, Judgment of 4 July 2023, paras. 88 and, especially, 90: "The processing of the applicant's personal data using facial recognition technology in the framework of administrative-offence proceedings – firstly, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground – cannot be regarded as 'necessary in a democratic society'".

4. Digital tools observed in assemblies across the OSCE region

Many audits have documented the range of surveillance technologies deployed at protests.[101] Rather than replicate these studies, this analysis instead seeks to emphasize the experiences of those actively monitoring these technologies. One key observation is how surveillance activities increasingly connect with each other. The surveillance of assemblies today relies on a blend of novel and more traditional approaches, of visible and invisible, remote and proximate remote techniques. Moreover, today's advanced surveillance technologies are designed to be adapted and repurposed. The software that drives these tools is also designed to interface with other systems and data. For example, the onset of AI has removed barriers to interpreting different images, text and other data coding formats. This allows unprecedented quantities of information to be brought together and analysed at speed. These developments are important, because they enhance the capability of surveillance technologies. They also allow data-reliant technologies intended for other (civic) objectives to be repurposed as surveillance tools. It is therefore accurate to consider the arrangements of surveillance activities as part of a wider monitoring ecosystem. These developments increase the risk of 'surveillance creep', complicating the determinations of necessity and proportionality, and creating challenges for external scrutiny of surveillance activities. They also alter the relationship between law enforcement and citizens and undermine the ability to remain anonymous in public.[102]

Remote biometric identification technologies

Remote biometric identification (RBI) technologies have transformed the ability of states and law enforcement agencies to monitor large gatherings. RBI covers an expanding range of technologies and uses, including face, voice, gait and behavioural analytics. In several regions of Germany, voice recognition tools are used for investigative purposes.[103] However, facial recognition technology (FRT) represents the most prominent and controversial form of RBI.

101 *Inter alia* Under Protected and Over Restricted: The State of The Right to Protest in 21 European Countries, Amnesty International, 8 July 2024; see also, Tracking Protest Surveillance webpage, Privacy International.

102 Pete Fussey and Daragh Murray, *Facial Recognition Surveillance*.

103 Feike Janson, Javier Sánchez-Monedero and Lina Dencik, Biometric identity systems in law enforcement and the politics of (voice) recognition: The case of SiiP, *Big Data and Society*, 21 December 2021.

Facial recognition technology (FRT)

FRT is widely used in the policing of protests and other assemblies. In analysing this technology, it is first important to distinguish between facial recognition technologies that verify an identity (e.g., to open a phone or confirm an identity at a border) and those that establish an identity (e.g., identifying individuals in a crowd). Both typically involve different data architecture. Verification usually does not need a reference database and normally compares a face to a record of that individual — so-called '1:1 matching' or, in other words, a database of one entry. Establishing identity requires a reference database, typically of thousands, sometimes millions, of candidate matches — so-called '1:n matching'. The latter clearly involves further consideration regarding data handling.

FRT is often classified into three categories, each with its own implications for the freedom of peaceful assembly, although some implications overlap across categories.

- **Live facial recognition** (LFR) is the real-time scanning of passers-by, processing the geometry of faces as individuals pass the cameras. Digital templates are made and compared to a 'reference database' (such as a law enforcement 'watchlist' of suspects). FRT therefore processes as well as captures. In some circumstances, it is the 'processing' that constitutes the intrusion.[104] UK police forces are among the law-enforcement agencies that have deployed live FRT most extensively in the OSCE region, giving rise to debate concerning the adequacy of the applicable external oversight or regulatory frameworks.[105]
- **Retrospective facial recognition** (RFR) is applied after an event. This allows users to compare and process large quantities of still images or video footage against extensive databases, such as custody images, national driver's license repositories, passport databases and others. RFR is currently the most widely used version of this technology. While often considered less intrusive (e.g., as reflected in the EU AI Act), RFR has the capability to identify those involved in demonstrations and other gatherings[106] and poses significant consequences for the freedom to retain anonymity in public places.
- **Operator-initiated facial recognition** (OIFR) is hosted on mobile devices and allows officers to photograph individuals on the street and then immediately process the captured images against police databases and other sources.

In their responses, assembly monitors were most concerned by FRT technology. They had encountered, evidenced or had strongly justified reasons to believe that law enforcement

104 *R (Catt) v Commissioner of Police of the Metropolis*, UK Supreme Court, UKSC/2013/0114, Judgment of 4 March 2015.

105 Fussey and Murray, *Facial Recognition Surveillance*.

106 ECtHR, *Glukhin v. Russia*.

used FRT across many settings, even when not disclosed by states. These included accounts from Kazakhstan, Moldova, Serbia, Türkiye, the UK and the US, while, in Armenia, new laws had been adopted to give police the authority to use remote biometric identification that can also be used in investigations.[107] Those monitoring assemblies in Belarus, Georgia and the Russian Federation highlighted the growing use of RFR to identify participants after protests, sometimes years after the event took place. Reports of protests in Belarus during 2020 highlight the recent identification and prosecution of participants through the use of a powerful facial recognition system.[108] This is a system first installed for the purposes of "combating crime and terrorism" and is capable of processing images from street-based cameras and social media.[109]

Those monitoring assemblies in Georgia reported on the use of facial recognition technology to identify and prosecute protesters, with court summonses arriving months after an event. Several elements are notable about such accounts. The first is how RFR is used as a means to punish misdemeanours adjacent to any assembly.[110] In the Georgian case, it was for minor civic infractions involving blocking highways or even pedestrian sidewalks, raising questions over lawfulness and the weighting of necessity and proportionality calculations with respect to the intrusive nature and decisive impact of this technology.

The growth of FRT in the Russian Federation has been documented via several sources.[111] One exiled assembly monitor described how the "pretext for [these systems] were safety and [to] provide safe city spaces, but we also have evidence that this system was used for politically motivated persecution in the context of freedom of assembly".[112] Furthermore, evidence of FRT use can be found in the use of surveillance footage in administrative and criminal justice processes. This is evident in several cases but, as reported by civil society sources, is perhaps most widely seen in relation to the nationwide "protests in support of Alexei Navalny at the time of his return to Russia during 2021, where an, estimate[d] 400

107 Interviews 1, 2, 3, 5 and 7. FRT has been used extensively across other OSCE pSs. This includes the "Traitement des antécédents judiciaires" (TAJ) owned by the French Gendarmerie which incorporates FRT capability (the FaceVACS-DBScan-LE), and the SARI system in Italy. Regarding the latter, SARI was found to lack sufficient legal basis by *Garante,* the Italian data protection authority in 2021, and its use discontinued. See Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy (Facial recognition: Sari Real Time does not comply with privacy regulations), GPDP, 16 April 2021 (in Italian).

108 Also documented by Privacy International: Belarus installs facial recognition surveillance, Privacy International, 15 March 2021 and the biometrics industry: Police facial recognition use in Belarus, Greece, Myanmar raises rights, data privacy concerns, Biometric update.com, 15 March 2021.

109 Interview 12.

110 Interview 15.

111 See, for example, Распознавание лиц внедрили в более чем 60 регионах России (Face recognition has been introduced in more than 60 regions of Russia), Roskomsvoboda, 24 October 2023 (in Russian).

112 Interview 8.

people were detained after the protest,[113] [with many believed to have been] detained because of the use of facial recognition system".[114]

These uses of facial recognition technology have also been linked to data leaks and extra-procedural practices. For example, *Roskomsvoboda* (a Russian NGO) initiated strategic litigation aimed at exposing the Russian Federation's facial recognition system, arguing it enabled massive personal data leaks onto the black market without adequate protection. While the court convicted two officers for selling data, the ruling failed to address the systemic governance and security flaws related to this technology.[115] In the Russian Federation, as elsewhere, Retrospective Facial Recognition (RFR) relies on extensive reference databases. In this specific context, RFR is integrated with the Russian Travel Pass database.[116] Similar to the driver's license databases used for RFR in the UK and the US, individuals are required to provide personal data as a prerequisite for basic mobility. This lack of choice raises vital questions about the extent to which such surveillance systems can truly be considered to be based on consent.

Accounts from the US reveal the use of a form of operator-initiated facial recognition (OIFR) by US Immigration Customs Enforcement (ICE), which has also been reportedly deployed at recent protests against forced deportations.[117] Mobile Fortify is an app developed by Japanese technology corporation NEC, a market leader in FRT. Concerns have also been raised regarding the circumstances in which this tool has been deployed:

> "We know what we know from whistle blowers and reporters (…), the news coming out of Minneapolis and the protests there, and the killing of Renee Good. You could see ICE agents walking up to people with their smartphones and them in front of different

113 Civil society organizations estimate around 17,000 people were detained during those protests, with an additional large number of detentions reportedly taking place afterwards, following police visits based on identifications believed to have been established through the application of facial recognition technology and footage from surveillance cameras. See also How the Russian state uses cameras against protesters, OVD-Info, 17 January 2022.

114 Interview 8. The same participant highlighted the use of FRT to identify attendees at Aleksei Navalny's funeral in 2024.

115 See Дело о «пробиве» по системе распознавания лиц вернулось в Басманный суд (The case of the "breakthrough" of the facial recognition system returned to the Basmanny Court), Roskomsvoboda, 25 July 2023.

116 In this case, the underpinning database is the Unified Biometric System (UBS), which was established in the Russian Federation in 2023-24. According to government statements, by 2024, the system contained the biometric profiles of more than 55 million Russian citizens. ЕБС содержит свыше 55 млн биометрических слепков россиян (The EBS contains over 55 million biometric profiles of Russians), Roskomsvoboda, 6 February 2024.

117 Joseph Cox, ICE Is Using a New Facial Recognition App to Identify People, Leaked Emails Show, 404 media, 26 June 2025.

> protesters' faces, and the app [Mobile Fortify] queries databases and [other] information, and it pulls up citizen status."[118,119]

Connecting to the discussion on appropriate oversight and governance of these technologies, the spread of OIFR increases the number of users, which brings challenges for instituting responsible and accountable use, as an account from the US reveals.[120] Interviewees' accounts of extraprocedural uses of OIFR for the purposes of intimidation are also supported by academic research.[121]

Digital infiltration

Organizing and mobilizing assemblies inevitably involves using digital communication technologies, thereby generating a large and residual digital footprint. This digital visibility provides law enforcement with more opportunities for surveillance, including through the use of remote and often invisible forms of surveillance to access networks, for strategic planning and to identify participants. Methods include the exploitation of local network infrastructures, such as campus and other public Wi-Fi networks, and the identification of participation-based, on-device connection logs.[122] Other tools include the use of sophisticated, third-party software platforms to continuously harvest data from social media networks.[123] Some techniques blend digital and traditional surveillance measures, such as the infiltration of WhatsApp groups and other communication platforms.[124]

Most controversial and intrusive have been targeted and aggressive surveillance operations using highly intrusive spyware to covertly monitor mobile devices. Many interviewees discussed their encounters with this technique, with documented cases of activists' mobile devices being infected by spyware in Armenia, Latvia, Lithuania, Poland, Spain and others.[125] The impact of these attacks is profound and is amplified by the limited

118 Interview 11.

119 This account goes on to describe how OIFR typically operates in a similar way to RFR, and differently to LFR. For example, LFR matches individuals with a single and specific database record. RFR returns a list of possible matches with the most likely one placed at the top (author observation of NEC LFR, RFR and OIFR systems). This holds specific implications for how the technology is used, how suspicion is constructed and which policing options are invited.

120 Interview 11.

121 Among others, Fussey and Murray, *Facial Recognition Surveillance*.

122 Privacy International, Tracking Protest Surveillance webpage.

123 Ilica Mahajan, The High-Tech Tools Police Can Use to Surveil Protesters, The Marshall Project, 11 December 2024.

124 Interview 3; also, Romero et al., "Pushed into the Shadows".

125 Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict, Amnesty International Security Lab, 25 May 2023; Exiled, then spied on: Civil society in Latvia, Lithuania, and Poland targeted with Pegasus, Access Now, 30 May 2024; CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru, CitizenLab, 18 April 2022.

awareness of those being targeted. In Serbia, participants described the limited capacity of NGOs to check mobile devices on the scale required to protect against advanced forms of spyware. As one participant described it, they became aware because Apple issued them an explicit warning.[126] Others described how this kind of surveillance is usually only confirmed retrospectively, when the content of infected mobile devices appears as evidence in court proceedings.[127]

Infection methods vary from remote, 'zero click' infections to manufactured situations that allow law enforcement agencies to gain physical access to devices. Protest monitors in Armenia, for example, described how law enforcement agents would develop pretexts to question activists at police stations and physically separate them from their mobile devices.

> "We monitored instances of putting malware [in]to the political activists' phones while they were in police stations (…). They basically ask someone to unblock their phone, and they have a camera in that room. Later, when they ask them to the Chief's room just for a small talk — but leave your phone here — that's when a specialist comes, because they already know the passcode. They open it; they put some malware there. How do we know? Because we were monitoring this person, whether he was called to the police and, later, he was experiencing that his phone is being discharged very quickly. And when a specialist looked, there was software using a lot of traffic — 24/7."[128]

Other assembly monitors described a variation on this practice, involving calling individuals in for informal questioning, forcing them to leave their phone in a designated location where it becomes compromised by spyware installation.[129] In another country, one protest monitor highlighted "cases of Pegasus surveillance against Belarusian activists, [which] we discovered through an investigative report from the CitizenLab".[130] They also described similar patterns of separating activists from their devices.

126 Interview 5.

127 Interview 3.

128 Interview 1.

129 Interview 8.

130 Interview 12. Access Now, Exiled, then spied on: Civil society in Latvia, Lithuania, and Poland targeted with Pegasus spyware.

> "People are called in for questioning. And [with the] KGB [RB],[131] it can be informal questioning. And sometimes you get released after, because [the] KGB can talk to you for many different reasons (…). It could be just a conversation, but you leave your phone in a special place (…). Yeah, it was detected that spyware was installed straight after this conversation."[132]

Other interviewees described similar strategies, sometimes identifying hundreds of victims who had been targeted in this manner.[133]

Open-source surveillance and social media patrolling

Open-source surveillance has increased significantly in recent years and has become a key method for monitoring assemblies. Protest monitors described multiple variants of this approach, largely focused on the surveillance of social media activity. Strategies included the targeted monitoring of individuals or communities of activists.

Also notable is how these recent and technologically advanced approaches connect with more traditional forms of surveillance. Most explicitly, this occurs when digital monitoring is followed up by a punitive physical interaction. This includes monitoring individual protesters online, followed by visits from police to protesters' homes shortly after they post or like content.[134]

These more targeted approaches are increasingly accompanied with systemic, large-scale scraping of social media data with sophisticated, covert tools. These include automated software applications, such as those developed by Palantir and Babel Street,[135] which facilitate the harvesting, aggregation, classification and analysis of huge quantities of data. This information is used, in turn, to conduct pattern recognition, behaviour and sentiment analysis, and network mapping and to provide intelligence on individuals, organizations and movements. Other forms of digital monitoring include the routine surveillance of online activity, such as through the use of deep packet inspection (DPI) of domestic internet traffic.[136]

131 Not to be confused with the former Russian security agency of a similar name. In the Belarusian context, the fuller name is 'KGB RB' with the RB acronym suffix denoting 'Respubliki Belarus'.

132 Interview 12.

133 Interview 8.

134 Interview 1.

135 USA/Global: Tech made by Palantir and Babel Street pose surveillance threats to pro-Palestine student protestors & migrants, Amnesty International, 21 August 2025.

136 Freedom on the Net: Kazakhstan, Freedom House, Key Developments, 1 June 2023 to 31 May 2024. Also highlighted consistently through the Edward Snowden revelations.

Communications and cellular monitoring

Technological innovations have enabled traditional forms of communications-based surveillance to become more adaptable and effective. The reliance on mobile technology to organize, mobilize and participate in assemblies, combined with advances in data analytics tools, has given authorities greater scope to gather information, for example, by intercepting mobile communications, harvesting location data and extracting encrypted information from devices.

International mobile subscriber identity catchers/cell tower monitoring

One technology increasingly associated with the compromise of mobile devices at assemblies is the deployment of International Mobile Subscriber Identity (IMSI) catchers.[137] These simulate legitimate cellular communication towers to deceive nearby mobile devices into connecting with them. Linked devices can then be manipulated in a range of ways, including to extract metadata and content, and elicit false messages. One key implication is the indiscriminate way in which IMSI catchers work, with individuals selected for surveillance due to their presence in a given location and the behaviour of their phone, rather than on the basis of an individualized form of suspicion. Further concerns were raised by assembly monitors in the US over the way this form of surveillance is linked to other geospatial monitoring to generate city-wide surveillance ecosystems that increasingly "build over time".[138] In this sense, surveillance tools become layered upon each other.

Communications data acquisition, metadata extraction and mobile phone tracking

Analysis of communications data in the digital age extends beyond traditional telecommunications (e.g., telephone calls, texts and electronic messaging) to include machine-to-machine interactions and the use of metadata to pinpoint location and other information. This communications data is used to reveal the composition of social networks, expose hierarchies and non-obvious associations, as well as wider 'patterns of life'.[139] As with other forms of digital surveillance, these methods extend the time window for investigations, with retained information holding potential relevance for years after acquisition.[140] This further demonstrates the importance of oversight that operates beyond the point of data collection.

137 Often referred to as 'stingrays' in some jurisdictions, owing to the original product name for the device manufactured by the Harris Corporation for military and intelligence uses.

138 Interview 11. Concerns also raised in Interview 5 and Interview 3.

139 For an unprecedented public analysis of how intelligence agencies use communications data see David Anderson, A question of trust: report of the investigatory powers review, (London: HMSO, June 2015).

140 Among others, see Peter Fussey and Ajay Sandhu, Surveillance Arbitration in the Era of Digital Policing, *Theoretical Criminology*, Vol. 26(1), 29 October 2020, pp. 3-22.

States typically possess the lawful authority to monitor communications in cases of national security and criminal investigation, subject to the three-part human rights test discussed in Section 2. While some surveillance authorization processes are clearly set out in law,[141] the abundance of digital data and the growth of commercial data managers have created new avenues for communications data surveillance. The availability of data brokers allows states to circumvent the process of obtaining legal warrants to formally acquire communications data — for example, commercial entities such as Webloc, which allow authorities to skirt the Fourth Amendment and other human rights safeguards to gain access to data on activists.[142]

Aerial surveillance and drones

Law enforcement agencies are increasingly using unmanned aerial vehicles (UAVs or 'drones') to monitor assemblies. One trend involves the redeployment of military and border patrol assets to monitor assemblies.[143] UAVs also alter the scale of surveillance operations, with cameras covering wider distances and fields of view than other forms of video monitoring. Drones can remain airborne for longer and at lower cost than other forms of aerial surveillance (such as helicopters, airships and fixed-wing surveillance aircraft). This capability is also relevant when considering how different surveillance assets can interact. For example, improved (and cheaper) lens optics can now make large quantities of drone surveillance footage available for RFR processing, compounding the challenges of retaining anonymity in public/outdoor settings.

One of the key concerns over this technology involves the limited notification or understanding of the purposes of deployment. Ambiguous uses restrict the opportunities for accountability and can enhance the chilling effects of surveillance. The following example from France elaborates this point:

> "There is absolutely no accountability on the images they take. We don't know what they are doing with it, and we don't know if they delete [the footage] or not, or how long they keep it (…). We have observed a lack of information provided to citizens, [and] we have also observed chilling effects. People were not able to

141 See, for example, the rush to legislate following the Edward Snowden revelations of June 2013 detailing the mass domestic surveillance programmes in the UK and US. Different authorization and oversight strategies exist for the legal acquisition of communications data, including judicial, parliamentary and regulatory approaches. For more details see Murray et al., Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective, pp. 743-770.

142 Interview 11.

143 Request Under Freedom of Information Act Concerning Nationwide Aerial Surveillance of George Floyd Protests, American Civil Liberties Union, 4 August 2020; Zolan Kanno-Youngs, U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance, *New York Times*, 19 June 2020.

> demonstrate alongside Olympic events, because they were afraid of being recorded by the surveillance. There's no police transparency about the use of drones and whether they are recording."[144]

Concerns over the absence of notification, specified purpose and accountability were also encountered in other countries. For example, in Moldova:

> "They have special units (…) operating unmanned vehicles, aerial vehicles, but the regulation of the police doesn't provide [for] information on the type of technology they use with these drones. It does not provide [for] information on what type of footage is collected, how it is stored and how it is used (…). It is just a matter of time and just a matter of availability until someone (…) will be able to apply different types of software and hardware [to] enable them to surveil public assemblies."[145]

The remote nature of this technology and the lack of notification means drones are both visible and inscrutable at the same time. Adding to this complexity is the particular capability of drones to adapt to different purposes. For example, drones deployed for crowd monitoring and situational awareness are easily repurposed for other, investigative, law enforcement aims. This demonstrates the importance of clear policies and boundaries governing specific purposes. In recognition of this, albeit rarely, some police agencies apply different operating procedures depending on drone use. For example, real time monitoring takes place if the aircraft are used for situational awareness and crowd monitoring, and recording only becomes enabled if a different, specific, law enforcement purpose becomes authorized.[146]

Data fusion and management

Prominent and visible forms of monitoring typically capture the most attention in discussions about surveillance. However, it is important to note the scale and intrusive capacity of more 'behind-the-scenes' processing. This includes data fusion infrastructure and various intelligence and data handling processes that occur within organizations and are rarely visible to external scrutiny. Assembly monitors remarked how such practices are

144 Interview 14. Observations on the use of drones to police protest and the similar absence of notification, specified purpose and accountability were encountered in Spain (Interview 10).

145 Interview 2.

146 Background contextual conversation with an officer from the Police Service of Northern Ireland.

not new, but they hold the potential to bring together different powerful technologies and data sources, and offer a step change in surveillance capability.[147]

Enduring forms of surveillance

Each of the newer approaches typically adds to, rather than replaces, existing surveillance infrastructure. Public, street-based surveillance cameras, the adoption of body-worn video cameras and the mass deployment of automatic number plate recognition systems continue to grow. However, the digital age expands the capacity of these more 'traditional' tools in two important ways. First, as noted above, feeds from these devices can be brought together, aggregated and analysed together. Second, is the way advanced video analytical software can be applied to video data. Examples include the application of facial recognition, object identification and behavioural analysis tools after footage has been captured.

The use of police body-worn video cameras has several implications for assembly monitoring. National guidance on the use of such tools is rare and, when present, often outdated.[148] Questions arise over the editorial control of camera footage, and how it is disseminated. Body worn video technology is often introduced as an accountability mechanism, to open up police behaviour to external scrutiny. However, many assembly monitors described practices where officers had control over when cameras were recording and when they were paused. Other research has highlighted how officers would sometimes intentionally obstruct the view of cameras or make statements that frame interactions in a particular way.[149] It is therefore important to recognize that, whilst intended and often used as a mechanism for accountability, there is the potential to curate footage in highly specific ways. Some legal observers aired concerns over the politicized broadcast of body-worn video footage, particularly during attempts to justify police violence against protesters.[150]

Repurposing civic infrastructure for the surveillance of assemblies

Assembly monitors also remarked on the adaptability of existing civic-centred technologies for the surveillance of protests. This account from Belarus highlights both the existence of this process and also the complexity of the state-commercial relationships involved:

147 For example, Interview 11.

148 Guidance for the Police Use of Body-worn Video Devices, Police and Crime Standards Directorate, July 2007.

149 Romero et al., "Pushed into the Shadows".

150 Interview 11. Also of note is how AI is increasingly used to edit and transcribe body-worn video footage. One of the largest global suppliers of this technology to police forces is Axon, who now market a product that uses AI to automatically transcribe video to text and pre-populates witness statements in the correct format.

> "They're still openly marketing [the surveillance system] as a smart city solution (…) the original concern [is its use] since the 2020 protests. You could tie it to the company called Synesis that was later put on the sanctions list in the EU, UK and US, precisely because it was a facial recognition technology, and there were concerns that it was used to identify protesters (…).[151] There were a few cases that also illustrate how post-protest [coercion] can be applied, especially to people who are serving [probationary-type] measures."[152, 153]

Informants and infiltration

In-person infiltration remains a concern for many assembly monitors, as borne out by public revelations of undercover infiltration into social movements, for example, in Spain and the UK.[154] This includes long-term monitoring of an environmental campaign, involving the formation of physical, sexual and familial relationships with activists.

151 See also Экс-силовики: политактивиста Дедка задержали с помощью программы "Синезиса" (Ex-security officials: political activist Dziadok was detained with the help of the Synesis program), *Euroradio*, 23 December 2020 (in Russian); Lukashenka's digital eyes, *Belsat*, 27 March 2025.

152 See also Aleksandra Shakova, 15 суток за то, что сходила на почту не по расписанию. Как камеры видеонаблюдения усложняют жизнь осужденным на домашнюю химию (15 days for going to the post office outside of the scheduled time. How surveillance cameras make life harder for those sentenced to house arrest), Mediazona Belarus, 19 February 2025 (in Russian).

153 Interview 12.

154 Interview 9; Interview 10; see also the UK public Undercover Policing Inquiry established in 2015 and ongoing at the time of writing (mid-2026).

5. The impact of surveillance of assemblies on the right to peaceful assembly

Advanced surveillance practices can have complex and often severe impacts on individuals and civil society.

Assemblies as surveillance opportunities and 'surveillance creep'

Widely formulated national security and public safety laws are regularly invoked as grounds for blanket authorizations of intrusive surveillance. While national security, public safety, counter-terrorism and child protection objectives may provide legitimate grounds for particular surveillance measures, where the applicable legal requirements are met, broadly formulated justifications can raise concerns regarding legality, necessity, proportionality and effective oversight. In particular, concerns arise where references to serious threats — including those concerning national security, terrorism and, separately, risks to children — are often used to justify, and claim necessity for, the deployment of powerful surveillance technologies in relation to conduct of substantially lesser gravity. Evidence suggests that, while serious offences are often used to legitimize these tools, they are frequently implicated in the investigation or prosecution of minor offences, as highlighted in Georgia, the Russian Federation, the UK and the US. Justifications based on serious offences may also restrict public accountability regarding allegations of excessive use of force, harassment and targeting of peaceful protesters. Assembly observers consistently highlighted the use of national security accountability exemptions being "used quite often" as a reason to avoid scrutiny.[155] This suggests that reliance on broadly defined national security grounds to restrict public accountability should be specifically justified and subject to appropriate safeguards and oversight.

Other assembly monitors identified variations on this theme, such as the procurement of powerful surveillance under the pretext of more innocuous civic and administrative purposes. For instance, in Moldova, observers stated that drones were procured under the justification of road traffic monitoring, only to creep into the sentencing of protest participants.[156]

155 Interview 11.

156 Interview 2.

It is also important to note how digital surveillance and other policing technologies often amplify existing discriminatory practices, such as the disproportionate stop and search and other targeting of visible minorities on the basis of categorical suspicion.[157] In addition, the disproportionate targeting of women in relation to public advocacy and assembly-related activities has been well documented[158] and is reproduced through digital technologies, particularly in the form of online harassment.[159] Added to this, some surveillance technologies and underlying datasets may reproduce or amplify existing biases. These include the over-representation of specific demographics in police databases used for predictive profiling, and the way facial recognition algorithms perform differently depending on gender and ethnicity.[160]

The banning and disruption of assemblies

Assembly monitors interviewed for this report cited the repeated use of surveillance tools to gather intelligence for later use in disrupting or banning assemblies. One account, for example, relating to activities in Kazakhstan, reveals how social media monitoring can be used to track religious minorities, political opponents and human rights defenders ahead of planned assemblies. The captured information is then used to prevent assemblies taking place:

> "Religious minorities, political opposition [and] human rights defenders are all followed by the IT extremist units inside the police or [state] security. Any time when organizers or protestors are facing some sort of prosecution, authorities usually rely on the information collected by these units (...). We have had dozens of cases where people just discussing the theme of possible protest action have been brought to justice with screenshots of their social networks or blogs [captured] by the police or intelligence (…). [Collection occurs] long before the peaceful assembly has even taken place."[161]

157 Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code*, (Cambridge: Polity, 2019).

158 *Inter alia* Human Rights Handbook on Policing Assemblies, OSCE/ODIHR, 11 March 2016; The Situation of Human Rights Defenders in Selected OSCE Participating States, OSCE/ODIHR, 28 July 2021.

159 Romero et al., "Pushed into the Shadows".

160 Patrick Grother, Mei Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, National Institute of Standards and Technology, US Department of Commerce, December 2019.

161 Interview 7.

Prosecution and detention

Surveillance technologies have been used to identify retrospectively those engaged in protest with the aim of prosecuting and detaining participants.[162] These practices are particularly connected to the growing use of FRT, where protesters are arrested weeks and sometimes months after an event. The use of FRT and recorded footage frequently leads to administrative or criminal charges. In Georgia, surveillance data is reportedly used to systematically identify protesters, resulting in convictions that carry up to 15 days' imprisonment. This first-hand account reveals how such tactics may work, and how specific activists can be selectively targeted:

> "I was there as a private individual, not as an observer (…). It took place in December [four months earlier]. And after this event, police started to monitor this camera, face recognition camera. They found me yesterday (…). But this, this rally, this demonstration, took place in December (…), and no police approached me personally, and no police warned me that I was committing any illegal act. My colleague was fined [the] previous year (…). In the same way. I was not the only one (…). [The penalty for] a first [offence] (…) is detention, and [a] fine is no longer an option (…). So that's how they found me. And it took three months to trace me."[163]

Assembly monitors also reported the use of other camera-based surveillance, notably Automatic License Plate Recognition, to gather evidence for the purposes of litigating against protesters after an event.[164] Other non-camera-based surveillance includes the use of internet service provider (ISP) log data and VPN intercepts to track individuals' identities and locations.[165] This data is often stored and can be used against assembly participants years later, as this example from Türkiye highlights:

> "[T]here's a time limitation on paper. However, they don't abide by it (…). You can be litigated [against] for participating in a protest ten years ago, so that footage taken ten years ago can easily be used as evidence against you."[166]

162 See ECtHR, *Glukhin v. Russia*.

163 Interview number redacted.

164 Interview 11.

165 Interview 3.

166 Interview 3.

Such accounts are important, because footage captured by more accepted forms of surveillance, such as street-based surveillance cameras, can be analysed by technologies that did not exist at the time, for the purposes of prosecuting individuals.

Retaliation and other coercive uses of surveillance data

Surveillance data has been used to facilitate additional punishments. In the Russian Federation, for example, FRT has also been used "since 2022 and, mostly, in 2023 (…) to find people who tried to escape military mobilization or [were] obligatory reservists in the Russian army". The strategy appears to be to use the technology to identify an individual and then generate a pretext in the form of a suspected transgression.[167]

167 Interview 8. See also, Russia Uses Facial Recognition to Hunt Down Draft Evaders, Human Rights Watch, 26 October 2022.

6. Obstacles to monitoring surveillance at assemblies

Monitoring state surveillance is obstructed by multiple systemic, physical and legal challenges. These assert themselves variously and place considerable obstacles to transparency and accountability.

The invisibility of technology and absence of transparency

The primary obstacle to effective monitoring is the inherent secrecy surrounding the procurement and deployment of modern surveillance tools. Limited disclosure occurs across all the jurisdictions studied. This applies in countries with strong accountability mechanisms as well as in those where such safeguards are absent. The remote nature of many of today's advanced surveillance tools means they largely operate out of sight. Several civil society activists reported how they "don't have the tools to anticipate things, because they don't know what is going to come next". Consequently, there is a growing sense that the increasing "use of AI (...) [lacks] visibility" and ensures that surveillance simply "becomes more invisible", making it "very difficult to spot or even impossible if it's [surveillance] not out in the open".[168] Another participant noted how the increasingly remote nature of surveillance made longstanding monitoring techniques, such as "walking the route before [and] spotting vehicles that look unusual (…) "more difficult as the tech evolves".[169]

Added to this is the invisibility of the data processing that drives these technologies.[170] Such 'behind-the-scenes' covert information processing makes it challenging to understand the nature of any interference. Therefore, in complex AI-enabled systems, understanding surveillance extends beyond knowing about the presence of specific tools, but requires knowledge of how data is processed, the way that information is used, and who has access to it. This lack of visibility also created challenges for monitors seeking greater public accountability — "We don't have any proof, so we cannot denounce it"[171] — and was considered to block trust building between different parties.[172] These limits on information mean having to apply to states for disclosure. This is seen as problematic and 'counterintuitive' and is compounded by the perception that oversight bodies in some jurisdictions hold 'zero independence'.[173]

168 Interview 16.
169 Interview 16.
170 Interview 11.
171 Interview 10.
172 Interview 4.
173 Interview 5.

This lack of transparency makes it difficult to target formal disclosure requests accurately, and poorly focused requests are more easily refused. A restricted information environment also risks inaccuracies in civil society reporting, which can then leave them with a difficult choice between silence or risking exposure to public criticism from poorly evidenced advocacy.[174] Assembly monitors noted how formal pathways for transparency were routinely shut down and highlighted frustrations with blanket refusals to answer formal requests for information. Sometimes such requests were stalled to the extent that they were no longer relevant, even when granted:

> "I remember I sent one [FOIA request] to ICE during the first Trump administration (…). I had forgotten I [had] even sent the request, and, three years later, I got a letter in the mail [with] one piece of something, and then [they] told me I wasn't privy to the other pieces."[175]

Other assembly monitors estimated that, for disclosure requests, "in 80 per cent of cases you don't get any answers". They added that, connecting to the discussion on police engagement, the success of disclosure requests was contingent on the individuals receiving them, rather than processes, as it "totally depends on the willingness of the authority or that civil servant".[176] Despite occasional successes in the use of FOIA and other disclosure mechanisms, and the targeted strategies designed to improve their chances, there was little faith in these processes. This reflection is representative. "That's the unfortunate truth about this (…). Even if we asked (…), all of these questions and requests for accessing public information [have] large exemptions (…). They [the requests] get denied, and I'm sure that if we would ask any civil society, they would say the same."[177]

Assembly monitors reported other limitations on dialogue with authorities. Some emphasized the politicized nature of these encounters. "We are not talking in a rational discussion. We are talking about the political implications. It's not about practical issues [including protester safety], how to provide people the right to for peaceful assembly."[178] This issue repeats in the context of sourcing information about legal proceedings, where monitors described obtaining, "less and less information about politically motivated cases [particularly] with the criminal prosecution or administrative persecution of people from our network".[179]

174 Interview 4.
175 Interview 11.
176 Interview 2.
177 Interview 4.
178 Interview 7.
179 Interview 8.

Legislative and administrative blocks to scrutiny

Assembly monitors routinely described the way legislative and administrative processes inhibited successful observation. This included rapid and unclear changes to the law. This was particularly common regarding legal frameworks governing surveillance and its oversight. Participants reported how lawmakers would develop legislation extremely quickly or introduce significant changes during late-stage passages of unrelated bills. Urgent parliamentary procedures were often invoked. These changes obstructed civil society engagement in legislative consultation before laws were passed. Other cases included shifting legal definitions of 'protests', such as in Armenia and the UK, and limited public disclosure regarding the use of police technologies. Elsewhere:

> "It's quite complicated to monitor the situation with Russian legislation. Because the Russian parliament [increasingly] (…) adopts new legislation in one or two days. Or they put significant changes throughout the legislation during the second reading (…). Also, [regarding] facial recognition technologies, they are applied in this grey zone without clear legislation (…). It's also quite complicated to [launch] strategic litigation. It's a little bit like the Kafka process, when you go to the court and try to say that something that doesn't exist on paper has violated your human rights."[180]

Others highlighted potential deliberate, strategic ambiguity over the criminalization of protests, including "completely arbitrary" decision-making over when assemblies are legally permitted.[181] Assembly monitors also reported highly discretionary practices concerning state accountability and access to remedy. For example, in Türkiye, observers highlighted the requirement for civil society actors to gain approval from a governor who is often deferential to the police. A variation of this obstacle is the intentional slowing down of remedy processes beyond the statute of limitations.[182] Others experienced direct criminalization and subsequent stigmatization for their activities.[183]

Another dimension to the impact of legislation concerns the running down of institutions and processes designed to regulate surveillance, either by restricting their functions or

180 Interview 8.

181 Interview 2. This wide scope for discretion in discerning the legality of assemblies has been a central criticism of the UK's Crime and Policing Act 2026.

182 Interview 3.

183 Interview 8.

limiting their independence.[184] This occurs in a context where the development of surveillance tools outpaces the capacity to develop meaningful legislative and regulatory control.

A related issue concerns the vulnerabilities of civil society organizations concerning material, gathered when monitoring assemblies, that could be subpoenaed by states and then used against people for whom the organization is trying to advocate.[185]

Intimidation, violence and chilling effects

Many observers reported incidents in which police conduct increased the physical risks faced by assembly monitors. This, in turn, deterred monitors from documenting surveillance and human rights abuses on the ground. This activity takes many different forms. One common approach is the refusal by law enforcement to differentiate between protesters and neutral monitors, and subjecting observers to violence:

> "We were assaulted by the police many times (…). Even, I had a call yesterday with one of the observers, and he told me they were standing alongside the protest, and the chief of the police came and said, 'Okay, today we are not going to treat you as an observer, but we are going to treat you as a protester. So, you should move now.' And (…), basically, they were assaulted just a few minutes after that. So, it was basically a (…) voluntary, random decision of a commander."[186]

Other monitors described being forced to physically relocate their monitoring activities. For example, in Finland, legal observers recounted a repeated practice of being forced to relocate their filming activities to a distance and position that was sometimes impossible to film from.[187]

The confiscation of, and intentional damage to, equipment was common in several jurisdictions. This included equipment necessary for monitoring and, on occasion, helmets and protective clothing, which increased the exposure and vulnerability of the observers.[188] Physical obstruction also took place before protests, where law enforcement officers preemptively visited protest organizers' houses:

184 Interview 4. Also highlighted in Changes to the functions of the BSCC: independent report, CRISP, 6 October 2023, on surveillance oversight in the UK.

185 Interview 9.

186 Interview 14.

187 Interview 6.

188 Interview 14.

> "The police come to the residence. [People] are arrested when leaving [and] held there until the planned rally is over, and then they are released without any kind of charges (…). And the person cannot leave the home, because they will be arrested. This is another method of intimidation."[189]

Another strategy of intimidation was focused on forced isolation, whereby other actors in civil society networks were criminalized for engaging with organizations. This account, detailing activism in the Russian Federation, relayed how, in 2023, the "authorities started to disseminate information among the local population [instructing them not to] work with human rights defenders. [They were then threatened and told], 'You will face harsh prosecution if you contact them.'"[190]

Others highlighted experiences where non-state actors were recruited to harass and intimidate protest organizers and participants.[191] One of the most common consequences was the reported severe chilling effect on protestors as well as on those monitoring assemblies. This fear was compounded by the threat of digital leaks and warnings that intimate and other personal information would be published widely. Chilling effects can arise from the suggested presence of surveillance but also in response to deliberate attempts at intimidation.[192]

Monitors consistently highlighted how the threat of surveillance affected their activities, obstructed mobilization and restricted the flow of volunteers.[193] Others pointed to individual physical and mental health impacts, including symptoms aligned with post-traumatic stress disorder.[194] Surveillance was implicated in intimidation tactics in several other ways. Examples include the use of surveillance footage for doxing; threats to family members and intimates; and a variety of humiliation tactics, including the threat to broadcast confession videos, and as a means to deliberately stigmatize individuals; in an example of an extreme case, all of the above was reported as occurring within the same jurisdiction.[195]

The tier of policing was considered relevant to the facilitation and blocking of monitoring. For example, relationships were easier to establish with local agencies. By contrast,

189 Interview 7.

190 Interview 8.

191 Interview 10.

192 Interview 11.

193 Interview 14.

194 See, for example, Alyasah Ali Sewell and Kevin Jefferson, Collateral Damage: The Health Effects of Invasive Police Encounters in New York, *Journal of Urban Health*, 93(S1), January 2016, pp. 42-67; Alyasah Ali Sewell, Kevin Jefferson and Hedwig Lee, Living under surveillance: Gender, psychological distress, and stop-question-and-frisk policing in New York City, *Social Science & Medicine*, 159(4), April 2016, p. 1.

195 Interview 12.

national bodies, often drafted in for major events, were seen as more difficult to engage with.[196]

Some authorities deployed economic penalties in order to paralyse and disincentivize monitoring activities. Levying significant fines through the administrative system also blocked organizations' ability to operate. Some of these fines became unpayable, critically damaging organizations and destabilizing movements. For example, one legal observer in Spain remarked on the particular impact of this approach for housing rights, Palestine solidarity and climate activist groups, and how this resulted in activists leaving their movements: "After that, they all received (…) fines. And they started to not identify in groups."[197]

Knowledge gaps on technology and human rights

Both law enforcement and civil society groups have significant gaps in their knowledge on surveillance and human rights. These prevent the proper identification and regulation of surveillance tools. Amplified by the limits of disclosure, civil society actors faced persistent challenges in accessing expertise on surveillance technologies. This left civil society organizations reliant on assembling fragments of information.[198] Limited technical understanding was common among public authorities involved in law enforcement and policymaking. [199] This inevitably diminished the capacity of surveillance users to uphold human rights-compliant use of these technologies. An adequate understanding of capability is fundamental to assessing proportionality, for example.[200] A more general issue concerns the lack of legal understanding among those using surveillance devices. For example, in the context of digital policing more generally, necessity is commonly conflated with vague notions of legitimacy to offer permissive justifications for intrusive surveillance.[201]

More generally, a major block to establishing accountability is when public authorities "don't associate the technical possibilities (...) with the possibility of somehow violating the freedom of peaceful assembly or other human rights".[202] Separating considerations of technology from rights is common, and leads to surveillance deployments on the basis of technical capability ('technology-led') rather than a legitimate aim.[203] Legal observers

196 Interview 11.

197 Interview 10.

198 Interview 2.

199 Interview 10; Interview 9. A growing body of academic work has highlighted how those using surveillance technologies routinely misunderstand its capabilities (among others, Fussey and Murray, *Facial Recognition Surveillance*).

200 See Section 2 on the three-part human rights test.

201 Among others, P. Johnson, The Impact of the Human Rights Act on the Police Service in England and Wales, *British Journal of Criminology*, Vol.52(3), May 2012, pp. 630-50.

202 Interview 2.

203 Interview 2.

repeatedly highlighted the way technology was deployed for this reason; that operations are "driven by its availability, not its necessity (…), [but] because they can".[204] This perspective is supported by academic research on the topic.[205]

Another complexity involves the hostile actions of law enforcement officers based on their misunderstanding of the law — for example, when being filmed themselves. This was particularly highlighted in the UK and US contexts.[206] In some cases, police intimidation has also encouraged monitors to write things down with pen and paper, rather than digitally record events; techniques intended to de-escalate police aggression. Individual safety is therefore prioritized over the quality of monitoring information.[207]

204 Interview 2.

205 Fussey and Murray, *Facial Recognition Surveillance*.

206 Interview 9; Interview 11.

207 Interview 11.

7. Recommendations and conclusions

The accounts of assembly monitors, the documentary sources and responses of pSs reveal a complex picture of the deployment, governance and accountability of surveillance technologies at assemblies. Surveillance tools are increasingly internationalized, driven by the globalization of technology industries. While the same technologies are being adopted in growing numbers of countries, their impacts are being unevenly felt. Despite this, some concerns arise in every context and apply in both democratic and authoritarian settings. These include, for example, the persistence of the chilling effects of surveillance on assembly organizers. Moreover, deficits in accountability and transparency, and the overall inadequate regulation applies to all jurisdictions. A further overarching theme is asymmetry; surveillance tools become more powerful, remote and invisible, and operate in a context where monitoring activities are increasingly difficult and threatened. The following recommendations are aimed at helping pSs to address this imbalance, promoting the facilitation of assembly and enhancing public trust and confidence in the use of these technologies.

Recommendations for participating States

1. Recognize and preserve the status of monitors.

The right to operate freely and without harassment in the monitoring of protests and other assemblies is recognized in several international human rights frameworks, including the UN Human Rights Committee General Comment No. 37 and the OSCE Vienna Document. While protection of monitor status exists in some jurisdictions, adherence to these standards is inconsistent across the OSCE region, with many monitors reporting vulnerability, harassment, threats and abuse.

2. Facilitate monitoring and ensure the safety of monitors and their equipment.

Assembly monitors routinely report surveillance, harassment, equipment confiscation, threats and violence, with obvious consequences for their ability to operate.[208] Recognizing their monitor status and implementing concrete measures to ensure their safety, alongside a principle of non-interference to preserve their autonomy, would support compliance with these international standards.

208 For more details see OSCE/ODIHR, The Right to Monitor Assemblies in the OSCE Region: Experiences from the Field.

3. Ensure transparency and develop meaningful democratic oversight of surveillance technologies and their use.

Secrecy is the primary obstacle faced by monitors attempting to identify surveillance tools and practices. Effective monitoring of these activities requires comprehensive public accountability and disclosure processes. Accountability measures require several conditions to be effective. These include:

- Transparency over the full lifecycle of surveillance activity, spanning procurement, authorization and deployment.
- Today's surveillance tools rely on hidden data capture and processing. These need to be brought into the scope of oversight and accountability activities. While data protection mechanisms are relevant, alone they are insufficient to address the wider scope and complexity of current surveillance activities.
- Full independence of external oversight bodies.
- Meaningful compliance mechanisms governing the uses of surveillance.
- The inclusion of civil society and other civic voices in oversight conversations.

4. Adhere meaningfully to legal disclosure obligations.

A common experience among monitors was the inconsistent, sometimes obstructive, approach of states to providing information under freedom of information or other legal disclosure obligations. Obfuscation, unexplained delays, no replies or blanket refusals on the grounds of confidentiality or operational secrecy were frequently encountered. Because requests of this nature are likely to involve law enforcement activities, they inevitably involve an appeal to operationally-relevant actions, and risk being declined on that basis. The logical extension of such refusals is to claim that legal accountability mechanisms for public bodies should apply less to law enforcement. Given the potentially significant impact of law enforcement powers on individual rights, effective accountability and appropriately reasoned disclosure processes are particularly important.

5. Foster constructive dialogue and the pursuit of de-escalation strategies.

Enhanced, meaningful, dialogue could frame interactions between civil society and law enforcement in a way that could engender better outcomes. It could help to de-escalate conflicts in advance, overturn preconceived suspicions and hostility, enhance public safety and increase accountability. In terms of practicalities, dedicated engagement/liaison roles within the police would improve consistent communication and outlast staffing changes within organizations.

6. Establish consistent mechanisms to ensure that the deployment of surveillance at assemblies is aligned with established standards of international human rights law.

Surveillance technology has "continued to creep, but the public safety argument has stayed the same".[209] Aligning surveillance use with the establishment of an adequate and explicit legal basis, and ensuring necessity and proportionality claims are properly substantiated, would support the responsible and accountable use of these technologies. Deliberations on proportionality need to address how highly intrusive surveillance technologies, such as facial recognition, become used in low-level cases, where the harm caused by the offence is outweighed by the impact of the interference. This consideration would be consistent with the European Court of Human Rights' ruling focused on this technology.[210] Possible approaches could include adapting rules on the admissibility of evidence in judicial proceedings. Such rules could recommend that courts exclude evidence obtained through such disproportionate and intrusive means for administrative and low-level cases. Added to this, relevant UN human rights guidance has called for the prohibition of or strict limitations on particularly intrusive surveillance tools — including spyware and remote biometric identification technologies — for the purposes of facilitating peaceful assemblies.[211]

7. Establish a requirement to evidence public safety and national security justifications for surveillance.

Advanced surveillance measures are frequently justified through appeals to public safety and national security. When such justifications are formulated in broad, vague terms, they risk providing scope for overly broad surveillance activities. Separately, extensive reliance on 'secrecy' may impede scrutiny and accountability. These elements, therefore, can make monitoring activities more difficult and risk creating conditions in which 'surveillance creep' may occur. PSs should pursue strategies that evidence national security/public safety requirements in a sufficiently specific and substantiated way, and maintain appropriate mechanisms for scrutiny and accountability, while safeguarding genuine operational confidentiality. This is possible to do. Moreover, 'national security' is an incomplete answer to rights-respecting public deployments of surveillance and, without elaboration, fails to satisfy the tests concerning legality, legitimacy and necessity that have been in place for over four decades.[212] A standard could be established to require such justifications to be properly evidenced — for example, by indicating the grading or quality of intelligence (rather than the intelligence itself) used to justify operations. These decisions should be available for external and democratic scrutiny where possible.

209 Interview 11.

210 See ECtHR, Glukhin v. Russia.

211 This prohibition is also set out in the UN Special Rapporteur's Model Protocol.

212 See, for example, the 1984 ICCPR 'Siracusa Principles' discussed in Section 2.

Recommendations for international organizations

The analysis highlights the growing role of private companies in the development and deployment of surveillance technologies. Many of these technologies are designed and supplied by private actors. In this regard, it may be useful for international organizations to encourage states to develop regulatory frameworks that govern private companies involved in the surveillance technology sector, as well as those that collaborate with states in law enforcement activities. Such frameworks could include requirements for transparency, human rights due diligence and independent oversight, including the meaningful participation of civil society in assessing the human rights implications of new technologies and in auditing their development and deployment.




Office for Democratic Institutions and Human Rights
OSCE
ODIHR